

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



MEMOIRE

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

En : TÉLÉCOMMUNICATIONS

Spécialité : Systèmes des Télécommunications

Par : BENDEDDOUCHE Mehdi Yacine

Sujet

Allocation Dynamique Multicritère du Spectre pour l'Internet des Objets Médicaux dans les Réseaux Radio Cognitifs 5G appliquée au Service de l'E-santé

Soutenu publiquement, le **15 / 06 / 2026**, devant le jury composé de :

Mme. SEDJELMACI Nadjat Amina

MCA

Université de Tlemcen

Présidente

Mme. GOURARI Fatima Zohra

MCB

Université de Tlemcen

Examinatrice

M. BABA-AHMED Mohammed Zakarya

Professeur

Université de Tlemcen

Encadrant

Année universitaire : 2025/2026

REMERCIEMENT

Je tiens tout d'abord à remercier **ALLAH** Tout-Puissant, qui m'a donné la force, le courage et la patience nécessaires pour mener à bien ce travail.

Je souhaite exprimer ma profonde gratitude à mon encadreur, **Mr Mohammed Zakarya BABA-AHMED** pour son accompagnement, sa disponibilité, ses précieux conseils ainsi que son soutien tout au long de la réalisation de ce projet. Son encadrement et ses orientations ont été d'une grande importance dans l'aboutissement de ce travail.

Mes remerciements s'adressent aux membres du jury, **Mme Nadjat Amina SEDJELMACI** et **Mme Fatima Zohra GOURARI**, qui me font l'honneur de siéger à cette soutenance. C'est un grand privilège de présenter les résultats de mes recherches devant leur regard expert et de bénéficier de leur haute bienveillance.

Enfin, j'adresse une pensée reconnaissante à ma famille ainsi qu'à mes proches pour leur soutien moral, leurs encouragements et leur confiance tout au long de mon parcours universitaire.

DÉDICACES

À ma très chère mère

Pour ton amour inconditionnel, tes sacrifices et ton soutien de chaque instant. Ce travail est le fruit de tes encouragements.

À mon très cher père

En témoignage de ma profonde gratitude pour ton soutien et la confiance que tu as toujours placée en moi.

À ma très chère sœur

Pour ta présence et ton soutien au quotidien. Je te souhaite tout le succès que tu mérites.

À ma très chère famille

Pour votre bienveillance et vos encouragements tout au long de mon parcours.

Résumé

Ce projet s'inscrit dans le cadre de l'évolution des réseaux radio cognitifs 5G, visant à répondre aux défis de l'allocation dynamique du spectre pour l'Internet des Objets Médicaux (IoMT). L'enjeu principal réside dans la gestion efficace des ressources spectrales tout en garantissant une Qualité de Service (QoS) et une sécurité optimale pour les données de e-santé hautement sensibles.

L'approche proposée repose sur des méthodes de décision multicritères (MCDM), intégrant le processus d'analyse hiérarchique (AHP) pour la pondération des critères et TOPSIS pour la sélection dynamique du canal le plus adapté. Pour modéliser les interactions complexes et les négociations entre les utilisateurs, le système a été implémenté sur la plateforme multi-agents JADE (Java Agent Development Framework).

L'originalité de ce travail tient à la classification des dispositifs Médicaux IoMT en deux catégories distinctes (critiques et non critiques) permettant une gestion flexible et adaptée au contexte médical. De plus, un volet sécuritaire approfondi a été intégré via l'utilisation de schémas cryptographiques hybrides afin de préserver l'intégrité et la confidentialité des échanges. Les résultats obtenus montrent que le système atteint un temps de convergence moyen d'environ 31 ms, inférieur aux meilleurs cas rapportés dans la littérature, tout en assurant une sécurisation efficace des échanges grâce au mode hybride ECC+AES.

Mots-clés : Allocation Dynamique du Spectre, Radio Cognitive 5G, IoMT, E-Santé, AHP, TOPSIS, JADE, Cryptographie Hybride.

Abstract

This project addresses the challenges of dynamic spectrum allocation in 5G cognitive radio networks specifically designed for the Internet of Medical Things (IoMT). The main objective is to manage spectral resources efficiently while ensuring strict Quality of Service (QoS) and optimal security for highly sensitive e-health data.

The proposed approach utilizes Multi-Criteria Decision Making (MCDM) methods, combining the Analytic Hierarchy Process (AHP) for criteria weighting and TOPSIS for the dynamic selection of the most suitable channel. To model the complex interactions and negotiations between users, the system was implemented using the JADE (Java Agent Development Framework) multi-agent platform.

The originality of this work lies in the classification of IoMT Medical devices into two distinct categories (critical and non-critical) allowing for flexible management tailored to the medical context. Furthermore, a robust security component was integrated through hybrid cryptographic schemes to ensure the integrity and confidentiality of exchanges. The results obtained show that the system achieves an average convergence time of about 31 ms, lower than the best cases reported in the literature, while ensuring effective protection of exchanges through the hybrid ECC+AES mode.

Keywords: Dynamic Spectrum Allocation, 5G Cognitive Radio, IoMT, E-health, AHP, TOPSIS, JADE, Hybrid Cryptography.

ملخص

يعالج هذا المشروع التحديات المرتبطة بالتخصيص الديناميكي للطيف الترددي في شبكات الجيل الخامس المعتمدة على الراديو المعرفي، والمصممة خصيصاً لتطبيقات إنترنت الأشياء الطبية. ويتمثل الهدف الرئيسي في إدارة الموارد الطيفية بكفاءة مع ضمان جودة خدمة صارمة ومستوى أمان عالٍ للبيانات الصحية الإلكترونية الحساسة.

تعتمد المقاربة المقترحة على أساليب اتخاذ القرار متعددة المعايير، من خلال الجمع بين عملية التحليل الهرمي (AHP) لتحديد أوزان المعايير، وطريقة TOPSIS للاختيار الديناميكي للقناة الأكثر ملاءمة. ومن أجل نمذجة التفاعلات وعمليات التفاوض المعقدة بين المستخدمين، تم تنفيذ النظام باستخدام منصة JADE متعددة الوكلاء.

تكمّن أصالة هذا العمل في تصنيف أجهزة إنترنت الأشياء الطبية إلى فئتين متميزتين (حرجة وغير حرجة)، مما يتيح إدارة مرنة تتلاءم مع السياق الطبي. إضافةً إلى ذلك، تم دمج مكّون أمني قوي يعتمد على مخططات تشفير هجينة لضمان سلامة وسرية عمليات التبادل. تُظهر النتائج المتحصّل عليها أن النظام يحقق زمن تقارب متوسطاً قدره حوالي 31 ميلي ثانية، أي أقل من أفضل الحالات المسجّلة في الأدبيات، مع ضمان حماية فعّالة للمبادلات بفضل النمط الهجين ECC+AES.

الكلمات المفتاحية: التخصيص الديناميكي للطيف الترددي، الراديو المعرفي للجيل الخامس، إنترنت الأشياء الطبية، الصحة الإلكترونية، عملية التحليل الهرمي (AHP)، طريقة TOPSIS، منصة JADE، التشفير الهجين.

Table des matières

<i>Remerciement</i>	I
<i>Dédicaces</i>	II
<i>Résumé</i>	III
<i>Table des matières</i>	VI
<i>Liste des figures</i>	XI
<i>Liste des tableaux</i>	XIII
<i>Acronymes et abréviations</i>	XIV
<i>Introduction générale</i>	1

Chapitre I : Internet des Objets Médicaux

I. Introduction.....	6
II. Définition et Concepts fondamentaux de l'IoMT	6
II.1. Définition de l'IoMT	6
II.2. Évolution historique : De l'IoT à l'IoMT	6
II.3. Écosystème IoMT	9
III. Architecture de l'IoMT	10
III.1 Architecture en couche	10
III.2. Les technologies de communication utilisées	11
IV. Exigences et contraintes spécifiques de l'IoMT	14
IV.1. Qualité de service QoS	14
IV.2. Sécurité et Contraintes Énergétiques	15
IV.2.1. Exigences de sécurité.....	15
IV.2.2. Contraintes énergétiques.....	17
IV.2.3. Stratégies de remédiation.....	18
IV.3. Cryptographie	18
IV.3.1. Cryptographie Symétrique.....	18
IV.3.2. Cryptographie Asymétrique.....	19
V. Défis et limitations de l'IoMT	21
V.1. Congestion et rareté de spectre	21
V.2. Interférences et coexistence avec d'autres utilisateurs	21
V.3. Mobilité des dispositifs médicaux	22

V.4. Hétérogénéité des réseaux.....	22
V.5. Vulnérabilités de sécurité	23
VI. Applications et services de l'IoMT	24
VI.1. Télémédecine	24
VI.2. Surveillance médicale à distance	24
VI.3. Diagnostic et traitement assistés	25
VI.4. Gestion hospitalière intelligente.....	25
VI.5. IoMT dans le contexte des réseaux 5G et post-5G	25
VI.5.1. Apports de la 5G pour l'IoMT	25
VI.5.2. Vision post-5G (6G) et e-santé.....	26
VI.5.3. Problématique de l'allocation spectrale.....	27
VI.5.4 Intérêt des réseaux radio cognitifs pour l'IoMT	27
VII. Conclusion	28

Chapitre II : Réseaux Radio Cognitifs et Systèmes Multi-Agents

I. Introduction.....	32
II. Contexte des réseaux sans fil.....	32
II.1. Catégories de réseaux sans fil.....	33
II.2. Défis spectraux pour l'IoMT.....	35
III. Radio Logicielle Restreinte (SDR) et Radio Cognitive (RC)	36
III.1. Historique et évolution	36
III.2. Radio logicielle restreinte (SDR)	37
III.3. Évolution vers la Radio Cognitive	38
III.4. Définition et concepts fondamentaux de la Radio Cognitive.....	39
III.4.1. Le paradoxe du spectre : motivation de la RC	39
III.4.2. Piliers technologiques : capacité et reconfigurabilité.....	39
III.4.3. Modèle d'accès et partage du spectre.....	40
III.4.4. Cadre normatif et évolutions	40
III.5. La relation entre la Radio Cognitive et la SDR.....	40
IV. Architecture et Cycle Cognitif.....	41
IV.1. Architecture de la Radio Cognitive	41

IV.2. Cycle de Mitola	43
IV.3. Composants de la RC	44
IV.3.1. Le Moteur de Cognition (Cognition Engine – CE)	44
IV.3.2. La Chaîne de Transmission et de Réception (SDR)	45
IV.3.3. Le Matériel Reconfigurable.....	45
V. Fonctions Cognitives Essentielles.....	46
V.1. Détection du spectre (Spectrum Sensing)	46
V.2. Gestion et décision spectrale (Spectrum Management).....	47
V.3. Partage du spectre (Spectrum Sharing).....	47
V.4. Mobilité spectrale (Spectrum Handoff)	47
VI. Allocation Dynamique du Spectre	48
VI.1. Formulation du problème d'allocation	48
VI.2. Approches et stratégies d'optimisation	48
VI.3. Méthodes de décision multicritère (MCDM)	49
VI.3.1. Méthodes de surclassement : ELECTRE et PROMETHEE	50
VI.3.2. Méthode AHP (Analytic Hierarchy Process)	50
VI.3.3. Méthode TOPSIS	50
VII. Sécurité de la Radio Cognitive	51
VII.1. Menaces et vulnérabilités.....	51
VII.2. Attaques au niveau de la couche physique	51
VII.3. Attaques au niveau de la couche liaison	52
VII.4. Attaques au niveau de la couche réseau.....	52
VII.5. Mécanismes de protection	52
VIII. Systèmes Multi-Agents (SMA) : Concepts et Architectures.....	53
VIII.1. Concepts fondamentaux des SMA	53
VIII.2. Architectures multi-agents.....	54
VIII.2.1. Types d'agents selon leur architecture interne	54
VIII.2.2. Structures d'organisation des agents	55
VIII.2.3. Mécanismes de communication	55
VIII.3. Plateformes de développement des Systèmes Multi-Agents.....	56
VIII.4. Intégration des SMA dans la RC	57
VIII.4.1. Coordination et coopération entre utilisateurs.....	58

VIII.4.2. Gestion des ressources et de la mobilité.....	58
VIII.4.3. Apprentissage et optimisation	58
VIII.4.4. Qualité de Service (QoS) pour les applications sensibles	59
IX. Domaines d'application de la Radio Cognitive	59
IX.1. Réseaux militaires et de sécurité publique	59
IX.2. Réseaux de secours et d'urgence	59
IX.3. Réseaux cellulaires (5G) et villes intelligentes (Smart Cities).....	60
IX.4. Réseaux IoMT	60
X. Conclusion.....	60

Chapitre III : Conception d'un Système d'Allocation Dynamique à Multicritère Sécurisé en IoMT dans les Réseaux Radio Cognitifs 5G

I. Introduction.....	65
II. Environnement et Outils de Développement.....	65
II.1. Choix du Langage Java.....	66
II.2. Plateforme de Développement NetBeans	66
III. La Plateforme JADE : Concepts et Architecture de Base	66
III.1. Philosophie FIPA et Architecture Distribuée : Services de Base (AMS et DF)	67
III.2. Modèle de Communication (ACL).....	68
IV. Conception de l'Architecture Multi-Agents de notre approche	69
IV.1. Architecture Globale du Système	71
IV.2. L'Agent Portail.....	71
IV.3. L'Agent PU	72
IV.4. L'Agent SU	73
IV.5. L'Agent SU_RECEIVER.....	74
IV.6. Protocole de Négociation.....	74
V. Modélisation Contextuelle IoMT.....	76
V.1. Taxonomie des Dispositifs Médicaux et Paramètres QoS	76
V.2. Affectation Dynamique des Poids TOPSIS par la Méthode AHP.....	77
V.2.1. Principe de la Méthode AHP.....	77
V.2.2. Construction des Matrices de Comparaison par Paires.....	77
V.2.3. Calcul des Poids et Vérification de Cohérence	79

V.2.4. Poids Obtenus et Validation de Cohérence	81
VI. Algorithme TOPSIS	81
VI.1. Construction de la Matrice de Décision	81
VI.2 Normalisation et Pondération.....	82
VI.3. Calcul des Solutions Idéales	82
VI.4. Classement des PU Candidats.....	83
VII. Sécurisation des Communications.....	84
VII.1. Architecture de Sécurité du Système	84
VII.2. Chiffrement des Données Médicales (AES).....	84
VII.3. Mode Hybride ECC+AES	85
VII.4. Mode Hybride RSA+AES	85
VII.5. Comparaison de notre contribution avec l'ECC vs RSA.....	86
VIII. Résultats et Évaluation des Performances.....	88
VIII.1. Environnement Expérimental.....	88
VIII.2. Mesures et métriques de latence.....	89
VIII.2.1. Métriques de base.....	89
VIII.2.2. Mesure de latence bout-en-bout	89
VIII.3. Impact de la Taille du Fichier	91
VIII.4. Résultats de Latence Bout-en-Bout.....	93
VIII.5. Comparaison avec des Travaux Précédents.....	96
VIII.6. Scalabilité du Système.....	97
IX. Conclusion	99
Conclusion générale	101
Bibliographies	103

Liste des figures

Chapitre I : Internet des Objets Médicaux

Figure I.1 : Écosystème de l'IoMT [8]	9
Figure I.2 : Architecture de l'IoMT [11]	10
Figure I.3 : Modèle complet des exigences de sécurité pour les systèmes IoMT [15]	16
Figure I.4 : Exemples d'attaques [24]	23

Chapitre II : Réseaux Radio Cognitifs et Systèmes Multi-Agents

Figure II.1 : Catégories des réseaux sans fil [27]	33
Figure II.2 : Capteurs et dispositifs médicaux d'un réseau WBAN [29]	34
Figure II.3 : La relation entre RC et SDR [45]	41
Figure II.4 : Les composants de l'architecture de la radio cognitive [45]	42
Figure II.5 : Cycle de cognition de Mitola [37]	44
Figure II.6 : Les différentes tâches d'un système de radio cognitive [49]	46
Figure II.7 : Approches de communication dans les SMA : a) échange de messages, b) Blackboard [57]	56

Chapitre III : Conception d'un Système d'Allocation Dynamique à Multicritère Sécurisé en IoMT dans les Réseaux Radio Cognitifs 5G

Figure III.1 : Architecture logicielle de la plateforme JADE [65]	68
Figure III.2 : Interface de gestion JADE et structure du Main Container	68
Figure III.3 : Inspection des messages ACL via l'interface graphique de JADE	69

Figure III.4 : Organigramme de notre approche	70
Figure III.5 : Architecture du Système Proposé.....	71
Figure III.6 : Interface graphique (GUI) de l'agent Portail pour la configuration et le déploiement du système	72
Figure III.7 : Négociation d'un SU avec 8 PU	74
Figure III.8 : Comparaison du temps d'établissement d'un canal sécurisé : ECC vs RSA (30 simulations)	87
Figure III.9 : Décomposition temporelle et composants de la latence bout-en-bout.....	90
Figure III.10 : Latence de transfert en fonction de la taille du fichier.....	92
Figure III.11 : Répartition de la latence bout-en-bout par phase	94
Figure III.12 : Comparaison de notre approche sur le temps de convergence avec les résultats de la littérature.....	96
Figure III.13 : Évolution des composantes en fonction de N	98

Liste des tableaux

Tableau I.1 : Comparaison entre l'IoT Général et l'IoMT [7]	8
Tableau I.2 : Comparaison des technologies de communication sans fil pour l'IoMT [12] ...	14
Tableau III.1 : Paramètres fondamentaux d'un message de communication ACL [66].....	69
Tableau III.2 : Spécifications techniques des profils 5G supportés par les agents PU	73
Tableau III.3 : Exigences de Qualité de Service (QoS) par type de dispositif IoMT	76
Tableau III.4 : Échelle de comparaison par paires de Saaty [68]	77
Tableau III.5 : Matrice de Comparaison par Paires pour les dispositifs Critiques	78
Tableau III.6 : Matrice de Comparaison par Paires pour les dispositifs non Critiques	79
Tableau III.7 : Valeurs de l'indice de cohérence aléatoire (RI) [73]	80
Tableau III.8 : Résultats AHP des poids des critères (CRITICAL).....	81
Tableau III.9 : Résultats AHP des poids des critères (NON_CRITICAL)	81
Tableau III.10 : Nature et objectifs d'optimisation des critères	82
Tableau III.11 : Analyse comparative des performances temporelles entre ECC et RSA	86
Tableau III.12 : Configuration matérielle et logicielle de la station de travail	88
Tableau III.13 : Latence de transfert des images	91
Tableau III.14 : Comparaison image / document	93
Tableau III.15 : Décomposition de la latence bout-en-bout (100 exécutions)	94
Tableau III.16 : Scalabilité des composantes de la phase de négociation	98

Acronymes et Abréviations

3G	La troisième génération
4G	La quatrième génération
5G	La cinquième génération
6G	La sixième génération
AAL	Ambient Assisted Living
ACC	Agent Communication Channel
ACL	Agent Communication Language
ADN	Acide Désoxyribonucléique
AES	Advanced Encryption Standard
AHP	Analytic Hierarchy Process
AID	Agent Identifier
AMS	Agent Management System
BDI	Belief-Desire-Intention
BLE	Bluetooth Low Energy
CAN	Convertisseur analogique-numérique
CCSD	Control Channel Saturation DoS
CE	Cognition Engine
CI	Indice de Cohérence
CNA	Convertisseur numérique-analogique
Cougaar	Cognitive Agent Architecture
CPE	Customer Premises Equipment
CPS	Cyber-Physical Systems
CR	Ratio de Cohérence
CSS	Cooperative Spectrum Sensing
DDoS	Distributed Denial of Service
DES	Data Encryption Standard
DF	Directory Facilitator
DoS	Denial of Service
DSA	Allocation Dynamique du Spectre
DSP	Digital Signal Processing
DSSS	Direct Sequence Spread Spectrum
ECC	Elliptic Curve Cryptography
ECDLP	Elliptic Curve Discrete Logarithm Problem
ECDSA	Elliptic Curve Digital Signature Algorithm
ECG	Électrocardiogramme
EEG	Électroencéphalogramme
EHR	Electronic Health Record
ELECTRE	ELimination Et Choix Traduisant la REalité
eMBB	enhanced Mobile Broadband
eURLLC	enhanced Ultra-Reliable Low-Latency Communications
FCC	Federal Communications Commission
FHSS	Frequency Hopping Spread Spectrum
FIPA	Foundation for Intelligent Physical Agents
FIPS	Federal Information Processing Standards

FPGA	Field Programmable Gate Array
GPP	General Purpose Processors
GPS	Global Positioning System
GUI	Graphical User Interface
HSPA+	High-Speed Packet Access Plus
IA	Intelligence Artificielle
IBM	International Business Machines
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IF	Fréquence intermédiaire
IoMT	Internet of Medical Things
IoT	Internet of Things
IPv6	Internet Protocol version 6
IRM	Imagerie par Résonance Magnétique
ISM	Industrielles, Scientifiques et Médicales
ITU	International Telecommunication Union
JACK	Java Agent Construction Kit
JADE	Java Agent Development Framework
JTRS	Joint Tactical Radio System
LBT	Listen Before Talk
LoRaWAN	Long Range Wide Area Network
LPWAN	Low Power Wide Area Network
LTE	Long Term Evolution
M2M	Machine-to-Machine
MAC	Medium Access Control
MadKIT	Multi-Agent Development Kit
MASON	Multi-Agent Simulator Of Neighborhoods
MCDM	Multi-Criteria Decision Making
MIMO	Multiple-Input Multiple-Output
m-IoT	mobile IoT
MIT	Massachusetts Institute of Technology
MiTM	Man-in-the-Middle
mMTC	Massive Machine-Type Communications
NB-IoT	Narrowband Internet of Things
NIST	National Institute of Standards and Technology
NR	New Radio
NVM	Non-Volatile Memory
OFA	Objective Function Attack
OFDMA	Orthogonal Frequency Division Multiple Access
PHY	La couche physique
PROMETHEE	Preference Ranking Organization METHod for Enrichment of Evaluation
pRRU	pico Remote Radio Unit
PU	Utilisateur Primaire
PUE	Primary User Emulation
QoS	Quality of Service
RC	Radio Cognitive

RF	Radiofréquence
RFID	Radio Frequency Identification
RI	Indice Aléatoire
RIS	Reconfigurable Intelligent Surfaces
RL	Reinforcement Learning
RPM	Remote Patient Monitoring
RRC	Réseaux de Radio Cognitive
RSA	Rivest-Shamir-Adleman
SCN	Selfish Channel Negotiation
SDR	Software Defined Radio
SINR	Signal-to-Interference-plus-Noise Ratio
SMA	Systèmes Multi-Agents
SoC	System on a Chip
SPN	Substitution-Permutation Network
SpO2	Saturation Pulsée en Oxygène
SQL	Structured Query Language
SSDF	Spectrum Sensing Data Falsification
SU	Utilisateur Secondaire
TOPSIS	Technique for Order of Preference by Similarity to Ideal Solution
UHF	Ultra-High Frequency
URLLC	Ultra-Reliable Low Latency Communications
USRP	Universal Software Radio Peripheral
UWB	Ultra-Wideband
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
VHF	Very High Frequency
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
XSS	Cross Site Scripting

Introduction générale

L'essor fulgurant des technologies sans fil et la numérisation croissante du secteur de la santé ont conduit à l'émergence de l'Internet des Objets Médicaux (IoMT), un écosystème interconnecté de dispositifs médicaux intelligents capables de collecter, transmettre et analyser des données physiologiques en temps réel. Cette révolution numérique, portée par les promesses des réseaux 5G et post-5G, ouvre des perspectives considérables pour la télémédecine, la surveillance médicale à distance et la gestion hospitalière intelligente. Cependant, elle soulève simultanément des défis technologiques majeurs qui constituent le cœur de ce travail.

Le premier défi est celui de la rareté et de la congestion spectrale. La multiplication exponentielle des dispositifs IoMT engendre une demande croissante en ressources radioélectriques, faisant du spectre un goulot d'étranglement critique. Les méthodes d'allocation statique traditionnelles, rigides et inadaptées aux environnements médicaux dynamiques, créent un paradoxe où certaines bandes de fréquences sont saturées tandis que d'autres restent largement inutilisées. Dans un contexte médical où la latence et la fiabilité des transmissions peuvent conditionner la vie des patients, cette inefficacité spectrale constitue une menace directe sur la qualité des soins.

Le second défi est celui de la sécurité des données médicales. La nature sensible des informations physiologiques échangées dans les réseaux IoMT impose des exigences strictes de confidentialité, d'intégrité et d'authenticité. Les mécanismes de sécurité traditionnels, conçus pour des environnements statiques, se révèlent inadaptés à la flexibilité et à la dynamique des réseaux radio cognitifs, exposant les communications médicales à des vulnérabilités critiques.

Face à ces enjeux, la Radio Cognitive (RC) s'impose comme une solution prometteuse, permettant une gestion dynamique et opportuniste du spectre radioélectrique en exploitant les espaces blancs laissés vacants par les utilisateurs primaires. Cependant, l'intelligence seule ne suffit pas : il faut également une architecture capable d'orchestrer de manière autonome et distribuée les décisions d'allocation, tout en garantissant la sécurité des échanges médicaux.

C'est dans ce contexte que s'inscrit ce travail de fin d'études, dont l'objectif principal est de concevoir et d'implémenter un système multi-agents sécurisé pour l'allocation dynamique multicritère du spectre dédié à l'IoMT dans les réseaux radio cognitifs 5G. La solution proposée repose sur trois contributions complémentaires :

- Une méthode d'allocation multicritère hybride AHP-TOPSIS, adaptée au contexte médical et intégrant cinq critères spécifiques de QoS médicale : la latence, la fiabilité, la bande

passante, le prix d'allocation et la durée de partage du spectre, permettant une sélection optimale et contextualisée des ressources spectrales disponibles.

- Une architecture multi-agents distribuée, développée sur la plateforme JADE, où des agents autonomes spécialisés collaborent pour orchestrer le processus d'allocation spectrale, garantissant une gestion intelligente, adaptative et résiliente des ressources.
- Un mécanisme de sécurité hybride, combinant le chiffrement asymétrique (RSA ou ECC) pour l'échange sécurisé de clés et le chiffrement symétrique AES pour la protection des données médicales transmises, avec une comparaison des performances des deux approches cryptographiques dans le contexte IoMT.

Ce mémoire est organisé en trois chapitres :

Le premier chapitre présente un état de l'art de l'Internet des Objets Médicaux, couvrant son architecture, ses exigences spécifiques de QoS et de sécurité, ses contraintes énergétiques et ses applications dans le contexte des réseaux 5G et post-5G.

Le deuxième chapitre est consacré aux fondements théoriques des réseaux radio cognitifs, de la Radio Logicielle à la Radio Cognitive, en détaillant leurs architectures, leurs fonctions cognitives essentielles, les méthodes d'allocation dynamique du spectre et les approches multicritères, ainsi que les systèmes multi-agents et leur application à la gestion spectrale.

Le troisième chapitre est consacré à la conception et à l'implémentation du système proposé. Il présente l'architecture multi-agents développée, la méthodologie d'allocation multicritère du spectre adoptée, les mécanismes de sécurité mis en œuvre et l'évaluation des performances obtenues à travers des simulations réalistes, permettant ainsi de valider l'efficacité de la solution proposée pour les applications IoMT en environnement radio cognitif 5G.

Enfin, une conclusion générale clôture ce mémoire en synthétisant les principaux résultats obtenus, en mettant en lumière les contributions de ce travail et en ouvrant des perspectives pour de futurs axes de recherche dans le domaine de la gestion intelligente du spectre pour l'IoMT.

Chapitre I

Internet des Objets Médicaux

Table des matières

I. Introduction.....	6
II. Définition et Concepts fondamentaux de l’IoMT.....	6
II.1. Définition de l’IoMT	6
II.2. Évolution historique : De l’IoT à l’IoMT	6
II.3. Écosystème IoMT	9
III. Architecture de l’IoMT	10
III.1 Architecture en couche	10
III.2. Les technologies de communication utilisées	11
IV. Exigences et contraintes spécifiques de l’IoMT	14
IV.1. Qualité de service QoS	14
IV.2. Sécurité et Contraintes Énergétiques	15
IV.2.1. Exigences de sécurité.....	15
IV.2.2. Contraintes énergétiques.....	17
IV.2.3. Stratégies de remédiation.....	18
IV.3. Cryptographie	18
IV.3.1. Cryptographie Symétrique.....	18
IV.3.2. Cryptographie Asymétrique.....	19
V. Défis et limitations de l’IoMT	21
V.1. Congestion et rareté de spectre	21
V.2. Interférences et coexistence avec d'autres utilisateurs	21
V.3. Mobilité des dispositifs médicaux	22
V.4. Hétérogénéité des réseaux.....	22
V.5. Vulnérabilités de sécurité	23
VI. Applications et services de l’IoMT	24
VI.1. Télémédecine	24
VI.2. Surveillance médicale à distance	24
VI.3. Diagnostic et traitement assistés	25
VI.4. Gestion hospitalière intelligente.....	25
VI.5. IoMT dans le contexte des réseaux 5G et post-5G	25
VI.5.1. Apports de la 5G pour l’IoMT	25
VI.5.2. Vision post-5G (6G) et e-santé.....	26
VI.5.3. Problématique de l'allocation spectrale.....	27
VI.5.4 Intérêt des réseaux radio cognitifs pour l’IoMT	27
VII. Conclusion	28

I. Introduction

La transformation numérique de la santé a engendré un écosystème en pleine expansion : l'Internet des Objets Médicaux (IoMT, Internet of Medical Things). Évolution de l'Internet des Objets (IoT, Internet of Things) vers des applications cliniques, l'IoMT regroupe les dispositifs connectés capables de collecter et d'analyser des données de santé en temps réel.

Contrairement à l'IoT classique, l'IoMT impose des exigences de service (QoS, Quality of Service) critiques : la latence, la fiabilité et la sécurité y sont vitales. Une défaillance, telle qu'un retard de transmission d'une alerte cardiaque ou l'interruption d'une commande chirurgicale, peut avoir des conséquences fatales. Ces impératifs se heurtent toutefois à une contrainte physique majeure : la rareté et la saturation du spectre radioélectrique face à la densification des réseaux sans fil.

Si la 5G et les réseaux futurs apportent des réponses prometteuses, l'allocation dynamique et efficace du spectre reste un défi complexe. Ce chapitre présente les fondements, l'architecture, les exigences et les contraintes de l'IoMT, ainsi que ses principales applications, en mettant en lumière la problématique de la congestion spectrale et l'intérêt des réseaux radio cognitifs comme solution adaptée aux environnements IoMT.

II. Définition et Concepts fondamentaux de l'IoMT

II.1. Définition de l'IoMT

L'IoMT désigne un réseau interconnecté de dispositifs médicaux intelligents, de capteurs biomédicaux, de systèmes d'information cliniques et d'infrastructures de communication, capables de collecter, transmettre, traiter et échanger des données de santé en temps réel. Ces dispositifs, intégrés dans des environnements hospitaliers, ambulatoires ou portables, s'appuient sur des protocoles de communication sans fil et des technologies avancées pour assurer une surveillance continue du patient, un diagnostic assisté et une prise de décision médicale automatisée, tout en répondant à des exigences strictes de qualité de service (QoS), de sécurité et de confidentialité des données médicales [1].

II.2. Évolution historique : De l'IoT à l'IoMT

La trajectoire qui mène de l'IoT à l'IoMT s'inscrit dans une évolution progressive, portée par les avancées technologiques et les besoins croissants du secteur de la santé.

- **Les origines de l'IoT (1999 – 2005)**

Le concept d'Internet des Objets a été introduit pour la première fois par Kevin Ashton en 1999, dans le cadre de ses travaux sur l'identification par radiofréquence (RFID, Radio Frequency Identification) au MIT (Massachusetts Institute of Technology). À cette époque, la vision consistait à connecter des objets physiques à Internet afin de permettre leur identification et leur suivi automatique [2]. Les premières applications étaient principalement logistiques et industrielles, loin du domaine médical.

- **L'émergence des capteurs intelligents et du M2M (2005 – 2010)**

Avec la miniaturisation des capteurs, l'amélioration des protocoles de communication sans fil (ZigBee, Bluetooth, Wi-Fi) et l'essor de la communication machine-à-machine (M2M), l'IoT a commencé à s'étendre vers de nouveaux domaines. Les premiers dispositifs de surveillance médicale connectés font leur apparition, notamment des capteurs de fréquence cardiaque et des glucomètres connectés, posant ainsi les premières bases de l'IoMT [3].

- **La naissance de l'IoMT (2010 – 2015)**

C'est dans cette période que le terme IoMT commence à être formalisé dans la littérature scientifique. Robert Istepanian, pionnier dans ce domaine, introduit en 2011 le concept de "m-IoT" (mobile IoT) appliqué à la santé, en démontrant le potentiel des objets connectés pour la surveillance non invasive de paramètres physiologiques. Les systèmes de surveillance à distance des patients (RPM, Remote Patient Monitoring) se développent, et les premières architectures IoMT dédiées aux environnements hospitaliers voient le jour [4].

- **La consolidation et la maturité (2015 – 2020)**

Cette période est marquée par une croissance exponentielle du nombre de dispositifs médicaux connectés. Les technologies médicales connectées (montres connectées, patches biomédicaux, implants intelligents) se multiplient, et les plateformes cloud dédiées à la santé émergent pour stocker et analyser les données collectées. Des standards et réglementations spécifiques à l'IoMT commencent à être définis par des organismes tels que la FDA (Food and Drug Administration) ou la Commission européenne [5].

