الجـــــــــــــــــــــــمهـوريـــــة الجـــــــــــــزائـريـة الديمـــــــقـراطيـة الشـــــــــعبيـة

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

وزارة التـــــــــــــــــــــــــــعـليـم العـــــــالي و البـــــــــحث العـــــلـمـــي

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جـــــــــــــــامعة أبي بكـــر بـلـقـايد– تـلمســـــــــــــان –

Université Aboubakr Belkaïd– Tlemcen –

Faculté de TECHNOLOGIE

MEMOIRE

Présenté pour l'obtention du

MASTER EN TELECOMMUNICATIONS

En : **TELECOMMUNICATIONS**

Spécialité : Réseaux et Télécommunications

Par:

BENLALDJ ZAKARIA

BOUZAHRI MOHAMMED CHAMS EDDINE

Thème

Conception d'un protocole d'authentification dédié à la détection des utilisateurs malveillants dans les réseaux radio cognitifs

Soutenu publiquement, le **27 /06 /2022**, devant le jury composé de :

Mr.M.HADIJALA	MCA	Université de Tlemcen	Président
Mme.N.SELADJI	MCB	Université de Tlemcen	Examinateur
Mr.M.Z BABA-AHMED	MCA	Université de Tlemcen	Encadreur
Mme.N SEGHIRI	Doctorant	Université de Tlemcen	Co-Encadreur

Année universitaire : **2021 / 2022**

Remerciements...

Tout d'abord, nous levons les mains bien haut vers le ciel, remerciant **ALLAH** Tout-Puissant, qui nous a donné force et santé pour mener à bien ce travail.

Je souhaite avant tout remercier notre encadreur de mémoire, **Mr BABA AHMED Mohammed Zakarya**, pour le temps qu'il a consacré à nous apporter les outils méthodologiques indispensables à la conduite de cette recherche. Son exigence nous a grandement stimulé.

Je tiens à témoigner toute ma reconnaissance aux personnes suivantes, pour leur aide dans la réalisation de ce mémoire :

Mr HOUARI Nadhir, pour nous avoir accordé des entretiens et avoir répondu à nos questions, ainsi que son expérience personnelle. Il a été d'un grand soutien dans l'élaboration de ce mémoire.

Mme SGHIRI Nawel, notre Co-encadreur qui nous a beaucoup appris sur les défis à relever dans le monde de télécommunication. Elle a partagé ses connaissances et expériences dans ce milieu, tout en nous accordant sa confiance et une large indépendance dans l'exécution de missions valorisantes.

Un autre remerciement au comité des jurys constitué de **Mr HADJILA Mourad** et de **Mme SELADJI Nawel** pour avoir accepté de présider et d'examiner notre projet de fin d'étude, sans oublier la famille, les parents et amis qui étaient et sont toujours un atout moral pour nous.

DEDICACES 1

A ma très chère mère

Quoi que je fasse ou que je dise, je ne saurai point te remercier comme il se doit. Ton affection me couvre, ta bienveillance me guide et ta présence à mes côtés a toujours été ma source de force pour affronter les différents obstacles.

A mon très cher père

Tu as toujours été à mes côtés pour me soutenir et m'encourager. Que ce travail traduit ma gratitude et mon affection.

A mes frères

Ceux qui ont partagé avec moi tous les moments d'émotion lors de la réalisation de ce travail, ils m'ont chaleureusement supporté et encouragé tout au long de mon parcours.

A mon oncle maternel ASSANI KHALED et toute la famille AISSANI

Merci pour votre soutien dans mon parcours universitaire

A mes collègues

Mon binôme BOUZAHRI CHEMSOU, Dali Youcef Mehdi et Belaidi Hichem, Ismail, Hichem, Mahir, Walid, Amine

A ma famille, mes proches et a tous ceux qui me donnent de l'amour et de la vivacité.

BENLALDJ ZAKARIA

DEDICACES 2

<u>À ma raison de vivre, ma chère mère BENYAHIA.H</u>

Qui m'a entouré d'amour, d'affection et qui fait tout pour mon succès, que Dieu la garde pour moi, merci beaucoup maman

<u>À l'âme de mon père BOUZAHRI ABDELAZIZ</u>

Que Dieu ait pitié de lui et le met dans son paradis

<u>À ma sœur BOUZAHRI.M</u>

Je te souhaite une vie heureuse pleine de succès

<u>À ma grand-mère</u>

Que Dieu la garde pour moi

<u>À mon oncle maternel ANOUAR BENYAHIA et sa femme HADJIDJ.S</u>

Merci pour tous vos efforts, et merci de m'avoir aidé à chaque étape de ma vie

<u>À mon oncle paternel BOUZAHRI MOHAMMED et mes cousins</u>

Merci pour tout.

<u>À tout la famille BEYAHIA</u>

Merci à vous.

<u>À tous mes amis</u>

Merci de m'avoir aidé dans les moments difficiles.

<u>À mes collègues</u>

Mon binôme Zakaria Benlaldj, Mehdi Dali Youcef, Hichem Belaidi et tous les amis de la promo télécommunication réseaux

Merci pour les beaux souvenirs

<u>CHEMSOU BOUZAHRI</u>

Résumé

La gestion dynamique et sécurisée du spectre radio devient un réel problème pour les réseaux radio. Divers facteurs peuvent causer des dommages et des interférences entre différents utilisateurs du même spectre radio. Dans le monde de la radio cognitive, on distingue deux catégories de réseaux, à savoir les réseaux primaires. Qui ont priorité et contrôle sur l'accès au spectre radioélectrique, et les secondaires, appelés réseaux radio cognitifs, qui allouent dynamiquement le spectre. Nous concentrons sur l'authentification honnête des utilisateurs primaires ayant une licence sur le spectre pour assurer la sécurité et la QoS des utilisateurs secondaires. Notre approche consiste à utiliser un système multi-agents basé sur un apprentissage autonome et axé sur un environnement cognitif compétitif.

Dans ce projet de fin d'étude, nous évaluons les performances de l'utilisateur secondaire dans un environnement idéal des systèmes radio cognitifs. Nous utilisons la plate-forme multi-agents appelée JADE, dans laquelle nous implémentons un algorithme de cryptage asymétrique qui applique l'authentification et la sécurité du partage des données entre utilisateurs dans les réseaux radio cognitifs.

Mots clés : Réseaux radio cognitifs, Authentification, Sécurité, Systèmes multi-agents, cryptage asymétrique.

Abstract

The dynamic and secure management of the radio spectrum becomes a real problem for radio networks. Various factors can cause damage and interference between different users of the same radio spectrum. In the world of cognitive radio, there are two categories of networks, namely primary networks, which have priority and control over access to the radio spectrum, and secondary networks, called cognitive radio networks, which dynamically allocate the spectrum. we focus on honest authentication of licensed primary users on the spectrum to ensure security and QoS (quality of service) of secondary users. Our approach is to use a multi-agent system based on autonomous learning and focused on a competitive cognitive environment.

In this thesis, we evaluate the performance of the secondary user in an ideal environment of cognitive radio systems; we use the multi-agent platform called JADE (Java Agent Development), in which we implement an asymmetric encryption algorithm that enforces authentication and security of user-to-user data sharing in cognitive radio networks.

Keywords: Cognitive radio networks, authentication, security, multi-agent systems, asymmetric encryption.

الملخص

أصبحت الإدارة الديناميكية والآمنة للطيف الراديوي مشكلة حقيقية لشبكات الراديو. بامكانها أن تسبب العديد من العوامل الضرر والتداخل بين مختلف المستخدمين من نفس الطيف الراديوي. في عالم الراديو المعرفي ، هناك فئتان من الشبكات ، وهما الشبكات الأولية ، والتي لها الأولوية والتحكم في الوصول إلى الطيف الراديوي ، والشبكات الثانوية ، والتي تسمى شبكات الراديو المعرفية ، والتي تخصص الطيف بشكل ديناميكي ، ونحن نركز على الصدق. مصادقة المستخدمين الأساسيين المرخصين على الطيف لضمان الأمن وجودة الخدمة (جودة الخدمة) للمستخدمين الثانويين. نهجنا هو استخدام نظام متعدد الوكلاء يعتمد على التعلم المستقل ويركز على بيئة معرفية تنافسية. في مشروع نهاية الدراسة هذا ، نقوم بتقييم أداء المستخدم الثانوي في بيئة مثالية لأنظمة الراديو الإدراكية ؛ استخدام النظام الأساسي متعدد الوكلاء المسمى JADE (تطوير وكيل Java) ، والذي نطبق فيه خوارزمية تشفير غير متماثل تفرض المصادقة والأمن لمشاركة البيانات بين المستخدمين في شبكات الراديو الإدراكية.