- **L'IoMT à l'ère de la 5G (2020 – aujourd'hui)**

L'avènement de la 5G constitue un tournant majeur pour l'IoMT. Les capacités offertes par la 5G en termes de faible latence et de haut débit permettent de répondre aux exigences

critiques des applications médicales en temps réel. Cela inclut la chirurgie robotique à distance (télésurgie), le diagnostic assisté par intelligence artificielle et la télémédecine avancée. Cette technologie assure une connectivité ubiquitaire et des communications ultra-fiables indispensables à l'évolution des services de santé [6].

Bien que l'IoMT soit considéré comme un sous-ensemble spécialisé de l'IoT, ces deux paradigmes présentent des différences fondamentales qu'il convient de distinguer clairement. Le tableau suivant résume les principales distinctions entre l'IoT général et l'IoMT selon plusieurs axes comparatifs :

Caractéristique	IoT	IoMT
Champ d'application	Transversal (Industrie, Smart Home, Logistique).	Exclusivement dédié au secteur de la santé (E-santé).
Objectifs principaux	Optimisation des processus, suivi d'actifs et gestion des stocks.	Suivi vital en temps réel, diagnostic précis et gestion des maladies chroniques.
Précision technique	Standard / Grand public.	Précision de qualité médicale (capteurs implantables et portables haute précision).
Sécurité des données	Défi standard de cybersécurité.	Criticité extrême : Données de santé sensibles, enjeux éthiques et protection de la vie privée.
Cadre réglementaire	Normes industrielles classiques.	Réglementation stricte et conformité aux dispositifs médicaux.
Intégration	Écosystèmes variés et ouverts.	Intégration complexe avec les dossiers de santé électroniques (EHR) et équipements hospitaliers.

Tableau I.1 : Comparaison entre l'IoT Général et l'IoMT [7]

II.3. Écosystème IoMT

L'écosystème de l'IoMT repose sur une architecture multicouche conçue pour transformer le suivi médical traditionnel :

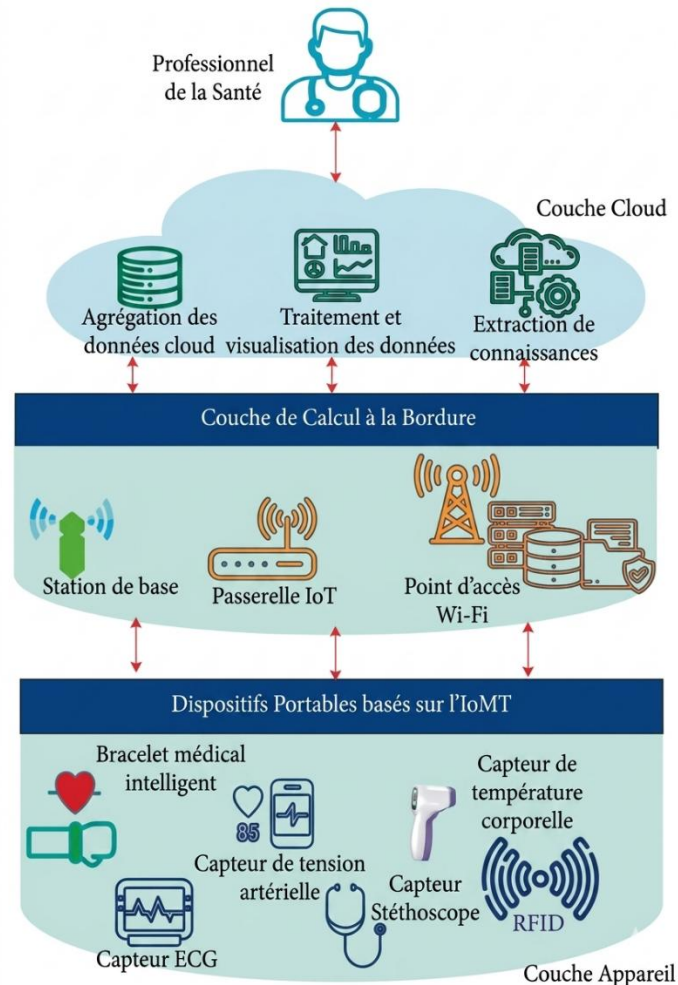


Figure I.1 : Écosystème de l'IoMT [8]

- **Dispositifs médicaux connectés (capteurs, équipements portables, implants) :** La couche de collecte se compose de capteurs intégrés dans un réseau corporel sans fil (WBAN, Wireless Body Area Network). Ces dispositifs incluent des capteurs de paramètres physiologiques (température, électrocardiogramme (ECG), rythme cardiaque, pression artérielle, saturation en oxygène (SpO2)) et émotionnels. Ces capteurs sont intégrés dans des dispositifs portables (montres, patches) ou des dispositifs de surveillance pour permettre une collecte de données en temps réel.
- **Passerelles (smartphones, hubs médicaux) :** Les données collectées par les capteurs sont transmises à un nœud passerelle (gateway). Les smartphones et les tablettes jouent souvent

ce rôle, utilisant des technologies comme le Bluetooth Low Energy (BLE) ou le Wi-Fi (Wireless Fidelity) pour acheminer les informations vers les serveurs distants. Ces passerelles intelligentes assurent la connectivité entre le réseau local de capteurs et l'infrastructure cloud.

- **Plateformes Cloud et Edge Computing :** Le Cloud est utilisé pour le stockage massif des données (Big Data) et les calculs complexes, comme l'exécution d'algorithmes d'intelligence artificielle pour le diagnostic. Pour pallier les problèmes de latence dans les situations d'urgence, l'edge computing (ou fog computing) rapproche le traitement des données de l'utilisateur (au niveau de la passerelle), permettant une analyse et une notification quasi instantanées.
- **Professionnels de santé et patients :** L'objectif final est de permettre aux patients de recevoir des soins de qualité dans le confort de leur domicile tout en réduisant la charge des hôpitaux. Les professionnels de santé (médecins généralistes, spécialistes, infirmiers) accèdent à ces données via des interfaces web sécurisées pour surveiller l'état de santé, vérifier les diagnostics et intervenir rapidement en cas d'anomalie [9].

III. Architecture de l'IoMT

III.1 Architecture en couche

L'architecture de l'IoMT est organisée en trois couches fonctionnelles distinctes, chacune assurant un rôle spécifique dans le traitement et l'acheminement des données médicales [10].

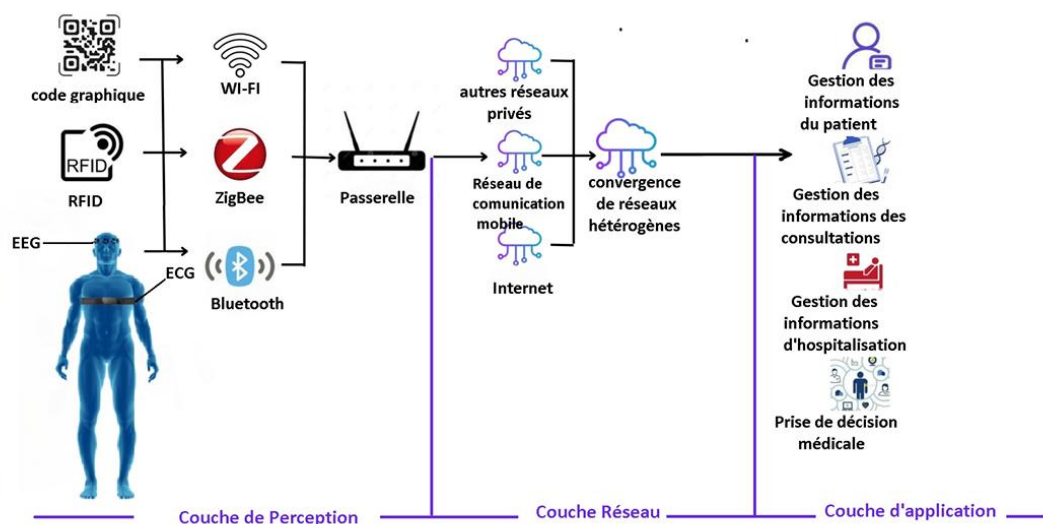


Figure I.2 : Architecture de l'IoMT [11]

- **Couche de Perception**

La couche de perception constitue la base de l'architecture IoMT. Elle est subdivisée en deux sous-couches : la sous-couche d'acquisition, qui s'appuie sur une diversité de capteurs médicaux (capteurs physiologiques, chimiques, ADN) ainsi que sur des technologies telles que la RFID et la reconnaissance d'images pour collecter les paramètres de santé des patients et les convertir en nœuds de systèmes cyber-physiques (CPS, Cyber-Physical Systems) ; et la sous-couche d'accès, qui assure la transmission de ces données vers la couche réseau via des technologies sans fil à courte portée telles que ZigBee, Bluetooth et Wi-Fi [10].

- **Couche Réseau**

La couche réseau constitue l'épine dorsale de l'architecture IoMT. Sa sous-couche de transmission assure l'acheminement fiable et en temps réel des données vers les destinations appropriées, en exploitant les réseaux mobiles, Internet et les réseaux spécialisés (LTE (Long Term Evolution), 5G, LoRaWAN (Long Range Wide Area Network)). Sa sous-couche de service assure quant à elle l'intégration des réseaux hétérogènes et la normalisation des formats de données, tout en fournissant des interfaces ouvertes pour les applications médicales tierces [10].

- **Couche Application**

La couche application représente le niveau le plus élevé de l'architecture IoMT. Elle intègre d'une part la gestion de l'information médicale (dossiers patients, suivi des traitements, gestion hospitalière) et d'autre part l'aide à la décision médicale (analyse des pathologies, diagnostic assisté, analyse des prescriptions). Elle s'appuie sur des technologies avancées telles que le Edge/Fog Computing pour le traitement temps réel, le Cloud Computing pour le stockage massif et l'Intelligence Artificielle pour le diagnostic automatisé [10].

III.2. Les technologies de communication utilisées

Les technologies de communication sans fil constituent l'épine dorsale de l'écosystème IoMT. Leur choix dépend de plusieurs critères : la portée, la consommation énergétique, le débit, la latence et la fiabilité. Nous présentons ci-dessous les principales technologies utilisées.

- **Bluetooth Low Energy (BLE)**

Le BLE est une technologie sans fil à très faible consommation énergétique, largement adoptée dans les applications médicales portables (montres connectées, patches, capteurs de

signes vitaux). Sa principale force réside dans sa capacité à assurer une surveillance continue et en temps réel tout en préservant la durée de vie des batteries des dispositifs médicaux. Cependant, sa portée limitée (environ 10 mètres) et sa faible bande passante le rendent inadapté aux applications nécessitant une transmission à longue distance ou un transfert de données volumineuses [12].

- **ZigBee**

ZigBee est un protocole basé sur le standard IEEE 802.15.4 (Institute of Electrical and Electronics Engineers), conçu pour les réseaux de capteurs à faible débit et faible consommation. Il est particulièrement adapté à la surveillance médicale à distance, notamment pour les glucomètres, tensiomètres et oxymètres connectés. Ses capacités de maillage réseau (mesh networking) permettent la création de systèmes de surveillance médicale à grande échelle facilement extensibles. Néanmoins, sa portée limitée (100 mètres) et son faible débit le rendent insuffisant pour les applications temps réel nécessitant un transfert massif de données [12].

- **Wireless Fidelity Wi-Fi**

Le Wi-Fi est la technologie dominante dans les environnements hospitaliers, offrant un débit élevé adapté à la transmission de données médicales volumineuses telles que l'imagerie médicale et la vidéoconférence. Il facilite la surveillance à distance, la télémédecine et la connexion des équipements médicaux aux systèmes centraux de surveillance. Sa principale limitation est sa consommation énergétique élevée, ce qui le rend peu adapté aux dispositifs médicaux fonctionnant sur batterie, nécessitant ainsi une gestion rigoureuse de l'alimentation [12].

- **LoRaWAN**

LoRaWAN est une technologie LPWAN (Low Power Wide Area Network) qui se distingue par sa très longue portée (jusqu'à 15 km) et sa très faible consommation énergétique. Elle est particulièrement adaptée à la surveillance médicale dans les zones rurales et reculées, ainsi qu'au suivi des équipements et patients mobiles. En revanche, sa bande passante restreinte limite son utilisation aux applications à faible débit, la rendant inadaptée aux applications médicales nécessitant un transfert de données en temps réel [12].

- **NB-IoT**

Le NB-IoT (Narrowband Internet of Things) est un standard cellulaire dédié aux objets connectés à faible débit, offrant une excellente couverture, une faible consommation énergétique et un coût réduit. Il est particulièrement adapté au suivi des patients mobiles et à la communication entre dispositifs médicaux distants. Sa principale limitation réside dans sa bande passante réduite, qui le rend inadapté aux applications nécessitant un transfert de données à haut débit, telles que la vidéo médicale ou la transmission d'images haute résolution [12].

- **Thread**

Thread est une technologie sans fil à faible consommation basée sur IPv6 (Internet Protocol version 6), utilisée dans les systèmes de surveillance médicale, le suivi des équipements et la surveillance environnementale des établissements de santé. Ses capacités de maillage réseau lui permettent d'assurer une connectivité fiable entre les dispositifs médicaux. Toutefois, sa portée limitée (environ 100 mètres) et sa latence non négligeable peuvent constituer des obstacles dans les grands établissements hospitaliers ou pour les applications médicales critiques en temps réel [12].

- **Réseaux Cellulaires (LTE, 5G)**

Les réseaux cellulaires, notamment LTE et 5G, jouent un rôle croissant dans l'IoMT grâce à leur large couverture et leur capacité à supporter des applications médicales critiques telles que la télémédecine, la surveillance à distance et la coordination des interventions d'urgence. La 5G représente une avancée majeure avec sa latence ultra-faible, son débit très élevé et sa connectivité massive, ouvrant la voie à des applications telles que la chirurgie robotique à distance. Cependant, les réseaux cellulaires classiques présentent des limitations importantes : forte consommation énergétique, vulnérabilités de sécurité et rareté du spectre radioélectrique [12]. Cette contrainte motive la recherche de stratégies d'allocation de ressources plus flexibles et efficaces, indispensables pour soutenir le déploiement massif de l'IoMT.

Afin de faciliter la compréhension des forces et des faiblesses de chaque protocole, le Tableau I.2 synthétise et compare les principales caractéristiques des technologies de communication sans fil présentées ci-dessus, en se basant sur des critères essentiels tels que la portée, le débit et l'efficacité énergétique :

Technologie	Portée (Approx.)	Débit / Bande passante	Consommation Énergétique
BLE	Courte (~10 m)	Faible	Très Faible
ZigBee	Moyenne (~100 m)	Faible	Faible
Wi-Fi	Moyenne (~50-100 m)	Élevé	Élevée
LoRaWAN	Très Longue (15 km)	Très Faible	Très Faible
NB-IoT	Longue	Faible	Faible
Thread	Moyenne (~100 m)	Faible	Faible
5G / LTE	Très Longue	Très Élevé	Élevée

Tableau I.2 : Comparaison des technologies de communication sans fil pour l'IoMT [12]

IV. Exigences et contraintes spécifiques de l'IoMT

IV.1. Qualité de service QoS

La qualité de service (QoS) désigne l'ensemble des paramètres qui définissent le niveau de performance, de fiabilité et d'efficacité d'un réseau ou d'un service. Dans le contexte de l'IoMT, la QoS joue un rôle crucial pour garantir une gestion efficace et sans interruption des données médicales critiques et d'urgence. En effet, la congestion du réseau et le remplissage du trafic constituent deux facteurs majeurs qui perturbent le flux de données et engendrent des latences de communication, ce qui peut s'avérer fatal dans un environnement médical.

Quatre caractéristiques fondamentales du trafic réseau permettent de mesurer la QoS dans les réseaux IoMT :

- **Bande passante (Bandwidth)** : Elle représente la vitesse maximale qu'un lien peut atteindre, exprimée en bits par seconde (bps). Dans l'IoMT, la QoS permet d'identifier les

applications médicales nécessitant une bande passante plus élevée, telles que la transmission d'images médicales haute résolution ou la vidéoconférence médicale.

- **Perte de paquets (Packet Loss)** : Elle survient lorsque des paquets de données n'atteignent pas leur destination en raison d'une surcharge ou d'une congestion du réseau. Dans l'IoMT, toute perte de données physiologiques telles que l'ECG, la **SpO2** ou la **pression artérielle** peut conduire à un diagnostic erroné ou à une absence de détection d'anomalie critique.
- **Latence** : Elle représente le temps total mis par un paquet pour traverser le réseau de la source à la destination. On distingue quatre types de délais contribuant à la latence totale :
 - *Délai de traitement* : temps nécessaire à un dispositif pour effectuer les opérations requises avant de transmettre le paquet.
 - *Délai de mise en file d'attente* : temps d'attente d'un paquet dans la file avant sa transmission.
 - *Délai de sérialisation* : temps nécessaire au transfert de tous les bits d'une trame vers l'interface physique.
 - *Délai de propagation* : temps mis par les bits pour traverser le support de transmission (fibre optique, liaison satellite...).
- **Gigue (Jitter)** : Ce phénomène désigne la variation du délai de transmission des paquets de données due à la congestion du réseau ou aux variations de routage. Dans l'IoMT, une gigue excessive peut dégrader la qualité des flux de données médicales en temps réel.

En prenant en compte ces caractéristiques de QoS, les systèmes IoMT peuvent garantir que la bonne information est délivrée au bon moment aux bonnes personnes, permettant ainsi une prise de décision rapide et des interventions potentiellement vitales [13].

IV.2. Sécurité et Contraintes Énergétiques

IV.2.1. Exigences de sécurité

La sécurité constitue une exigence fondamentale de l'IoMT en raison de la nature hautement sensible des données médicales échangées entre les différentes entités du réseau. Un environnement IoMT est considéré comme sécurisé s'il garantit la protection de l'ensemble des entités impliquées, qu'il s'agisse des patients, des dispositifs médicaux, des passerelles ou des serveurs cloud. Les principales exigences de sécurité dans l'IoMT sont les suivantes [14]. Les principales exigences de sécurité dans l'IoMT sont résumées dans la Figure I.3, qui présente les différents objectifs à garantir au sein du système.

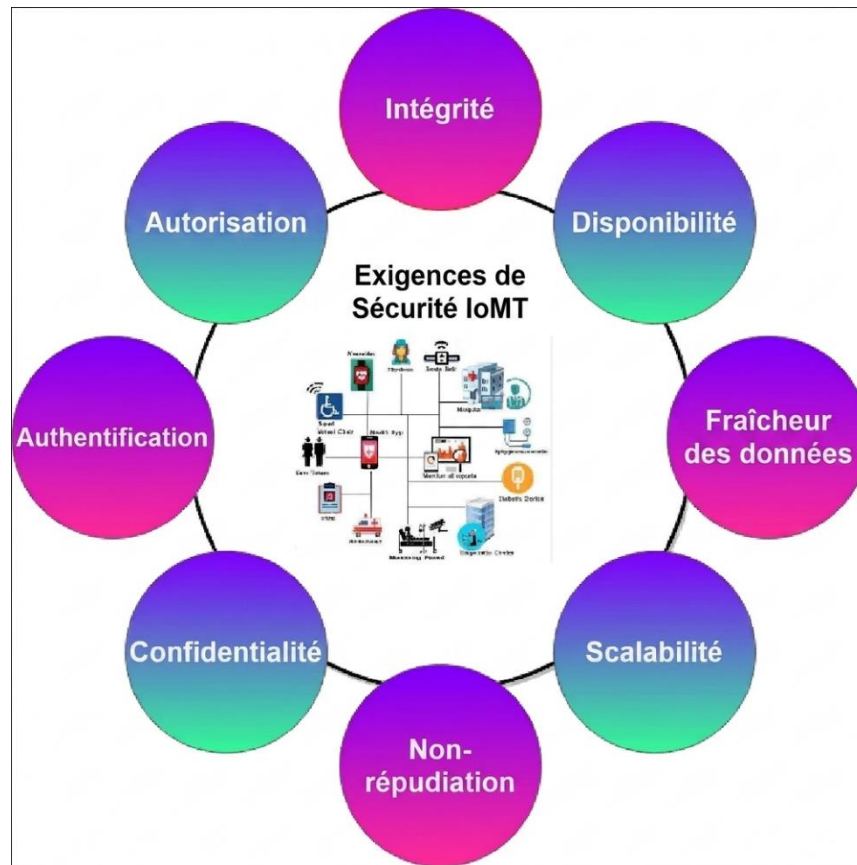


Figure I.3 : Modèle complet des exigences de sécurité pour les systèmes IoMT [15]

- **Confidentialité** : La confidentialité vise à préserver la vie privée des patients en garantissant que les données médicales sensibles transmises entre les différentes entités du réseau IoMT ne sont accessibles qu'aux utilisateurs légitimes et autorisés, et restent inaccessibles à tout tiers non autorisé.
- **Intégrité** : L'intégrité assure que les données transmises entre les entités du réseau IoMT ne sont ni altérées ni manipulées, que ce soit accidentellement ou intentionnellement par un utilisateur malveillant. Elle garantit que les données sont délivrées intactes à leur destinataire.
- **Authentification** : L'authentification permet de vérifier l'identité des entités communicantes (utilisateurs, dispositifs intelligents, serveurs, passerelles) dans l'environnement IoMT. Les différentes entités du réseau s'authentifient mutuellement et établissent des clés de session sécurisées avant toute transmission de données, afin de résister aux attaques potentielles.
- **Non-répudiation** : La non-répudiation garantit qu'aucune entité ne peut nier la validité des messages envoyés ou reçus dans l'environnement IoMT. Elle fournit une preuve d'origine

(le message a bien été généré par l'expéditeur original) et une preuve de destination (le message a bien été reçu par le destinataire prévu).

- **Autorisation** : L'autorisation définit les droits d'accès et les privilèges accordés à un utilisateur ou dispositif authentifié pour accéder aux différentes ressources du réseau IoMT. Elle est généralement appliquée en complément de l'authentification pour renforcer la protection contre les accès non autorisés.
- **Fraîcheur des données (Freshness)** : La fraîcheur assure que les messages transmis entre les entités du réseau sont fraîchement générés et non des anciens messages rejoués par un attaquant. Elle permet de résister aux attaques par rejeu (replay attacks) dans les réseaux IoMT.
- **Disponibilité** : La disponibilité garantit que les services et ressources du réseau IoMT restent accessibles aux utilisateurs légitimes à tout moment, même en cas d'attaques telles que les attaques par déni de service (DoS, Denial-of-Service). Elle est particulièrement critique dans les applications médicales d'urgence où toute interruption de service peut mettre en danger la vie des patients [14].

Ces exigences de sécurité sont interdépendantes et doivent être considérées conjointement pour assurer une protection globale et efficace de l'environnement IoMT [14]. Cependant, leur mise en œuvre n'est pas sans impact sur les ressources des dispositifs médicaux. En effet, l'intégration de chiffrements complexes ou de protocoles d'authentification lourds augmente la charge de calcul et de transmission, ce qui peut mener à un épuisement prématuré de la batterie. Cette contrainte est particulièrement critique pour les dispositifs implantables ou ingérables, où une défaillance énergétique peut nécessiter une nouvelle intervention chirurgicale ou, dans le pire des cas, s'avérer fatale pour le patient [16].

IV.2.2. Contraintes énergétiques

La gestion de l'énergie est l'une des contraintes les plus critiques de l'écosystème IoMT. La majorité des dispositifs médicaux connectés (capteurs portables, implants, dispositifs ingérables) sont limités en ressources et dépendent de batteries à autonomie restreinte, ce qui impose des compromis importants sur les plans des performances et de la fiabilité [16].

Les contraintes énergétiques constituent également une vulnérabilité exploitée par les cyberattaquants pour compromettre les dispositifs médicaux. Les principales attaques ciblant l'énergie des dispositifs IoMT sont :

- **Attaques par épuisement de batterie (Battery Exhaustion)** : Des attaquants peuvent envoyer des requêtes malveillantes répétées ou de faux signaux de réveil pour forcer un capteur à rester actif en permanence, vidant ainsi sa batterie en un temps record.
- **Attaques "Low and Slow"** : Ces attaques à faible débit visent spécifiquement à consommer l'énergie du dispositif de manière imperceptible par les systèmes de détection classiques.
- **Brouillage (Jamming)** : En manipulant les séquences de sauts de fréquence, un attaquant peut forcer le nœud à consommer davantage d'énergie lors des tentatives de transmission, accélérant ainsi l'épuisement de sa batterie [16].

IV.2.3. Stratégies de remédiation

Pour pallier ces contraintes énergétiques, plusieurs solutions techniques sont proposées dans la littérature :

- **Mémoire Non-Volatile (NVM)** : Utilisée pour stocker les états du dispositif afin qu'ils ne soient pas perdus lors d'une coupure d'énergie, évitant ainsi des cycles de reconnexion coûteux en énergie.
- **Chargeurs sans fil** : Pour les dispositifs médicaux implantés, l'utilisation de chargeurs externes sans fil permet de prolonger la durée de vie de l'appareil sans intervention chirurgicale.
- **Optimisation logicielle** : L'utilisation d'algorithmes de gestion de clés simplifiés et de protocoles de routage privilégiant la survie énergétique des nœuds permet de réduire significativement la consommation [16].

IV.3. Cryptographie

La cryptographie joue un rôle fondamental dans la sécurisation des données médicales transmises dans les réseaux IoMT. Les mécanismes cryptographiques doivent être adaptés aux contraintes spécifiques de ces environnements, notamment la limitation des ressources énergétiques et computationnelles des dispositifs médicaux. On distingue deux grandes catégories [17][18].

IV.3.1. Cryptographie Symétrique

La cryptographie symétrique repose sur l'utilisation d'une clé secrète unique partagée entre l'émetteur et le récepteur pour les opérations de chiffrement et de déchiffrement. Elle est généralement reconnue pour son efficacité et sa rapidité par rapport aux méthodes asymétriques [17]. Parmi les algorithmes les plus représentatifs de cette catégorie, on distingue :

- **DES (Data Encryption Standard)**

Développé par IBM (International Business Machines) en 1972 et adopté comme standard fédéral (FIPS, Federal Information Processing Standards) en 1977, le DES est un algorithme de chiffrement par blocs. Il traite les données par blocs de 64 bits en utilisant une clé de 56 bits. Son architecture repose sur la structure de Feistel, qui divise le texte en deux moitiés traitées à travers 16 tours de substitutions et de permutations [17].

- **3DES (Triple DES)**

Pour pallier les vulnérabilités du DES sans concevoir un nouvel algorithme, le Triple DES a été proposé, appliquant l'algorithme DES trois fois sur chaque bloc de données. Il existe en versions à deux ou trois clés indépendantes, offrant respectivement environ 80 et 112 bits de sécurité effective. Cependant, le principal inconvénient du 3DES est sa lenteur importante par rapport à d'autres méthodes modernes, ce qui a mené à son remplacement progressif [19].

- **AES (Advanced Encryption Standard)**

Sélectionné par le NIST (National Institute of Standards and Technology) en 2000 pour remplacer le DES, l'AES (basé sur l'algorithme Rijndael) est devenu le standard mondial actuel. Contrairement au DES, il utilise un réseau de substitution-permutation (SPN, Substitution-Permutation Network) et traite des blocs fixes de 128 bits. Il supporte trois longueurs de clés : 128, 192 et 256 bits, impliquant respectivement 10, 12 ou 14 tours de transformation. L'AES est privilégié pour sa haute vitesse d'exécution, son efficacité tant matérielle que logicielle, et l'absence actuelle de preuve de cassage [20].

IV.3.2. Cryptographie Asymétrique

La cryptographie asymétrique utilise une paire de clés mathématiquement liées : une clé publique pour chiffrer et une clé privée pour déchiffrer. Ce mécanisme renforce la sécurité en éliminant le besoin de partager une clé secrète via un canal potentiellement compromis [21]. Les deux algorithmes les plus représentatifs de cette catégorie sont le RSA et l'ECC :

- **RSA (Rivest-Shamir-Adleman)**

Le RSA, introduit en 1977, est l'un des systèmes cryptographiques asymétriques les plus répandus. Sa sécurité repose sur une propriété mathématique fondamentale des grands nombres premiers : bien que multiplier deux grands nombres premiers pour obtenir un nombre semi-premier soit une opération simple, il est computationnellement infaisable de factoriser ce grand

nombre pour retrouver ses facteurs premiers d'origine. Le système génère une paire de clés mathématiquement liées : une clé publique pour le chiffrement et une clé privée pour le déchiffrement. La génération des clés suit les étapes suivantes :

1. Sélection de deux grands nombres premiers p et q
2. Calcul du module $n = p \times q$
3. Calcul de l'indicatrice d'Euler $\varphi(n) = (p - 1)(q - 1)$
4. Choix de l'exposant public e tel que $\text{pgcd}(e, \varphi(n)) = 1$
5. Calcul de la clé privée d tel que $d \times e \equiv 1 \pmod{\varphi(n)}$
6. La clé publique est (n, e) et la clé privée est (n, d)

Le chiffrement s'effectue par $C = M^e \pmod{n}$ et le déchiffrement par $M = C^d \pmod{n}$, où M est le message original et C le message chiffré. Pour maintenir un niveau de sécurité acceptable face aux attaques modernes, il est recommandé d'utiliser des clés d'au moins **2048 bits**, ce qui engendre une consommation importante en ressources computationnelles et énergétiques, le rendant peu adapté aux dispositifs IoMT à ressources limitées [21].

- **ECC (Elliptic Curve Cryptography)**

L'ECC est une technique cryptographique asymétrique s'appuyant sur les propriétés mathématiques des courbes elliptiques, définies par l'équation $y^2 = x^3 + ax + b$. Sa sécurité repose sur la difficulté du problème du logarithme discret sur les courbes elliptiques (ECDLP, Elliptic Curve Discrete Logarithm Problem).

Le mécanisme opérationnel de l'ECC fonctionne comme suit : un utilisateur choisit un point de base (B) sur la courbe et une clé privée (k), puis calcule la clé publique ($A = kB$). Il est computationnellement infaisable de retrouver k en ne connaissant que A et B . Le chiffrement transforme le message (P) en texte chiffré ($Q = (xB, P + xA)$) en utilisant un nombre aléatoire (x) et la clé publique du destinataire. Le déchiffrement utilise la clé privée pour retrouver le message original via $(P + xA) - kxB = P$.

Par rapport au RSA, l'ECC offre des avantages significatifs pour l'IoMT : une clé ECC de 256 bits offre une sécurité équivalente à une clé RSA de 3072 bits, une génération de clés plus rapide et une consommation énergétique réduite, le rendant particulièrement adapté aux dispositifs médicaux à ressources limitées. L'ECC est notamment utilisé dans l'ECDSA (Elliptic Curve Digital Signature Algorithm) pour l'authentification des dispositifs médicaux [22].

V. Défis et limitations de l'IoMT

Malgré son potentiel révolutionnaire pour le secteur de la santé, l'IoMT fait face à plusieurs défis majeurs qui limitent son déploiement à grande échelle. Ces défis sont d'ordre technique, spectral et sécuritaire.

V.1. Congestion et rareté de spectre

La multiplication exponentielle des dispositifs IoMT exerce une pression sans précédent sur des ressources spectrales déjà limitées. Les bandes **Industrielles, Scientifiques et Médicales (ISM)** (2.4 GHz et 5 GHz), partagées avec de nombreuses technologies sans fil, sont particulièrement sujettes à la congestion, notamment dans les environnements hospitaliers urbains où la densité des équipements connectés est très élevée. Cette congestion a des conséquences directes sur les performances des systèmes IoMT : réduction du débit, augmentation des pertes de paquets et dégradation du rapport signal sur bruit (SINR, Signal-to-Interference-plus-Noise Ratio), pouvant faire dépasser les seuils de latence acceptables pour des applications critiques comme la télé chirurgie, qui exige une latence inférieure à 10 ms. Avec l'avènement de la 5G et ses nouvelles bandes de fréquences (sub-6 GHz et mmWave), cette problématique s'intensifie davantage. La connectivité massive (mMTC, Massive Machine-Type Communications) introduite par la 5G permet certes de connecter un grand nombre de dispositifs IoMT simultanément, mais elle accentue également la compétition pour l'accès aux ressources spectrales. De plus, les méthodes d'allocation statique du spectre, trop rigides pour s'adapter aux fluctuations dynamiques de la demande, aggravent encore cette situation en conduisant soit à une sous-utilisation, soit à une saturation de certaines bandes [23].

V.2. Interférences et coexistence avec d'autres utilisateurs

Les établissements hospitaliers, généralement situés dans des zones urbaines densément peuplées, sont confrontés à des niveaux d'interférence particulièrement élevés dus à la coexistence de dispositifs IoMT avec d'autres équipements médicaux et réseaux d'accès radio environnants. Ces interférences se traduisent par des dégradations mesurables des performances : réduction du débit de données pouvant atteindre 30% durant les heures de pointe, des niveaux de SINR tombant en dessous du seuil acceptable de 10 dB, et des taux de perte de paquets atteignant 15%, compromettant ainsi la fiabilité des systèmes de surveillance en temps réel.