الكلمات المفتاحية: شبكات الراديو المعرفية ،المصادقة ، الأمن ، الأنظمة متعددة الوكلاء ، التشفير غير المتماثل.

Table des matières

Table des matières

Chapitre 1 : La technologie de la Radio Cognitive

Chapitre 2 : SMA et Algorithme d'Authentification dans les RRC

Chapitre 3 : SMA et Algorithme d'Authentification dans les RRC

Chapitre 4 : Résultats des allocations dynamiques et sécurisées des réseaux RC

Lise des tableaux

Acronymes et abréviations

AACR **Aware, Adaptive and Cognitive Radio**

ACl **Agent Communication Language**

AES **Advanced Encryption Standard**

AP **Access Point**

AMS **Agent Management System**

BSS **Basic Service Set**

BS **Bande Spectrale**

BDI **Beliefs-Desires-Intentions**

CCSD **Control Channel Saturation DoSAttack**

CORBA **Common Object Request Broker Architecture**

CSMA **Carrier Sensing Multiple Access**

CDDL **Common Development and Distribution License**

DLP **Discrete Logarithm Problem**

DECT **Digital Enhanced Cordless Telecommunications**

DoS **Deny of Service**

DRT **Test du Rapport de Distance**

DF **Director Facilitor**

DDT **Test de Différence de Distance**

DES **Data Encryption Standard**

DSA **Digital Signature Algorithm**

DH **Diffie-Hellman**

ETSI **European Telecommunications Standards Institute**

EDI **Environnement de Développement Intégré**

EMI **Interférences Electro-Magnétiques**

EMC **Compatibilité Electro-Magnétique**

EDE **Encryption, Decryption, Encryption**

ECC ***Elliptic Curve Cryptography***

ECMQV **Elliptic Curve Menezes Qu Vanstone**

ECDH **Elliptic Curve Diffie-Hellman**

ECDLP **Elliptic Curve Discrete Logarithm Problem**

ECDHP **Courbe Elliptique Diffie-Hellman Problème**

ECB **Electronic Code Book**

ECIES	**Elliptic Curve Integrated Encryption Scheme**
ECDSA	**Elliptic Curve Digital Signature Algorithm**
FCC	**Federal Communications Commission**
FIPA	**Foundation for Intelligent Physical Agents**
Fu	**Fusion Center**
GSM	**Global System for Mobile Communications**
GPRS	**General Packet Radio Service**
IEEE	**Institute of Electrical and Electronics Engineers**
ICT	**Information and Communication Technologies**
ITU	**Union Internationale des Télécommunications**
IBSS	**Independent Basic Service Set**
IDL	**Langage de Définition d'Interface**
ISM	**Industriel, Scientifique et Médicale**
IA	**Intelligence Artificielle**
JDK	**Java Development Kit**
JADE	**Java Agent DEveloppement Framework**
KQML	**Knowledge Query and Manipulation Language**
KIF	**Knowledge Interchange Format**
KDF	**Key Derivation Function**
LCC	**Location Consistency Checks**
LocDef	**Localization Based Defense**
LGPL	**Lesser General Public License**
MAC	**Media Access Control**
MSU	**Malicious Secondary User**
MU	**Malicious User**
MADM	**Multiple Attribute Decision Making**
NIST	**National Institute of Standards and Technology**
OFDMA	**Orthogonal Frequency Division Multiple Access**
PU	**Utilisateur Primaire**
PUE	**Emulation de l'Utilisateur Primaire**
PDR	**Packet Delivery Ratio**
QoS	**Quality of Service**
RSA	**Rivest Shamir Adleman**
RC	**Radio Cognitive**

RKRL **Radio Knowledge Representation Language**

RCN **Radio Cognitive Network**

RFF **Réseau Ferré de France**

RRC **Réseaux Radio Cognitifs**

SB **Station de Base**

SDR **Software Defined Radio**

SPARC **Scalable Processor ARChitecture**

SU **Utilisateur Secondaire**

SCC41 **Standards Coordinating Committee 41**

SP **Sensory Perception**

SS **Signal Strength**

SSDF **Spectrum Sensing Data Falsification**

SDF **Several Data Fusion**

SCN **Selfish Channel Negociation**

SEAD **Secure Efficient Adhoc Distance Vector**

SMA **Systèmes Multi-Agents**

SSL ***Secure Socket Layer***

TILAB **Groupe de recherche de Gruppo Telecom, Italie**

TOPSIS **Technique for Order Preference by Similarity to Idéale Solution**

UWB **Ultra Wide Band**

UM **Unités Mobiles**

WSN **Wireless Sensor Network**

WMAN **Wireless Metropolitan Area Network**

WIMAX **Worldwide Interoperability for Microwave Access**

WWAN **Wireless Wide Area Network**

WRAN **Wireless Regional Area Network**

WBAN **Wireless Body Area Network**

WPAN **Wireless Personal Area Network**

WLAN **Wireless Local Area Network**

WSRT **Weighted Sequential Ratio Test**

Introduction Générale

Nous assistons actuellement à la multiplication des normes et des standards de télécommunication vu les progrès récents dans ce domaine. Le nombre croissant de standards normalisés permet d'élargir l'éventail des offres et des services disponibles pour chaque consommateur, d'ailleurs, la plupart des radiofréquences disponibles ont déjà été allouées.

Une étude réalisée par la Fédérale Communications Commission (FCC) a montré que certaines bandes de fréquences sont partiellement occupées dans des emplacements particuliers et à des moments particuliers. Et c'est pour toutes ces raisons que la Radio Cognitive (RC) est apparue.

L'idée de la RC est de partager le spectre entre un utilisateur dit primaire, et un utilisateur dit secondaire. L'objectif principal de cette gestion du spectre consiste à obtenir un taux maximum de l'exploitation du spectre radio.

Pour que cela fonctionne, l'utilisateur secondaire doit être capable de détecter l'espace blanc, de se configurer pour transmettre, de détecter le retour de l'utilisateur primaire et ensuite cesser de transmettre et chercher un autre espace blanc.

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

Les réseaux RC doivent pouvoir coexister pour rendre les systèmes de la RC pratiques, ce qui peut générer des interférences aux autres utilisateurs. Afin de traiter ce problème, l'idée de la coopération entre les utilisateurs pour détecter et partager le spectre sans causer d'interférences est mise en place.

Nous considérons la coopération comme une attitude adoptée par les agents qui décident de travailler ensemble. Dans le cas de la RC, avant de faire la coopération il faut passer par une autre étape « la négociation », car il y a plusieurs utilisateurs qui veulent satisfaire leurs besoins.

Par rapport aux réseaux sans fil classiques, les réseaux RC sont en outre soumis à une émulation d'utilisateurs autorisés et à des attaques contre les gestionnaires du spectre, à moins que des mécanismes de sécurité robustes ne soient mis en place. L'un des types les plus courants d'attaques dans les réseaux RC est l'attaque d'émulation de l'utilisateur primaire (un utilisateur primaire malicieux).

Puisque le spectre du RRC est ciblé par les attaques du réseau radio cognitif, donc il faut des solutions et des approches à suivre pour une utilisation fiable et optimale de cette technologie.

Dans le premier chapitre, nous donnerons un aperçu des réseaux sans fil et mobiles, et nous parlerons en particulier sur la technologie radio cognitive avec l'aspect de la sécurité dans ses réseaux.

Dans le deuxième chapitre, nous aborderons d'abord les systèmes multi-agents, puis la sécurité dans les réseaux radio cognitifs et le concept de chiffrement et déchiffrement et les différents protocoles d'authentification qui peuvent nous aider à renforcer les systèmes radio cognitive.

Dans le troisième chapitre, nous allons décrire les algorithmes utilisés pour notre approche à savoir ceux de l'authentification, du multicritère de choix ainsi du mode de chiffrement ainsi que l'organigramme proposé.

Le quatrième et dernier chapitre, sera consacré aux résultats de simulations des réseaux radio cognitive avec une chaine d'authentification et de chiffrement des données avec les utilisateurs honnêtes et malicieux ainsi le choix du meilleur utilisateur primaire à partager le spectre avec lui, terminant avec une comparaison avec d'autres travails réalisés auparavant.

Nous terminons notre PFE avec une conclusion et des perspectives pour de prochaines études.