La coexistence non gérée avec d'autres utilisateurs empêche de respecter les exigences strictes de l'eURLLC (enhanced Ultra-Reliable Low-Latency Communications), faisant grimper les délais au-delà de 150 ms, bien au-dessus de la tolérance de 10 ms requise pour des

applications critiques comme la télé chirurgie. Les méthodes d'allocation statique traditionnelles, trop rigides pour s'adapter à la nature imprévisible des signaux dans ces environnements encombrés, aggravent encore cette situation. Des technologies avancées telles que la Radio Cognitive, le Massive MIMO (Multiple-Input Multiple-Output) et les algorithmes d'annulation d'interférence apparaissent comme des solutions prometteuses pour gérer efficacement cette coexistence et protéger les communications médicales critiques [23].

V.3. Mobilité des dispositifs médicaux

La mobilité des patients et des dispositifs médicaux constitue un défi important pour les réseaux IoMT. Les patients portant des dispositifs de surveillance médicale se déplacent au sein des établissements hospitaliers ou dans leur vie quotidienne, ce qui nécessite une gestion efficace de la mobilité pour maintenir une connectivité continue et fiable. Les handovers fréquents entre points d'accès peuvent engendrer des interruptions de service, des pertes de données médicales et des augmentations de latence, ce qui est particulièrement problématique pour les applications médicales critiques nécessitant une surveillance en temps réel [23].

V.4. Hétérogénéité des réseaux

L'écosystème IoMT est caractérisé par une grande hétérogénéité, tant au niveau des dispositifs que des protocoles et des technologies de communication utilisés. Cette hétérogénéité se manifeste à plusieurs niveaux :

- **Hétérogénéité des dispositifs** : Les réseaux IoMT intègrent une grande diversité de dispositifs médicaux (capteurs portables, implants, équipements hospitaliers) provenant de fabricants différents, avec des capacités de traitement, des protocoles de communication et des formats de données variés et souvent propriétaires.
- **Hétérogénéité des protocoles** : La coexistence de multiples protocoles de communication (BLE, ZigBee, Wi-Fi, NB-IoT, 5G) au sein d'un même environnement médical pose des problèmes majeurs d'interopérabilité, rendant l'intégration et la gestion unifiée des dispositifs IoMT particulièrement complexe.
- **Hétérogénéité des réseaux** : Les dispositifs IoMT s'appuient sur des infrastructures réseau hétérogènes (WBAN, WPAN, WLAN, réseaux cellulaires en anglais Wireless Body, Personal or Local Area Network) qui coexistent et doivent interagir de manière transparente pour assurer une continuité de service médicale.

Cette hétérogénéité complique considérablement la gestion des ressources spectrales et la garantie d'une QoS médicale homogène à travers l'ensemble du réseau IoMT [12].

V.5. Vulnérabilités de sécurité

Les réseaux IoMT sont exposés à une multitude de menaces et d'attaques qui exploitent les vulnérabilités inhérentes à leur architecture distribuée et à leurs contraintes en ressources. Les principales attaques auxquelles sont confrontés les dispositifs IoMT sont :

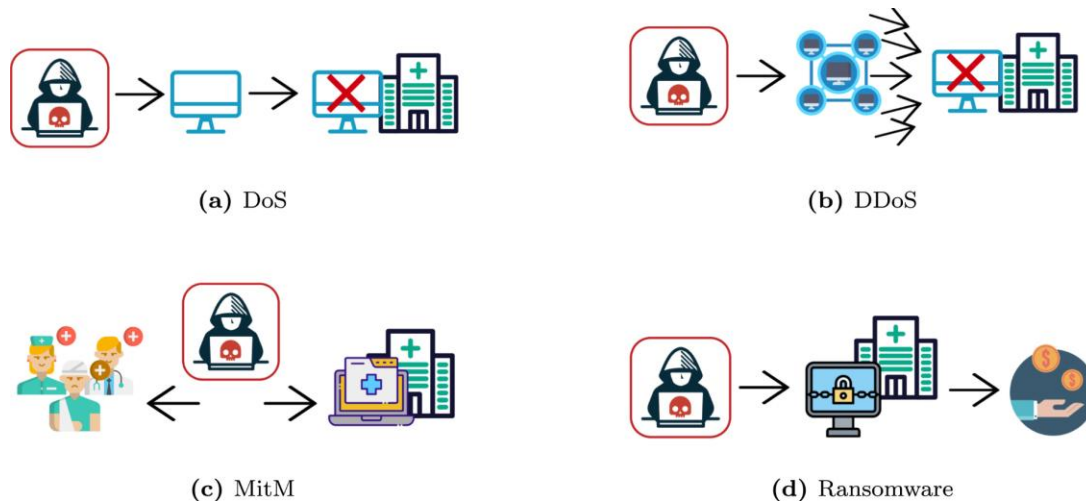


Figure I.4 : Exemples d'attaques [24]

- **Écoute passive (Eavesdropping)** : Un attaquant intercepte secrètement les communications médicales pour accéder aux données sensibles des patients, pouvant mener à des violations de confidentialité et à des usurpations d'identité.
- **Attaque par rejeu (Replay Attack)** : Un attaquant capture et retransmet des messages médicaux légitimes pour tromper le système et provoquer des actions non autorisées, telles que l'administration incorrecte de médicaments.
- **Attaque de l'homme du milieu (MitM, Man-in-the-Middle)** : Un attaquant s'interpose entre deux entités communicantes pour intercepter, modifier ou injecter des données médicales sans que les parties légitimes ne s'en aperçoivent.
- **Attaque par déni de service (DoS/DDoS)** : Un attaquant surcharge le réseau IoMT avec des requêtes malveillantes, rendant les services médicaux inaccessibles aux utilisateurs légitimes, ce qui peut s'avérer fatal dans des situations d'urgence médicale.
- **Attaque par épuisement de batterie (Battery Exhaustion)** : Un attaquant envoie des requêtes répétées pour forcer les dispositifs médicaux à rester actifs en permanence, vidant ainsi leur batterie et provoquant une interruption de service.

- **Attaque par usurpation d'identité (Impersonation)** : Un attaquant imite l'identité d'une entité légitime du réseau pour accéder aux ressources médicales ou injecter des données erronées dans le système.
- **Attaque sur les bases de données (Database Attack)** : Des techniques telles que l'injection SQL (Structured Query Language) ou le cross-site scripting (XSS) peuvent être utilisées pour accéder aux données médicales confidentielles stockées sur les serveurs cloud [14].
- **Attaque par ransomware** : Le ransomware chiffre les fichiers des systèmes médicaux et exige une rançon, privant ainsi les professionnels de santé d'accès aux dossiers patients et aux informations médicales critiques [24].

Ces vulnérabilités soulignent la nécessité de mécanismes de sécurité robustes et adaptés aux contraintes spécifiques de l'IoMT, notamment en termes de consommation énergétique et de latence [14].

VI. Applications et services de l'IoMT

VI.1. Télémédecine

La télémédecine représente l'un des piliers de la transformation numérique de la santé, visant à surmonter les barrières géographiques et temporelles entre les patients et les praticiens. Elle s'appuie sur des terminaux variés tels que les smartphones, les tablettes et les ordinateurs pour faciliter des consultations spécialisées via la transmission d'images et de vidéos en temps réel. Grâce aux infrastructures cloud, elle permet une collaboration inter-expertises pour des cas complexes, augmentant ainsi les chances de guérison tout en réduisant les coûts d'infrastructure pour les institutions [10]. L'avènement de la 5G ouvre la voie à des applications critiques telles que la télé chirurgie et l'échographie à distance, qui exigent une latence ultra-faible (inférieure à 10 ms) et une haute définition d'image pour garantir la précision des actes opératoires [23].

VI.2. Surveillance médicale à distance

Cette application permet un suivi continu et ubiquitaire de l'état de santé des patients, brisant ainsi le cadre traditionnel de l'hôpital. Elle repose sur le déploiement de réseaux corporels sans fil (WBAN) composés de capteurs portables ou d'implants capables de capturer en temps réel des paramètres vitaux tels que l'ECG, la fréquence cardiaque, la SpO2 et la température. Les données collectées sont transmises via des passerelles intelligentes (comme les smartphones) vers des serveurs médicaux ou des plateformes cloud pour analyse [9]. Ce système favorise l'autonomie des patients, notamment les personnes âgées via l'Assistance à

l'autonomie à domicile (AAL, Ambient Assisted Living), tout en permettant une intervention immédiate des services d'urgence grâce à des notifications automatiques en cas d'anomalie détectée [5].

VI.3. Diagnostic et traitement assistés

L'IoMT révolutionne le processus clinique en intégrant l'intelligence artificielle (IA) et l'apprentissage automatique (Machine Learning) pour traiter les volumes massifs de données médicales (Big Data). Des algorithmes avancés sont utilisés pour prédire l'apparition de maladies chroniques comme le diabète ou les maladies cardiovasculaires, et pour assister les médecins dans l'interprétation rapide d'images médicales (imagerie par résonance magnétique (IRM), Rayons X) [10]. Au-delà du diagnostic, l'IoMT permet des traitements automatisés et personnalisés, tels que les pompes à insuline intelligentes qui ajustent automatiquement les doses en fonction des niveaux de glucose mesurés, le tout pouvant être supervisé à distance par un médecin pour garantir la sécurité thérapeutique [9].

VI.4. Gestion hospitalière intelligente

La gestion hospitalière intelligente utilise l'IoMT pour optimiser l'efficacité opérationnelle et la logistique interne des établissements de santé. Cette technologie facilite la traçabilité des actifs en permettant la localisation instantanée d'équipements critiques, comme les bouteilles d'oxygène ou les défibrillateurs, réduisant ainsi le temps de recherche en situation d'urgence [14]. Elle assure également une gestion proactive et sécurisée de la chaîne d'approvisionnement des médicaments via des étiquettes intelligentes pour éviter la contrefaçon. Enfin, l'intégration des dossiers de santé électroniques (EHR, Electronic Health Record) permet une centralisation des données, améliorant la coordination entre les services et la supervision du personnel soignant [5].

VI.5. IoMT dans le contexte des réseaux 5G et post-5G

VI.5.1. Apports de la 5G pour l'IoMT

La 5G agit comme un catalyseur pour l'IoMT en répondant à des exigences hétérogènes à travers trois scénarios clés définis par l'ITU (International Telecommunication Union) :

- **L'eMBB (enhanced Mobile Broadband) :** Offre les débits nécessaires au transfert de volumes massifs de données, tels que l'imagerie médicale HD (High Definition) ou les flux vidéo pour la télémédecine.

- **L'URLLC (Ultra-Reliable Low Latency Communications)** : Pilier central pour les services critiques (télé-chirurgie, alertes cardiaques), garantissant une latence ultra-faible (proche de 1 ms) et une fiabilité de transmission quasi absolue.
- **Le mMTC (massive Machine Type Communications)** : Permet la densification du réseau en supportant la connexion simultanée d'un grand nombre de dispositifs médicaux à faible consommation d'énergie (capteurs de signes vitaux, montres connectées).

Pour optimiser la qualité de service (QoS) en intérieur, notamment dans les environnements hospitaliers ou domestiques, le déploiement de pico-unités radio distantes (pRRU, pico Remote Radio Unit) assure une couverture continue et robuste. Cette architecture facilite l'acheminement fluide des données critiques vers les infrastructures de Edge ou de Cloud Computing, permettant un traitement des données en temps quasi-réel [25].

Néanmoins, l'explosion du nombre de dispositifs connectés engendre une congestion spectrale majeure. C'est ici que l'intégration de mécanismes d'allocation dynamique du spectre, couplés à la radio cognitive, devient impérative pour garantir la priorité aux flux médicaux urgents.

VI.5.2. Vision post-5G (6G) et e-santé

La vision de la 6G repose sur le paradigme eURLLC, qui vise une latence sub-milliseconde (inférieure à 0,1 ms) et une fiabilité extrême de 99,99999%. Pour atteindre de telles performances, la 6G intègre des technologies de rupture :

- **Les communications TéraHertz (THz)** : Exploitant des fréquences entre 0,1 et 10 THz, cette technologie offre une bande passante massive. Elle ouvre la voie à une imagerie biomédicale haute résolution non invasive, capable de détecter des tissus pathogènes ou des agents bactériens sans ioniser les cellules, garantissant ainsi la sécurité biologique du patient.
- **L'Ultra-Massive MIMO et les surfaces intelligentes (RIS, Reconfigurable Intelligent Surfaces)** : Ces technologies permettent de gérer la connectivité simultanée de millions de capteurs par « km² » (densification extrême) tout en éliminant les zones d'ombre dans les environnements hospitaliers complexes par une focalisation précise du signal (beamforming).
- **L'Intelligence Artificielle Native** : Contrairement à la 5G, la 6G intègre l'IA au cœur de la couche physique pour une gestion prédictive de la mobilité des patients et une auto-optimisation des ressources spectrales en temps réel.

Cette évolution vers la 6G positionne le réseau non plus comme un simple canal de transmission, mais comme un système de détection et de communication intégré, indispensable pour la gestion massive et ultra-fiable des données médicales critiques [23].

VI.5.3. Problématique de l'allocation spectrale

La rareté du spectre radio constitue un goulot d'étranglement majeur pour les systèmes IoMT, aggravé par l'augmentation rapide du nombre de dispositifs connectés, notamment les dispositifs portables, dont la croissance est estimée à environ 20 % par an. Les méthodes traditionnelles d'allocation statique du spectre se révèlent inadaptées face à la nature dynamique et imprévisible des environnements médicaux, en particulier dans les zones urbaines denses.

Cette rigidité entraîne une utilisation inefficace des ressources spectrales, se traduisant par une congestion accrue du réseau. En conséquence, les performances du système se dégradent, avec une réduction du débit pouvant atteindre environ 30 % et des taux de perte de paquets pouvant s'élever jusqu'à 15 % lors des périodes de forte activité.

Par ailleurs, le rapport signal sur interférence et bruit (SINR) peut chuter en dessous de seuils critiques, parfois inférieurs à 10 dB, ce qui impacte directement la qualité des communications. Cette dégradation se traduit par une augmentation significative de la latence, pouvant dépasser 150 ms, alors que certaines applications médicales critiques exigent des délais inférieurs à 10 ms [23].

Face à ces limitations, il devient indispensable de développer des approches d'allocation dynamique du spectre, capables de s'adapter en temps réel aux conditions du réseau et de prendre en compte plusieurs critères, tels que la qualité de service, la fiabilité et les exigences spécifiques des applications IoMT.

VI.5.4 Intérêt des réseaux radio cognitifs pour l'IoMT

Face aux limites de l'allocation statique, les Réseaux Radio Cognitifs (RC) apparaissent comme une solution prometteuse pour l'écosystème IoMT. En permettant un accès dynamique et opportuniste au spectre, cette technologie transforme la gestion des ressources de réactive à proactive, optimisant ainsi l'utilisation des bandes de fréquences tout en garantissant la priorité aux flux médicaux critiques [23].

Cette approche constitue le socle nécessaire au développement de méthodes d'allocation multicritères, telles que TOPSIS (Technique for Order of Preference by Similarity to Ideal Solution), capables de répondre aux exigences de fiabilité de l'e-santé. Le chapitre suivant sera

consacré à l'étude approfondie du cycle cognitif et des mécanismes d'intelligence distribuée permettant de concrétiser cette vision.

VII. Conclusion

Ce chapitre a présenté un état de l'art complet sur l'IoMT, en abordant ses concepts, son architecture, ses exigences spécifiques et ses applications dans l'e-santé, de la télémédecine à la gestion hospitalière intelligente.

Le déploiement à grande échelle de l'IoMT se heurte à des défis majeurs : congestion et rareté du spectre, interférences, mobilité des dispositifs, hétérogénéité des réseaux et vulnérabilités de sécurité. Ces contraintes sont particulièrement critiques dans le contexte des réseaux 5G et post-5G, où la connectivité massive accentue la pression sur des ressources limitées.

Face à ces enjeux de saturation et de priorité médicale, les méthodes d'allocation statique du spectre s'avèrent désormais insuffisantes. Pour garantir la fiabilité des soins, il devient impératif d'évoluer vers une gestion plus flexible, capable d'orchestrer les ressources de manière autonome et de s'adapter en temps réel aux variations de l'environnement radio.

C'est dans cette perspective que le chapitre suivant explore les fondements des Réseaux Radio Cognitifs (RC) et des Systèmes Multi-Agents (SMA). Nous y détaillerons leurs concepts fondamentaux, leurs fonctions essentielles ainsi que les mécanismes de décision multicritère, posant ainsi le cadre théorique nécessaire au développement d'une gestion intelligente et adaptative dédiée aux services de l'e-santé.

Chapitre II

Réseaux Radio Cognitifs et Systèmes Multi-Agents

Table des matières

I. Introduction.....	32
II. Contexte des réseaux sans fil.....	32
II.1. Catégories de réseaux sans fil.....	33
II.2. Défis spectraux pour l'IoMT.....	35
III. Radio Logicielle Restreinte (SDR) et Radio Cognitive (RC)	36
III.1. Historique et évolution	36
III.2. Radio logicielle restreinte (SDR)	37
III.3. Évolution vers la Radio Cognitive	38
III.4. Définition et concepts fondamentaux de la Radio Cognitive.....	39
III.4.1. Le paradoxe du spectre : motivation de la RC	39
III.4.2. Piliers technologiques : capacité et reconfigurabilité.....	39
III.4.3. Modèle d'accès et partage du spectre.....	40
III.4.4. Cadre normatif et évolutions	40
III.5. La relation entre la Radio Cognitive et la SDR.....	40
IV. Architecture et Cycle Cognitif.....	41
IV.1. Architecture de la Radio Cognitive	41
IV.2. Cycle de Mitola	43
IV.3. Composants de la RC	44
IV.3.1. Le Moteur de Cognition (Cognition Engine – CE)	44
IV.3.2. La Chaîne de Transmission et de Réception (SDR)	45
IV.3.3. Le Matériel Reconfigurable.....	45
V. Fonctions Cognitives Essentielles.....	46
V.1. Détection du spectre (Spectrum Sensing)	46
V.2. Gestion et décision spectrale (Spectrum Management).....	47
V.3. Partage du spectre (Spectrum Sharing).....	47
V.4. Mobilité spectrale (Spectrum Handoff)	47
VI. Allocation Dynamique du Spectre	48
VI.1. Formulation du problème d'allocation	48
VI.2. Approches et stratégies d'optimisation	48
VI.3. Méthodes de décision multicritère (MCDM)	49
VI.3.1. Méthodes de surclassement : ELECTRE et PROMETHEE	50
VI.3.2. Méthode AHP (Analytic Hierarchy Process)	50
VI.3.3. Méthode TOPSIS	50
VII. Sécurité de la Radio Cognitive	51
VII.1. Menaces et vulnérabilités.....	51
VII.2. Attaques au niveau de la couche physique	51

VII.3. Attaques au niveau de la couche liaison	52
VII.4. Attaques au niveau de la couche réseau.....	52
VII.5. Mécanismes de protection	52
VIII. Systèmes Multi-Agents (SMA) : Concepts et Architectures.....	53
VIII.1. Concepts fondamentaux des SMA	53
VIII.2. Architectures multi-agents.....	54
VIII.2.1. Types d'agents selon leur architecture interne	54
VIII.2.2. Structures d'organisation des agents.....	55
VIII.2.3. Mécanismes de communication	55
VIII.3. Plateformes de développement des Systèmes Multi-Agents.....	56
VIII.4. Intégration des SMA dans la RC	57
VIII.4.1. Coordination et coopération entre utilisateurs.....	58
VIII.4.2. Gestion des ressources et de la mobilité.....	58
VIII.4.3. Apprentissage et optimisation	58
VIII.4.4. Qualité de Service (QoS) pour les applications sensibles	59
IX. Domaines d'application de la Radio Cognitive	59
IX.1. Réseaux militaires et de sécurité publique	59
IX.2. Réseaux de secours et d'urgence	59
IX.3. Réseaux cellulaires (5G) et villes intelligentes (Smart Cities).....	60
IX.4. Réseaux IoMT.....	60
X. Conclusion.....	60

I. Introduction

Le chapitre précédent a mis en évidence les défis majeurs auxquels est confronté l'IoMT, notamment la congestion spectrale, les interférences et la nécessité d'une gestion dynamique et adaptative des ressources radioélectriques. Face à ces enjeux, les réseaux sans fil classiques atteignent leurs limites, et de nouvelles approches s'imposent pour garantir la qualité de service (QoS) extrêmement stricte requise par les applications e-santé critiques.

Ce chapitre est consacré à l'état de l'art de la Radio Cognitive (RC) et de l'intelligence distribuée, qui constituent le cœur technologique de ce travail. Nous commencerons par rappeler le contexte général des réseaux sans fil et les défis spectraux spécifiques à l'IoMT. Nous introduirons ensuite la Radio Logicielle (SDR, Software Defined Radio) comme fondement technologique, avant d'aborder en détail la Radio Cognitive elle-même : son architecture, son cycle cognitif et ses fonctions essentielles (détection, gestion, partage et mobilité spectrale). Nous traiterons également les méthodes d'allocation dynamique du spectre et les approches multicritères associées, ainsi que les vulnérabilités de sécurité inhérentes à ces réseaux flexibles.

Par la suite, nous présenterons les Systèmes Multi-Agents (SMA) et leur intégration avec la RC comme outil d'orchestration et de décision intelligente. Enfin, nous concluons en explorant les différents domaines d'application de la Radio Cognitive, illustrant son impact depuis les réseaux critiques (militaires, secours) et cellulaires (5G/Smart Cities) jusqu'à notre cas d'étude principal : les réseaux IoMT.

II. Contexte des réseaux sans fil

Le terme « sans fil » désigne la transmission d'informations sur une distance donnée sans l'utilisation de conducteurs électriques physiques tels que les câbles ou les fils. Contrairement aux communications filaires qui s'appuient sur un support « guidé » (câbles coaxiaux, fibre optique), les réseaux sans fil exploitent un support non guidé, à savoir l'espace libre ou l'air, pour la propagation des signaux.

Cette technologie repose sur l'utilisation d'ondes électromagnétiques, telles que les fréquences radio (RF), l'infrarouge ou les micro-ondes, pour transporter les données entre deux points.

L'avantage prédominant et le plus critique de ces systèmes est la mobilité, offrant aux utilisateurs la liberté de rester connectés tout en se déplaçant. En complément, la flexibilité, la facilité d'installation et les coûts d'infrastructure réduits par rapport au câblage physique font

des réseaux sans fil une solution incontournable, particulièrement dans les zones reculées ou lors de situations d'urgence.

Aujourd'hui, l'évolution de ces technologies permet une connectivité ubiquitaire « n'importe où et n'importe quand », transformant radicalement les réseaux de données et les télécommunications. Pour répondre à la diversité des besoins, allant de la surveillance de capteurs corporels à la communication globale par satellite, ces réseaux sont classifiés selon leur portée géographique et leurs applications spécifiques [26]. Cette classification constitue le point de départ pour comprendre les défis spectraux auxquels font face les réseaux sans fil dédiés à l'IIoT, et qui motivent le recours aux réseaux radio cognitifs.

II.1. Catégories de réseaux sans fil

Les réseaux sans fil sont classifiés selon leur portée géographique et leurs caractéristiques techniques. On distingue six catégories principales, allant du réseau corporel au réseau régional, chacune adaptée à des besoins et des environnements spécifiques [26], que nous détaillons ci-après. La Figure II.1 illustre les différentes zones de couverture de ces catégories.

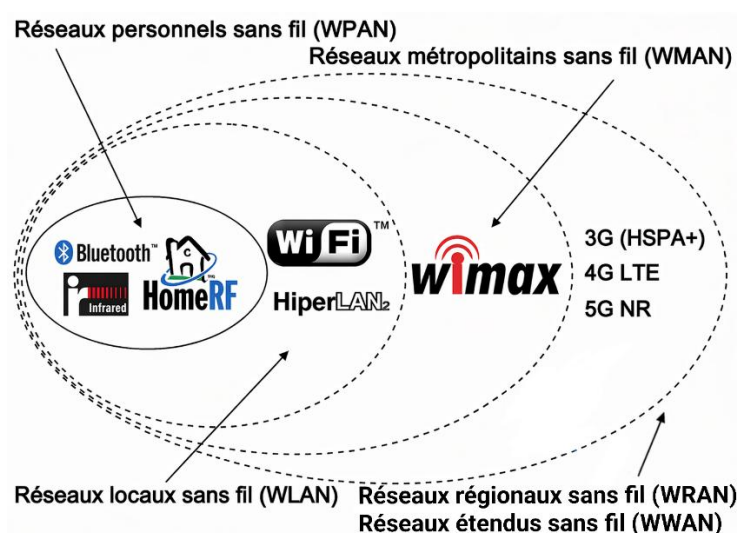


Figure II.1 : Catégories des réseaux sans fil [27]

- **WBAN – Wireless Body Area Network**

Les réseaux corporels sans fil (WBAN) sont composés de micro-capteurs intelligents, portables ou implantables, capables de mesurer en continu des paramètres physiologiques tels que la fréquence cardiaque, la pression artérielle, le taux d'oxygène et l'activité cérébrale

(électroencéphalogramme (EEG)). Adoptant généralement une topologie en étoile, ils utilisent des technologies à faible consommation telles que ZigBee, Bluetooth et l'Ultra-Wideband (UWB) pour transmettre les données médicales vers des plateformes de traitement distantes [28]. Les WBAN constituent la couche la plus proche du patient dans l'écosystème IoMT.

La Figure II.2 illustre la diversité de ces capteurs ainsi que leur positionnement stratégique sur le corps humain pour assurer un suivi médical complet.

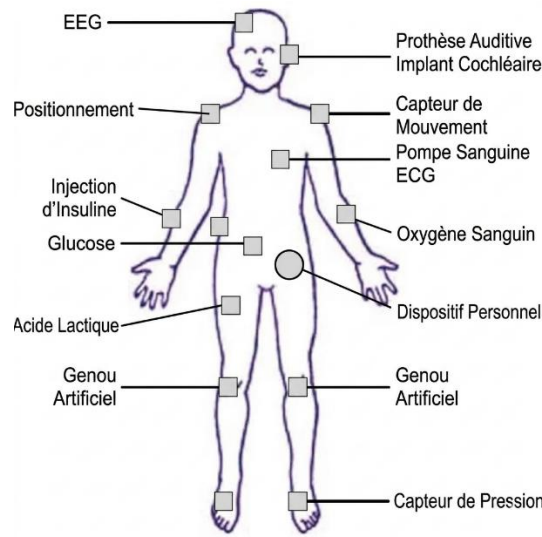


Figure II.2 : Capteurs et dispositifs médicaux d'un réseau WBAN [29]

- **WPAN–Wireless Personal Area Networks**

Les réseaux personnels sans fil (WPAN) reposent sur le standard IEEE 802.15 et sont conçus pour des communications à très courte portée (~10 mètres), avec peu d'infrastructure et une faible consommation énergétique [23]. Fonctionnant sur des bandes ISM non licenciées (2.4 GHz), ils intègrent plusieurs technologies adaptées à l'IoMT : Bluetooth (IEEE 802.15.1) pour les communications maître-esclave entre dispositifs médicaux, ZigBee (IEEE 802.15.4) pour les réseaux de capteurs à faible consommation supportant des topologies en étoile, maille et arbre, et UWB (Ultra Wide Band) (IEEE 802.15.3) pour les liaisons multimédias à haut débit [30].

- **WLAN–Wireless Local Area Networks**

Les réseaux locaux sans fil (WLAN) reposent sur le standard IEEE 802.11, connu sous le nom de Wi-Fi (Wireless Fidelity). Conçus pour des communications à courte portée (~100 mètres), ils offrent un débit élevé grâce aux amendements successifs (802.11n, 802.11ac,

802.11ax). Les WLAN modernes intègrent des algorithmes d'allocation dynamique des ressources pour optimiser les performances dans des environnements denses [31].

- **WMAN–Wireless Metropolitan Area Networks**

Les réseaux métropolitains sans fil (WMAN) permettent la connexion de plusieurs réseaux sur une zone géographique étendue, telle qu'une ville ou un campus universitaire. Basés sur le standard IEEE 802.16 (WiMAX, Worldwide Interoperability for Microwave Access), ils offrent des débits effectifs de 1 à 10 Mbps sur une portée de 4 à 10 kilomètres, constituant ainsi une alternative au câblage physique (cuivre ou fibre optique) pour les opérateurs de télécommunications [26].

- **WWAN–Wireless Wide Area Network**

Les réseaux étendus sans fil (WWAN) offrent la couverture géographique la plus vaste, à l'échelle nationale voire internationale, en s'appuyant sur les infrastructures des opérateurs de télécommunications mobiles. Leur évolution a été marquée par des sauts technologiques majeurs : la 3G (HSPA+, High-Speed Packet Access Plus) avec des débits moyens de 8 Mbps, la 4G (LTE) avec des débits de 10 à 30 Mbps et une latence de 50 à 100 ms, et la 5G (NR, New Radio) avec des débits théoriques atteignant 10 Gbps et une latence ultra-faible de 1 à 10 ms grâce au Massive MIMO (Multi Input Multi Output) et aux ondes millimétriques (mmWave) [32].

- **WRAN–Wireless Regional Area Network**

Les réseaux régionaux sans fil (WRAN), régis par le standard IEEE 802.22, exploitent les fréquences TV UHF/VHF (Ultra/Very High Frequency) inutilisées (54 MHz à 862 MHz) pour fournir une connectivité sur de vastes zones géographiques pouvant atteindre 100 km. Fonctionnant sur un paradigme maître-esclave, chaque cellule comprend une station de base centrale gérant plusieurs équipements locaux clients (CPE, Customer Premises Equipment). Ces réseaux utilisent l'OFDMA (Orthogonal Frequency Division Multiple Access) et la détection coopérative de spectre (CSS, Cooperative Spectrum Sensing) pour gérer efficacement les ressources spectrales disponibles [33].

II.2. Défis spectraux pour l'IoMT

Le déploiement massif des dispositifs IoMT s'inscrit dans un contexte de croissance exponentielle de la connectivité sans fil. Avec des prévisions atteignant 50 milliards de dispositifs connectés échangeant des dizaines d'exaoctets de données chaque mois, la

compétition pour l'accès à un spectre de ressources finies devient un obstacle majeur à l'innovation médicale.

Les politiques d'allocation statique du spectre créent un paradoxe : certaines bandes de fréquences sont saturées tandis que d'autres restent largement inutilisées selon les zones géographiques ou les périodes temporelles. Pour l'IoMT, cela signifie que des dispositifs vitaux pourraient ne pas trouver de canal disponible malgré l'existence de vides spectraux inexploités. Cette inefficacité est accentuée par la complexité multidimensionnelle de l'environnement hospitalier, où l'occupation du spectre varie selon trois dimensions critiques : le temps, l'espace et la fréquence, rendant le comportement des signaux difficile à prédire.

Cette imprévisibilité engendre des trous de couverture et de routage, des zones où la connectivité requise n'est pas atteinte, pouvant entraîner une perte de surveillance médicale critique. Parallèlement, la valeur des données de santé attire des acteurs malveillants exploitant plusieurs types d'attaques : le brouillage (jamming) créant des zones d'ombre empêchant toute propagation d'alertes médicales, l'injection de fausses données compromettant l'intégrité des transmissions, et les attaques par drainage (sinkholes) épuisant les ressources énergétiques des nano-capteurs.

Face à ces défis, le passage vers une Allocation Dynamique du Spectre (DSA, Dynamic Spectrum Allocation) s'appuyant sur la Radio Cognitive et des capacités d'inférence sophistiquées apparaît comme la solution nécessaire pour optimiser l'utilisation des ressources tout en gérant efficacement les interférences [34].

III. Radio Logicielle Restreinte (SDR) et Radio Cognitive (RC)

III.1. Historique et évolution

L'évolution menant aux systèmes de radio cognitive actuels s'articule autour de plusieurs jalons fondamentaux qui ont progressivement transformé la radio d'un système purement matériel en un système intelligent et adaptatif. Cette genèse prend racine dans les fondations scientifiques du XIXe siècle, notamment avec les travaux de James Clerk Maxwell (1864) sur l'électromagnétisme, confirmés expérimentalement par Heinrich Hertz entre 1885 et 1889. Ces avancées ont ouvert la voie à l'ère des pionniers, illustrée par Guglielmo Marconi qui réalisa, en 1901, la première transmission transatlantique, libérant ainsi les communications des contraintes du câblage [35].

Un tournant technologique majeur s'opère en 1971 avec l'invention du premier microprocesseur commercial, marquant le début de la révolution numérique. Cette avancée a permis d'intégrer des capacités de traitement dans les systèmes de communication, ouvrant la voie à des radios plus flexibles. Dans ce contexte, le concept de radio logicielle (SDR, Software-Defined Radio) a été introduit au début des années 1990, notamment par Joseph Mitola en 1991. Cette approche consiste à remplacer les composants matériels traditionnels par des fonctions logicielles reconfigurables [36].

Dans la continuité de ces travaux, Joseph Mitola III a ensuite introduit le concept de radio cognitive (RC) en 1999. Il décrit la radio cognitive comme un système intelligent capable d'optimiser dynamiquement l'utilisation du spectre, une vision approfondie dans sa thèse de doctorat en 2000 [37].

La reconnaissance institutionnelle de cette technologie a été renforcée par le rapport de la FCC (Federal Communications Commission) en 2002, qui préconise une utilisation plus flexible et dynamique du spectre pour faire face à sa rareté. Enfin, en 2005, Simon Haykin a formalisé le concept de radio cognitive en définissant sa capacité à détecter les « espaces blancs » (spectrum holes), posant ainsi les bases d'une utilisation plus efficace des ressources radioélectriques [38].

III.2. Radio logicielle restreinte (SDR)

La Radio Logicielle restreinte (SDR) se définit comme un émetteur-récepteur programmable capable de prendre en charge divers protocoles de communication sans modification matérielle de l'équipement. Contrairement aux solutions traditionnelles figées par le matériel, la technologie SDR déporte la complexité vers des fonctions implémentées par logiciel. Cette approche offre une grande flexibilité, permettant l'intégration de nouvelles fonctionnalités et la mise à jour des systèmes par simple reprogrammation logicielle.

L'architecture d'un émetteur-récepteur SDR repose sur plusieurs composants clés assurant l'interface entre les domaines analogique et numérique. En amont, une antenne large bande ou reconfigurable permet la réception de signaux sur différentes bandes de fréquences. Le signal est ensuite traité par le Front End RF, qui assure la transmission, la réception et la conversion vers une fréquence intermédiaire (IF) ou directement en bande de base. La transition vers le domaine numérique est réalisée grâce aux convertisseurs de données : le convertisseur analogique-numérique (CAN) numérise le signal reçu, tandis que le convertisseur numérique-analogique (CNA) génère le signal à transmettre. La chaîne de

traitement numérique prend ensuite en charge les opérations de bande de base telles que le filtrage, la synchronisation, le codage et la modulation.

L'implémentation de ces fonctions repose sur différentes architectures matérielles offrant des compromis entre flexibilité et performance. Les processeurs à usage général (GPP, General Purpose Processors) sont privilégiés pour le prototypage en raison de leur facilité de programmation, tandis que les processeurs de signaux numériques (DSP, Digital Signal Processing) et les circuits FPGA (Field Programmable Gate Array) permettent d'atteindre des performances élevées pour le traitement en temps réel. Les architectures hybrides, combinant processeurs logiciels et FPGA au sein de systèmes sur puce (SoC, System on a Chip), représentent aujourd'hui une solution efficace pour optimiser les performances tout en maîtrisant la consommation énergétique.

Grâce à cette adaptabilité, la SDR connaît un développement croissant et trouve des applications dans de nombreux domaines, notamment les réseaux sans fil avancés, les systèmes de sécurité, les communications véhicule-à-véhicule (V2V) et l'Internet des Objets (IoT), y compris l'Internet des Objets Médicaux (IoMT) [39].

III.3. Évolution vers la Radio Cognitive

L'évolution vers la Radio Cognitive (RC) représente une étape majeure dans le développement des systèmes de communication sans fil, transformant une plateforme flexible en une entité dotée d'intelligence et d'autonomie. Une radio cognitive peut être définie comme une extension de la radio logicielle (SDR), capable de percevoir son environnement, de suivre les variations contextuelles et d'adapter dynamiquement son fonctionnement en conséquence.

Cette évolution s'inscrit dans une hiérarchie technologique où la radio numérique (DR, Digital Radio) constitue la base, suivie par la SDR, puis par la RC. Le principal moteur de cette transition réside dans l'inefficacité de l'allocation statique du spectre, caractérisée par une sous-utilisation des bandes de fréquences licenciées. La radio cognitive permet ainsi de mettre en œuvre le concept de spectrum pooling, dans lequel des utilisateurs secondaires exploitent temporairement les espaces blancs du spectre sans perturber les utilisateurs primaires.

Contrairement à la SDR traditionnelle, qui se reconfigure selon des paramètres prédéfinis, la RC réalise une adaptation en temps réel basée sur l'observation de son environnement électromagnétique. Elle intègre des mécanismes d'apprentissage et de prise de

décision afin d'optimiser l'utilisation du spectre. Dans ce cadre, elle doit respecter un ensemble de règles de coexistence, notamment le principe de (LBT, Listen Before Talk), garantissant une utilisation équitable des ressources radio.

En définitive, la radio cognitive transforme le terminal en une entité autonome capable d'interagir intelligemment avec son environnement et avec d'autres dispositifs, contribuant ainsi à une utilisation plus efficace et dynamique du spectre radioélectrique [40].

III.4. Définition et concepts fondamentaux de la Radio Cognitive

Le paradigme de la Radio Cognitive (RC) a été introduit par Joseph Mitola III à la fin des années 1990. Il constitue une évolution majeure des systèmes de communication sans fil, transformant une radio programmable (SDR) en un système intelligent capable d'adaptation autonome. La RC est définie comme une technologie de communication capable de percevoir son environnement radio, d'analyser son contexte et d'ajuster dynamiquement ses paramètres de transmission afin d'optimiser l'efficacité spectrale et la qualité de service [41].

III.4.1. Le paradoxe du spectre : motivation de la RC

Le développement de la RC repose sur le constat du « paradoxe du spectre » : bien que la majorité des bandes de fréquences soient officiellement allouées par les organismes de régulation, une grande partie du spectre reste sous-utilisée à un instant et dans un lieu donné en raison de l'allocation statique des ressources. Selon plusieurs études, jusqu'à 80 % du spectre peut être inoccupé de manière temporaire.

Ce phénomène conduit à un gaspillage important des ressources spectrales, particulièrement critique dans le contexte de la croissance massive des objets connectés et des applications IoMT. La RC propose de résoudre ce problème en identifiant les « espaces blancs » (spectrum holes), permettant une utilisation opportuniste du spectre disponible sans perturber les utilisateurs licenciés [41].

III.4.2. Piliers technologiques : capacité et reconfigurabilité

L'intelligence de la RC repose principalement sur deux capacités fondamentales :

- **La capacité cognitive** : elle correspond à la faculté du système de percevoir et analyser l'environnement radiofréquence (fréquence, puissance, bande passante, modulation, etc.) afin de détecter les opportunités d'accès au spectre.
- **La reconfigurabilité** : elle permet au système d'adapter dynamiquement ses paramètres de transmission (fréquence, puissance, modulation et protocole) en fonction des

informations perçues, sans modification matérielle. Cette capacité est rendue possible grâce à la SDR [41].

III.4.3. Modèle d'accès et partage du spectre

Dans un réseau radio cognitif, l'accès au spectre repose sur une hiérarchie d'accès entre deux types d'utilisateurs :

- **Utilisateur Primaire (PU)** : détenteur de la licence officielle, il possède la priorité d'utilisation du spectre et ne doit subir aucune interférence.
- **Utilisateur Secondaire (SU)** : utilisateur cognitif qui exploite le spectre de manière opportuniste lorsque celui-ci est libre, tout en garantissant une coexistence non intrusive avec le PU.

Quatre paradigmes principaux définissent les stratégies d'accès au spectre :

- **Interweave (Entrelacement)** : le SU utilise uniquement les bandes totalement inoccupées.
- **Underlay (Sous-couche)** : le SU transmet simultanément avec le PU tout en respectant un seuil strict d'interférence.
- **Overlay (Superposition)** : le SU exploite des informations sur le PU pour optimiser sa transmission tout en limitant les interférences.
- **Hybrid** : combinaison adaptative des approches précédentes selon les conditions du réseau [41].

III.4.4. Cadre normatif et évolutions

Le standard IEEE 802.22 formalise les principes d'utilisation opportuniste du spectre pour les réseaux régionaux sans fil (WRAN), en s'appuyant sur le concept d'accès dynamique au spectre. Ce standard impose notamment le principe du « Listen Before Talk », selon lequel un utilisateur secondaire doit vérifier l'absence d'activité primaire avant toute transmission.

Aujourd'hui, l'évolution de la Radio Cognitive intègre de plus en plus les techniques d'Intelligence Artificielle (IA) et d'Apprentissage Automatique (Machine Learning), permettant de prédire la disponibilité du spectre et d'améliorer l'autonomie des systèmes IoMT dans des environnements radio complexes et dynamiques [42].

III.5. La relation entre la Radio Cognitive et la SDR

La Radio Logicielle Restreinte (SDR) constitue la plateforme technologique indispensable à la mise en œuvre de la Radio Cognitive (RC). En tant que technologie

habilitante (enabling technology), la SDR fournit l'infrastructure matérielle et logicielle nécessaire pour exécuter des fonctions adaptatives critiques, telles que le balayage spectral pour l'observation et le basculement de fréquence pour l'action. Il est important de noter qu'une plateforme SDR peut exister de manière autonome en tant que système programmable mais statique ; en revanche, la Radio Cognitive s'appuie impérativement sur la flexibilité de la SDR pour traduire ses capacités de raisonnement en ajustements physiques (puissance, modulation, bande passante) [43][44].

La synergie entre ces deux entités, illustrée à la Figure II.3, repose sur le moteur cognitif. Ce dernier agit comme l'organe de contrôle qui optimise le module SDR en analysant simultanément la perception de l'environnement radio, le contexte de l'utilisateur et l'état global du réseau. En résumé, la SDR offre la reconfigurabilité et la portabilité nécessaires (le « corps »), tandis que la RC apporte l'intelligence et l'apprentissage (le « cerveau » ou l'esprit) essentiels pour assurer une communication robuste et autonome.

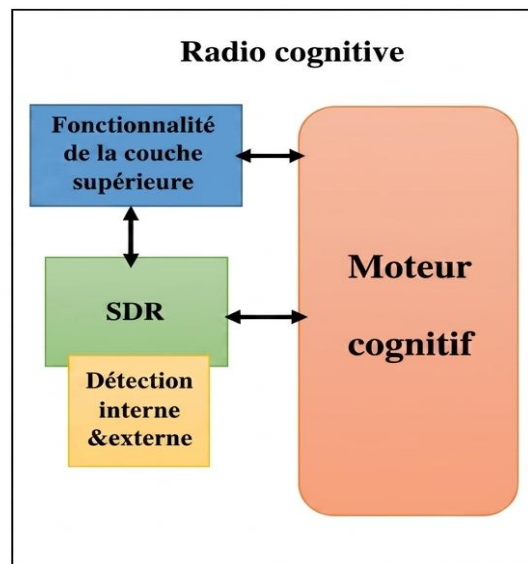


Figure II.3 : La relation entre RC et SDR [45]

IV. Architecture et Cycle Cognitif

IV.1. Architecture de la Radio Cognitive

L'architecture d'une Radio Cognitive, telle que conceptualisée par Joseph Mitola, dépasse le cadre simple de la transmission sans fil pour devenir un système conscient de son contexte. Selon ce modèle, l'architecture se structure autour de six composantes majeures qui interagissent pour fournir des services intelligents et adaptatifs [45], comme l'illustre la Figure II.4.

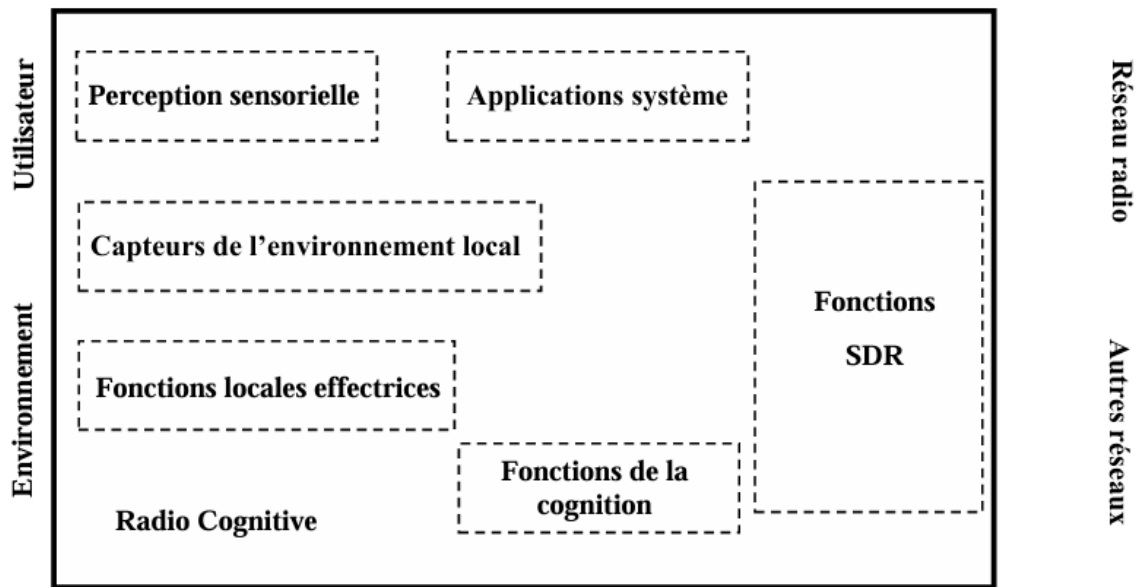


Figure II.4 : Les composants de l'architecture de la radio cognitive [45]

La Perception Sensorielle (Sensory Perception) : Cette composante permet à la radio d'interagir avec l'utilisateur via diverses interfaces (acoustique, vidéo, haptique). Elle constitue les « sens » de la radio.

Les Capteurs d'Environnement Local : Ils collectent des données contextuelles physiques telles que la géolocalisation (GPS, Global Positioning System), la température ou les mouvements (accéléromètre), permettant à la radio de comprendre son environnement immédiat.

Les Applications Système : Elles regroupent les services et les logiciels indépendants du média de transmission, comme les protocoles de jeux en réseau ou les flux de services multimédias.

Les Fonctions SDR (SDR Functions) : Elles constituent le cœur de l'interface radio. Elles gèrent la détection RF et l'implémentation logicielle des protocoles de communication.

Les Fonctions de Cognition : C'est le « cerveau » du système. Elles assurent les mécanismes de haut niveau : le contrôle, la planification stratégique et l'apprentissage à partir des expériences passées.

Les Fonctions Effectrices Locales : Elles traduisent les décisions du système en actions perceptibles pour l'utilisateur, comme la synthèse vocale, l'affichage graphique ou la génération de texte.

Cette architecture s'appuie sur une interaction forte entre les couches. Les protocoles de la couche MAC (Medium Access Control) servent d'interface entre le matériel SDR et les applications, tandis que la couche physique (PHY) utilise des algorithmes intelligents pour traiter le signal numérique de manière logicielle. Cette approche multicouche permet une adaptation fine de la puissance, de la modulation et du débit en fonction de l'état changeant du réseau [45].

IV.2. Cycle de Mitola

Le cycle de cognition, couramment appelé « cycle de Mitola », constitue le moteur décisionnel et opérationnel de la radio cognitive. Il confère à l'équipement matériel sa capacité d'agent autonome et intelligent. Ce processus itératif se présente sous la forme d'une boucle continue de type « observer-décider-agir », permettant à la radio de raisonner sur son environnement, de s'adapter aux besoins des utilisateurs et d'ajuster dynamiquement son comportement.

L'architecture de ce cycle se décompose en deux grandes phases, regroupant six étapes fondamentales :

- **Phase 1 : Observation, Orientation et Planification**

L'Observation (Observe) : La radio collecte et analyse les informations issues de l'environnement radiofréquence. Cette étape consiste à identifier le contexte, notamment le niveau d'interférence, la disponibilité des canaux ou les demandes de communication.

L'Orientation (Orient) : À partir des informations observées, le système interprète la situation en tenant compte des contraintes de qualité de service (QoS) et des conditions du spectre, afin d'établir des priorités.

La Planification (Plan) : Le système élabore différentes stratégies possibles, incluant la sélection des bandes de fréquences et des paramètres de transmission les plus adaptés au contexte.

- **Phase 2 : Décision, Action et Apprentissage**

La Décision (Decide) : Le moteur cognitif sélectionne la meilleure stratégie en fonction des critères de QoS et alloue les ressources nécessaires à la radio logicielle (SDR).

L'Action (Act) : La radio met en œuvre les décisions prises en ajustant ses paramètres de transmission, tels que la fréquence, la puissance ou la modulation.

L'Apprentissage (Learn) : Le système analyse les performances des actions entreprises à l'aide d'algorithmes d'apprentissage automatique (Machine Learning). Cette étape permet d'améliorer progressivement les décisions futures, notamment dans des environnements IoMT dynamiques et complexes.

En définitive, ce cycle continu permet à la radio cognitive d'évoluer d'un simple système de communication vers une entité intelligente capable de gérer de manière adaptative et efficace l'utilisation du spectre [37]. La dynamique du cycle cognitif ainsi que l'enchaînement de ses six phases sont illustrées dans la Figure II.5 ci-dessous.

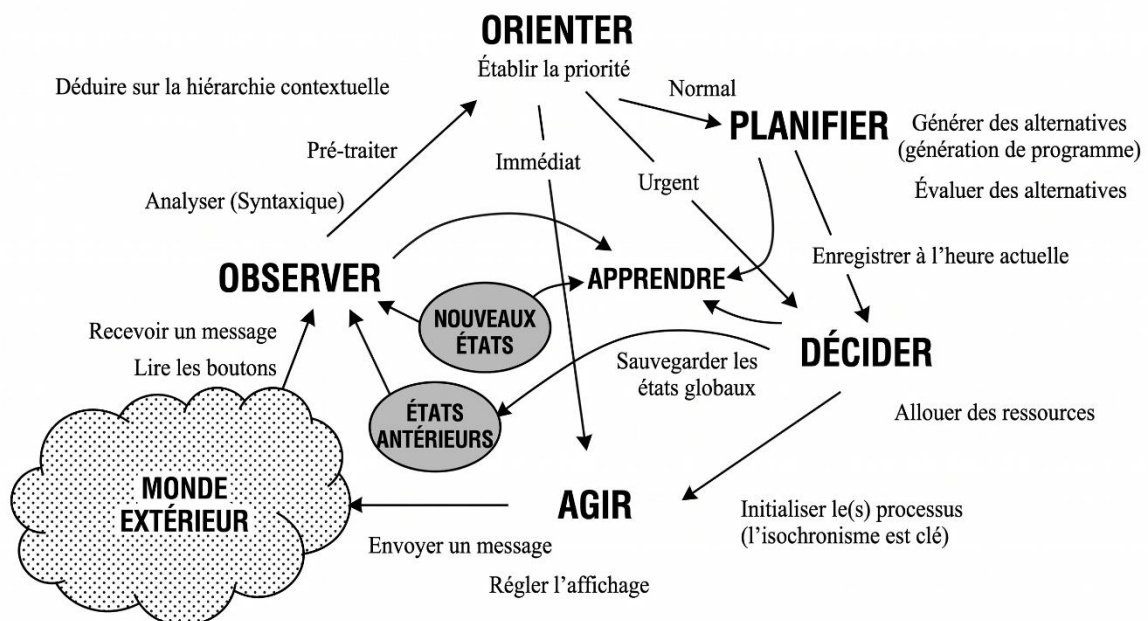


Figure II.5 : Cycle de cognition de Mitola [37]

IV.3. Composants de la RC

Un système de radio cognitive se compose de deux composantes principales : une composante logique, responsable de l'intelligence et de la prise de décision, et une composante physique, chargée de la transmission et de la réception des signaux [46].

IV.3.1. Le Moteur de Cognition (CE, Cognition Engine)

Le moteur de cognition constitue le composant central du système. Il est responsable de la prise de décision intelligente en exploitant les informations issues de l'environnement afin de reconfigurer dynamiquement les paramètres des couches physique (PHY) et liaison (MAC). Il se décompose en plusieurs modules fonctionnels :

- **Module de détection (Sensing Module)** : Il assure l'analyse du spectre radioélectrique afin d'identifier l'activité des utilisateurs primaires, caractériser le canal et détecter les espaces blancs disponibles.
- **Module d'apprentissage automatique (Machine Learning Module)** : Il exploite des algorithmes d'apprentissage automatique pour analyser les données collectées, extraire des connaissances et adapter le comportement du système en fonction des conditions de l'environnement.
- **Module de prise de décision dynamique** : Il traite les informations disponibles afin de déterminer les paramètres optimaux de transmission (bande de fréquence, modulation, puissance). Cette décision repose sur des méthodes d'optimisation avancées, telles que la théorie des jeux ou l'optimisation stochastique.
- **Répertoire d'information (Information Repository)** : Il stocke les connaissances acquises, incluant les politiques de gestion du spectre, les historiques d'utilisation et les informations contextuelles nécessaires à la prise de décision [46].

IV.3.2. La Chaîne de Transmission et de Réception (SDR)

La mise en œuvre des décisions du moteur cognitif repose sur une radio logicielle restreinte (SDR), qui permet une reconfiguration flexible des paramètres de transmission. Cette chaîne se compose de trois parties principales :

- **Front-End radiofréquence (RF)** : Il comprend l'antenne, les filtres, l'amplificateur à faible bruit (LNA, Low Noise Amplifier), les mélangeurs et l'oscillateur local (OL), assurant la conversion de fréquence et l'adaptation du signal.
- **Front-End numérique** : Il réalise la conversion analogique-numérique et numérique-analogique (CAN/CNA), ainsi que les opérations de filtrage et de traitement intermédiaire.
- **Traitement en bande de base** : Les opérations de modulation, codage et traitement du signal sont exécutées par des unités de calcul dédiées [47].

IV.3.3. Le Matériel Reconfigurable

Les performances et la capacité d'adaptation de la radio cognitive dépendent fortement des technologies matérielles utilisées :

- **FPGA (Field Programmable Gate Array)** : Ces circuits permettent une reconfiguration matérielle dynamique, offrant un excellent compromis entre performance et flexibilité.

- **USRP (Universal Software Radio Peripheral)** : Ces plateformes sont largement utilisées pour le prototypage des systèmes SDR. Elles offrent une large plage de fréquences et permettent un contrôle complet via logiciel [46].

V. Fonctions Cognitives Essentielles

Le cycle opérationnel d'un système de radio cognitive (RC) repose sur quatre fonctions majeures qui permettent une gestion efficace, dynamique et autonome des ressources fréquentielles [48].

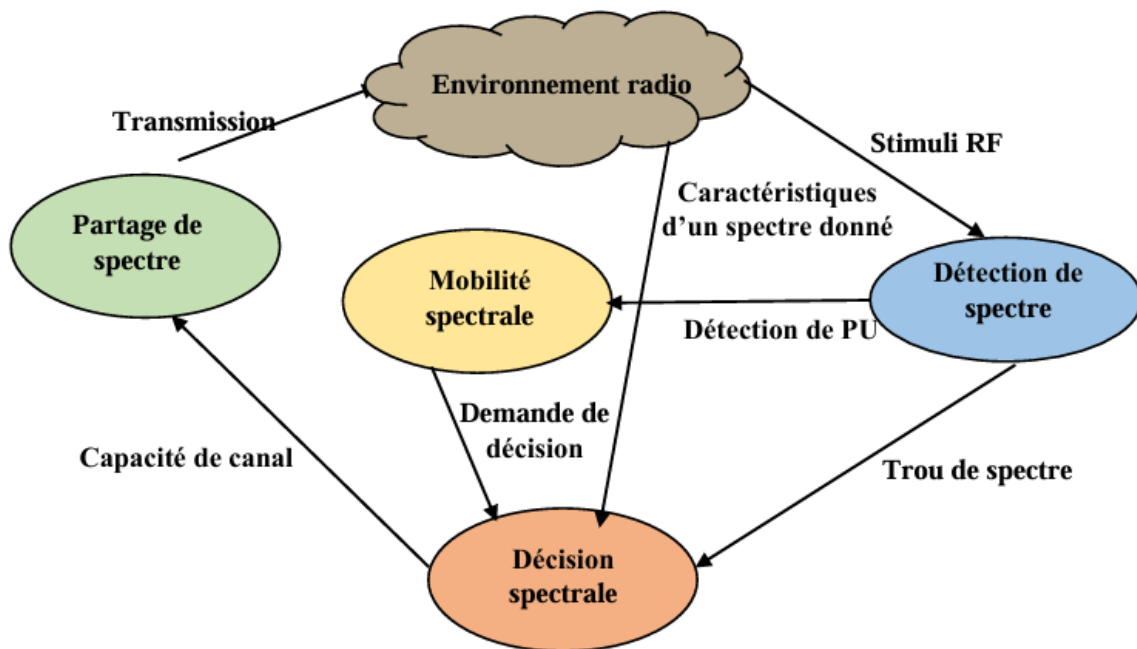


Figure II.6 : Les différentes tâches d'un système de radio cognitive [49]

La répartition de ces tâches et leur interconnexion, illustrées à la Figure II.6, peuvent être résumées comme suit :

V.1. Détection du spectre (Spectrum Sensing)

La détection du spectre est l'étape initiale et critique consistant à scruter l'environnement radio pour identifier les « espaces blancs » (spectrum holes), c'est-à-dire les canaux vacants pouvant être exploités. Son objectif principal est de déterminer avec une haute précision si les signaux d'un Utilisateur Primaire (PU) sont présents ou absents dans les bandes licenciées. Récemment, l'intégration de l'apprentissage automatique (Machine Learning) a transformé cette étape en un problème complexe de reconnaissance de formes. Cette évolution technologique facilite grandement l'identification des opportunités spectrales,

et ce, même en présence de dégradations physiques sévères du signal telles que les évanouissements par trajets multiples (multipath fading) [48].

V.2. Gestion et décision spectrale (Spectrum Management)

Une fois les opportunités spectrales identifiées, la fonction de gestion entre en jeu pour permettre à l'Utilisateur Secondaire (SU) de sélectionner la bande de fréquences la plus adaptée et de définir sa stratégie d'accès. Ce processus décisionnel repose sur l'évaluation simultanée de plusieurs critères fondamentaux : les exigences de Qualité de Service (QoS) spécifiques à l'application du SU, les caractéristiques physiques et intrinsèques du canal (comme le taux d'erreur ou le niveau prévisible d'interférence), ainsi que l'activité statistique observée sur le réseau primaire. Sur la base de cette analyse multivariée, le moteur cognitif reconfigure automatiquement les paramètres de transmission afin d'optimiser la liaison radioélectrique sur le nouveau canal [48].

V.3. Partage du spectre (Spectrum Sharing)

Puisque le spectre est une ressource partagée entre les PU et de multiples SU potentiels, une fonction de coordination est indispensable pour garantir un accès ordonné et prévenir les collisions. Principalement régie par les protocoles de la couche MAC (Medium Access Control), la fonction de partage du spectre orchestre l'accès aux ressources selon différents paradigmes. Sur le plan architectural, le partage peut être centralisé, situation dans laquelle un nœud maître alloue les ressources pour chaque SU, ou distribué, permettant aux utilisateurs d'accéder aux canaux indépendamment selon des politiques locales. De plus, le comportement des nœuds peut être coopératif, favorisant l'échange d'informations pour une optimisation globale du réseau, ou non-coopératif, où chaque nœud agit dans son propre intérêt, une dynamique souvent modélisée par la théorie des jeux [48].

V.4. Mobilité spectrale (Spectrum Handoff)

La mobilité spectrale, également appelée transfert spectral, désigne la capacité d'un SU à libérer un canal et à basculer vers une nouvelle fréquence de manière dynamique et autonome. Ce basculement est généralement imposé par la réapparition soudaine d'une activité primaire sur la bande occupée, imposant au SU de se retirer pour éviter toute interférence, ou par une dégradation inacceptable de la QoS sur la liaison en cours. L'enjeu critique de cette phase réside dans la minimisation stricte du délai de transition (handoff delay). Une gestion rigoureuse et anticipative est donc indispensable pour garantir un transfert fluide et transparent (seamless handover), évitant ainsi la rupture de la communication et la dégradation des performances de l'application en cours d'exécution [48].

VI. Allocation Dynamique du Spectre

L'Allocation Dynamique du Spectre (DSA) constitue l'une des applications majeures de la radio cognitive. Elle vise à exploiter les « espaces blancs » (white spaces) pour pallier l'inefficacité de l'allocation statique traditionnelle. Ce concept fondamental permet de faire évoluer un modèle de gestion rigide vers un écosystème flexible, capable de répondre à la demande exponentielle des services de communication sans fil modernes [50].

VI.1. Formulation du problème d'allocation

Le problème de l'allocation dynamique repose sur une hiérarchie stricte entre deux catégories d'utilisateurs : les Utilisateurs Primaires (PU), détenteurs de la licence et prioritaires absolus, et les Utilisateurs Secondaires (SU), qui accèdent à la ressource de manière purement opportuniste. La formulation mathématique et systémique de ce problème consiste à optimiser plusieurs objectifs simultanés, soumis à des contraintes strictes :

- **Maximisation de l'efficacité spectrale** : L'objectif est d'identifier et d'exploiter les bandes de fréquences laissées vacantes par les PU afin de maximiser le débit global et l'utilité du réseau cognitif.
- **Protection stricte des utilisateurs primaires** : La contrainte absolue du DSA est que le SU ne doit générer aucune interférence nuisible aux transmissions du PU. Dans le paradigme d'accès Underlay, cela se traduit par l'obligation de maintenir la puissance d'émission du SU sous un seuil d'interférence tolérable (température de bruit).
- **Garantie de la Qualité de Service (QoS)** : L'allocation doit satisfaire les exigences spécifiques des applications secondaires (débit minimal, contrainte de latence) tout en respectant l'accès inconditionnel du PU.
- **Gestion de l'efficacité énergétique** : L'optimisation doit impérativement intégrer la dimension énergétique. C'est un critère critique pour les réseaux de capteurs et l'Internet des Objets (IoT / IoMT), dont la durée de vie opérationnelle dépend intimement de la sobriété des protocoles d'accès au canal [50].

VI.2. Approches et stratégies d'optimisation

Plusieurs approches sont proposées dans la littérature pour résoudre ce problème complexe :

- **Approches basées sur l'apprentissage automatique** : Les techniques d'apprentissage automatique (Machine Learning et Deep Learning) permettent de prédire l'occupation du spectre et d'optimiser les décisions d'allocation. Elles

facilitent la construction de modèles spatio-temporels pour améliorer le choix des canaux et réduire les changements fréquents de fréquence (handover).

- **Paradigmes d'accès au spectre :** Les stratégies d'accès influencent directement l'optimisation :
 - **Interweave** : exploitation des canaux libres
 - **Underlay** : transmission à faible puissance sous contrainte d'interférence
 - **Overlay** : transmission assistée avec connaissance du PU
- **Optimisation pour l'IoT et l'IoMT :** Dans les réseaux massifs, l'allocation peut intégrer une priorisation des données. Les informations critiques (ex. données médicales) sont traitées en priorité afin de garantir la fiabilité des services.
- **Approches coopératives et compétitives :** Les interactions entre utilisateurs secondaires peuvent suivre une approche coopérative, visant un partage équitable et coordonné des ressources, ou une approche compétitive pour l'accès au spectre ; dans ce contexte, des modèles mathématiques tels que les Multi-Armed Bandits s'avèrent essentiels pour arbitrer ces dynamiques et optimiser les décisions d'accès en temps réel.
- **Optimisation multidimensionnelle :** Avec l'avènement des réseaux 5G et post-5G, l'optimisation du spectre s'étend à la dimension spatiale, grâce aux techniques de formation de faisceaux (beamforming), ainsi qu'à la dimension spectrale, via la détection à large bande (wideband sensing), permettant ainsi une utilisation plus fine et plus efficace des ressources radioélectriques.

Face à la complexité multidimensionnelle de ce problème d'optimisation, les méthodes de décision multicritère (MCDM, Multi-Criteria Decision Making) apparaissent comme une approche particulièrement adaptée, que nous détaillons dans la section suivante [50].

VI.3. Méthodes de décision multicritère (MCDM)

La prise de décision multicritère (MCDM), également appelée analyse décisionnelle multicritère (MCDA, Multi-Criteria Decision Analysis), désigne un ensemble de méthodes permettant de déterminer la meilleure alternative en tenant compte simultanément de plusieurs critères, souvent conflictuels.

Dans des environnements complexes tels que les réseaux de radio cognitive, ces approches permettent de structurer le problème décisionnel, d'établir un ordre de préférence

entre différentes alternatives et d'aboutir à une solution optimale en fonction des priorités du décideur.

VI.3.1. Méthodes de surclassement : ELECTRE et PROMETHEE

Les méthodes de surclassement reposent sur l'établissement de relations de préférence entre alternatives, en tenant compte de plusieurs critères.

- **ELECTRE (ELimination Et Choix Traduisant la REalité)** : Développée par Benayoun et al., cette méthode compare les alternatives deux à deux afin d'identifier celles qui dominent les autres selon des seuils de préférence et d'indifférence.
- **PROMETHEE (Preference Ranking Organization METHod for Enrichment Evaluation)** : Proposée par Brans, cette méthode constitue une extension d'ELECTRE, permettant un classement plus fin des alternatives grâce à une évaluation progressive des préférences.

VI.3.2. Méthode AHP (Analytic Hierarchy Process)

Développée par Saaty, la méthode AHP repose sur une structuration hiérarchique du problème et sur des comparaisons par paires entre critères et alternatives. Elle est largement utilisée en raison de sa simplicité et de sa facilité d'interprétation. Cependant, elle présente certaines limites, notamment lorsque les critères sont interdépendants, ce qui peut affecter la cohérence des résultats. Malgré cela, l'AHP reste particulièrement efficace pour la pondération et la hiérarchisation des critères dans les problèmes de décision multicritère.