Chapitre 1

La technologie de la Radio Cognitive

Sommaire

1.1 Introduction

La radio cognitive est une nouvelle génération de réseaux caractérisé par l'intelligence par rapport à ses ancêtres, avec l'avantage de pouvoir collecter des informations dans des environnements sur les réseaux (WLAN, GSM/HSPA, LTE, WiMax, TV, Réseaux Militaires) et d'utiliser leurs bandes de fréquences pour maximiser le débit des utilisateurs. L'avènement de cette technologie nous a également ouvert les yeux sur le domaine de la sécurité, car ce réseau présente de nombreuses faiblesses en termes de sécurité.

Dans ce chapitre on va parler brièvement sur le réseau sans fil, puis donner une vue générale sur la technologie de radio cognitive, son principe de fonctionnement, ses composants, son impact et ses domaines d'application, ensuite nous évoquerons la sécurité dans les Réseaux Radio Cognitifs (RRC) et quelques menaces qui peuvent les attaquer.

1.2 Réseau sans fil

1.2.1 Définition

Un réseau sans fil (Wireless network), comme son nom l'indique est un réseau dans lequel au moins deux terminaux peuvent communiquer sans liaison filaire. Un réseau local sans fil véhicule les informations soit par infrarouge, soit par onde radio, Soit par onde ultra-violet ou rayon X et Gamma [1].

La transmission par onde radio est la méthode la plus répandue en raison de sa plus large couverture géographique et d'autre part, par son débit qui est plus grand par rapport à celui de l'infrarouge. Les réseaux sans fil permettent de relier très facilement des équipements distants d'une dizaine de mètres à quelques kilomètres. De plus, l'installation de tels réseaux ne demande pas de lourds aménagements des infrastructures comme c'est le cas avec les réseaux filaires, ce qui a valu un développement rapide de ce type de technologies. Les transmissions radioélectriques servent pour un grand nombre d'applications, mais sont sensibles aux interférences, c'est la raison pour laquelle une réglementation est nécessaire dans chaque pays afin de définir les plages de fréquences et les puissances auxquelles il est possible d'émettre pour chaque catégorie d'utilisation [2].

1.2.2 Catégories de réseaux sans fils

Les réseaux sans fil sont en plein développement du fait de la flexibilité de leur interface, qui permet à un utilisateur de changer de place tout en restant connecté. Plusieurs gammes de produits sont actuellement commercialisés, mais la normalisation pourrait encore modifier les choses. Les groupes de travail qui se chargent de cette normalisation proviennent de l'IEEE (Institute of Electrical and Electronics Engineers) est une association regroupant des milliers de professionnels du domaine de l'informatique et des télécommunications à travers le monde. Son objectif principal se résume à la promotion de la connaissance dans le domaine de l'ingénierie électrique et électronique aux Etats-Unis.et de l'ETSI (European Telecommunications Standards Institute), est un organisme de normalisation indépendant et à but non lucratif, qui produit des normes pour l'industrie des technologies de l'information et de la communication (ICT).L'ETSI est responsable du développement et des tests des normes techniques applicables aux systèmes, aux applications et aux services ICT du monde entier en Europe. La figure I.1 décrit les différentes catégories de réseaux suivant leur étendue et la norme existante [3].

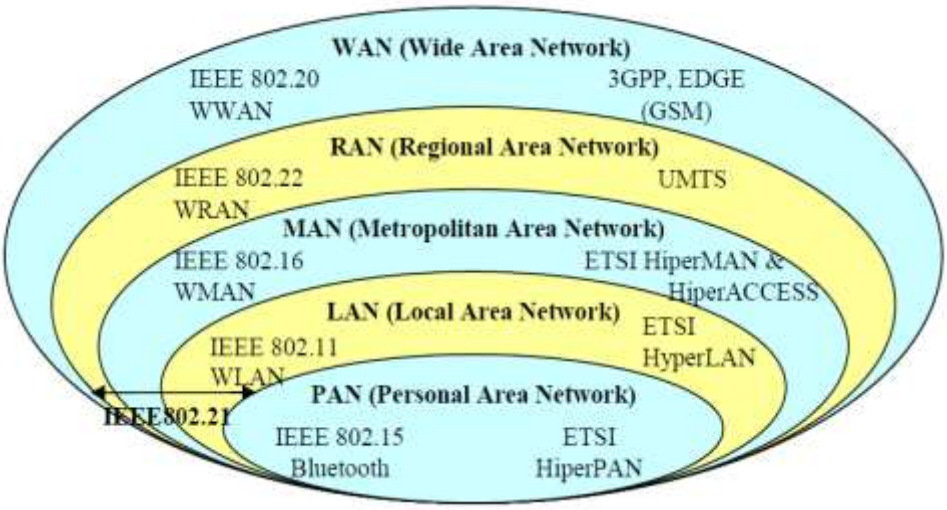


Figure I.1 : Catégories des réseaux sans fil [3].

1.2.2.1 WBAN (Wireless Body Area Network)

WBAN fait référence aux applications médicales des réseaux sans fil ; on peut l'appeler une technologie sans fil des soins de santé. Un réseau corporel (BAN), aussi appelé réseau sans fil de zone corporelle (WBAN) ou réseau de capteurs corporels (BSN), qui est un réseau sans fil de dispositifs informatiques portable [4].

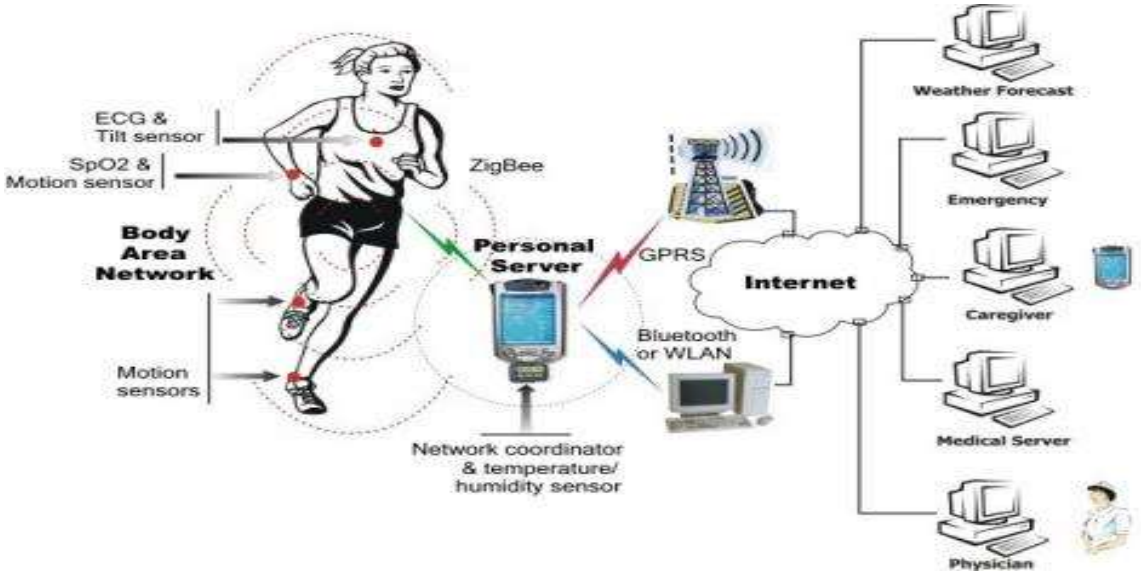


Figure I.2: WBAN [4].

1.2.2.2 WPAN (Wireless Personal Area Network)

Les réseaux personnels permettent la communication entre différents appareils dans un rayon réduit. Actuellement, le réseau personnel le plus communément utilisé est celui basé sur la technologie Bluetooth. Deux nouvelles technologies émergent pour ce type de réseaux : une adaptée à des débits élevés UWB (Ultra Wide Band ou Ultra large bande), tandis que ZigBee autorise des connexions d'équipements plus bas débit et à faible consommation [3].

1.2.2.3. Les WLAN (Wireless Local Area Network)

Le réseau local sans fil correspond au périmètre d'un réseau local installé dans une entreprise, dans un foyer ou encore dans un espace public. Tous les terminaux situés dans la zone de couverture du WLAN peuvent s'y connecter. Plusieurs WLAN peuvent être synchronisés et configurés de telle manière que le fait de traverser plusieurs zones de couverture est pratiquement indécelable pour un utilisateur [1].

1.2.2.4 WMAN (Wireless Metropolitan Area Network)

Le réseau sans fil WMAN utilise le Standard IEEE 802.16, autrement dit WIMAX (Worldwide Interoperability for Microwave Access), il fournit un accès réseau sans fil à des immeubles connectés par ondes radio à travers une antenne extérieure à des stations centrales reliées au réseau filaire [2].