VI.3.3. Méthode TOPSIS

La méthode TOPSIS proposée par Hwang et Yoon, est une technique de décision multicritère largement utilisée. Elle repose sur le principe selon lequel la meilleure alternative est celle qui est la plus proche d'une solution idéale et la plus éloignée d'une solution anti-idéale [51]. En raison de sa simplicité et de son efficacité, cette méthode est particulièrement adaptée aux problèmes d'allocation de ressources dans des environnements complexes comme les réseaux radio cognitifs. Toutefois, afin d'améliorer l'évaluation des critères de décision, TOPSIS peut être couplée à la méthode AHP. Dans cette approche hybride, l'AHP permet de déterminer les poids des critères, tandis que TOPSIS assure le classement des alternatives et la sélection de la solution la plus appropriée. Cette méthode sera étudiée plus en détail dans le chapitre suivant, car elle est particulièrement adaptée à notre approche d'allocation dynamique du spectre.

VII. Sécurité de la Radio Cognitive

La sécurité des Réseaux de Radio Cognitive (RRC) constitue un enjeu majeur en raison de leur nature dynamique, flexible et fortement exposée aux menaces, contrairement aux réseaux traditionnels. Les vulnérabilités spécifiques des RRC, combinées à l'accès dynamique au spectre, exigent la mise en place de mécanismes de protection multicouches afin de garantir la confidentialité, l'intégrité et la disponibilité des communications [52].

VII.1. Menaces et vulnérabilités

Les réseaux de radio cognitive (RRC) se caractérisent par une grande flexibilité, mais également par une exposition accrue aux menaces par rapport aux réseaux traditionnels. Cette vulnérabilité est principalement liée à leurs mécanismes dynamiques, notamment la détection spectrale (spectrum sensing), où une altération malveillante des résultats peut perturber, voire paralyser le trafic.

Le problème du terminal caché constitue également un risque important, pouvant conduire un utilisateur secondaire (SU) à provoquer des interférences involontaires avec un utilisateur primaire (PU). Par ailleurs, les systèmes de RC sont exposés à plusieurs types d'attaques, notamment l'injection de fausses politiques de décision et la manipulation des données d'apprentissage, susceptibles de fausser le comportement du système

Les motivations des attaquants se divisent généralement en deux catégories : les attaques égoïstes, visant à obtenir un accès prioritaire au spectre, et les attaques malveillantes, destinées à perturber le réseau, notamment par des attaques de type déni de service (DoS, Denial-of-Service) [52].

VII.2. Attaques au niveau de la couche physique

La couche physique constitue une cible privilégiée, car elle influence directement la perception de l'environnement radio :

- **Primary User Emulation (PUE)** : L'attaquant imite les caractéristiques d'un utilisateur primaire afin de tromper les utilisateurs secondaires et les contraindre à libérer une bande de fréquences.
- **Brouillage (Jamming)** : Cette attaque consiste à émettre intentionnellement des signaux parasites afin de perturber ou bloquer les communications légitimes.

- **Objective Function Attack (OFA)** : L'attaquant manipule les paramètres d'entrée du moteur cognitif (puissance, débit, sécurité) afin de contraindre le système à adopter des configurations sous-optimales ou moins sécurisées [53].

VII.3. Attaques au niveau de la couche liaison

Au niveau de la couche liaison (MAC), les attaques ciblent les mécanismes de coordination et de partage des ressources :

- **Spectrum Sensing Data Falsification (SSDF)** : Dans ce type d'attaque, également appelée attaque byzantine, des nœuds malveillants transmettent de fausses informations de détection au centre de fusion, compromettant la décision collective.
- **Control Channel Saturation DoS (CCSD)** : L'attaquant sature le canal de contrôle commun en injectant de fausses trames, provoquant un blocage des échanges de coordination entre les nœuds.
- **Selfish Channel Negotiation (SCN)** : Un nœud adopte un comportement strictement égoïste en refusant de relayer les messages des autres ou en dissimulant la disponibilité d'un canal, afin de préserver son propre débit au détriment de l'équité du réseau [53].

VII.4. Attaques au niveau de la couche réseau

Les attaques au niveau réseau exploitent principalement les protocoles de routage dans des architectures multi-sauts :

- **Sinkhole** : Un nœud malveillant attire le trafic en annonçant des routes avantageuses, afin de pouvoir intercepter, modifier ou supprimer les paquets.
- **Hello Flood** : L'attaquant envoie des messages avec une puissance élevée pour se faire passer pour un voisin direct, perturbant ainsi la construction de la topologie du réseau [54].

VII.5. Mécanismes de protection

La sécurisation des réseaux de radio cognitive repose sur une approche multicouche visant à protéger la confidentialité, l'intégrité et la disponibilité des communications. En raison de leur nature dynamique et adaptative, ces réseaux nécessitent des mécanismes de protection capables de s'adapter aux variations de l'environnement radio et aux comportements des utilisateurs [52] [53].

À la couche physique, plusieurs techniques permettent de contrer les attaques telles que le brouillage et l'interception. Les méthodes d'étalement de spectre, comme le saut de fréquence (FHSS, Frequency Hopping Spread Spectrum) ou l'étalement direct (DSSS, Direct Sequence Spread Spectrum), améliorent la robustesse face aux interférences intentionnelles. De plus, des approches issues de la sécurité physique, telles que le beamforming ou l'ajout de bruit artificiel, permettent de limiter l'accès aux communications par des attaquants [55].

Au niveau des couches supérieures, la sécurisation repose sur des mécanismes de cryptographie et d'authentification. Dans les environnements contraints, des algorithmes de cryptographie légère sont privilégiés afin de réduire la consommation énergétique tout en assurant un niveau de sécurité suffisant [48]. Par ailleurs, l'authentification basée sur les caractéristiques physiques du signal, telle que l'empreinte radio (RF Fingerprinting), permet de distinguer les équipements légitimes des nœuds malveillants [55].

En complément, des systèmes de détection d'intrusion (IDS, Intrusion Detection System) et des mécanismes de réputation peuvent être utilisés pour identifier et isoler les comportements anormaux, notamment dans les scénarios de détection collaborative du spectre. Ces approches renforcent la fiabilité des décisions prises par les utilisateurs secondaires [52].

Enfin, les approches récentes intègrent des techniques d'intelligence artificielle et, dans certains cas, des solutions basées sur la blockchain pour améliorer la détection des attaques et assurer une gestion sécurisée et transparente du spectre [56].

Ces mécanismes de protection sont particulièrement critiques dans les applications sensibles, telles que l'IoMT, où toute défaillance de sécurité peut avoir des conséquences directes sur la santé des patients.

VIII. Systèmes Multi-Agents (SMA) : Concepts et Architectures

Les Systèmes Multi-Agents (SMA) se sont imposés comme un paradigme de calcul puissant pour résoudre des problèmes complexes en les décomposant en tâches granulaires, allouées à des entités autonomes [57].

VIII.1. Concepts fondamentaux des SMA

Un agent est défini comme une entité informatique (exclusivement logicielle, ou couplée à du matériel) située dans un environnement donné, et capable d'actions autonomes pour atteindre ses objectifs de conception. Contrairement aux systèmes experts traditionnels,

un agent agit directement sur son environnement après avoir pris une décision basée sur ses buts, son historique et les paramètres captés.

Les propriétés fondamentales d'un agent incluent :

- **L'autonomie** : Capacité à exécuter indépendamment son processus décisionnel et à agir sans intervention humaine directe.
- **La sociabilité** : Capacité à interagir et coopérer avec d'autres agents (artificiels ou humains) pour partager des connaissances, négocier ou demander des informations.
- **La réactivité** : Capacité à percevoir son environnement en temps réel et à répondre dynamiquement aux changements qui s'y produisent.
- **La proactivité** : Capacité à prendre l'initiative et à anticiper les actions futures pour atteindre ses objectifs de manière proactive.

Un SMA est donc un système composé de deux agents ou plus qui collaborent pour résoudre des tâches que des individus isolés ne pourraient accomplir efficacement. Cette approche distribuée offre une flexibilité majeure, une fiabilité accrue (en cas de défaillance d'un agent, la tâche peut être réassignée dynamiquement) et une optimisation par la division du travail. L'environnement dans lequel évoluent ces agents est qualifié selon plusieurs critères mathématiques et physiques : son accessibilité (précision des capteurs), son déterminisme (prévisibilité des actions), son dynamisme (évolution indépendante des agents) et sa continuité (espace d'états discret ou continu) [57].

VIII.2. Architectures multi-agents

Les architectures de SMA peuvent être classées en modèles abstraits (définissant la structure logique globale) et en modèles concrets (implémentant les composants logiciels spécifiques) [58].

VIII.2.1. Types d'agents selon leur architecture interne

- **Agents purement réactifs** : Ils prennent des décisions basées uniquement sur l'état présent de l'environnement, sans conserver d'historique, via une correspondance directe de type « situation-action ».
- **Agents basés sur la logique** : Ils s'appuient sur des moteurs d'inférence et la déduction logique formelle pour prendre des décisions.
- **Agents BDI (Belief-Desire-Intention)** : Ils reposent sur des représentations symboliques de l'intelligence artificielle regroupant les croyances (connaissances sur

le monde), les désirs (objectifs à atteindre) et les intentions (plans d'action engagés par l'agent).

- **Architectures en couches** : Elles organisent les agents en plusieurs strates logicielles, chacune traitant un niveau d'abstraction différent de l'environnement [58].

VIII.2.2. Structures d'organisation des agents

Pour coordonner leurs activités, les agents s'organisent selon diverses topologies :

- **Plate (Flat)** : Tous les agents sont sur un pied d'égalité et communiquent directement avec leurs voisins.
- **Hiérarchique** : Structure en arbre où des agents « maîtres » (parents) supervisent et contrôlent des agents « subordonnés » (enfants).
- **Holonique** : Les agents sont regroupés en « holons » (super-agents ou entités récursives) qui peuvent eux-mêmes être composés d'une multitude de sous-agents.
- **Coalition** : Groupement temporaire et opportuniste d'agents réunis autour d'un but commun afin de réduire les coûts opérationnels.
- **Équipe (Team)** : Collaboration pérenne pour atteindre un objectif d'équipe strictement distinct des objectifs individuels de chaque agent.
- **Congrégation** : Regroupement topologique ou logique d'agents réunis pour satisfaire un besoin spécifique qu'ils ne pourraient résoudre seuls [57].

VIII.2.3. Mécanismes de communication

La communication constitue un élément fondamental des systèmes multi-agents, permettant d'assurer la coordination et l'atteinte d'un consensus au sein du réseau. Elle peut s'effectuer par échange de messages, soit de manière directe (peer-to-peer), soit par diffusion. Une autre approche repose sur l'architecture de type Blackboard, qui correspond à un espace de mémoire partagé où les agents peuvent déposer et consulter des informations de manière asynchrone. La Figure II.7 illustre conceptuellement la différence de flux de données entre ces deux paradigmes de communication.

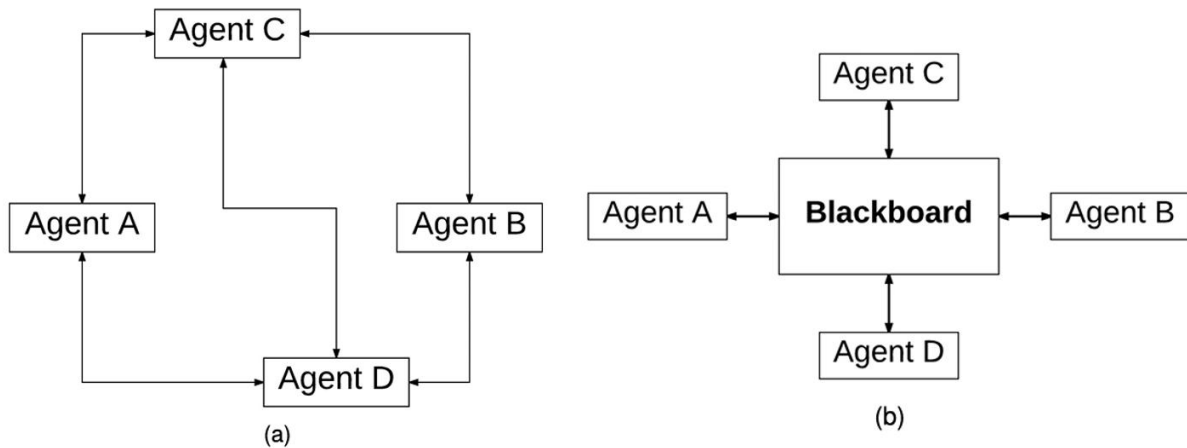


Figure II.7 : Approches de communication dans les SMA : a) échange de messages, b) Blackboard [57]

Dans les systèmes de grande envergure, la communication peut être facilitée par l'introduction d'agents intermédiaires. Les facilitateurs assurent des fonctions de routage et de mise en relation entre agents, tandis que les médiateurs permettent d'établir une communication directe avant de se retirer du processus [57].

VIII.3. Plateformes de développement des Systèmes Multi-Agents

Le développement de systèmes multi-agents (SMA) s'appuie sur une large gamme de plateformes logicielles dédiées. La majorité de ces plateformes est basée sur le langage Java, afin d'assurer une compatibilité multiplateforme sur différents systèmes d'exploitation. Ces environnements se distinguent principalement par leurs modèles conceptuels, leurs outils de développement intégrés ainsi que leur approche organisationnelle et structurelle. Parmi les principales plateformes, on peut citer :

- **MadKIT (Multi-Agent Development Kit) :** Plateforme modulaire et évolutive, elle s'appuie sur le modèle organisationnel AGR (Agent / Groupe / Rôle). Contrairement aux approches classiques centrées sur l'individu, MadKIT privilégie une approche OCMAS (Organization-Centered Multi-Agent System). Ses fonctionnalités incluent la gestion du cycle de vie des agents et la création d'infrastructures pour structurer les groupes de communication.
- **JACK (Java Agent Construction Kit) :** Cet environnement commercial multiplateforme est spécifiquement conçu pour le développement de systèmes multi-agents complexes basés sur le modèle logique BDI (Belief-Desire-Intention). Dans

cette approche, les agents prennent des décisions en fonction de leurs croyances, de leurs désirs et de leurs intentions afin d'atteindre leurs objectifs. JACK se distingue par son efficacité et sa robustesse, permettant l'exécution de centaines d'agents même sur des plateformes aux ressources limitées.

- **Agent Builder** : Suite d'outils intégrée (payante) pour la création d'agents logiciels intelligents. Elle se compose de deux éléments majeurs : une boîte à outils pour la conception et un environnement de compilation pour le débogage. Elle inclut des outils spécifiques avancés, comme l'Ontology Manager pour l'analyse sémantique du domaine et l'Agent Debugger, simplifiant ainsi la création de SMA robustes.
- **Cougaar (Cognitive Agent Architecture)** : Architecture orientée vers les systèmes distribués à très grande échelle, utilisant des topologies peer-to-peer et un système de tableau noir (Blackboard) pour la communication interne.
- **MASON (Multi-Agent Simulator Of Neighborhoods)** : Plateforme de haute performance, spécialisée dans la simulation intensive de processus complexes avec des capacités de visualisation 2D et 3D.
- **JADE (Java Agent Development Framework)** Parmi toutes les solutions existantes, JADE s'impose comme la plateforme la plus répandue et la plus ouverte pour le développement de SMA. Strictement conforme aux standards FIPA (Foundation for Intelligent Physical Agents), son architecture repose sur trois modules fondamentaux :
 - **AMS (Agent Management System)** : Il contrôle l'enregistrement, l'authentification et le cycle de vie complet des agents.
 - **DF (Directory Facilitator)** : Il fournit un service d'annuaire (système de « pages jaunes ») où les agents enregistrent et découvrent des services.
 - **ACC (Agent Communication Channel)** : Il gère le routage et la communication entre les agents. Les agents JADE communiquent via le langage standardisé ACL (Agent Communication Language) en s'appuyant sur un paradigme de messagerie asynchrone [59].

En raison de sa robustesse et de sa conformité aux standards, JADE a été sélectionnée comme plateforme d'implémentation pour ce projet. Son architecture détaillée et son utilisation seront abordées en profondeur dans le Chapitre III.

VIII.4. Intégration des SMA dans la RC

L'intégration des SMA dans la Radio RC représente une avancée significative pour l'optimisation de l'utilisation du spectre et l'amélioration de la fiabilité des réseaux sans fil.

Cette approche permet de distribuer l'intelligence au sein du réseau en déléguant la prise de décision à des entités autonomes capables d'interagir avec leur environnement [60].

VIII.4.1. Coordination et coopération entre utilisateurs

Dans un environnement de RC, chaque terminal peut être équipé d'un agent intelligent chargé de collecter des informations sur l'environnement radiofréquence. Ces données peuvent être partagées via une base de connaissances commune, facilitant ainsi la coordination entre les agents. Les SMA adoptent généralement une approche coopérative, où les agents échangent leurs informations afin de maximiser l'efficacité globale du spectre tout en évitant les interférences.

Les agents sont déployés aussi bien au niveau des Utilisateurs Primaires (PU) que des Utilisateurs Secondaires (SU), permettant plusieurs formes d'interaction :

- **Négociation** : Les agents SU peuvent dialoguer avec les agents PU pour établir des accords dynamiques d'accès au spectre.
- **Modèles économiques** : L'accès au spectre peut être conditionné par des mécanismes de paiement (Spectrum Trading) ou de compensation.
- **Agents intermédiaires (brokers)** : Des agents spécialisés peuvent gérer la négociation au nom des nœuds, simplifiant ainsi les exigences en calcul et en intelligence des terminaux limités en ressources (comme les capteurs IoT) [60].

VIII.4.2. Gestion des ressources et de la mobilité

Les SMA offrent une solution efficace pour la gestion distribuée des ressources radio, notamment dans les environnements décentralisés. Ils jouent un rôle clé dans la gestion du handover, en assurant la continuité du service lors du déplacement physique des utilisateurs. Grâce à des capacités de raisonnement et de prédiction, les agents peuvent anticiper les changements d'environnement et adapter dynamiquement les paramètres de communication [60].

VIII.4.3. Apprentissage et optimisation

L'intégration de techniques d'IA renforce les capacités cognitives des agents :

- **Apprentissage par renforcement (RL, Reinforcement Learning)** : Utilisé en mode mono-agent ou multi-agents pour optimiser mathématiquement l'allocation du spectre.
- **Q-learning** : Cet algorithme permet aux agents secondaires d'apprendre par essais et erreurs à sélectionner des canaux de manière à éviter naturellement les collisions.

- **Mécanismes coopératifs** : Des approches telles que la propagation de gain local (LCPP, Local Convergence and Performance Propagation) améliorent la coordination et assurent la convergence des décisions locales vers des solutions globalement optimales pour le réseau [60].

VIII.4.4. Qualité de Service (QoS) pour les applications sensibles

Les SMA contribuent également au maintien des exigences de QoS, un enjeu crucial pour des applications critiques comme la vidéoconférence médicale ou les services IoMT. Les agents veillent à garantir des paramètres stricts tels qu'un débit suffisant, une latence réduite et une faible gigue. En anticipant les variations de l'environnement réseau, ils permettent d'activer dynamiquement les mécanismes de basculement de la radio cognitive afin d'assurer une continuité de service transparente et sans coupure [60].

IX. Domaines d'application de la Radio Cognitive

La RC transforme la gestion du spectre d'une approche statique en un modèle dynamique, permettant de répondre aux besoins croissants en bande passante de diverses infrastructures critiques [61].

IX.1. Réseaux militaires et de sécurité publique

Le domaine militaire est l'un des secteurs les plus significatifs pour l'usage de la RC, où elle est déployée via des technologies comme le Joint Tactical Radio System (JTRS) et le projet SPEAKEasy. Ces systèmes utilisent l'intelligence de la RC pour basculer dynamiquement entre les fréquences afin de contrer le brouillage intentionnel (anti-jamming) et assurer des communications robustes sur le champ de bataille. Pour la sécurité publique, elle permet une interopérabilité vitale entre différents systèmes de communication d'urgence dont les bandes de fréquences ou les formats ne sont initialement pas compatibles [52].

IX.2. Réseaux de secours et d'urgence

En situation de catastrophe naturelle, la RC peut modifier ses paramètres opérationnels en temps réel pour fournir des connexions ad hoc immédiates lorsque les infrastructures traditionnelles sont défaillantes. Elle joue un rôle crucial dans les opérations de recherche et sauvetage, où les capacités GPS couplées à la détection de trous spectraux permettent de créer des balises de détresse sur des canaux libres pour localiser les survivants. Elle aide également à établir des communications claires dans des environnements hostiles, comme lors d'accidents miniers, en adaptant dynamiquement les formes d'onde aux contraintes physiques du milieu [52].

IX.3. Réseaux cellulaires (5G) et villes intelligentes (Smart Cities)

L'intégration de la RC dans la 5G est essentielle pour soutenir les piliers URLLC et mMTC. Dans les Smart Cities [56], la RC optimise la gestion du trafic urbain grâce aux communications V2X (Vehicle-to-Everything), permettant aux capteurs de transmettre des données en temps réel sur la congestion ou les accidents sans saturer le réseau. Elle constitue également un pilier des Smart Grids (réseaux électriques intelligents), facilitant un flux bidirectionnel d'informations entre les compteurs et les centres de contrôle via un accès opportuniste au spectre inutilisé [61] [62].

IX.4. Réseaux IoMT

L'intégration de la radio cognitive dans le domaine de la santé, à travers l'IoMT, permet d'améliorer la fiabilité et l'efficacité des communications entre dispositifs médicaux. Grâce à sa capacité d'adaptation dynamique, la RC optimise l'utilisation du spectre tout en garantissant une transmission fiable des données critiques.

Dans les applications de surveillance à distance et de télémédecine, les capteurs médicaux intelligents peuvent transmettre en temps réel des paramètres vitaux tels que le rythme cardiaque, la pression artérielle ou le niveau d'oxygène. Cette surveillance continue permet une détection précoce des anomalies et améliore la qualité des soins, notamment dans les zones isolées [61].

Au sein des environnements hospitaliers, la RC contribue à renforcer la sécurité et la gestion des patients. Elle permet, par exemple, le suivi en temps réel des équipements et des patients, ainsi que la détection rapide de situations anormales grâce à des systèmes intelligents et autonomes [52].

Par ailleurs, l'utilisation de l'Accès Dynamique au Spectre (DSA) permet de prioriser les données médicales critiques, garantissant une faible latence et une qualité de service adaptée aux applications sensibles [62]. Enfin, la radio cognitive améliore la sécurité des communications en offrant une meilleure résistance aux interférences et aux attaques, tout en contribuant à la protection des données médicales [61].

X. Conclusion

Ce chapitre a permis d'établir un état de l'art approfondi des technologies fondamentales sous-jacentes à la gestion intelligente des réseaux sans fil modernes. Face au paradoxe de la rareté spectrale et à l'explosion du nombre d'appareils connectés, la Radio

Cognitive (RC), issue de l'évolution de la Radio Logicielle Restreinte (SDR), s'impose comme une solution particulièrement prometteuse. En conférant aux équipements la capacité d'observer, d'apprendre et d'adapter dynamiquement leurs paramètres de transmission, la RC permet d'optimiser l'allocation spectrale de manière opportuniste et adaptative.

Toutefois, le déploiement de ces réseaux cognitifs soulève des défis critiques, notamment en matière de sécurité, la flexibilité du spectre ouvrant la voie à de nouvelles vulnérabilités (brouillage, falsification de données). Pour pallier ces failles et gérer la complexité algorithmique de l'allocation des ressources, l'intégration des Systèmes Multi-Agents (SMA) s'avère être une approche particulièrement puissante. En distribuant l'intelligence au sein d'entités autonomes capables de coopérer, de négocier et d'apprendre de leur environnement, il devient possible de garantir une Qualité de Service (QoS) résiliente et optimale.

Ces exigences de fiabilité, de sécurité et de faible latence trouvent leur application la plus critique dans l'Internet des Objets Médicaux (IoMT), où la continuité des transmissions constitue une nécessité vitale. Les mécanismes d'allocation dynamique du spectre étudiés dans ce chapitre, combinés aux approches multicritères telles que TOPSIS, constituent ainsi le socle théorique sur lequel repose la solution proposée dans ce travail.

Le chapitre suivant sera consacré à la conception et à l'implémentation de notre architecture cognitive multi-agents et à multicritères sécurisé dédiée à l'IoMT, en nous appuyant sur la plateforme de développement JADE.

Chapitre III

Conception d'un Système d'Allocation Dynamique à Multicritère Sécurisé en IoMT dans les Réseaux Radio Cognitifs 5G

Table des matières

I. Introduction.....	65
II. Environnement et Outils de Développement.....	65
II.1. Choix du Langage Java.....	66
II.2. Plateforme de Développement NetBeans	66
III. La Plateforme JADE : Concepts et Architecture de Base	66
III.1. Philosophie FIPA et Architecture Distribuée : Services de Base (AMS et DF)	67
III.2. Modèle de Communication (ACL).....	68
IV. Conception de l'Architecture Multi-Agents de notre approche	69
IV.1. Architecture Globale du Système	71
IV.2. L'Agent Portail.....	71
IV.3. L'Agent PU	72
IV.4. L'Agent SU	73
IV.5. L'Agent SU_RECEIVER.....	74
IV.6. Protocole de Négociation.....	74
V. Modélisation Contextuelle IoMT.....	76
V.1. Taxonomie des Dispositifs Médicaux et Paramètres QoS	76
V.2. Affectation Dynamique des Poids TOPSIS par la Méthode AHP.....	77
V.2.1. Principe de la Méthode AHP.....	77
V.2.2. Construction des Matrices de Comparaison par Paires.....	77
V.2.3. Calcul des Poids et Vérification de Cohérence	79
V.2.4. Poids Obtenus et Validation de Cohérence	81
VI. Algorithme TOPSIS	81
VI.1. Construction de la Matrice de Décision	81
VI.2 Normalisation et Pondération.....	82
VI.3. Calcul des Solutions Idéales	82
VI.4. Classement des PU Candidats.....	83
VII. Sécurisation des Communications	84
VII.1. Architecture de Sécurité du Système	84
VII.2. Chiffrement des Données Médicales (AES).....	84
VII.3. Mode Hybride ECC+AES	85
VII.4. Mode Hybride RSA+AES	85
VII.5. Comparaison de notre contribution avec l'ECC vs RSA.....	86
VIII. Résultats et Évaluation des Performances	88
VIII.1. Environnement Expérimental.....	88
VIII.2. Mesures et métriques de latence.....	89
VIII.2.1. Métriques de base	89

VIII.2.2. Mesure de latence bout-en-bout	89
VIII.3. Impact de la Taille du Fichier	91
VIII.4. Résultats de Latence Bout-en-Bout	93
VIII.5. Comparaison avec des Travaux Précédents.....	96
VIII.6. Scalabilité du Système.....	97
IX. Conclusion	99

I. Introduction

Avec l'essor rapide des technologies de santé connectée et de l'IoMT, les systèmes médicaux intelligents occupent aujourd'hui une place essentielle dans l'amélioration de la qualité des soins, la surveillance à distance des patients et la réactivité des services de santé. Cependant, l'augmentation continue du nombre d'équipements connectés engendre une pression croissante sur les ressources radio disponibles, rendant indispensable le développement de solutions capables d'assurer une gestion efficace, fiable et sécurisée du spectre. Dans ce contexte, l'intégration de la radio cognitive et des systèmes multi-agents constitue une approche prometteuse pour répondre aux exigences de performance et de qualité de service des applications médicales critiques.

Ce dernier chapitre est consacré à la conception et à la mise en œuvre d'un système multi-agents sécurisé dédié à l'allocation dynamique du spectre dans un environnement IoMT reposant sur les principes de la radio cognitive. L'approche proposée s'appuie sur la combinaison des méthodes d'aide à la décision multicritères AHP et TOPSIS afin d'améliorer le processus de sélection des ressources radio en tenant compte simultanément de plusieurs paramètres de qualité de service, notamment la latence, la fiabilité, la disponibilité du canal et la bande passante.

Dans un premier temps, nous présentons l'environnement de développement ainsi que les outils logiciels mobilisés pour la réalisation du système. Nous décrivons ensuite l'architecture multi-agents développée sous la plateforme JADE, en mettant en évidence les rôles des différents agents et les mécanismes d'interaction mis en place. Par la suite, nous détaillons la démarche de prise de décision fondée sur l'approche hybride AHP-TOPSIS ainsi que les mécanismes de sécurité intégrés pour garantir la protection des échanges et des ressources du réseau. Enfin, des scénarios de simulation sont présentés afin d'analyser et d'évaluer les performances de la solution proposée dans différentes conditions d'exploitation.

II. Environnement et Outils de Développement

La mise en œuvre du système proposé nécessite un environnement de développement adapté aux exigences des systèmes multi-agents et aux contraintes de la plateforme JADE. Les outils retenus ont été sélectionnés pour leur maturité technologique, leur compatibilité avec JADE et leur large adoption dans la communauté scientifique.

II.1. Choix du Langage Java

Le langage Java constitue le choix naturel et incontournable pour le développement de systèmes multi-agents basés sur JADE, ce dernier étant entièrement implémenté en Java. L'adoption de Java comme langage de développement principal repose sur plusieurs critères techniques déterminants :

- **Compatibilité totale avec JADE** : JADE est développé et optimisé pour Java, garantissant une intégration native et sans friction
- **Portabilité** : Le principe "Write Once, Run Anywhere" de Java permet le déploiement du système sur différentes plateformes (Windows, Linux, macOS) sans modification du code
- **Orienté Objet** : Le paradigme orienté objet de Java s'aligne parfaitement avec la modélisation des agents comme entités autonomes encapsulant leurs comportements
- **Bibliothèques cryptographiques** : Java dispose de bibliothèques natives robustes (javax.crypto, java.security) pour l'implémentation des algorithmes de sécurité AES, RSA et ECC utilisés dans ce travail [63].

II.2. Plateforme de Développement NetBeans

NetBeans IDE a été retenu comme environnement de développement intégré pour ce projet. C'est un IDE open-source développé par Apache, offrant un support natif et complet pour le langage Java. Les principales raisons de ce choix sont :

- **Support Java natif** : NetBeans offre une intégration complète avec le JDK, incluant la complétion automatique du code, le débogage et la gestion des dépendances.
- **Gestion de projet** : NetBeans facilite l'organisation du projet en packages et modules, adaptée à l'architecture multi-agents proposée.
- **Débogage avancé** : Les outils de débogage intégrés permettent de suivre le comportement des agents JADE en temps réel, facilitant la détection et la correction des erreurs
- **Gratuité et open-source** : NetBeans est entièrement gratuit, ce qui facilite sa reproduction et sa validation par la communauté scientifique [64].

III. La Plateforme JADE : Concepts et Architecture de Base

JADE (Java Agent Development Framework) est une plateforme middleware open-source entièrement développée en Java, conçue pour simplifier le développement de systèmes multi-agents conformes aux standards FIPA (Foundation for Intelligent Physical Agents). Elle constitue la plateforme de référence dans la communauté des systèmes multi-agents, grâce à sa

robustesse, sa conformité aux standards internationaux et sa large adoption dans les travaux de recherche académique et industrielle [65].

III.1. Philosophie FIPA et Architecture Distribuée : Services de Base (AMS et DF)

La philosophie de JADE repose sur la conformité aux spécifications FIPA, un ensemble de standards internationaux définissant les protocoles et les architectures pour les systèmes multi-agents interopérables. Cette conformité garantit que les agents développés sous JADE peuvent interagir avec des agents d'autres plateformes compatibles FIPA.

L'architecture de JADE est organisée autour de deux services de base fondamentaux :

AMS (Agent Management System) : L'AMS est le composant central de gestion de la plateforme JADE. Il joue le rôle d'autorité de contrôle unique sur la plateforme et assure les fonctions suivantes :

- **Enregistrement des agents :** Tout agent créé sur la plateforme doit obligatoirement s'enregistrer auprès de l'AMS pour obtenir une identité unique (AID, Agent Identifier).
- **Authentification :** L'AMS vérifie l'identité des agents lors de leur enregistrement.
- **Gestion du cycle de vie :** L'AMS supervise les états des agents (actif, suspendu, en attente, supprimé) et contrôle les transitions entre ces états.
- **Point d'entrée unique :** L'AMS constitue le point de contact obligatoire pour toute communication inter-plateformes.

DF (Directory Facilitator) : Le DF fournit un service d'annuaire de type "pages jaunes" permettant aux agents de publier et de découvrir des services :

- **Publication de services :** Les agents enregistrent leurs capacités et services auprès du DF.
- **Découverte de services :** Les agents peuvent interroger le DF pour trouver d'autres agents offrant des services spécifiques.
- **Fédération :** Plusieurs DF peuvent être fédérés pour former un annuaire distribué à grande échelle.