1.2.2.5 WWAN (Wireless Wide Area Network)

Le réseau sans fil WWAN englobe les réseaux cellulaires tels que le GSM, GPRS, UMTS, et les réseaux satellitaires. La distance entre les périphériques peut aller jusqu'à 3Km, le coût de la mise en place d'un tel réseau est plus élevé que celui des réseaux cités au paravent [2].

1.2.2.6 WRAN (Wireless Regional Area Network)

IEEE 802.22 est une norme pour les réseaux régionaux sans fil (WRAN) qui fonctionneront dans des canaux de télévision inutilisés, et fourniront un accès aux services sans fil. La norme finale va supporter des canaux de (6,7 et 8 Mhz) pour une opération mondiale. Le WRAN est basé sur l'OFDMA (Orthogonal Frequency Division Multiple Access). Cette norme est actuellement sous forme d'ébauche [2].

1.2.3 Fonctionnement de réseaux sans fil

Le téléphone sans fil communique avec un correspondant par l'intermédiaire du socle qui fait office de point d'accès (AP) vers le réseau téléphonique. De même, chaque ordinateur du réseau sans fil muni d'une carte réseau adéquate peut émettre (et recevoir) des données vers (et depuis) un point d'accès réseau. Ce dernier peut être physiquement connecté au réseau câblé et fait alors office de point d'accès vers le réseau câblé. Bien entendu plus on s'éloigne du point d'accès, plus le débit diminue : pour un débit de 1 Mbps, la portée est de 460 m dans un environnement sans obstacle et de 90 m dans un environnement de bureau classique. Suivant la manière de communication entres les mobiles, le réseau sans fil offre deux modes de fonctionnement différents : Le mode avec infrastructure et le mode sans infrastructure [2].

1.2.3.1 Réseaux sans fil avec infrastructure

Dans ce mode de fonctionnement, également appelé BSS (Basic Service Set), le réseau est obligatoirement composé d'un point d'accès appelé station de base (SB), munis d'une interface de communication sans fil pour la communication directe avec les sites ou unités mobiles (UM). Une station de base couvre une zone géographique limitée. Une unité mobile rattachée à un moment donné qu'a une station de base lui offrant tous les services tant que l'UM est à l'intérieure de la zone de couverture de la SB [5].

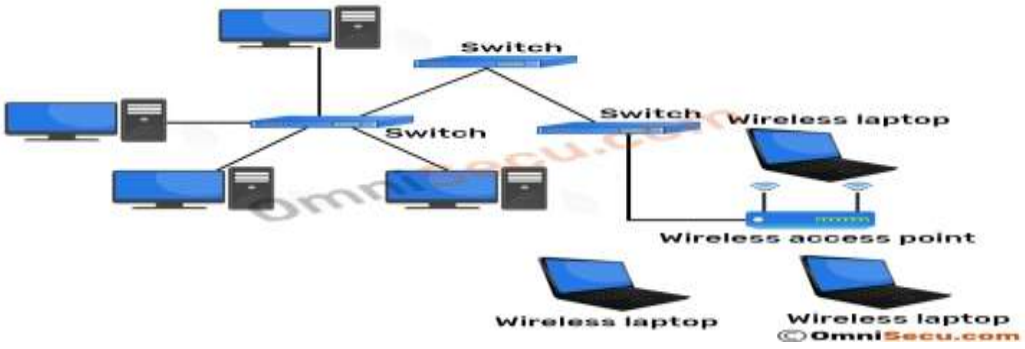


Figure I.3 : Réseaux sans fil avec infrastructure [2].

1.2.3.2 Réseaux sans fil sans infrastructure

Également appelé réseau Ad-hoc ou IBSS (Independent Basic Service Set), il s'agit d'un mode point à point, nécessitant pas de points d'accès. Il permet de connecter les stations quand aucun point d'accès n'est disponible. L'absence d'infrastructure oblige les UM à jouer le rôle de routeurs [5].

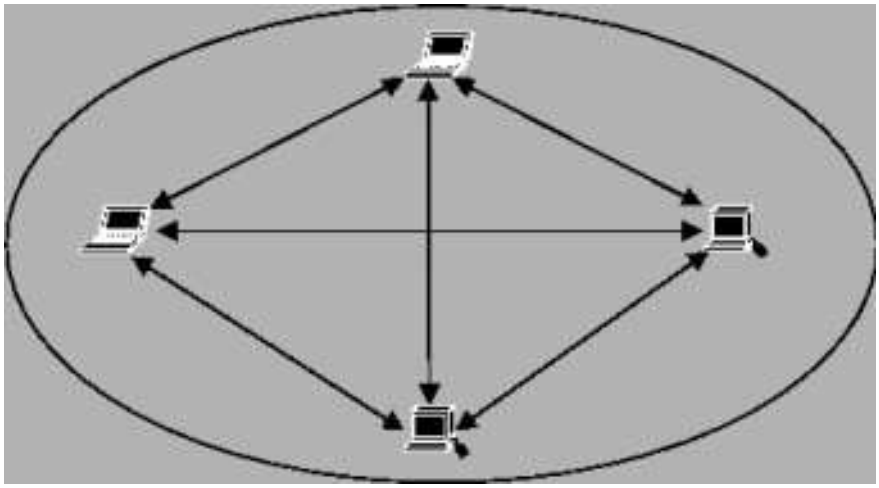


Figure I.4 : réseau sans fil sans infrastructure IBSS (ad-hoc) [2].

1.3 Réseau mobile

1.3.1 Réseau mobile et sans fil

Les termes mobiles et sans fil sont souvent utilisés pour décrire les systèmes de communication sans fil existants, il est important de distinguer les deux catégories de réseaux. Dans les réseaux sans fil, le support de communication utilise l'interface radio : sans cordon, GSM, GPRS, UMTS…

Un utilisateur mobile est défini théoriquement comme un utilisateur capable de communiquer à l'extérieur de son réseau d'abonnement tout en conservant une même adresse.

- Le système sans cordon est un système sans fil mais il n'est pas mobile.
- Certains systèmes tels que le GSM offre la mobilité et le sans-fil simultanément [2].

1.4 Radio logiciel

C'est grâce aux travaux de Joseph Mitola que le terme Radio logicielle est apparu en 1991 pour définir une classe de radio reprogrammable et reconfigurable. La radio logicielle est une radio dans laquelle les fonctions typiques de l'interface radio généralement réalisées en matériel, telles que la fréquence porteuse, la largeur de bande du signal, la modulation et l'accès au réseau sont réalisés sous forme logicielle.

La radio logicielle moderne intègre également l'implantation logicielle des procédés de cryptographie, codage correcteur d'erreur, codage source de la voix, de la vidéo ou des données. Le concept de radio logicielle doit également être considéré comme une manière de rendre les usagers, les fournisseurs de services et les fabricants plus indépendants des normes. Ainsi, avec cette solution, les interfaces radio peuvent, en principe, être adaptées aux besoins d'un service particulier pour un usager particulier dans un environnement donné à un instant donné. On distingue plusieurs niveaux d'avancement dans le domaine : la radio logicielle est le but ultime intégrant toutes les fonctionnalités en logiciel, mais elle impose des phases intermédiaires combinant anciennes et nouvelles techniques, on parle alors de radio logicielle restreinte SDR (Software Defined Radio en anglais). Les contraintes de puissance de calcul, de consommation électrique, de coûts, etc. imposent actuellement de passer par cette phase intermédiaire [2].

1.4.1 Radio logicielle restreinte SDR (Software Defined Radio)

La radio logicielle restreinte est un système de communication radio qui peut s'adapter à n'importe quelle bande de fréquence et recevoir n'importe quelle modulation en utilisant le même matériel.

Les opportunités qu'offre le SDR lui permettent de résoudre des problèmes de la gestion dynamique du spectre. Les équipements SDR peuvent fonctionner dans des réseaux sans fil hétérogènes c'est-à-dire qu'un SDR idéal peut s'adapter automatiquement aux nouvelles fréquences et aux nouvelles modulations [2].

1.5 La Radio cognitive

1.5.1 Historique

L'idée de la radio cognitive a été présentée officiellement par Joseph Mitola III à un séminaire à KTH, l'Institut royal de technologie, en 1998, publié plus tard dans un article avec Gerald Q. Maguire, Jr en 1999. Connu comme le « Père de la radio logicielle ». Dr. Mitola est l'un des auteurs les plus cités dans le domaine. Mitola combine son expérience de la radio logicielle ainsi que sa passion pour l'apprentissage automatique et l'intelligence artificielle pour mettre en place la technologie de la radio cognitive. Et donc d'après lui : « Une radio cognitive peut connaître, percevoir et apprendre de son environnement puis agir pour simplifier la vie de l'utilisateur » [2].