La structure globale et l'interaction entre ces composants logiciels sont illustrées par la Figure III.1 ci-dessous :

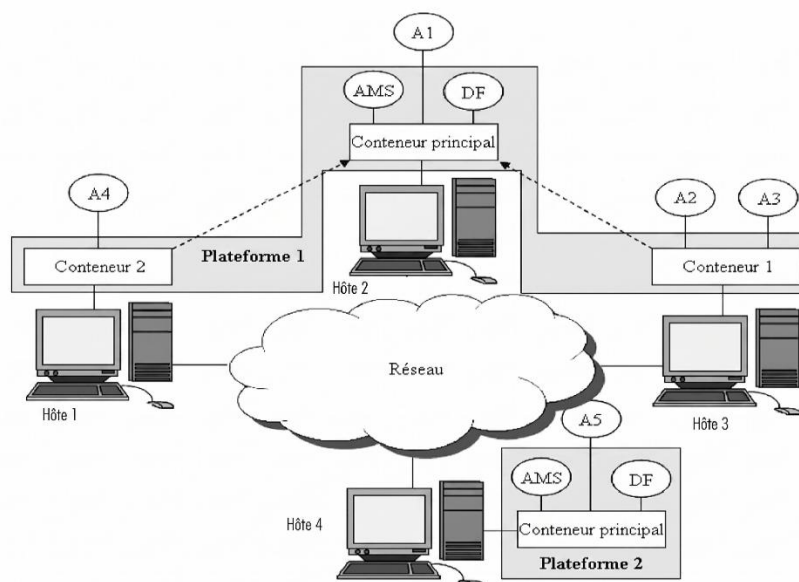


Figure III.1 : Architecture logicielle de la plateforme JADE [65]

L'architecture distribuée de JADE permet le déploiement de la plateforme sur plusieurs machines physiques interconnectées, chaque machine hébergeant un ou plusieurs conteneurs (containers) d'agents. Un conteneur principal (Main Container) héberge obligatoirement l'AMS et le DF [65], comme le montre la vue d'ensemble de la plateforme présentée en Figure III.2, tandis que des conteneurs secondaires peuvent être déployés pour distribuer la charge.

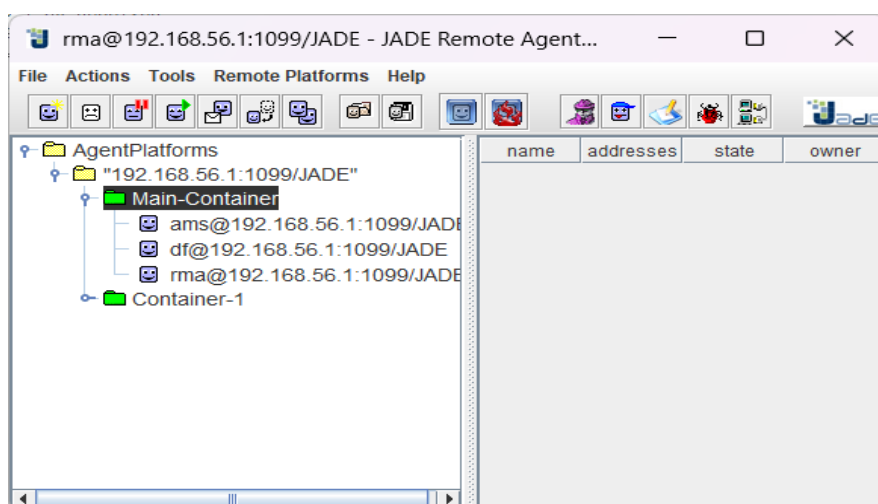


Figure III.2 : Interface de gestion JADE et structure du Main Container.

III.2. Modèle de Communication (ACL)

La communication entre agents dans JADE repose sur le langage ACL (Agent Communication Language), défini par la FIPA. L'ACL est un langage de communication standardisé permettant aux agents d'échanger des messages structurés et sémantiquement riches. Un message ACL est composé de plusieurs champs essentiels :

Champ	Description
Performative	Type d'acte de langage (REQUEST, INFORM, PROPOSE, ACCEPT, REJECT...)
Sender	Identifiant de l'agent émetteur
Receiver	Identifiant de l'agent destinataire
Content	Contenu du message (données, requêtes, propositions)
Language	Langage utilisé pour exprimer le contenu
Ontology	Ontologie définissant la sémantique du contenu

Tableau III.1 : Paramètres fondamentaux d'un message de communication ACL [66]

Pour illustrer concrètement la structure de ces échanges, la Figure III.3 présente une capture d'écran de l'inspecteur de messages de la plateforme JADE. Cette vue permet de visualiser comment les paramètres théoriques détaillés dans le Tableau III.1 sont encapsulés et transmis en temps réel entre les agents.

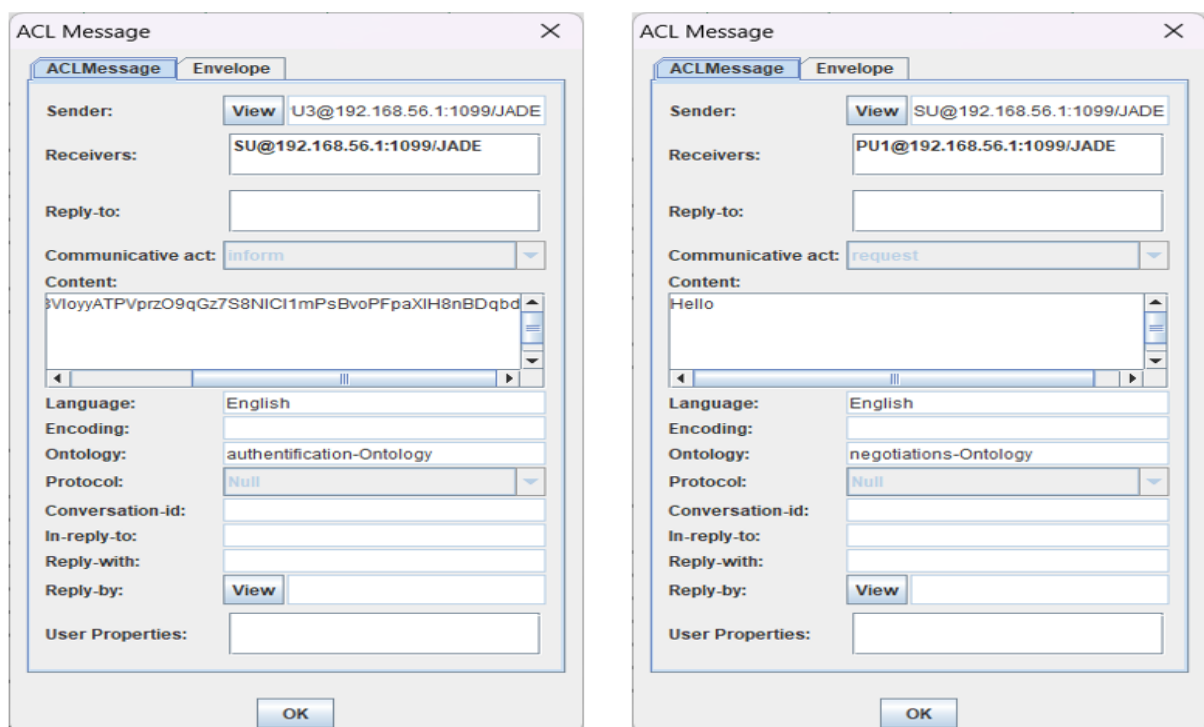


Figure III.3 : Inspection des messages ACL via l'interface graphique de JADE

IV. Conception de l'Architecture Multi-Agents de notre approche

La figure III.4 présente l'organigramme général du système proposé, illustrant le déroulement complet du processus d'allocation dynamique du spectre depuis la configuration du dispositif IoMT jusqu'au transfert sécurisé des données médicales.

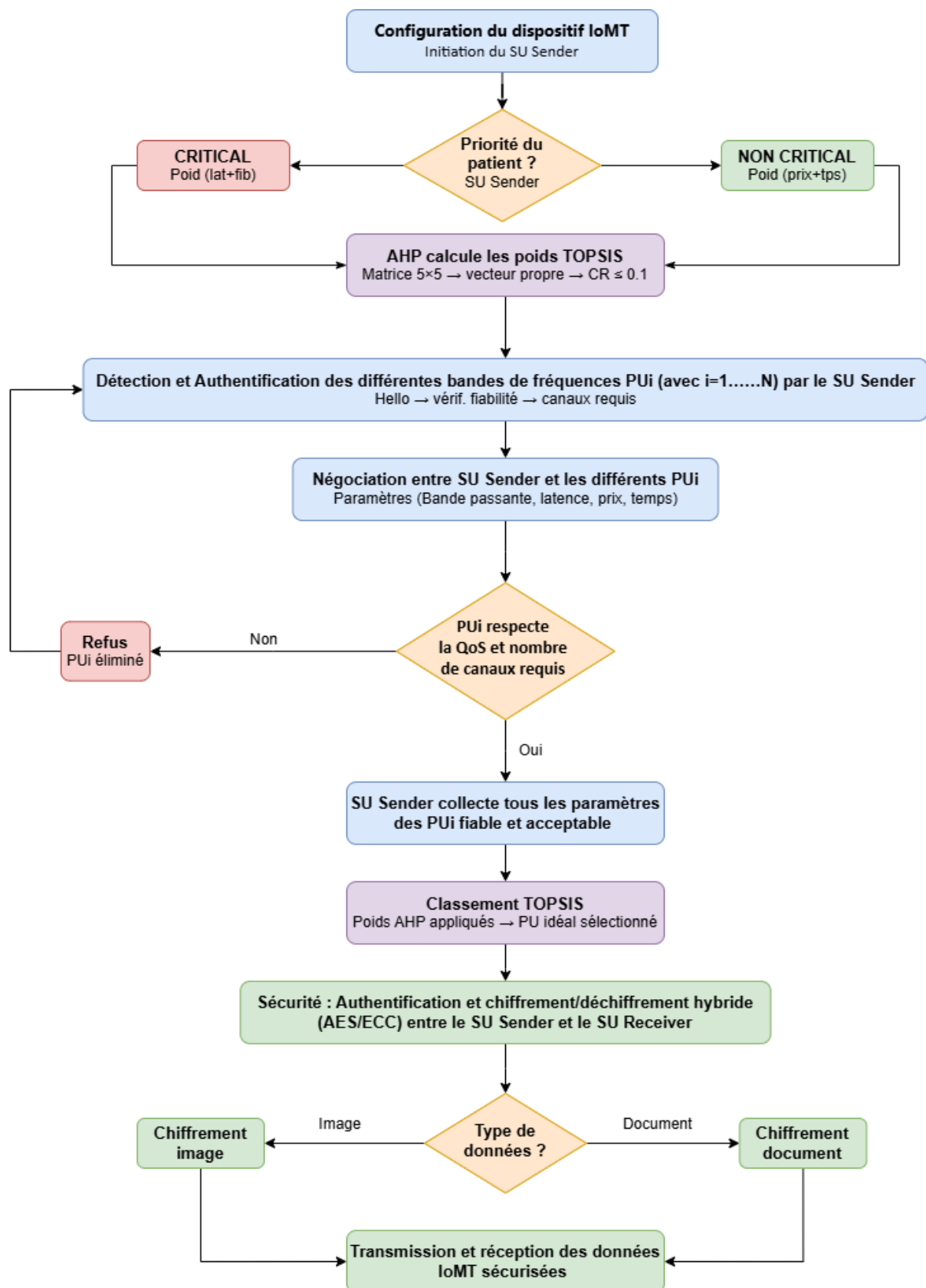


Figure III.4 : Organigramme de notre approche

IV.1. Architecture Globale du Système

Le système développé dans ce travail repose sur une architecture multi-agents distribuée implémentée sur la plateforme JADE. L'objectif est de modéliser le processus d'allocation dynamique du spectre radioélectrique pour les dispositifs IoMT dans un environnement de réseau radio cognitif 5G, en intégrant des mécanismes de décision multicritère et de sécurité des communications.

Le système est structuré autour de six packages Java interdépendants, chacun ayant une responsabilité bien définie. Le package « négociation » constitue le noyau central — il regroupe les quatre agents JADE ainsi que les classes de modélisation IoMT. Il s'appuie sur trois packages spécialisés : « ECC », « RSA » Modes de chiffrement asymétriques utilisé pour l'échange et le transport de clés cryptographiques symétriques non sécurisé à la base, et « encryption » pour le chiffrement/déchiffrement symétrique avec l'AES des données médicales. Le package « TOPSIS » est invoqué par l'agent SU à l'issue de la phase de négociation pour classer les offres de spectre selon les critères multicritères définis. Le package « AHP » calcule dynamiquement les poids des critères TOPSIS à partir de matrices de comparaison par paires définies selon les priorités médicales des dispositifs IoMT.

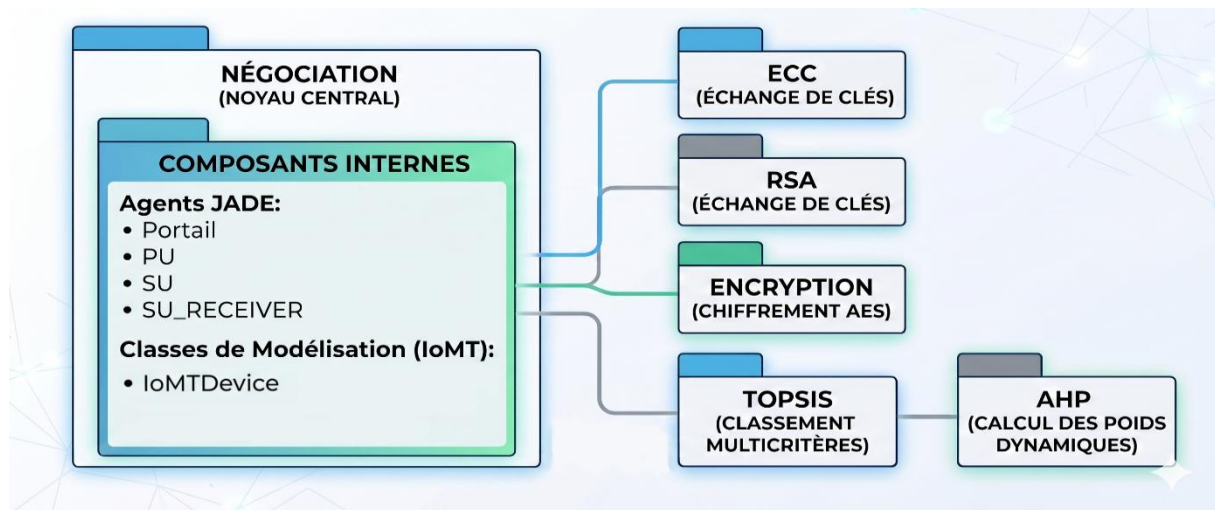


Figure III.5 : Architecture du Système Proposé

IV.2. L'Agent Portail

L'agent Portail constitue le point d'entrée et le nœud central de coordination du système. Premier agent instancié au démarrage de la plateforme JADE, il joue un double rôle initial : il sert d'interface graphique (GUI, Graphical User Interface) pour la configuration de la simulation et orchestre le déploiement de l'ensemble des entités du réseau.

La responsabilité principale du Portail réside dans la création dynamique de l'architecture : il instancie les N agents PU selon les paramètres saisis par l'utilisateur, puis déploie les agents SU et SU_RECEIVER au sein du même conteneur JADE. Cette approche centralisée garantit que tous les agents partagent le même espace de communication et peuvent s'identifier mutuellement via leurs identifiants respectifs (AID).

Une fois cette phase d'initialisation terminée, le Portail agit comme un agent éphémère : après avoir lancé l'interface et configuré l'écosystème, il se supprime automatiquement de la plateforme. Il laisse ainsi les agents PU, SU et SU_RECEIVER gérer en toute autonomie la suite du processus de simulation, optimisant ainsi les ressources du système.

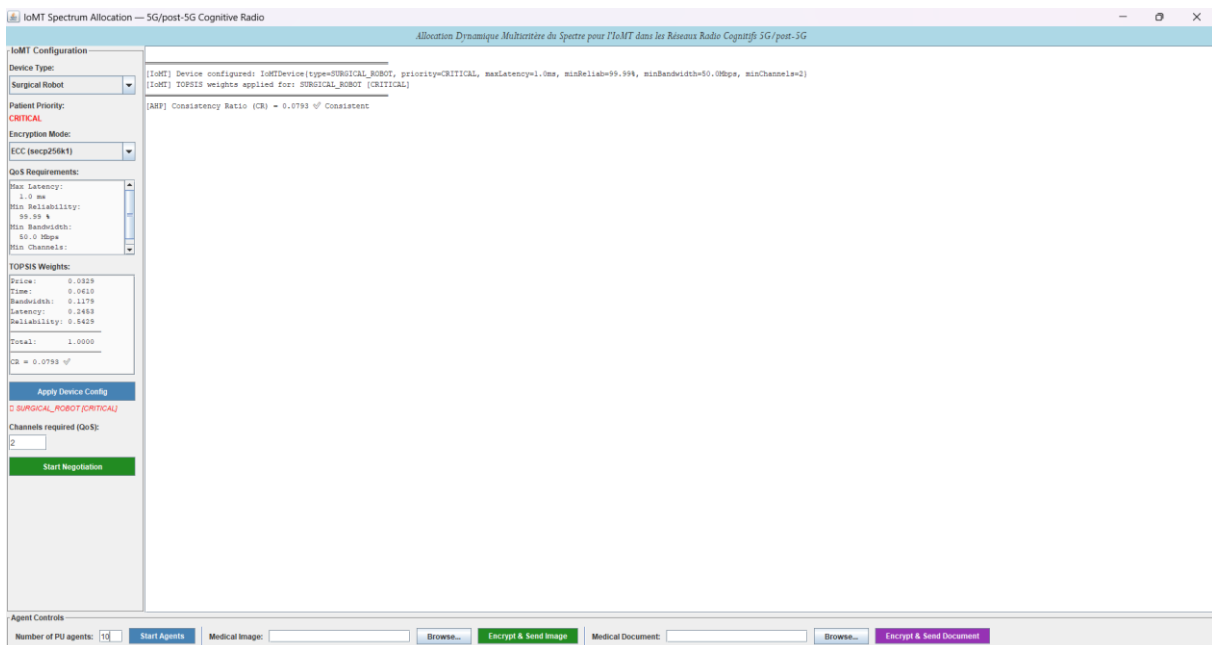


Figure III.6 : Interface graphique (GUI) de l'agent Portail pour la configuration et le déploiement du système

IV.3. L'Agent PU

L'agent PU représente un utilisateur primaire du spectre radioélectrique dans le réseau radio cognitif. Il détient des droits prioritaires sur certaines bandes de fréquences et peut les céder temporairement à des utilisateurs secondaires moyennant une négociation ou une allocation.

À la réception d'une demande de canaux de la part de l'agent SU, chaque agent PU génère aléatoirement ses paramètres de spectre disponibles : le nombre de canaux disponibles, la classe de service 5G supportée parmi le mMTC, l'eMBB et l'URLLC, la bande passante associée, la latence, la fiabilité, le prix et la durée d'allocation. Deux niveaux de filtrage sont

ensuite appliqués séquentiellement. Le premier vérifie si le nombre de canaux disponibles est suffisant pour satisfaire la demande du SU. Le second évalue si les paramètres générés satisfont les exigences QoS minimales du dispositif IoMT actif en termes de latence maximale, de fiabilité minimale et de bande passante minimale. Tout agent PU ne satisfaisant pas ces critères envoie un message de refus et se termine. Les agents PU qualifiés transmettent leur offre complète à l'agent SU pour évaluation TOPSIS.

Les trois classes de service 5G (mMTC, eMBB et URLLC) correspondent aux scénarios d'usage définis par la recommandation ITU, et largement étudiés dans la littérature [67]. L'eMBB privilégie un débit très élevé, l'URLLC une latence très faible et une fiabilité extrême, tandis que le mMTC assure la connectivité d'un grand nombre de dispositifs à faible débit. Les caractéristiques de chaque classe sont résumées dans le tableau suivant :

Classe de service	Bande passante	Latence	Fiabilité
mMTC	1 – 10 Mbps	10 – 50 ms	95 – 99%
eMBB	100 – 1000 Mbps	4 – 20 ms	99 – 99.9%
URLLC	50 – 100 Mbps	0.5 – 1 ms	99.99 – 99.999%

Tableau III.2 : Spécifications techniques des profils 5G supportés par les agents PU

Les plages de valeurs retenues dans notre modèle constituent des valeurs représentatives, inspirées de la littérature sur la 5G [67], et ajustées aux besoins de la simulation ainsi qu'à la cohérence avec les seuils QoS des dispositifs IoMT considérés.

IV.4. L'Agent SU

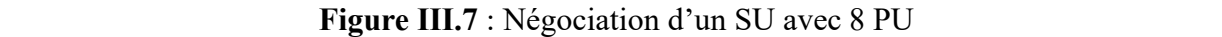
L'agent SU, aussi appelé agent cognitif, représente l'utilisateur secondaire du spectre — le dispositif IoMT médical qui cherche à accéder dynamiquement aux canaux libérés par les utilisateurs primaires. Il constitue le cœur décisionnel du système et orchestre l'intégralité du protocole de négociation.

L'agent SU maintient plusieurs responsabilités simultanées. Il diffuse les demandes de canaux à l'ensemble des agents PU au démarrage de la négociation. Il collecte et enregistre les propositions reçues. Il déclenche l'algorithme TOPSIS une fois toutes les réponses collectées et sélectionne le PU idéal. Il établit ensuite le canal sécurisé avec ce PU et gère le transfert chiffré des données médicales vers l'agent SU_RECEIVER.

L'agent SU_RECEIVER est un agent spécialisé dans la réception et le traitement sécurisé des données médicales. Instancié au démarrage du système, il reste en attente permanente de transferts entrants.

IV.6. Protocole de Négociation

Le protocole de négociation constitue le mécanisme central par lequel l'agent SU identifie et sélectionne le meilleur canal de spectre disponible parmi les agents PU. Ce protocole se déroule en cinq phases séquentielles.



- **Phase 1 : Découverte du Spectre**

La négociation est initiée par l'utilisateur via l'interface Portail. L'agent SU diffuse simultanément un message Hello à l'ensemble des N agents PU enregistrés sur la plateforme. Chaque PU répond par un message de vérification de fiabilité, auquel le SU réplique en indiquant le nombre de canaux requis par le dispositif IoMT configuré.

- **Phase 2 : Négociation et Filtrage QoS**

À la réception de la demande de canaux, chaque agent PU génère dynamiquement ses paramètres de spectre et applique deux niveaux de filtrage séquentiels. Le premier vérifie la disponibilité suffisante de canaux. Le second évalue la conformité aux exigences QoS du dispositif IoMT actif. Tout PU ne satisfaisant pas le premier critère défaillant envoie un message REFUSE et se termine immédiatement. Les PU qualifiés transmettent leur offre complète via un message PROPOSE.

- **Phase 3 : Sélection AHP-TOPSIS**

Lorsque l'ensemble des agents PU ont répondu, l'agent SU calcule d'abord les poids des critères via l'algorithme AHP selon la priorité du dispositif IoMT, puis déclenche TOPSIS sur les offres valides collectées. Le PU ayant le score de proximité idéale le plus élevé est désigné comme PU idéal. Un message CANCEL est immédiatement envoyé à tous les PU non sélectionnés.

- **Phase 4 : Établissement du Canal Sécurisé**

Une fois le PU idéal identifié, l'agent SU initie une procédure d'établissement de connexion sécurisée. Un protocole d'échange de clés basé sur la cryptographie asymétrique (ECC ou RSA) est mis en œuvre pour générer une clé de session AES partagée. Cette clé unique est ensuite utilisée pour assurer la confidentialité de l'ensemble des échanges de données médicales durant la session de transmission hybride.

- **Phase 5 : Transfert des Données Médicales**

Une fois le canal sécurisé établi, l'utilisateur peut transmettre des données médicales via l'interface Portail. L'agent SU chiffre le fichier en hybride (AES/ RSA ou ECC) et l'achemine vers l'agent SU_RECEIVER qui le déchiffre, le sauvegarde et retourne un accusé de réception contenant les métriques de performance du transfert.

V. Modélisation Contextuelle IoMT

V.1. Taxonomie des Dispositifs Médicaux et Paramètres QoS

L'Internet des Objets Médicaux regroupe une grande diversité de dispositifs aux caractéristiques et aux exigences très différentes. Dans notre système, sept types de dispositifs IoMT sont modélisés, répartis en deux catégories selon leur criticité médicale.

- **Dispositifs critiques** : leur priorité est fixe et ne peut être modifiée, car toute défaillance de communication peut engager directement le pronostic vital du patient. Cette catégorie inclut le robot chirurgical, le ventilateur, la pompe à insuline et la pompe à perfusion. Ces dispositifs exigent une latence faible et une fiabilité élevée, satisfaites uniquement par les classes de service eMBB et URLLC.
- **Dispositifs non critiques** : leur priorité est fixe en mode non critique, car ils assurent une surveillance périodique sans impact immédiat sur la vie du patient. Cette catégorie inclut le moniteur patient, le moniteur de pression artérielle et le capteur portable. Leurs exigences relâchées en matière de latence et de fiabilité peuvent être satisfaites par l'ensemble des classes de service 5G.

Les paramètres QoS associés à chaque dispositif sont résumés dans le tableau suivant :

Dispositif	Priorité	Latence max (ms)	Fiabilité min (%)	Bande passante min (Mbps)
Robot chirurgical	Critique	1	99.99	50
Ventilateur	Critique	20	99.9	5
Pompe à perfusion	Critique	20	99	1
Pompe à insuline	Critique	20	99	0.5
Moniteur patient	Non Critique	50	95	10
Moniteur de pression artérielle	Non Critique	50	95	1
Capteur portable	Non Critique	50	95	0.5

Tableau III.3 : Exigences de Qualité de Service (QoS) par type de dispositif IoMT [68] [69]

Ces paramètres constituent des seuils minimaux absolus, tout agent PU ne satisfaisant pas l'ensemble de ces critères est automatiquement éliminé de la négociation avant même d'atteindre l'étape TOPSIS. Ce filtrage préalable garantit que seules les offres médicalement acceptables sont soumises à l'évaluation multicritère.

V.2. Affectation Dynamique des Poids TOPSIS par la Méthode AHP

V.2.1. Principe de la Méthode AHP

La méthode AHP (Analytic Hierarchy Process) est une méthode d'aide à la décision multicritère qui permet de calculer les poids d'importance relative de plusieurs critères à partir de comparaisons par paires. Contrairement à une affectation arbitraire des poids, AHP repose sur des jugements d'experts structurés et vérifie mathématiquement la cohérence de ces jugements [70]. Le principe fondamental d'AHP est de répondre à la question : "*Le critère A est combien de fois plus important que le critère B ?*" en utilisant l'échelle de Saaty définie dans le tableau suivant :

Valeur	Définition
1	Importance égale
2	Importance faible ou légère
3	Importance modérée
4	Importance modérée plus
5	Importance forte
6	Importance forte plus
7	Importance très forte
8	Importance très, très forte
9	Importance extrême

Tableau III.4 : Échelle de comparaison par paires de Saaty [70]

V.2.2. Construction des Matrices de Comparaison par Paires

Notre système définit cinq critères d'évaluation des offres de spectre : prix, durée d'allocation, bande passante, latence et fiabilité. Deux matrices de comparaison 5×5 sont définies selon la priorité du dispositif IoMT actif.

- **Matrice CRITICAL**

Pour les dispositifs critiques (robot chirurgical, ventilateur, pompe à perfusion), la fiabilité et la latence dominent l'ensemble des critères, toute dégradation de ces paramètres pouvant avoir des conséquences directes sur la vie du patient.

Critère	Prix	Durée	B.passante	Latence	Fiabilité
Prix	1	1/3	1/5	1/8	1/9
Durée	3	1	1/3	1/6	1/8
B.passante	5	3	1	1/5	1/7
Latence	8	6	5	1	1/3
Fiabilité	9	8	7	3	1

Tableau III.5 : Matrice de Comparaison par Paires pour les dispositifs Critiques

La fiabilité est jugée modérément plus importante que la latence (3:1). Bien que les deux soient des métriques critiques définissant l'URLLC, la perte d'un seul paquet lors de la transmission d'une commande de contrôle chirurgical peut entraîner des conséquences catastrophiques, rendant la garantie de l'intégrité des données prioritaire sur toute autre contrainte [68]. La fiabilité requise pour la télé-chirurgie atteint 99,999 % (probabilité de perte de paquet de 10^{-5}) [71].

La fiabilité domine très fortement la bande passante (7:1) et de manière extrême la durée (8:1) et le prix (9:1). Si la diffusion vidéo haute définition nécessite un débit élevé, celui-ci peut être satisfait par le découpage du réseau (network slicing), tandis que la fiabilité des commandes de contrôle ne souffre aucun compromis [68].

La latence est fortement plus importante que la bande passante (5:1) et fortement à très fortement plus importante que la durée (6:1) et le prix (8:1). Le retour haptique de l'Internet tactile impose des allers-retours inférieurs à la milliseconde, contrainte plus difficile à satisfaire qu'un débit élevé [68].

La bande passante précède modérément la durée (3:1) et fortement le prix (5:1), un débit suffisant étant requis pour la visualisation temps réel. Enfin, la durée précède modérément le prix (3:1), la stabilité de l'allocation durant l'intervention justifiant un coût supérieur.

- **Matrice NON_CRITICAL**

Pour les dispositifs non critiques (capteurs portables, tensiomètre), l'objectif est l'optimisation économique de l'utilisation du spectre tout en maintenant un débit acceptable. Les exigences de latence et de fiabilité sont nettement relâchées : une latence allant jusqu'à 250 ms et une fiabilité de l'ordre de $(1 - 10^{-3})$ sont jugées suffisantes pour la surveillance périodique [69].

Critère	Prix	Durée	B.passante	Latence	Fiabilité
Prix	1	2	5	7	4
Durée	1/2	1	3	5	3
B.passante	1/5	1/3	1	3	1
Latence	1/7	1/5	1/3	1	1/2
Fiabilité	1/4	1/3	1	2	1

Tableau III.6 : Matrice de Comparaison par Paires pour les dispositifs non Critiques

Le prix précède légèrement à modérément la durée (2:1) : pour les déploiements massifs de capteurs portables (jusqu'à 10^6 dispositifs/km²), la réduction du coût par dispositif est un objectif primordial. Le prix domine fortement la bande passante (5:1), les capteurs portables ne générant que de faibles volumes de données, et très fortement la latence (7:1), la surveillance non temps réel n'exigeant pas de latence ultra-faible. Le prix précède modérément à fortement la fiabilité (4:1), une perte de paquet mineure étant tolérable grâce aux retransmissions périodiques [69].

La durée précède modérément la bande passante (3:1) et la fiabilité (3:1), et fortement la latence (5:1) : pour la surveillance continue sur de longues périodes, une allocation stable réduit la surcharge de signalisation et la consommation énergétique, paramètres déterminants pour les dispositifs alimentés par batterie [72].

La bande passante et la fiabilité sont jugées d'égale importance (1:1), toutes deux modérément importantes pour assurer un débit suffisant et une livraison acceptable des paquets. La bande passante précède modérément la latence (3:1) afin d'éviter la congestion lorsque de nombreux capteurs émettent simultanément. Enfin, la fiabilité précède légèrement la latence (2:1), l'évitement de la perte de données primant marginalement sur la rapidité pour des rapports périodiques non critiques.

V.2.3. Calcul des Poids et Vérification de Cohérence

Le calcul des poids à partir des matrices de comparaison est effectué par le système selon un algorithme défini en sept étapes [73] :

Étape 1 — Sommes de colonnes : Pour chaque colonne j calculer :

$$S_j = \sum_{i=1}^n P_{ij} \quad (\text{III. 1})$$

Étape 2 — Normalisation : Diviser chaque valeur par la somme de sa colonne :

$$N_{ij} = \frac{P_{ij}}{S_j} \quad (\text{III. 2})$$

Étape 3 — Vecteur propre (poids) : Calculer la moyenne de chaque ligne :

$$W_i = \frac{1}{n} \sum_{j=1}^n N_{ij} \quad (\text{III. 3})$$

Étape 4 — Matrice de cohérence :

$$C_{ij} = P_{ij} \times W_j \quad (\text{III. 4})$$

Étape 5 — Sommes pondérées :

$$WS_i = \sum_{j=1}^n C_{ij} \quad (\text{III. 5})$$

Étape 6 — Calcul de λ_{max} (La valeur propre maximale), CI (l'Indice de Cohérence) et CR (Ratio de Cohérence) :

$$\lambda_{max} = \frac{1}{n} \sum_{i=1}^n \frac{WS_i}{W_i} \quad (\text{III. 6})$$

$$CI = \frac{\lambda_{max} - n}{n - 1} \quad (\text{III. 7})$$

$$CR = \frac{CI}{RI} \quad (\text{III. 8})$$

Les équations de (III.1) à (III.8) sont référencées en [73].

Où RI représente l'indice aléatoire standard dépendant de la taille n de la matrice (Tableau III.7).

Pour notre étude comportant cinq critères (n=5), la valeur de référence est RI=1.12

n	1	2	3	4	5	6	7	8	9	10
RI	0	0	0.58	0.90	1.12	1.24	1.32	1.41	1.45	1.49

Tableau III.7 : Valeurs de l'indice de cohérence aléatoire (RI) [73]

Étape 7 — Validation : Lorsque le ratio de cohérence est inférieur à 0.1, les vecteurs de priorité sont validés. Dans le cas contraire ($CR > 0.1$), la matrice est considérée comme incohérente, nécessitant un ajustement des jugements.

V.2.4. Poids Obtenus et Validation de Cohérence

L'application de l'algorithme AHP sur les deux matrices définies produit les résultats suivants :

- **Dispositifs CRITICAL**

Critère	Prix	Durée	B.passante	Latence	Fiabilité
Poids	3.28%	6.09%	11.16%	28.43%	51.03%

Tableau III.8 : Résultats AHP des poids des critères (CRITICAL)

Le ratio de cohérence obtenu est $CR = 0.0865$, inférieur au seuil de 0.10 recommandé par Saaty, ce qui valide la cohérence des jugements.