1.5.2 Définition

Le paradigme radio cognitive (RC) émerge pour la première fois en 1998 dans un article de Mitola présenté lors d'une conférence à la Royal Institute of Technology (Suède). Dès lors, la RC constitua un domaine de recherche très attrayant. Ce qui rend ce concept si attractif, c'est l'idée qu'une interface radio puisse elle-même modifier son comportement en fonction de l'environnement dans lequel elle transmet et ajuster ses paramètres de fonctionnement de manière dynamique et autonome. De ce fait la RC peut être définit comme un nouveau système de communication sans fil dans laquelle un utilisateur peut détecter intelligemment les canaux de communication libres et/ou occupés, et transmettre sur les canaux inutilisés. Ceci permet d'optimiser l'utilisation des fréquences radio disponibles du spectre tout en minimisant les interférences avec d'autres utilisateurs. Cette capacité d'exploitation en temps-réel des informations disponibles dans son environnement permet l'adaptation de chaque interface radio aux conditions spectrales du moment et offrir une certaine flexibilité d'utilisation du spectre.

Toute communication radio cognitive fait intervenir au moins deux éléments principaux :

- Le premier est l'utilisateur primaire (PU) qui reçoit de façon permanente ou du moins pour une longue durée, une plage spécifique de fréquences attribuée par les organismes de régulation du spectre (cités plus haut). Le système primaire est donc prioritaire et possède toutes les autorisations pour émettre dans la bande considérée (e.g., GSM, aviation, communication militaire, etc).

- Le second élément est l'utilisateur secondaire (SU) ou utilisateur cognitif ayant pour objectif principal la transmission de données quelques soit leurs types, sur les mêmes bandes fréquentielles que le PU, tout en minimisant la dégradation de la qualité des transmissions de ce dernier. De ce fait, la radio cognitive parait comme étant la solution la plus adéquate au problème de l'encombrement et de sous-utilisation spectrale en permettant le partage du spectre entre PU et SU.

Le principe de la radio cognitive, est décrit dans la norme IEEE 802.22, qui suggère une utilisation plus optimale du spectre : un équipement radio dit secondaire pourra à tout moment accéder à des bandes de fréquences licenciées libres c'est-à-dire, non occupées par l'utilisateur primaire (possédant une licence sur cette bande). L'utilisateur secondaire pourra aussi exploiter de manière opportuniste les bandes licenciées sous-utilisées, dont l'utilisateur primaire n'occupe pas toute la largeur de bande. De même, l'utilisateur secondaire peut interrompre une transmission une fois terminée ou lorsqu'un utilisateur primaire souhaitera transmettre sur la même bande (ou occuper toute la largeur du canal). La norme IEEE 802.22 vise à réutiliser les espaces vides alloués à la télévision analogique pour les technologies RC. La littérature met en exergue d'autres standards tels que le IEEE-SCC41 (Standards Coordinating Committee 41) pour les réseaux avec un accès dynamique au spectre.

Un Réseau Radio Cognitif (RRC) coordonne les transmissions secondaires sur différentes bandes de fréquences et selon différentes technologies en exploitant les bandes licenciées disponibles ou sous-utilisées à un instant et à un endroit donné. Un RRC peut être structuré ou non (avec ou sans station de base), les nœuds cognitifs ou secondaires ont la capacité d'opérer sur une large gamme de fréquences afin de reconnaitre différents signaux présents dans le réseau et se reconfigurer intelligemment [6].

1.5.3 Relation entre la Radio cognitive et le SDR

L'une des principales caractéristiques de la RC est la capacité d'adaptation où les paramètres de la radio (fréquence porteuse, puissance, modulation, bande passante) peuvent être modifiés en fonction de : l'environnement radio, la situation, les besoins de l'utilisateur, l'état du réseau, la géolocalisation, ...etc. La radio logicielle est capable d'offrir les fonctionnalités de flexibilité, de reconfigurabilité et de portabilité inhérente à l'aspect d'adaptation de la radio cognitive.

Cette dernière doit être mise en œuvre autour d'une radio logicielle. En d'autres termes, la radio logicielle est une "technologie habilitante" pour la radio cognitive.

Bien que de nombreux modèles différents soient possibles, l'un des plus simples modèles conceptuels qui décrit la relation entre la radio cognitive et la radio logicielle restreinte est illustré dans la Figure I.5. Dans ce modèle simple, les éléments de la radio cognitive entourent le support radio logicielle restreinte. Le "cognitive engine" représente la partie chargée de l'optimisation ou du contrôle du module radio logicielle restreinte en se basant sur quelques paramètres d'entrée tels que les informations issues de la perception sensorielle ou de l'apprentissage de l'environnement radio, du contexte utilisateur, et de l'état du réseau [2].

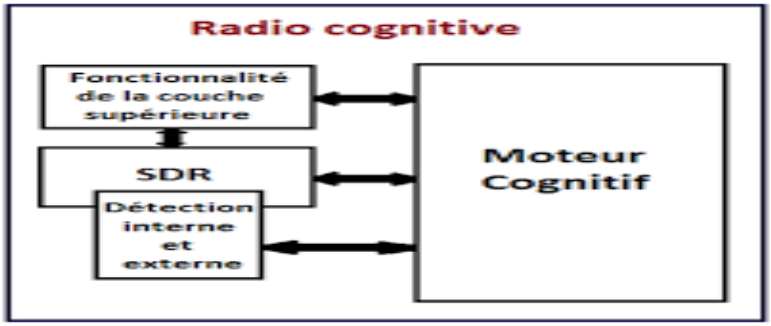


Figure I.5 : Relation entre la radio cognitive et la radio logicielle restreinte [2].

1.5.4 Architecture de Radio Cognitive

Mitola a défini l'architecture d'une radio cognitive par un ensemble cohérent de règles de conception par lequel un ensemble spécifique de composants réalise une série de fonctions de produits et de services.

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

- La perception sensorielle (Sensory Perception : SP) de l'utilisateur qui inclut l'interface haptique (du toucher), acoustique, la vidéo et les fonctions de détection et de la perception.
- Les capteurs de l'environnement local (emplacement, température, accéléromètre, etc.)
- Les applications système (les services médias indépendants comme un jeu en réseau).

- Les fonctions SDR (qui incluent la détection RF et les applications radio de la SDR).
- Les fonctions de la cognition (pour les systèmes de contrôle, de planification, d'apprentissage).
- Les fonctions locales effectrices (synthèse de la parole, du texte, des graphiques et des affiches multimédias).

L'architecture du protocole de la radio cognitive est représentée dans la figure ci-dessous. Dans la couche physique, le RF est mis en œuvre à base de radio définie par logiciel. Les protocoles d'adaptation de la couche MAC (Media Access Control), réseau, transport, et applications doivent être conscients des variations de l'environnement radio cognitif. En particulier, les protocoles d'adaptation devraient envisager l'activité du trafic des principaux utilisateurs, les exigences de transmission d'utilisateurs secondaires, et les variations de qualité du canal [2].

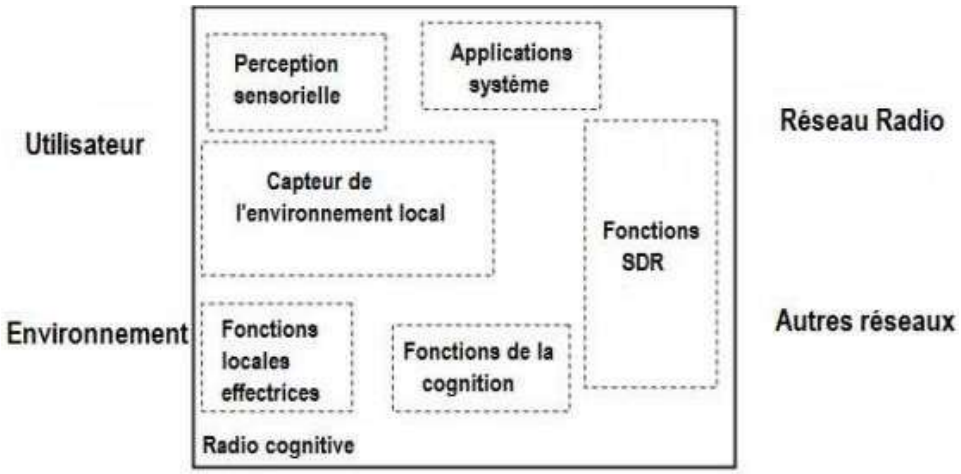


Figure I.6 : Architecture de Radio Cognitive [7]

1.5.5 Cycle de cognition (Cycle de MITOLA)

Plus une interface radio est consciente de son environnement plus elle sera décrite comme étant une RC idéale (AACR : Aware Adaptive and Cognitive Radio).