- **Dispositifs NON_CRITICAL**

Critère	Prix	Durée	B.passante	Latence	Fiabilité
Poids	45.78%	27.26%	11.01%	5.21%	10.38%

Tableau III.9 : Résultats AHP des poids des critères (NON_CRITICAL)

Le ratio de cohérence obtenu est $CR = 0.0138$, très inférieur au seuil de 0.10, confirmant la forte cohérence de la matrice.

VI. Algorithme TOPSIS

L'algorithme TOPSIS (Technique for Order of Preference by Similarity to Ideal Solution) est une méthode d'aide à la décision multicritère. Son principe fondamental repose sur le choix de l'alternative la plus proche de la solution idéale positive et la plus éloignée de la solution idéale négative [74]. Dans notre système, chaque agent PU ayant passé le filtrage QoS constitue une alternative, et les cinq critères retenus (prix, durée, bande passante, latence et fiabilité) constituent les axes d'évaluation. Les poids de ces critères sont calculés dynamiquement par la méthode AHP présentée en section V.2 selon la priorité du dispositif IoMT actif.

VI.1. Construction de la Matrice de Décision

La matrice de décision constitue le point de départ de l'algorithme TOPSIS. Elle est construite à partir des propositions reçues par l'agent SU après la phase de négociation. Chaque ligne représente un agent PU qualifié et chaque colonne représente un critère d'évaluation.

Soit m le nombre d'agents PU qualifiés et n le nombre de critères [74]. La matrice de décision X est définie comme :

$$X = \begin{pmatrix} x_{11} & \cdots & x_{1n} \\ \vdots & \ddots & \vdots \\ x_{m1} & \cdots & x_{mn} \end{pmatrix}$$

Où x_{ij} représente la valeur du critère j pour l'agent PU_i . Dans notre système, chaque proposition PU est transmise sous la forme d'un vecteur contenant les cinq valeurs des critères retenus après filtrage QoS.

Chaque critère est caractérisé par son objectif d'optimisation (soit à maximiser, soit à minimiser) qui détermine son traitement dans les étapes suivantes :

Critere	Objectif	Raison
Prix	Minimisation	Réduire les coûts d'accès pour l'utilisateur
Durée	Maximisation	Augmenter le temps d'occupation du canal
B.passante	Maximisation	Offrir le débit de données le plus élevé
Latence	Minimisation	Réduire le délai de transmission des données
Fiabilité	Maximisation	Garantir la stabilité de la connexion médicale

Tableau III.10 : Nature et objectifs d'optimisation des critères

VI.2 Normalisation et Pondération

La normalisation permet de rendre les critères comparables entre eux en éliminant les effets des unités de mesure. TOPSIS utilise la normalisation euclidienne, chaque valeur est divisée par la norme de sa colonne [74] :

$$r_{ij} = \frac{x_{ij}}{\sqrt{\sum_{k=1}^m x_{kj}^2}} \quad (\text{III. 9})$$

Une fois normalisée, la matrice est pondérée en multipliant chaque valeur par le poids w_j du critère correspondant (calculé par AHP) pour obtenir la matrice pondérée V :

$$v_{ij} = w_j \times r_{ij} \quad (\text{III. 10})$$

VI.3. Calcul des Solutions Idéales

TOPSIS définit deux solutions de référence à partir de la matrice pondérée V :

- **Solution Idéale Positive A^+** : représente le meilleur scénario théorique, c'est-à-dire la combinaison des meilleures valeurs observées pour chaque critère.

$$A^+ = \{v_1^+, v_2^+, \dots, v_n^+\}$$

- **Solution Idéale Négative A^-** : représente le pire scénario théorique, c'est-à-dire la combinaison des moins bonnes valeurs observées.

$$A^- = \{v_1^-, v_2^-, \dots, v_n^-\}$$

La distance euclidienne de chaque alternative aux deux solutions idéales est ensuite calculée [74] :

$$D_i^+ = \sqrt{\sum_{j=1}^n (v_{ij} - v_j^+)^2} \quad (\text{III. 11})$$

$$D_i^- = \sqrt{\sum_{j=1}^n (v_{ij} - v_j^-)^2} \quad (\text{III. 12})$$

VI.4. Classement des PU Candidats

Le score de proximité relative C_i (appelé aussi coefficient de proximité) est calculé pour chaque agent PU candidat comme le rapport entre sa distance à la solution idéale négative et la somme de ses distances aux deux solutions idéales :

$$C_i = \frac{D_i^-}{D_i^+ + D_i^-} \quad \text{avec} \quad C_i \in [0,1] \quad (\text{III. 13})$$

Les équations de (III.9) à (III.13) sont référencées en [74].

Un score C_i proche de 1 indique que l'alternative est très proche de la solution idéale positive et très éloignée de la solution idéale négative, c'est donc la meilleure offre de spectre pour le dispositif IoMT concerné. Un score proche de 0 indique l'inverse [74].

Les agents PU sont classés par ordre décroissant de leur score C_i . L'agent PU ayant le score le plus élevé est désigné comme PU idéal et sélectionné pour l'établissement du canal sécurisé. Tous les autres agents PU reçoivent un message CANCEL et se terminent.

VII. Sécurisation des Communications

La sécurisation des communications constitue un aspect fondamental de notre système d'allocation de spectre IoMT. Les données médicales échangées entre agents sont particulièrement sensibles, toute interception ou altération peut avoir des conséquences directes sur la prise en charge des patients. Notre système implémente une architecture de sécurité multicouche combinant cryptographie asymétrique pour l'échange de clés et chiffrement symétrique pour la protection des données.

VII.1. Architecture de Sécurité du Système

L'architecture de sécurité du système repose sur deux couches complémentaires. La première couche assure l'échange sécurisé de clés entre les agents via deux modes cryptographiques asymétriques (ECC ou RSA) sélectionnables par l'utilisateur via l'interface Portail. La seconde couche assure le chiffrement des données médicales via l'algorithme symétrique AES en utilisant la clé partagée établie lors de la première couche.

La gestion des clés est assurée par une Autorité de Certification (CA), une seule instance existe pour toute la plateforme JADE et est partagée par tous les agents. Elle joue le rôle de tiers de confiance centralisé responsable de la génération et de la distribution des clés cryptographiques entre les agents PU, SU et SU_RECEIVER selon le mode sélectionné.

Tous les messages échangés entre agents après la phase d'authentification voient leur contenu chiffré en AES, le contenu en clair ne transite jamais sur le canal de communication inter-agents une fois la session sécurisée établie.

VII.2. Chiffrement des Données Médicales (AES)

Comme présenté dans le Chapitre I Section IV.3.1, l'AES (Advanced Encryption Standard) est l'algorithme de chiffrement symétrique standard actuel. Dans notre système, AES est utilisé pour deux usages distincts.

Le premier usage concerne le chiffrement des messages ACL échangés entre les agents après l'établissement du canal sécurisé (demandes de connexion, confirmations et accusés de réception). Le second usage concerne le chiffrement des données médicales (images et documents) transmises de l'agent SU vers l'agent SU_RECEIVER.

Les données chiffrées sont encodées en Base64 avant d'être transportées dans le champ Content des messages ACL, ce format garantit la compatibilité avec le protocole texte FIPA-ACL qui ne supporte pas les données binaires brutes.

VII.3. Mode Hybride ECC+AES

Comme présenté dans le Chapitre I Section IV.3.2, l'ECC (Elliptic Curve Cryptography) utilise les propriétés algébriques des courbes elliptiques pour établir un secret partagé entre deux parties sans jamais transmettre ce secret sur le canal de communication.

Dans notre système, le protocole ECDH (Elliptic Curve Diffie-Hellman) est implémenté sur la courbe secp256r1. L'établissement de la clé partagée via ECDH se déroule en quatre étapes :

1. L'agent SU génère sa paire de clés ECC sur la courbe secp256r1, une clé privée $priv_{SU}$ gardée secrète et une clé publique pub_{SU} partageable.
2. L'agent PU génère de son côté sa propre paire de clés ECC, une clé privée $priv_{PU}$ et une clé publique pub_{PU} .
3. Chaque agent calcule indépendamment le secret partagé en combinant sa clé privée avec la clé publique de l'autre partie :

$$S_{SU} = ECDH(priv_{SU}, pub_{PU})$$

$$S_{PU} = ECDH(priv_{PU}, pub_{SU})$$

La propriété mathématique fondamentale d'ECDH garantit que les deux calculs aboutissent au même résultat :

$$priv_{SU} \times pub_{PU} = priv_{PU} \times pub_{SU} = S$$

4. Le secret partagé S est utilisé comme clé AES pour chiffrer l'ensemble des communications entre SU et PU idéal. Ce secret ne transitant jamais sur le réseau, toute interception est rendue impossible.

VII.4. Mode Hybride RSA+AES

Comme présenté dans le Chapitre I Section IV.3.2, le RSA repose sur la difficulté de factorisation de grands nombres premiers. Contrairement à ECC qui permet un accord de clé mathématique, RSA utilise un mécanisme de transport de clé, une partie génère la clé AES et la chiffre avec la clé publique du destinataire qui la déchiffre avec sa clé privée.

Dans notre système, RSA 2048 bits est implémenté avec un remplissage sécurisé conforme aux standards modernes. Le processus de transport de clé se déroule en quatre étapes :

1. L'agent PU génère une paire de clés RSA 2048 bits, une clé privée $priv_{PU}$ gardée secrète et une clé publique pub_{PU} partageable.
2. Une clé AES 256 bits est générée aléatoirement, c'est cette clé qui sera utilisée pour chiffrer les communications entre SU et PU.
3. La clé AES est chiffrée avec la clé publique pub_{PU} de l'agent PU :

$$C_{AES} = RSA_{Chiffrement}(K_{AES}, pub_{PU})$$

La clé AES chiffrée C_{AES} est transmise à l'agent PU qui la déchiffre avec sa clé privée $priv_{PU}$:

$$K_{AES} = RSA_{Déchiffrement}(C_{AES}, priv_{PU})$$

4. SU et PU partagent désormais la même clé AES K_{AES} , utilisée pour chiffrer l'ensemble des communications. Contrairement à ECC où le secret est calculé mathématiquement des deux côtés, en RSA la clé AES transite sur le réseau sous forme chiffrée, sa sécurité repose donc entièrement sur la robustesse du chiffrement RSA 2048 bits.

VII.5. Comparaison de notre contribution avec l'ECC vs RSA

La sélection du mode cryptographique approprié pour un système IoMT médical constitue un choix architectural critique. Notre système supporte deux modes hybrides (ECC+AES et RSA+AES) et permet leur comparaison expérimentale via les métriques temporelles mesurées lors de l'établissement du canal sécurisé.

Pour mesurer objectivement le coût cryptographique de chaque mode, 30 simulations ont été effectuées dans des conditions identiques (dispositif Blood Pressure avec 8 agents PU). Le temps d'établissement du canal sécurisé mesure la durée depuis la demande de connexion jusqu'à la confirmation.

Statistique	ECC	RSA
Moyenne	16.13 ms	125.43 ms
Minimum	12 ms	60 ms
Maximum	23 ms	273 ms
Écart-type	3.54 ms	51.43 ms

Tableau III.11 : Analyse comparative des performances temporelles entre ECC et RSA

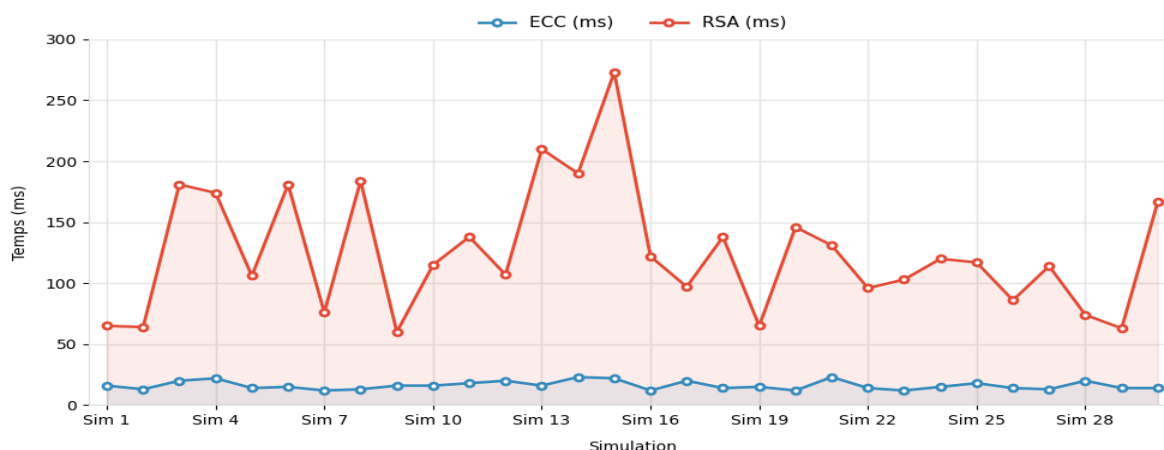


Figure III.8 : Comparaison du temps d'établissement d'un canal sécurisé : ECC vs RSA (30 simulations)

Analyse des Résultats

Les résultats expérimentaux révèlent une différence significative entre les deux modes cryptographiques.

- **ECC** affiche un temps moyen d'établissement du canal sécurisé de 16.13 ms avec un écart-type de seulement 3.54 ms, ce qui témoigne d'une grande stabilité et prévisibilité du comportement. La plage de variation étroite entre 12 ms et 23 ms confirme que le calcul ECDH sur la courbe secp256r1 est peu sensible aux variations de charge du système.
- **RSA** affiche un temps moyen de 125.43 ms (soit 7.77 fois plus lent que ECC) avec un écart-type de 51.43 ms, révélant une forte instabilité. La plage de variation très large entre 60 ms et 273 ms s'explique par la complexité de l'opération d'exponentiation modulaire RSA 2048 bits qui est particulièrement sensible à la charge CPU au moment de l'exécution.

Deux facteurs expliquent la supériorité d'ECC sur RSA dans ce contexte :

- **La taille de clé** : ECC utilise une clé de 256 bits contre 2048 bits pour RSA (soit 8 fois plus petite) ce qui réduit considérablement le coût des opérations cryptographiques.
- **La nature de l'opération** : ECDH calcule le secret partagé via des opérations sur courbes elliptiques naturellement plus efficaces que l'exponentiation modulaire sur grands nombres premiers utilisée par RSA.

Conclusion

Les résultats obtenus confirment que ECC est nettement plus adapté que RSA pour les systèmes IoMT médicaux pour trois raisons :

- **Performance** : Un temps d'établissement de 16.13 ms contre 125.43 ms pour RSA est décisif dans un contexte médical temps réel où chaque milliseconde compte, notamment pour les dispositifs critiques comme le robot chirurgical ou le ventilateur.
- **Stabilité** : L'écart-type de 3.54 ms d'ECC garantit un comportement prévisible, essentiel pour les systèmes médicaux où les délais doivent être garantis. La variabilité de RSA (51.43 ms) le rend imprévisible et donc risqué dans un contexte critique.
- **Efficacité énergétique** : Comme présenté dans le Chapitre I Section IV.3.2, ECC consomme significativement moins de ressources que RSA, un avantage crucial pour les dispositifs IoMT fonctionnant sur batterie comme les capteurs implantables et les capteurs portables.

VIII. Résultats et Évaluation des Performances

VIII.1. Environnement Expérimental

Les expérimentations ont été réalisées sur une station de travail dont les caractéristiques matérielles et logicielles sont résumées dans le tableau suivant.

Composant	Spécification
Processeur CPU	AMD Ryzen 5 7600
Mémoire vive RAM	16 Go
Carte graphique GPU	NVIDIA GeForce RTX 3060 (12 Go)
Système d'exploitation	Windows 11
Environnement d'exécution	Java SE 1.8 (JDK 8)
Plateforme multi-agents	JADE
Environnement de développement	Apache NetBeans IDE 28

Tableau III.12 : Configuration matérielle et logicielle de la station de travail

L'ensemble des agents (Portail, SU, SU_RECEIVER et les agents PU) s'exécutent sur une même machine au sein d'une unique plateforme JADE. En conséquence, les latences de transmission mesurées correspondent au temps d'acheminement interne à la plateforme et non à une transmission radio réelle sur un réseau 5G.

Configuration de référence

Sauf indication contraire, l'ensemble des expérimentations adopte la configuration par défaut suivante :

- **Mode de chiffrement** : ECC, courbe secp256r1, avec dérivation d'une clé de session AES.
- **Dispositif IoMT actif** : moniteur patient (priorité non critique).
- **Nombre d'agents PU** : 10.

VIII.2. Mesures et métriques de latence

VIII.2.1. Métriques de base

L'évaluation des performances temporelles du système repose sur deux métriques fondamentales, dont la distinction est essentielle pour interpréter correctement les résultats expérimentaux.

- **Latence réseau (Network Latency)**

La latence réseau désigne le temps de transmission unidirectionnel d'un message entre l'agent émetteur (SU) et l'agent récepteur (SU_Receiver). Elle est mesurée à partir de l'instant où l'agent SU achève le chiffrement et invoque l'envoi du message, jusqu'à l'instant où l'agent SU_Receiver récupère ce message dans sa file de réception. Cette métrique isole le coût de l'acheminement, indépendamment des traitements applicatifs effectués aux extrémités (chiffrement, déchiffrement). Dans l'environnement de simulation considéré, la latence réseau correspond au temps de transport interne à la plateforme JADE.

- **Latence bout-en-bout (End-to-End Latency)**

La latence bout-en-bout désigne le délai total perçu par le système, depuis l'émission du premier message de découverte (Hello) par l'agent SU jusqu'au dernier échange confirmant la réussite de la transmission entre l'agent SU et l'agent SU_Receiver. Contrairement à la latence réseau, qui ne mesure qu'un segment de transport, la latence bout-en-bout englobe l'intégralité du cycle de service : la phase de négociation et d'allocation du spectre, suivie de la phase de transfert sécurisé des données médicales. Elle représente donc la durée complète nécessaire pour qu'un dispositif IoMT obtienne un canal et achemine ses données de manière confirmée.

VIII.2.2. Mesure de latence bout-en-bout

La latence bout-en-bout se décompose selon les phases du protocole de négociation décrit en section IV.6. À chaque phase est associé un ou plusieurs minuteurs (timers) mesurant sa contribution au délai global.

La phase de négociation et d'allocation (phases 1 à 4 du protocole) regroupe trois intervalles :

- **T1 — Découverte du spectre** : du premier message Hello à la réception de la dernière proposition PU (phases 1 et 2).
- **T2 — Décision TOPSIS** : durée du calcul de classement multicritère (phase 3).
- **T3 — Établissement du canal sécurisé** : de la requête d'authentification à la confirmation de connexion (phase 4).

Sa durée totale, la phase de négociation, est la somme des intervalles T1 à T3

La phase de transfert sécurisé (phase 5 du protocole) regroupe quatre intervalles :

- **T4 — Chiffrement (SU)** : chiffrement AES des données avant l'envoi.
- **T5 — Latence réseau (SU → SU_Receiver)** : transmission unidirectionnelle du message chiffré.
- **T6 — Déchiffrement (SU_Receiver)** : déchiffrement AES par le récepteur.
- **T7 — Retour de l'accusé de réception (ACK, Acknowledgement) (SU_Receiver → SU)** : transmission du message d'acquiescement.

Sa durée totale, la latence bout-en-bout de transfert, est la somme des intervalles T4 à T7.

La latence bout-en-bout combinée résulte de l'addition de la phase de négociation et de la latence bout-en-bout de transfert. Cette sommation des deux phases actives exclut le temps d'attente intermédiaire lié à l'action de l'utilisateur, et reflète ainsi le coût temporel intrinsèque au système.

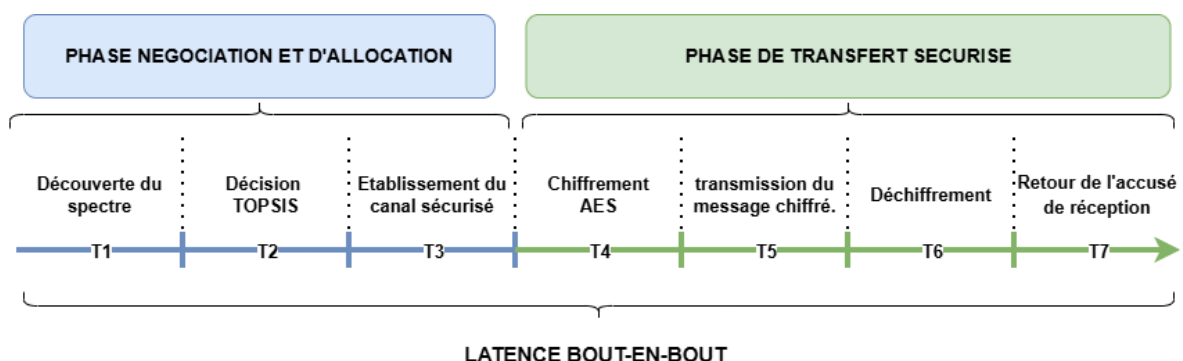


Figure III.9 : Décomposition temporelle et composants de la latence bout-en-bout

VIII.3. Impact de la Taille du Fichier

Cette première série d'expérimentations vise à caractériser l'influence de la taille du fichier transmis sur la latence de transfert des données médicales. Conformément à la configuration de référence, les mesures ont été réalisées avec un dispositif de type moniteur patient, dix agents PU et le mode de chiffrement ECC. Seule la taille du fichier varie ; tous les autres paramètres demeurent constants.

Pour chaque taille, la latence de transfert est décomposée selon les quatre intervalles définis en section VIII.2 : le chiffrement à l'émission (T4), la latence réseau de transmission (T5), le déchiffrement à la réception (T6) et le retour de l'accusé de réception (T7). La latence de transfert bout-en-bout correspond à la somme de ces quatre intervalles. Chaque valeur rapportée est la moyenne de trois exécutions en régime stable.

Résultats pour les images médicales

Six tailles de fichiers images, échelonnées de 24 Ko à 5142 Ko, ont été évaluées. Les résultats moyens sont présentés dans le tableau suivant.

Taille (Ko)	T4 Chiffr. (ms)	T5 Réseau (ms)	T6 Déchiffr. (ms)	T7 ACK (ms)	Transfert de bout en bout (ms)
24	0.00	0.67	0.00	0.33	1.00
142	0.00	1.33	0.00	0.33	1.67
512	5.33	3.67	5.33	0.67	15.00
1075	4.67	11.33	4.67	0.67	21.33
2552	6.00	20.00	12.00	0.67	38,67
5142	14.67	55.67	28.67	1.67	100.67

Tableau III.13 : Latence de transfert des images

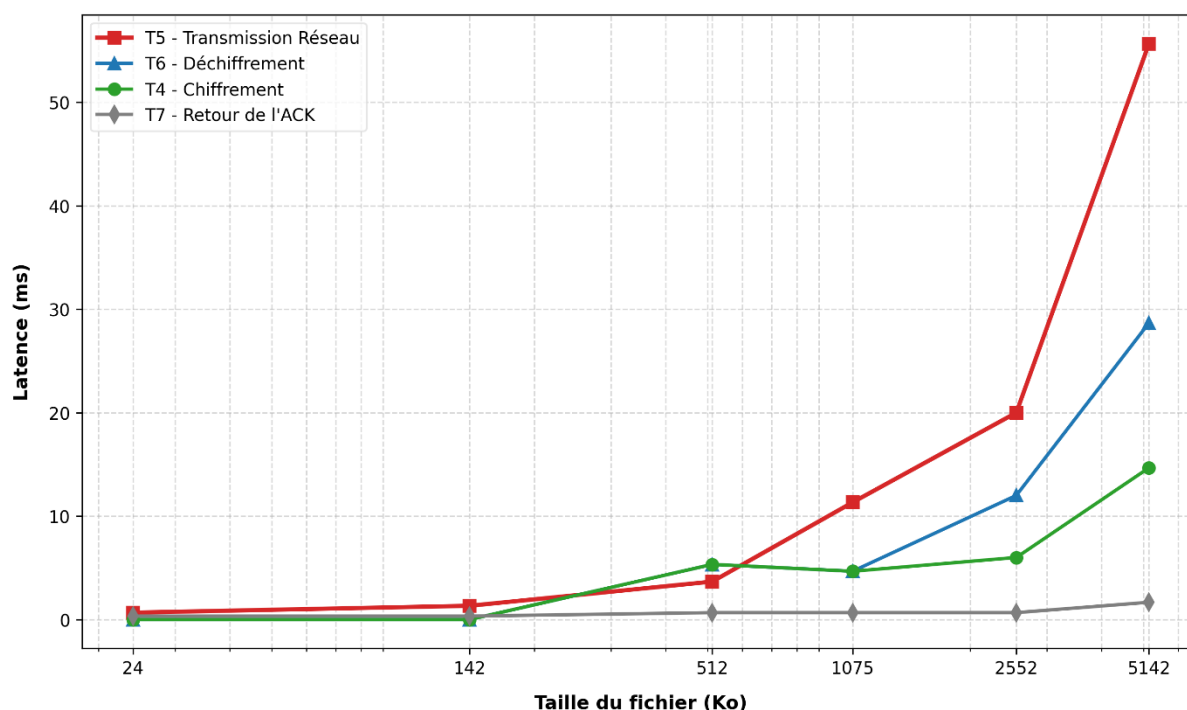


Figure III.10 : Latence de transfert en fonction de la taille du fichier

L'analyse de ces résultats met en évidence plusieurs tendances.

D'abord, la latence de transfert bout-en-bout croît de manière monotone avec la taille du fichier, passant de 1 ms pour un fichier de 24 Ko à environ 101 ms pour un fichier de 5142 Ko. Cette progression confirme la dépendance directe entre le volume de données et le délai de transmission sécurisée.

Ensuite, la latence réseau (T5) constitue la composante prépondérante du délai pour toutes les tailles supérieures à 512 Ko, et présente la croissance la plus marquée (de 0.67 ms à 55.67 ms). Ce comportement s'explique d'une part par l'encodage Base64 du fichier chiffré, qui accroît d'environ un tiers le volume des données transmises, et d'autre part par la surcharge liée à la sérialisation et à l'acheminement de messages volumineux au sein de la plateforme multi-agents.

Les temps de chiffrement (T4) et de déchiffrement (T6) augmentent quant à eux de façon globalement linéaire avec la taille du fichier, conformément au comportement attendu de l'algorithme AES dont le coût est proportionnel au nombre d'octets traités.

Enfin, le retour de l'accusé de réception (T7) demeure quasiment constant (entre 0.3 et 1.7 ms), indépendamment de la taille du fichier transmis. Ce résultat est cohérent avec la nature

de l'accusé de réception, message de taille fixe et réduite, dont le coût ne dépend pas du volume des données préalablement échangées.

On notera que pour les fichiers de petite taille (24 Ko et 142 Ko), les temps de chiffrement et de déchiffrement apparaissent nuls : ces opérations s'effectuent en réalité en deçà de la milliseconde, résolution temporelle de la mesure, et sont donc arrondies à zéro.

Comparaison entre images et documents

Afin de vérifier que la latence dépend du volume de données et non de la nature du fichier, des mesures complémentaires ont été réalisées sur des documents médicaux à deux tailles correspondant à celles des images.

Taille (Ko)	Image — Transfert (ms)	Document — Transfert (ms)	Écart (ms)
142	1.67	2.00	0.33
2552	38.67	36.00	2.67

Tableau III.14 : Comparaison image / document

Les résultats confirment cette hypothèse : à taille égale, les latences de transfert des images et des documents sont quasiment identiques. Pour un fichier de 142 Ko, la latence de transfert est de 1.67 ms pour une image contre 2.00 ms pour un document, soit un écart de 0.33 ms. Pour un fichier de 2552 Ko, elle est de 38.67 ms pour une image contre 36.00 ms pour un document, soit un écart de 2.67 ms. Ces écarts demeurent dans la marge de variation observée entre exécutions successives.

Cette équivalence s'explique par le fonctionnement de l'algorithme AES, qui opère sur la séquence d'octets bruts du fichier sans tenir compte de son format. La latence de la chaîne de transmission sécurisée est donc déterminée par le volume de données et non par le type de fichier transmis, ce qui valide la généralité de l'approche pour l'ensemble des types de données médicales.

VIII.4. Résultats de Latence Bout-en-Bout

Cette section présente la décomposition complète de la latence bout-en-bout d'une session de transmission. Contrairement à la section précédente qui faisait varier la taille du fichier, l'objectif est ici d'analyser la répartition du délai total entre les différentes phases du système pour une configuration représentative.

Les mesures ont été réalisées sur **100 exécutions** d'une session complète, avec la configuration de référence (moniteur patient, 10 agents PU, chiffrement ECC) et un **fichier**

image de 512 Ko. Le recours à un grand nombre d'exécutions permet d'obtenir des valeurs statistiquement robustes et d'évaluer la variabilité du système. Les résultats sont présentés dans le tableau suivant.

Intervalle	Moyenne (ms)	Ecart-type (ms)	Min (ms)	Max (ms)
T1	19.04	3.98	14	31
T2	<1(≈ 0)	0	0	0
T3	11.68	4.00	8	27
Phase de négociation	30.72	5.99	22	48
T4	5.14	1.27	2	9
T5	3.87	1.22	3	9
T6	4.85	1.14	2	8
T7	0.71	0.70	0	3
Phase de transfert	14.57	2.83	9	23
Bout-en-bout	45.29	6.67	34	61

Tableau III.15 : Décomposition de la latence bout-en-bout (100 exécutions)

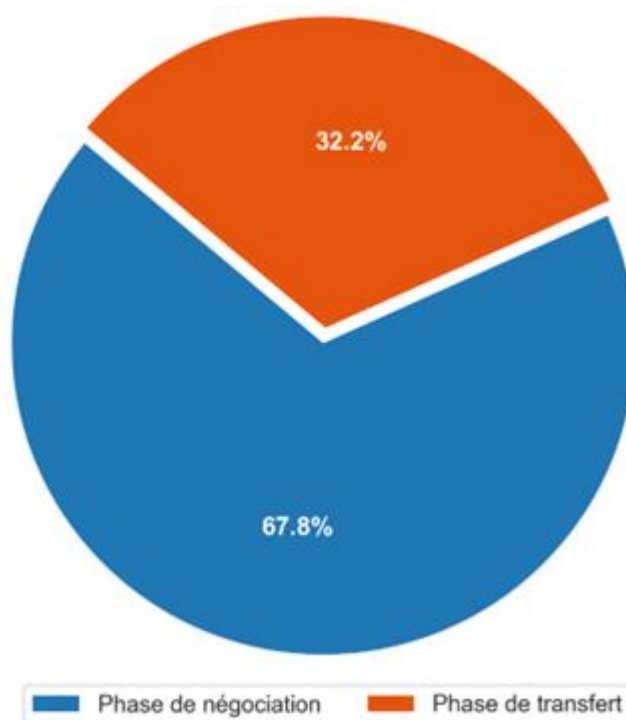


Figure III.11 : Répartition de la latence bout-en-bout par phase

Analyse de la phase de négociation

La phase de négociation, définie comme la somme des intervalles T1, T2 et T3, présente une durée moyenne de 30.72. Elle constitue la composante prépondérante de la latence bout-en-bout, représentant à elle seule 67.8 % du délai total.

Au sein de cette phase, la découverte du spectre ($T1 = 19,04$) est l'opération la plus coûteuse, comptant pour 62 % de la durée de négociation. Ce coût s'explique par l'attente des réponses de l'ensemble des dix agents PU avant le déclenchement de la sélection. L'établissement du canal sécurisé ($T3 = 11,68$) représente les 38 % restants, correspondant à l'échange de clés asymétriques et à la confirmation de la connexion.

Il convient de souligner que la décision multicritère TOPSIS (T2) s'effectue en un temps inférieur à la milliseconde, mesuré comme nul à la résolution employée. Ce résultat est particulièrement significatif : le cœur décisionnel du système (le classement AHP-TOPSIS des offres de spectre) n'introduit aucune surcharge temporelle perceptible, même pour dix alternatives évaluées selon cinq critères. La méthode multicritère est donc parfaitement compatible avec les contraintes temps réel de l'IoMT.

Analyse de la phase de transfert

La phase de transfert sécurisé (T4 à T7) présente une durée moyenne de 14.57, soit 32.2 % de la latence totale. Pour un fichier de 512 Ko, ses composantes sont relativement équilibrées : le chiffrement ($T4 = 5.14$) et le déchiffrement ($T6 = 4.85$) sont du même ordre de grandeur, suivis de la latence réseau ($T5 = 3.87$), tandis que le retour de l'accusé de réception ($T7 = 0.71$) demeure négligeable.

On notera que cette répartition équilibrée est spécifique aux fichiers de taille modérée. Comme l'a montré la section 8.3, pour des fichiers volumineux la latence réseau et le déchiffrement deviennent prépondérants et croissent linéairement avec le volume de données.

Latence bout-en-bout combinée

La latence bout-en-bout combinée, somme des phases de négociation et de transfert, s'établit à 45.29 en moyenne, avec des valeurs comprises entre 34 et 61 ms sur les 100 exécutions. Le faible écart-type relatif témoigne de la stabilité et de la prévisibilité du comportement temporel du système.

Le résultat majeur de cette analyse est la prédominance de la phase de négociation (67.8 %) sur la phase de transfert (32.2 %). Pour des charges utiles de taille modérée, typiques de nombreuses applications IoMT (relevés de signes vitaux, images compressées), le coût d'établissement de l'allocation spectrale dépasse celui du transfert des données lui-même. Ce constat souligne l'importance d'optimiser la phase de découverte et de négociation pour réduire la latence globale perçue par les dispositifs médicaux.

VIII.5. Comparaison avec des Travaux Précédents

Pour évaluer notre système, nous comparons nos résultats de temps de convergence à ceux de travaux antérieurs sur l'allocation multicritère du spectre dans les réseaux radio cognitifs. Ce temps désigne le délai entre le début et la fin de la négociation, incluant l'authentification et la sécurisation du canal. Dans notre système, cette métrique correspond à la phase ($T1 + T2 + T3$), avec une moyenne de 30,72 ms. Tous les travaux reposant sur la plateforme multi-agents JADE, la comparaison s'effectue à paradigme expérimental équivalent

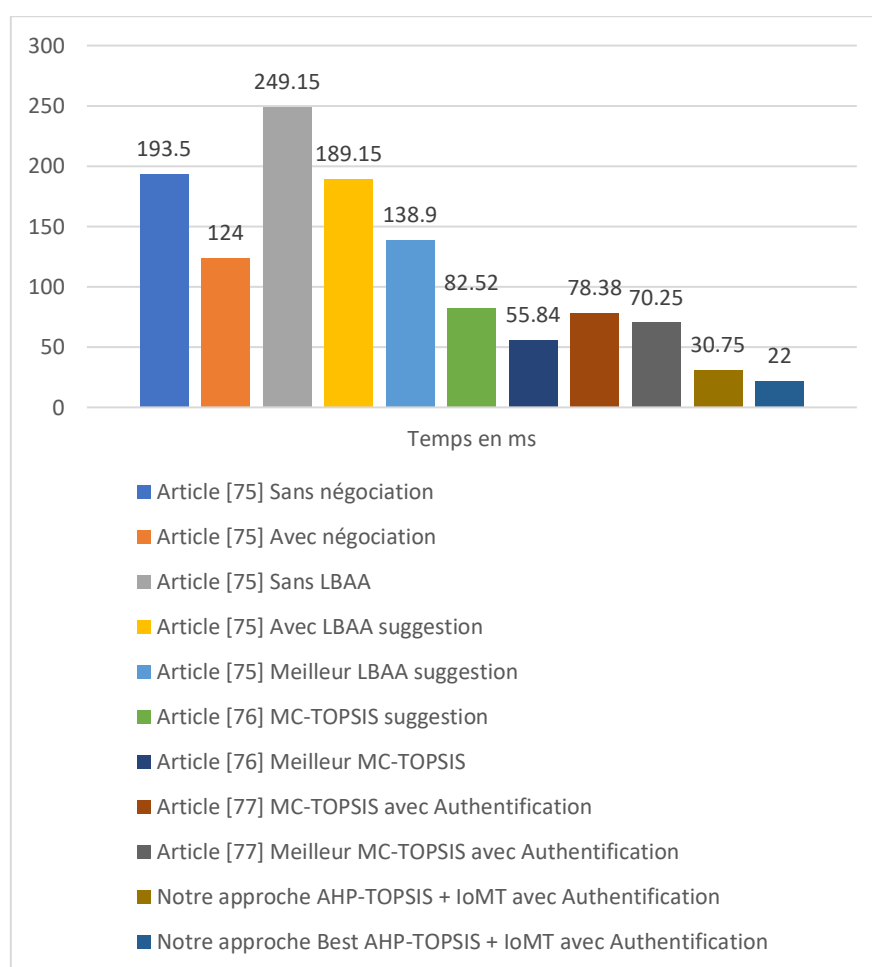


Figure III.12 : Comparaison de notre approche sur le temps de convergence avec les résultats de la littérature

Analyse comparative

Les travaux comparés s'échelonnent selon des approches de complexité croissante.

Le travail de [75] repose sur une approche fondée sur la négociation entre agents et la suggestion LBAA. Ses différentes variantes présentent les temps de convergence les plus élevés : la variante avec négociation atteint 124.0 ms, tandis que les variantes liées à la suggestion LBAA s'échelonnent de 138.9 ms (meilleur cas) à 249.15 ms (sans suggestion LBAA).

L'approche de [76], reposant sur MC-TOPSIS, réduit sensiblement ce délai, avec un meilleur cas de 55.84 ms et une moyenne de 82.52 ms. Le travail de [77], qui ajoute un mécanisme d'authentification et de sécurité des données ainsi qu'un cinquième critère (le taux de fiabilité), atteint un meilleur cas de 70.25 ms et une moyenne de 78.38 ms.

Notre système atteint un temps de convergence moyen de **30.72 ms**, inférieur non seulement aux moyennes rapportées par l'ensemble de ces travaux, mais également à leurs meilleurs cas mesurés. Ce résultat est d'autant plus notable que notre contribution enrichit le système par rapport aux approches précédentes :

- L'intégration d'une modélisation contextuelle des dispositifs IoMT, avec des profils QoS différenciés selon la criticité médicale.
- La pondération dynamique des critères via la méthode AHP selon la priorité du dispositif.
- Le support de deux mécanismes de cryptographie asymétrique (ECC et RSA) pour l'établissement de la clé de session.
- Le maintien des cinq critères d'évaluation et de l'étape d'authentification présents dans les travaux les plus récents.

Ainsi, à l'instar de la démarche adoptée dans [77] (où l'ajout de l'authentification et d'un cinquième critère n'avait pas dégradé les performances globales) notre système ajoute une complexité fonctionnelle substantielle tout en réduisant le temps de convergence par rapport à l'ensemble des travaux antérieurs.

VIII.6. Scalabilité du Système

Cette section évalue le comportement du système face à la croissance du nombre d'utilisateurs primaires (PU) candidats. L'objectif est de déterminer comment les différentes composantes de la phase de négociation évoluent lorsque le nombre d'agents PU augmente, et d'identifier les éventuels goulots d'étranglement.

Cinq configurations ont été évaluées : $N = 5, 10, 20, 50$ et 100 agents PU. Conformément à la configuration de référence, un dispositif de type capteur portable (priorité non critique) a été utilisé. Ce choix garantit que la quasi-totalité des PU candidats satisfont les exigences QoS, permettant ainsi de mesurer la scalabilité intrinsèque du système plutôt que l'effet du filtrage QoS. Pour chaque valeur de N , dix exécutions ont été réalisées, puis moyennées.

N PUs	T1 (ms)	T2 (ms)	T3 (ms)	Négociation (ms)
5	14.50 ± 3.85	$< 1 (\approx 0)$	10.90 ± 2.12	25.40 ± 5.22
10	16.90 ± 1.97	$< 1 (\approx 0)$	9.90 ± 1.22	26.80 ± 2.82
20	25.90 ± 1.92	$< 1 (\approx 0)$	15.60 ± 6.15	41.50 ± 6.42
50	54.00 ± 9.37	$< 1 (\approx 0)$	15.90 ± 4.78	69.90 ± 9.47
100	88.30 ± 10.54	$< 1 (\approx 0)$	17.80 ± 1.25	106.10 ± 10.44

Tableau III.16 : Scalabilité des composantes de la phase de négociation

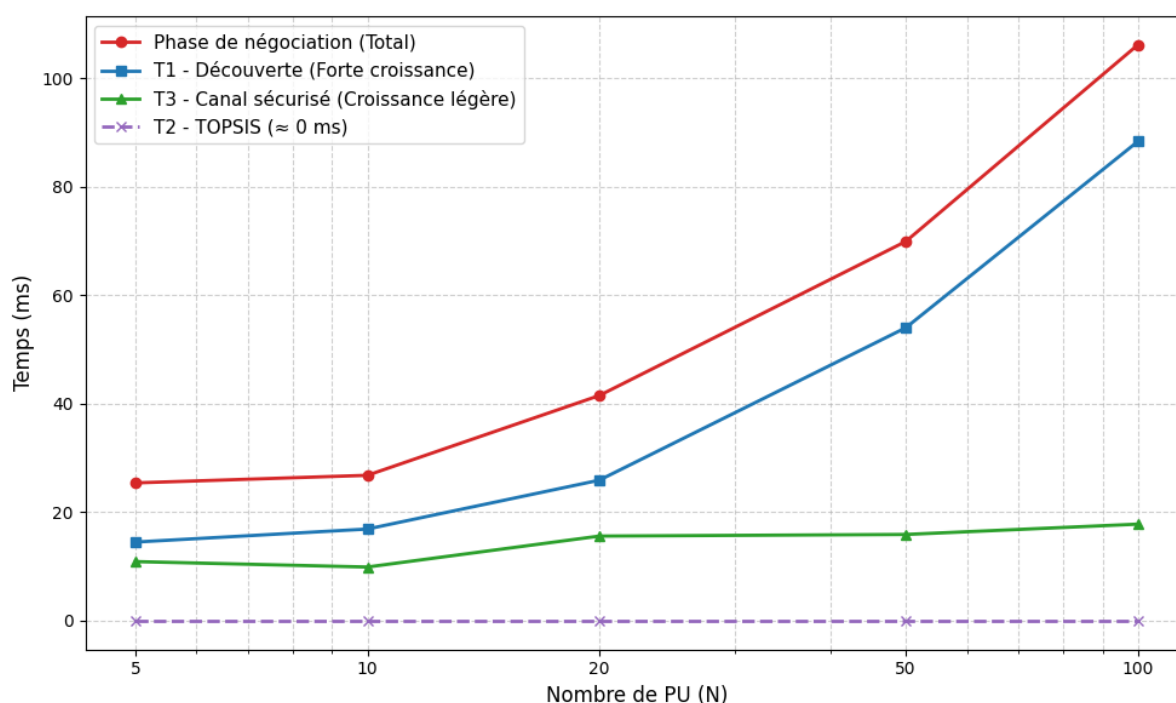


Figure III.13 : Évolution des composantes en fonction de N

Analyse des composantes

- **Découverte du spectre (T1) :** La latence de découverte croît de manière sensible avec le nombre de PU, passant de 14.50 ± 3.85 ms pour $N = 5$ à 88.30 ± 10.54 ms pour $N = 100$. Cette progression demeure néanmoins sous-linéaire : un facteur 20 sur le nombre d'agents

n'engendre qu'un facteur 6 environ sur le temps de découverte. Ce comportement reflète le fait que les agents PU répondent en parallèle au message Hello initial, le temps de découverte étant principalement déterminé par le PU le plus lent à répondre plutôt que par la somme des temps de réponse individuels.

- **Décision TOPSIS (T2) :** Le coût de la décision multicritère demeure inférieur à la milliseconde pour l'ensemble des configurations testées, y compris à $N = 100$ alternatives évaluées selon cinq critères. Ce résultat est particulièrement significatif : il établit que l'étape décisionnelle, cœur intellectuel du système, n'introduit aucune surcharge temporelle perceptible quelle que soit la densité du réseau. La méthode AHP-TOPSIS est donc parfaitement adaptée aux contraintes temps réel des applications IoMT.
- **Établissement du canal sécurisé (T3) :** Le temps d'établissement du canal sécurisé croît modérément avec N , passant de 10.90 ± 2.12 ms à $N = 5$ à 17.80 ± 1.25 ms à $N = 100$. Bien que cette étape ne concerne que le PU sélectionné, l'augmentation observée s'explique par la contention des ressources d'exécution : l'envoi des messages d'annulation (CANCEL) aux PU non retenus, simultanément à l'établissement du canal, sollicite davantage l'ordonnanceur lorsque le nombre d'agents augmente.
- **Phase de négociation globale :** La durée totale de la phase de négociation suit logiquement la dynamique de ses composantes, passant de 25.40 ± 5.22 ms à $N = 5$ à 106.10 ± 10.44 ms à $N = 100$. La croissance est sous-linéaire : multiplier le nombre de PU par 20 ne multiplie le temps total que par environ 4. La phase est dominée par la découverte (T1), qui représente la composante la plus sensible au nombre de PU.

Synthèse

Le système démontre une scalabilité satisfaisante jusqu'à 100 agents PU, l'ensemble du processus de négociation se complétant en environ 100 ms dans cette configuration extrême. Le principal facteur limitant identifié est la phase de découverte (T1), tandis que la décision multicritère (T2) reste essentiellement gratuite et que l'établissement du canal sécurisé (T3) ne souffre que marginalement de l'augmentation du nombre d'agents. Ces résultats confirment l'aptitude du système à fonctionner dans des environnements 5G denses, typiques des déploiements hospitaliers ou urbains où de nombreux utilisateurs primaires peuvent coexister.

IX. Conclusion

Ce chapitre a présenté la conception et l'évaluation expérimentale du système d'allocation dynamique multicritère du spectre pour l'IoMT.

Le système repose sur une architecture multi-agents JADE structurée autour des rôles Portail, SU, SU_Receiver et PU, communiquant via le langage ACL. La modélisation contextuelle des dispositifs IoMT, fondée sur deux classes de criticité associées à des profils QoS différenciés, alimente un cadre décisionnel combinant AHP pour la pondération dynamique des critères et TOPSIS pour le classement multicritère des offres de spectre. La cohérence des matrices de comparaison construites a été validée par des ratios CR bien inférieurs au seuil de Saaty. La sécurisation des communications repose sur deux mécanismes complémentaires de cryptographie asymétrique (ECC et RSA) assurant l'établissement d'une clé de session AES.

L'évaluation expérimentale a confirmé la pertinence de l'approche. L'analyse de la latence bout-en-bout, fondée sur cent exécutions, a mis en évidence la prédominance de la phase de négociation, tandis que la décision TOPSIS demeure inférieure à la milliseconde, y compris à grande échelle. La comparaison avec les travaux antérieurs a positionné favorablement notre contribution, malgré l'enrichissement fonctionnel apporté par la modélisation IoMT et la double cryptographie. Enfin, l'étude de scalabilité a démontré la capacité du système à fonctionner efficacement jusqu'à cent utilisateurs primaires avec une croissance sous-linéaire de la phase de négociation.

L'ensemble de ces résultats valide l'approche proposée pour l'allocation dynamique du spectre dans les réseaux radio cognitifs 5G appliqués à l'e-santé.

Conclusion générale

L'essor fulgurant de l'Internet des Objets Médicaux (IoMT) et la multiplication des dispositifs médicaux connectés ont fait de la gestion intelligente du spectre radioélectrique un enjeu critique pour la e-santé. Face à la congestion spectrale croissante et à l'inefficacité des méthodes d'allocation statique traditionnelles, les réseaux radio cognitifs 5G s'imposent comme une solution prometteuse, capable d'offrir un accès dynamique et opportuniste aux ressources spectrales tout en répondant aux exigences strictes de qualité de service des applications médicales critiques.

Dans ce cadre, ce travail a présenté la conception d'un système multi-agents sécurisé pour l'allocation dynamique multicritère du spectre dédié à l'IoMT.

Le premier chapitre a établi un état de l'art approfondi sur l'Internet des Objets Médicaux, couvrant son architecture, ses exigences spécifiques de QoS, ses contraintes de sécurité et ses défis spectraux dans le contexte des réseaux 5G et post-5G.

Le deuxième chapitre a présenté les fondements théoriques des réseaux radio cognitifs, des méthodes d'allocation dynamique du spectre, des approches multicritères et des systèmes multi-agents, constituant ainsi le socle sur lequel repose la solution proposée.

Le troisième chapitre a été consacré à la conception du système proposé, détaillant l'architecture multi-agents développée sur la plateforme JADE, la méthode AHP-TOPSIS adaptée au contexte médical avec cinq critères d'évaluation (prix, durée d'allocation, bande passante, latence et fiabilité), ainsi que les mécanismes de sécurité cryptographiques hybrides implémentés.

Les résultats obtenus ont démontré l'efficacité de l'approche proposée. La méthode AHP-TOPSIS a permis une allocation spectrale optimale et adaptative, prenant en compte les besoins spécifiques des dispositifs médicaux IoMT. La comparaison des deux modes de sécurité implémentés a révélé la supériorité de l'approche ECC+AES sur RSA+AES en termes de vitesse de traitement, justifiant son adoption pour les simulations finales. La comparaison avec les travaux de la littérature a confirmé que le système proposé offre une amélioration significative en termes de latence, validant ainsi sa pertinence pour les applications médicales critiques nécessitant des communications en temps réel.

Bibliographies

- [1] Mutua, J.M. and Bitok, H.J., 2025. The Internet of Medical Things (IoMT): A Comprehensive Review of Architecture, Enabling Technologies, Security Challenges, And Future Perspectives. *Engineering and Technology Journal*, 10(8), pp.145-160.
- [2] Ashton, K., 2009. That ‘internet of things’ thing. *RFID journal*, 22(7), pp.97-114.
- [3] Miorandi, D., Sicari, S., De Pellegrini, F. and Chlamtac, I., 2012. Internet of things: Vision, applications and research challenges. *Ad hoc networks*, 10(7), pp.1497-1516.
- [4] Istepanian, R.S., Hu, S., Philip, N.Y. and Sungoor, A., 2011, August. The potential of Internet of m-health Things “m-IoT” for non-invasive glucose level sensing. In *2011 annual international conference of the IEEE engineering in medicine and biology society* (pp. 5264-5266). IEEE.
- [5] Islam, S.R., Kwak, D., Kabir, M.H., Hossain, M. and Kwak, K.S., 2015. The internet of things for health care: a comprehensive survey. *IEEE access*, 3, pp.678-708.
- [6] Aceto, G., Persico, V. and Pescapé, A., 2020. Industry 4.0 and health: Internet of things, big data, and cloud computing for healthcare 4.0. *Journal of Industrial Information Integration*, 18, p.100129
- [7] Saha, J. and Sen, R., 2024. IoT vs IoMT—A comparative study based on knowledge among medical professionals. *Int. J. Multidiscip. Educ. Res*, 13, pp.99-109.
- [8] Rahmani, M.K.I., Shuaib, M., Alam, S., Siddiqui, S.T., Ahmad, S., Bhatia, S. and Mashat, A., 2022. [Retracted] Blockchain-Based Trust Management Framework for Cloud Computing-Based Internet of Medical Things (IoMT): A Systematic Review. *Computational Intelligence and Neuroscience*, 2022(1), p.9766844.
- [9] Ashfaq, Z., Rafay, A., Mumtaz, R., Zaidi, S.M.H., Saleem, H., Zaidi, S.A.R., Mumtaz, S. and Haque, A., 2022. A review of enabling technologies for Internet of Medical Things (IoMT) Ecosystem. *Ain Shams Engineering Journal*, 13(4), p.101660.
- [10] L. Sun, X. Jiang, H. Ren, and Y. Guo, "Edge-cloud computing and artificial intelligence in internet of medical things: architecture, technology and application," *IEEE Access*, vol. 8, pp. 101079–101092, 2020.
- [11] F. Muheidat and L. A. Tawalbeh, “Aiomt artificial intelligence (ai) and internet of medical things (iomt) : applications, challenges, and future trends,” in Computational
- [12] Chaaben, A.B., 2022. A survey of different IoMT protocols for healthcare applications. *ResearchBerg Review of Science and Technology*, 2(1), pp.41-57.
- [13] Ouakasse, F., Mosaif, A. and Rakrak, S., 2024. A QoS-gateway-based framework for prioritizing emergency data in IoMT applications. *Ingénierie des Systemes d'Information*, 29(1), p.369.
- [14] Garg, N., Wazid, M., Singh, J., Singh, D.P. and Das, A.K., 2022. Security in IoMT-driven smart healthcare: A comprehensive review and open challenges. *Security and Privacy*, 5(5), p.e235.

- [15] Manoharan, A. and Thathan, M., 2024. Enhanced IoMT security framework using group teaching optimized auto-encoder for intrusion detection. *Scientific Reports*, 14(1), p.30360.
- [16] Koutras, D., Stergiopoulos, G., Dasaklis, T., Kotzanikolaou, P., Glynos, D. and Douligeris, C., 2020. Security in IoMT communications: A survey. *Sensors*, 20(17), p.4828.
- [17] Al-Shabi, M.A., 2019. A survey on symmetric and asymmetric cryptography algorithms in information security. *International Journal of Scientific and Research Publications (IJSRP)*, 9(3), pp.576-589.
- [18] Jenifer, R.R. and Prakash, V.S.J., 2024. Rivest-Shamir-Adleman algorithm optimized to protect iot devices from specific attacks. *Информатика и автоматизация*, 23(5), pp.1423-1453.
- [19] Smid, M.E., 2021. Development of the advanced encryption standard. *Journal of Research of the National Institute of Standards and Technology*, 126, p.126024.
- [20] Abdullah, A.M., 2017. Advanced encryption standard (AES) algorithm to encrypt and decrypt data. *Cryptography and Network Security*, 16(1), p.11.
- [21] Alhassan, A.B., Mahama, A.H. and Alhassan, S., 2022. Residue architecture enhanced audio data encryption scheme using the rivest, shamir, adleman algorithm.
- [22] Yan, Y., 2022, December. The overview of elliptic curve cryptography (ECC). In *Journal of Physics: Conference Series* (Vol. 2386, No. 1, p. 012019). IOP Publishing.
- [23] Iqbal, A., Nauman, A., Qadri, Y.A. and Kim, S.W., 2025. Optimizing spectral utilization in healthcare internet of things. *Sensors*, 25(3), p.615.
- [24] Hernandez-Jaimes, M.L., Martinez-Cruz, A., Ramírez-Gutiérrez, K.A. and Feregrino-Uribe, C., 2023. Artificial intelligence for IoMT security: A review of intrusion detection systems, attacks, datasets and Cloud–Fog–Edge architectures. *Internet of Things*, 23, p.100887.
- [25] Zhang, C. and Su, L., 2024, June. An IoMT Framework Integrating 5G and Wireless Body Area Networks for Home Healthcare. In *Proceedings of the 2024 3rd International Conference on Networks, Communications and Information Technology* (pp. 166-171).
- [26] Islam, M., 2019. An overview research on wireless communication network. *Advances in Wireless Communications and Networks*.
- [27] Benmammar, Badr, and Asma Amraoui. "Réseaux de radio cognitive: Allocation des ressources radio et accès dynamique au spectre." arXiv preprint arXiv:1407.2705 (2014).
- [28] Qu, Y., Zheng, G., Ma, H., Wang, X., Ji, B. and Wu, H., 2019. A survey of routing protocols in WBAN for healthcare applications. *Sensors*, 19(7), p.1638.
- [29] Yaghoubi, M., Ahmed, K. and Miao, Y., 2022. Wireless body area network (WBAN): A survey on architecture, technologies, energy consumption, and security challenges. *Journal of Sensor and Actuator Networks*, 11(4), p.67.

- [30] Koriipi, M., 2021. A review on secure communications and wireless personalarea networks (WPAN). *Wutan Huatan Jisuan Jishu*, 17.
- [31] Parashar, V., Kashyap, R., Rizwan, A., Karras, D.A., Altamirano, G.C., Dixit, E. and Ahmadi, F., 2022. Aggregation-based dynamic channel bonding to maximise the performance of wireless local area networks (WLAN). *Wireless Communications and Mobile Computing*, 2022(1), p.4464447.
- [32] Skosana, S., Mlambo, S., Madiope, T. and Thango, B., 2024. Evaluating wireless network technologies (3G, 4G, 5G) and their infrastructure: A systematic review. *Available at SSRN 4992432*.
- [33] Shabir, A., Kanwal, K., Ayesha, H., Almas, A., Raza, S. and Jaffar, S., 2024. A hybrid cognitive radio reporting scheme for wireless regional area networks. *Journal of Computing & Biomedical Informatics*.
- [34] Cullen, A.C., Rubinstein, B.I., Kandeepan, S., Flower, B. and Leong, P.H., 2023. Predicting dynamic spectrum allocation: a review covering simulation, modelling, and prediction. *Artificial Intelligence Review*, 56(10), pp.10921-10959.
- [35] Nassa, V.K., 2011. Wireless communications: Past, present and future. *Dronacharya Research Journal*, 50.
- [36] Mitola, Joseph. "The software radio architecture." IEEE Communications magazine 33.5 (1995) : 26-38.
- [37] Mitola, J., 1999, November. Cognitive radio for flexible mobile multimedia communications. In *1999 IEEE International Workshop on Mobile Multimedia Communications (MoMuC'99)(Cat. No. 99EX384)* (pp. 3-10). IEEE.
- [38] Haykin, S., 2005. Cognitive radio: brain-empowered wireless communications. *IEEE journal on selected areas in communications*, 23(2), pp.201-220.
- [39] Akeela, R. and Dezfouli, B., 2018. Software-defined Radios: Architecture, state-of-the-art, and challenges. *Computer Communications*, 128, pp.106-125.
- [40] Jondral, F.K., 2005. Software-defined radio—basics and evolution to cognitive radio. *EURASIP journal on wireless communications and networking*, 2005(3), p.652784.
- [41] Gupta, M.S. and Kumar, K., 2019. Progression on spectrum sensing for cognitive radio networks: A survey, classification, challenges and future research issues. *Journal of Network and Computer Applications*, 143, pp.47-76.
- [42] Mijwil, M.M., 2023. Unlocking the full potential of spectrum: a comprehensive review of cognitive radio technology. *Mesopotamian Journal of Computer Science*, 2023, pp.64-71.
- [43] Kassri, N., Ennouaary, A., Bah, S., & Baghdadi, H. (2021). A review on SDR, spectrum sensing, and CR-based IoT in cognitive radio networks. *International Journal of Advanced Computer Science and Applications*, 12(6).

- [44] Manco, J., Dayoub, I., Nafkha, A., Alibakhshikenari, M., & Thameur, H. B. (2022). Spectrum sensing using Software Defined Radio for cognitive radio networks: A survey. *IEEE Access*, 10, 131887-131908.
- [45] Larbi, I., & Benmammar, B. (2014). Négociation de spectre dans les réseaux de radio cognitive. *arXiv preprint arXiv:1407.2217*.
- [46] Nurmi, J. and Perera, D.G., 2021, October. Intelligent cognitive radio architecture applying machine learning and reconfigurability. In *2021 IEEE Nordic circuits and systems conference (NorCAS)* (pp. 1-6). IEEE.
- [47] Manco, J., Dayoub, I., Nafkha, A., Alibakhshikenari, M. and Thameur, H.B., 2022. Spectrum sensing using software defined radio for cognitive radio networks: A survey. *IEEE Access*, 10, pp.131887-131908.
- [48] Idris, M.Y.I., Ahmedy, I., Soon, T.K., Yahuza, M., Tambuwal, A.B. and Ali, U., 2024. Cognitive radio and machine learning modalities for enhancing the smart transportation system: A systematic literature review. *ICT express*, 10(4), pp.693-734.
- [49] Moawad, A. (2020). Enhancement of spectrum sensing in cognitive radio: providing reliable spectral opportunities (These de Doctorat, Université de Bretagne occidentale-Brest).
- [50] Nasser, A., Al Haj Hassan, H., Abou Chaaya, J., Mansour, A. and Yao, K.C., 2021. Spectrum sensing for cognitive radio: Recent advances and future challenge. *Sensors*, 21(7), p.2408.
- [51] Taherdoost, H. and Madanchian, M., 2023. Multi-criteria decision making (MCDM) methods and concepts. *Encyclopedia*, 3(1), pp.77-87.
- [52] Parvin, S., Hussain, F.K., Hussain, O.K., Han, S., Tian, B. and Chang, E., 2012. Cognitive radio network security: A survey. *Journal of Network and Computer Applications*, 35(6), pp.1691-1708.
- [53] Hamood, A.S. and Sadkhan, S.B., 2017, March. Cognitive radio network security status and challenges. In *2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT)* (pp. 1-6). IEEE.
- [54] Jahangeer, A., Bazai, S.U., Aslam, S., Marjan, S., Anas, M. and Hashemi, S.H., 2023. A review on the security of IoT networks: From network layer's perspective. *IEEE Access*, 11, pp.71073-71087.
- [55] Angueira, P., Val, I., Montalban, J., Seijo, Ó., Iradier, E., Fontaneda, P.S., Fanari, L. and Arriola, A., 2022. A survey of physical layer techniques for secure wireless communications in industry. *IEEE Communications Surveys & Tutorials*, 24(2), pp.810-838.
- [56] Khoei, T.T., Slimane, H.O. and Kaabouch, N., 2022. A comprehensive survey on the cyber-security of smart grids: Cyber-attacks, detection, countermeasure techniques, and future directions. *arXiv preprint arXiv:2207.07738*.
- [57] Dorri, A., Kanhere, S.S. and Jurdak, R., 2018. Multi-agent systems: A survey. *Ieee Access*, 6, pp.28573-28593.

- [58] Xie, J. and Liu, C.C., 2017. Multi-agent systems and their applications. *Journal of International Council on Electrical Engineering*, 7(1), pp.188-197.
- [59] Samigulina, G.A., Nyusupov, A.T. and Shayakhmetova, A.S., 2018. Analytical review of software for multi-agent systems and their applications. *News of the National Academy of Sciences of the Republic of Kazakhstan, Series of Geology and Technical Sciences*.-3 (429), pp.173-181.
- [60] Haldorai, A. and Kandaswamy, U., 2019. Intelligent cognitive radio communications: A detailed approach. In *Intelligent Spectrum Handovers in Cognitive Radio Networks* (pp. 19-40). Cham: Springer International Publishing.
- [61] Khasawneh, M., Azab, A., Alrabaei, S., Sakkal, H. and Bakhit, H.H., 2023. Convergence of IoT and cognitive radio networks: A survey of applications, techniques, and challenges. *Ieee Access*, 11, pp.71097-71112.
- [62] Rachakonda, L.P., Siddula, M. and Sathya, V., 2024. A comprehensive study on IoT privacy and security challenges with focus on spectrum sharing in Next-Generation networks (5G/6G/beyond). *High-Confidence Computing*, 4(2), p.100220.
- [63] Nikraz, M., Caire, G. and Bahri, P.A., 2006. A methodology for the analysis and design of multi-agent systems using JADE. *International Journal of Computer Systems Science and Engineering*, 21(2), pp.1-40.
- [64] <https://fr.wikipedia.org/wiki/NetBeans> (dernière consultation le 14/06/2026)
- [65] Samigulina, G.A., Nyusupov, A.T. and Shayakhmetova, A.S., 2018. Analytical review of software for multi-agent systems and their applications. *News of the National Academy of Sciences of the Republic of Kazakhstan, Series of Geology and Technical Sciences*.-3 (429), pp.173-181.
- [66] NASIR, N., ITO, T. and HASHIM, A.Y.B., 2015. Agent-Based Communication in JADE Platform for Manufacturing Processes.
- [67] Popovski, P., Trillingsgaard, K.F., Simeone, O. and Durisi, G., 2018. 5G wireless network slicing for eMBB, URLLC, and mMTC: A communication-theoretic view. *Ieee Access*, 6, pp.55765-55779.
- [68] Soldani, D., Fadini, F., Rasanen, H., Duran, J., Niemela, T., Chandramouli, D., Hoglund, T., Doppler, K., Himanen, T., Laiho, J. and Nanavaty, N., 2017, June. 5G mobile systems for healthcare. In *2017 IEEE 85th vehicular technology conference (VTC Spring)* (pp. 1-5). Ieee.
- [69] Cisotto, G., Casarin, E. and Tomasin, S., 2020. Requirements and enablers of advanced healthcare services over future cellular systems. *IEEE Communications Magazine*, 58(3), pp.76-81.
- [70] Saaty, T.L., 2008. Decision making with the analytic hierarchy process. *International journal of services sciences*, 1(1), pp.83-98.
- [71] Gupta, R., Tanwar, S., Tyagi, S. and Kumar, N., 2019. Tactile-internet-based telesurgery system for healthcare 4.0: An architecture, research challenges, and future directions. *IEEE network*, 33(6), pp.22-29.

- [72] Ahad, A., Tahir, M. and Yau, K.L.A., 2019. 5G-based smart healthcare network: architecture, taxonomy, challenges and future research directions. *IEEE access*, 7, pp.100747-100762.
- [73] Velmurugan, R., Selvamuthukumar, S. and Manavalan, R., 2011. Multi criteria decision making to select the suitable method for the preparation of nanoparticles using an analytical hierarchy process. *Die Pharmazie-An International Journal of Pharmaceutical Sciences*, 66(11), pp.836-842.
- [74] Mohaghar, A., 2013. Developing TOPSIS method using statistical normalization for selecting knowledge management strategies. *Journal of industrial engineering and management*.
- [75] Baba-Ahmed, M.Z., Tahraoui, S., Sedjelmaci, A., Bouregaa, M. and Rabah, M.A., 2019, November. Self-management of autonomous agents dedicated to cognitive radio networks. In *International Conference in Artificial Intelligence in Renewable Energetic Systems* (pp. 372-380). Cham: Springer International Publishing.
- [76] Seghiri, N., Baba-Ahmed, M.Z., Benmammar, B. and Houari, N., 2021. Optimization of a Multi-criteria Cognitive Radio User Through Autonomous Learning. In *Networking, Intelligent Systems and Security: Proceedings of NISS 2021* (pp. 117-132). Singapore: Springer Singapore.
- [77] Naouel, S., Zakarya, B.A.M., Badr, B., Nadhir, H., Kamal, K.M. and Ayyoub, A.M., 2022. Data security of a cognitive radio network for multicriteria secondary users. *Journal of Electrical and Electronics Engineering*, 15(2), pp.82-87.