Mitola propose dans un schéma récapitulatif du cycle de cognition pour cette RC idéale. La figure 1.7 reprend et illustre ce cycle du concept de la radio idéale.

La RC analyse son environnement, observe le comportement des différents systèmes communicants sur le réseau, reconnait les interactions, apprend le but des autres usagers,

propose de nouvelles solutions alternatives et agit en conséquence. Elle négocie de nouveaux schémas de communication ainsi que de nouveaux protocoles avec les autres radios opérant sur le réseau [6].

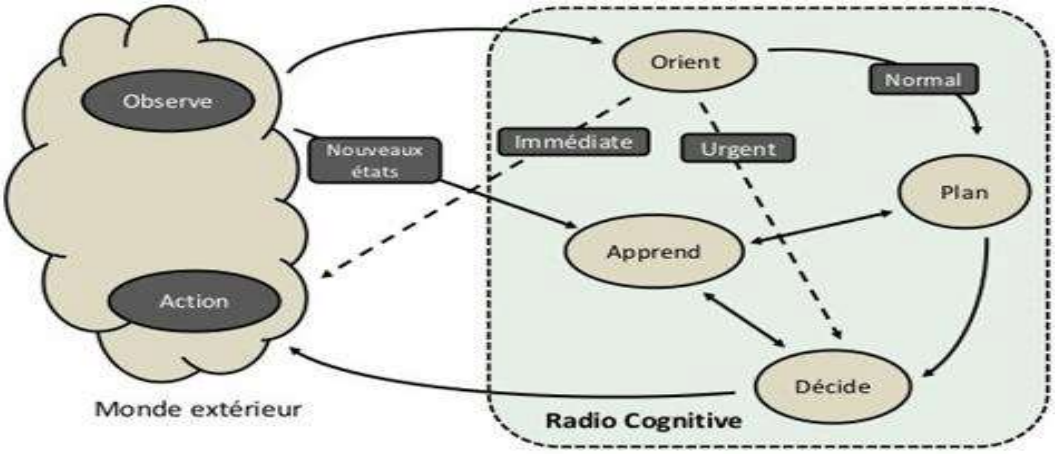


Figure 1.7 : Cycle cognitive de MITOLA [7]

1.5.5.1 Phase d'observation

La RC observe son environnement par l'analyse des transmissions radio effectuées dans la bande sur laquelle elle opère elle associe les fréquences, la puissance de transmission …etc. Pour en déduire le contexte de communication [6].

1.5.5.2 Phase d'orientation

Cette phase traite les résultats inhérents à la phase d'observation, on les associant à des scénarios de transmission antérieure similaire afin de pouvoir discerner les différents modèles de communication [6].

1.5.5.3 Phase de planification

La plupart des informations réseau collectées sont leurs contextes de traitement (état normal, urgence ou immédiat). Un message entrant du réseau extérieur enclenche la génération d'un plan, dans le cas d'un traitement d'état normal, ce plan devrait également inclure la phase de raisonnement dans le temps. En autre, la génération d'un plan pour des états immédiats est préprogrammée ou apprise via des expériences antérieures [6].

1.5.5.4 Phase de décision

La phase de décision sélectionne un schéma d'allocation parmi un ensemble de solutions faisables. L'interface radio peut avertir l'utilisateur d'un message entrant ou reporter la notification ultérieurement [6].

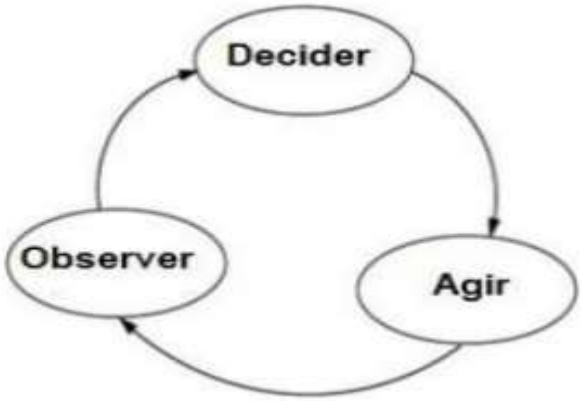


Figure I.8 : Cycle de MITOLA simplifié [7]

1.5.5.5 Phase d'action

Cette phase exécute le schéma d'allocation sélectionné suite à la phase décisionnelle, le processus d'allocation inhérent, a la capacité d'interagir avec le monde extérieur (état de transmission des autres utilisateurs sur le réseau, état des bandes de transmissions), en d'autres termes, selon les besoins de l'utilisateur, ce schéma d'allocation peut à tout moment être modifier, et ce en accédant à l'état interne de la radio cognitive [6].

1.5.5.6 Phase d'apprentissage

L'apprentissage dépend des résultats collectés lors des phases d'observation, et de décisions entreprises.

L'apprentissage initial, est réalisé à travers la phase d'observation dans laquelle toutes les informations sur l'état d'occupation du réseau sont comparées à l'ensemble des expériences antérieure. La phase d'apprentissage se déclenche quand un nouveau modèle d'allocation est créé.

Par exemple, les états antérieurs et courants sont comparés avec les attentes des utilisateurs pour en apprendre davantage sur l'efficacité d'un mode de communication.

Il est clair que malgré les avancées notables dans le domaine du traitement de signal et des télécommunications, de multiples contraintes s'opposent à la réalisation pratique d'un système RC idéal, le rendant de fait fastidieux à implémenter. Pour pallier ce problème, la littérature propose une version simplifiée du cycle de cognition. Cette version est décrite dans la figure 1.8, elle se focalise principalement sur trois fonctions : l'observation (le seing), la décision et l'adaptation (l'action).

L'implémentation pratique de la radio cognitive met en relief de nombreux chalenges, la détermination de solutions adéquates par exemple, fait l'objet de nombreux sujets de recherche. Dans la section suivante, la classification RC est abordée selon le modèle de partage du spectre, cette classification permet d'aborder la radio cognitive sous un aspect plus pragmatique [6].

1.5.6 Composants de la Radio Cognitive

La figure 1.9 montre les différents composants d'un émetteur/récepteur radio cognitive

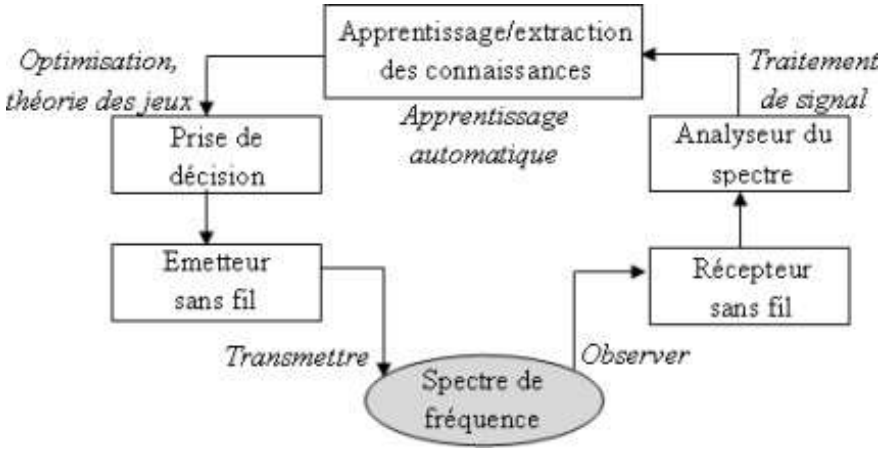


Figure I.9 : Composantes de la radio cognitive [7]

- Emetteur / Récepteur : un émetteur/récepteur SDR sans fil est le composant majeur avec les fonctions du signal de transmission de données et de réception. En outre, un récepteur sans fil est également utilisé pour observer l'activité sur le spectre de fréquence (spectre de détection). Les paramètres émetteur/récepteur dans le nœud de la radio cognitive peuvent être modifiés dynamiquement comme dicté par les protocoles de couche supérieure.
- Analyseur de spectre (Spectrum analyser) : L'analyseur de spectre utilise les signaux mesurés pour analyser l'utilisation du spectre (par exemple pour

détecter la signature d'un signal provenant d'un utilisateur primaire et trouver les espaces blancs du spectre pour les utilisateurs secondaires). L'analyseur de spectre doit s'assurer que la transmission d'un utilisateur primaire n'est pas perturbée si un utilisateur secondaire décide d'accéder au spectre. Dans ce cas, diverses techniques de traitement du signal peuvent être utilisées pour obtenir des informations sur l'utilisation du spectre.

- Extraction de connaissances et apprentissage (Knowledge extraction/learning) : L'apprentissage et l'extraction de connaissances utilisent les informations sur l'utilisation du spectre pour comprendre l'environnement ambiant RF (par exemple le comportement des utilisateurs sous licence). Une base de connaissances de l'environnement d'accès au spectre est construite et entretenue, qui est ensuite utilisée pour optimiser et adapter les paramètres de transmission pour atteindre l'objectif désiré sous diverses contraintes. Les algorithmes d'apprentissage peuvent être appliqués pour l'apprentissage et l'extraction de connaissances.
- Prise de décision (Decision making) : Après que la connaissance de l'utilisation du spectre soit disponible, la décision sur l'accès au spectre doit être faite. La décision optimale dépend du milieu ambiant, elle dépend du comportement coopératif ou compétitif des utilisateurs secondaires. Différentes techniques peuvent être utilisées pour obtenir une solution optimale. Par exemple, la théorie d'optimisation peut être appliquée lorsque le système peut être modélisé comme une seule entité avec un seul objectif. En revanche, les modèles de la théorie des jeux peuvent être utilisés lorsque le système est composé d'entités multiples, chacun avec son propre objectif. L'optimisation stochastique peut être appliquée lorsque les états du système sont aléatoires [2].

1.5.7 Fonctions de la Radio Cognitive

Les principales fonctions d'un RRC sont : l'analyse du spectre, le partage et la gestion du spectre ainsi que la mobilité spectrale.

1.5.7.1 Détection du spectre

La détection du spectre (en anglais spectrum sensing) permet au RRC de collecter les informations sur l'état d'utilisation des bandes du spectre. Le RRC doit donc détecter les bandes

utilisées par les PUs et les SUs ainsi que les espaces blancs (en anglais spectrum holes) avant d'effectuer l'affectation des SUs aux bandes du spectre.

Afin d'éviter les interférences ou estimer l'interférence que les PU peuvent tolérer en cas de coexistence avec des utilisateurs secondaires, les techniques de détection du spectre sont divisées en trois catégories : la détection d'émetteur (locale/compétitive), la détection coopérative et la détection basée sur l'interférence [6].

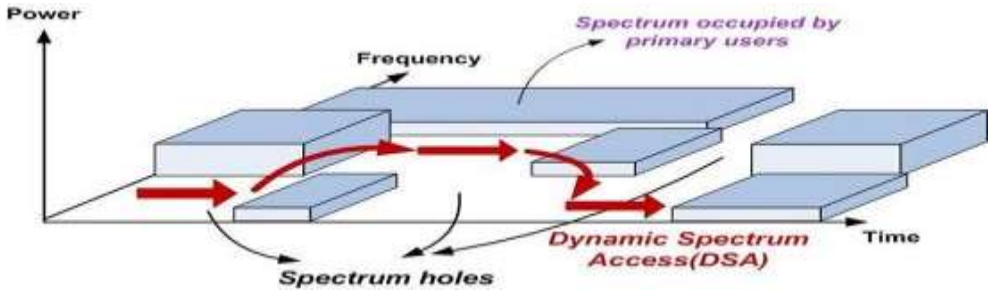


Figure I.10 : Exemple d'utilisation de spectre radio [7]

La Figure I.10 montre un exemple des espaces blancs (spectrum hole) dans le spectre radio. Elle montre deux types de bandes : les bandes utilisées (spectrum in use) par les utilisateurs qu'ils soient primaires ou secondaires, et les espaces blancs ou les bandes non utilisées [6].

1.5.7.2 Gestion du spectre

Il est nécessaire de réutiliser les fréquences disponibles pour répondre aux besoins de communication des utilisateurs, répondant ainsi aux exigences de qualité de service sur toutes les bandes de fréquences. De ce fait, la gestion et le partage du spectre est une fonctionnalité de base dans les RRC, en utilisant les informations collectées dans la phase de détection, le RRC décide sur l'allocation des bandes disponibles aux utilisateurs secondaires, en se basant sur la disponibilité du spectre. Le RRC décide des utilisateurs secondaires qui vont être servis et leurs bandes associées. Selon la technique de partage du spectre utilisé par le RRC, le partage peut soit inclure uniquement l'allocation des espaces blancs ou aussi les bandes licenciées occupées par les utilisateurs primaires.

Le schéma d'allocation doit donc prendre en compte les exigences de qualité de service des PUs et des SUs, dans le cas contraire les transmissions seront effectuées avec le débit et la puissance possibles (Best Effort Transmission). Les contraintes du partage sont en général des

contraintes d'interférence par rapport aux utilisateurs primaires. Les exigences sont, elles, en général des exigences de qualité de service que chaque utilisateur secondaire doit satisfaire (comme un débit de transmission minimum, un taux d'erreur BER minimum, etc) [6].

1.5.7.3 Mobilité du spectre

La mobilité spectrale est le processus par lequel un utilisateur cognitif peut changer sa fréquence de transmission, sa largeur de bande...etc. Cette fonctionnalité vise à utiliser le spectre de manière dynamique en permettant aux interfaces radio de fonctionner dans la meilleure bande de fréquences disponible, le RRC doit par exemple assurer le déplacement de l'utilisateur secondaire vers une autre portion du spectre dans le cas où la bande spécifiée doit être réutilisée par un utilisateur primaire [6].

1.5.8 Langages de la Radio cognitive

Deux problèmes surgissent. D'abord, le réseau n'a aucun langage standard avec lequel il peut poser ses questions. En second lieu, la destination possède la réponse, mais elle ne peut pas accéder à cette information. Elle n'a aucune description de sa propre structure. RKRL (Radio Knowledge Representation Language), fournit un langage standard dans lequel de tels échanges de données peuvent être définis dynamiquement. Il est conçu pour être employé par des agents logiciels ayant un haut niveau de compétence conduite en partie par un grand stock de connaissances a priori. En plus de la langue naturelle, plusieurs langages sont utilisés pour la radio (tableau ci-dessous). L'Union Internationale des Télécommunications (ITU) a adopté les spécifications et le langage de description (SDL) dans ses recommandations. SDL exprime aisément l'état des machines radio, les diagrammes d'ordre de message, et les dictionnaires des données relatifs. L'Institut européen des normes de télécommunications a récemment adopté SDL en tant que l'expression normative des protocoles radio, ainsi on s'attend à ce que la modélisation SDL de la radio continue à avancer. Cependant, SDL manque de primitives pour la connaissance générale des ontologies [2].

Language	Points forts	Points faibles
SDL	Etat des machines, diagramme de séquence, base d'utilisateur très large, connaissances bien codée	Plan de représentation, incertitude
UML	Ontologies générales, structure, relations	Matériel, propagation RF
IDL	Interfaces, encapsulation des objets	Informatique générale
KQML	Primitives(ask/tell), sémantique	Informatique générale
KIF	Traitement axiomatique des ensembles, relations, frames, ontologies	Informatique générale, matériel, propagation RF

Tableau I.1: Langage de la Radio Cognitive [1].

Le langage de modélisation unifiée (UML) exprime aisément un logiciel objet, y compris des procédures, des cas d'utilisation, etc. En pratique, il a une présence forte dans la conception et le développement des logiciels, mais il est faible dans la modélisation des dispositifs câblés. En outre, bien qu'UML puisse fournir un cadre de conception pour la propagation radioélectrique, les langages cibles sont susceptibles d'être en C ou en Fortran pour l'efficacité en traçant des dizaines de milliers de rayons d'ondes radio.

Le Common Object Request Broker Architecture (CORBA) définit un langage de définition d'interface (IDL) comme une syntaxe d'exécution indépendante pour décrire des encapsulations d'objets. Ce langage est spécifiquement conçu pour déclarer les encapsulations, il manque de la puissance des langages comme le C ou Java.

Le Knowledge Query and Manipulation Language (KQML), d'autre part, était explicitement conçu pour faciliter l'échange d'une telle connaissance. Basé sur des performatives comme « tell » et « ask ». Le plan de KQML pour prendre un flux d'information à l'emploie de la performance « tell » pour indiquer le plan du réseau suivant les indications de la figure ci-dessous. Dans cet exemple, la radio avertit également le réseau que son utilisateur compose un certain email et ainsi il va avoir besoin d'une voie de transmission de données de DECT (Digital Enhanced Cordless Telecommunications) ou de la transmission radioélectrique par paquet de GSM (Global System for Mobile Communications) GPRS (General Packet Radio Service) en transit.

Le Knowledge Interchange Format (KIF) fournit un cadre axiomatique pour la connaissance générale comprenant des ensembles, des relations, des quantités, des unités, de la géométrie simple, etc. Sa contribution principale est forte. Sa structure est comme celle de LIPS,

mais comme IDL et KQML, il n'est pas spécifiquement conçu pour l'usage « interne ». Le langage naturel souffre des ambiguïtés et de la complexité qui limitent actuellement son utilisation comme langage formel. La version 0.1 de RKRL a été créée pour remplir ces vides dans la puissance expressive des langages de programmation tout en imposant une parcelle de structure sur l'utilisation du langage naturel [2].

1.6 Sécurité de la Radio Cognitive

L'une des exigences fondamentales pour tout type de réseau est la sécurité. Cette section présente la question de la sécurité dans les RCN (Radio Cognitive Network) , décrit les exigences de sécurité et examine les attaques contre les RCN ainsi que les techniques de pointe actuelles pour détecter ou/et combattre les attaques correspondantes. Par rapport aux réseaux traditionnels, la sécurité dans les RCN devient un problème crucial et difficile, car plus de chances sont exposées aux attaquants en raison de l'introduction de CR. La plupart des attaques (p. ex., déni de service (DoS), brouillage, débordement de tampon, etc.) sur les files d'attente réseau sont toutes ciblées 5 pour rendre le réseau indisponible temporairement ou définitivement. L'avenir de la recherche sur la sécurité dans les RCN est également présenté [8].

1.6.1 Menaces contre la Radio Cognitive

Nous classons les attaques selon les couches qu'elles ciblent : physique, liaison, réseau et transport. Puisque les RRCs peuvent être considérés comme un type spécial de réseau Ad Hoc, la plupart des attaques ciblant les réseaux Ad Hoc peuvent également cibler les RRCs.

Toute solution suggérée pour contrer les attaques du RRC devrait respecter l'exigence de la FCC (Federal Communications Commission) selon laquelle « aucune modification au système en place ne devrait être nécessaire pour permettre aux utilisateurs secondaires d'utiliser le spectre de façon opportuniste » [9].

Compte tenu de cette exigence, toute solution de sécurité suggérée pour protéger ou contrecarrer une attaque contre RCN doit être introduite dans le système de l'utilisateur secondaire, et non dans le système primaire [10].

Les attaques dans la RC ciblent les deux types radio :

- **Radio politique (Policy Radio) :** permet de déterminer le comportement de la radio selon une certaine stratégie, ce qui fait que les informations de

l'environnement seront transformées en statistique pour mesurer l'état de la radio [11].

- **Radio d'apprentissage (Learning Radio) :** contiennent un moteur d'apprentissage qui définit une stratégie à base de ces connaissances, si ses informations changent la stratégie sera changée.

Il permet de déterminer un bon fonctionnement des paramètres dans un environnement particulier, ce type de radio est connu pour être difficile contre les attaques.

La nécessité de citer les types de la RC permet d'établir les différentes attaques sur eux, par exemple dans la Policy Radio à l'aide de la connaissance de la manière de calcul des statistiques, l'attaquant peut attribuer et forcer une sortie souhaitée [9]. Les attaques dans les RRC sont classées en fonction des couches OSI qu'elles ciblent : la couche physique, liaison, réseau et transport. Les attaques ciblent en particulier les réseaux Ad hoc et puisque les RRC sont considérés comme un type de réseau Ad hoc, cela implique que les attaques peuvent également se pointer contre un RRC [11].

1.6.1.1 Les attaques de la couche physique (physical layer attacks)

1.6.1.1.1 Emulation de l'utilisateur Primaire (PUE)

Le mécanisme de la RC permet à un SU d'utiliser une bande de fréquence libre d'un PU. Après la détection de la BS (Bande Spectrale), le SU doit permuter les canaux vers la bande périodique pendant une durée d'allocation pour éviter les interférences avec le PU. Dans le cas où un autre utilisateur secondaire utilise la même bande, une utilisation des dispositifs pour le partage du spectre d'une manière raisonnable est nécessaire. L'attaque d'émulation de l'utilisateur primaire est composée de deux classes :

- **L'attaque PUE égoïste :** un SU malveillant émule un PU pour agrandir sa part du spectre. Elle peut être effectuée par deux attaquants pour mettre une liaison entre eux.
- **L'attaque PUE malveillant :** une attaque qui interdit les SU autorisés d'utiliser les espaces blancs d'un spectre [9], la figure au-dessous montre le mécanisme de l'attaque PUE :

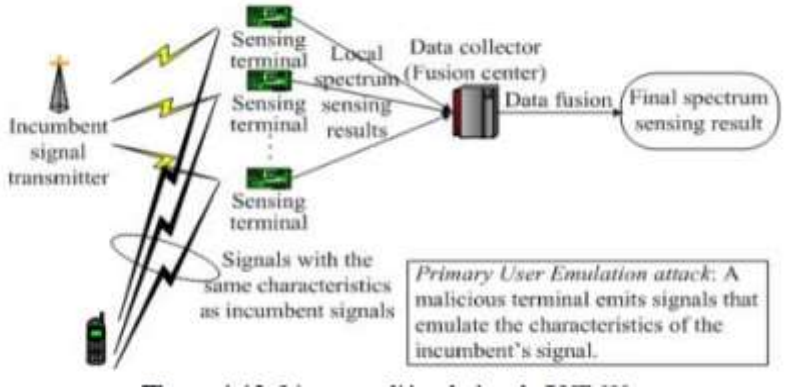


Figure I.11: L'attaque d'émulation de PUE [9].

Policy Radio et Learning Radio peuvent être provoquées par l'attaque d'émulation de l'utilisateur primaire. Ainsi que dans Policy Radio l'effet de l'attaque disparait aussitôt que l'attaquant quitte le canal [11], alors que dans Learning Radio l'attaquant collecte les informations du comportement de PU pour connaitre quand il va libérer le canal (temps mort), après il peut faire une attaque durant ce temps mort. Les informations sur le RRC facilitent le fonctionnement des attaques PUE. Un exemple sur l'attaque PUE : l'attaquant profite du temps où les SU se refusent la transmission pour bien détecter le spectre. Un deuxième exemple quand le dispositif radio cognitive fait un changement de fréquence (Handoff), l'attaque peut être conduite à un faible débit ou entièrement à un DoS (Deny of Service) [12].

Solution contre l'attaque PUE : Pour se défendre contre l'attaque PUE, il faut d'abord connaitre la source du canal si c'est un PU ou bien un MSU (Malicious Secondary User) qui émule le PU. L'identification d'un émetteur PU permet de séparer entre un PU légitime et un PU malveillant. La technique de l'authentification cryptographique permet la connaissance de l'identité de PU, mais la restriction de la FCC interdit la modification du système PU. Donc, les chercheurs ont trouvé une solution efficace pour vérifier l'emplacement de la source PU c'est-à-dire une approche pour faire la correspondance entre l'emplacement de la source et l'emplacement de PU [11].

Il existe deux techniques pour l'identification de l'emplacement de la source PU :

- **Test du rapport de distance (DRT) :** c'est-à-dire le calcul de la force de signal reçu.

- **Test de différence de distance (DDT) :** c'est-à-dire la différence de la phase du signal.

Les deux techniques utilisent une procédure de vérification de la source PU. L'objectif de cette procédure est de séparer entre les signaux primaires légitimes et les signaux malveillants. Les tests de DRT et DDT sont effectués par des vérificateurs de localisation fiable LV qui sont classés en deux catégories :

- **Un maitre LV :** contient une base de données avec les coordonnées des tours de télévisions grâce à un système GPS.
- **Un esclave LV :** qui calcule la distance entre lui et le transmetteur par force du signal et le compare avec celui de la tour TV, les données ici doivent être cryptées et authentifiées pour ne pas les modifier ou les intercepter.

Les deux catégories sont liées pour contrôler leur communication. Une attaque de l'émetteur d'un signal est considérée si la vérification échoue [8]. Mais comme inconvénient à cette solution c'est que l'implémentation peut être couteuse de plus qu'elle peut être appliquée que dans un ad hoc à cause du mauvais signal émis [13].

Le DRT et DDT peut être faux si un attaquant est près de la station TV comme solution à ce problème l'énergie des transmetteurs est la preuve de l'identité du transmetteur vue que celle du PU dépasser les 100 000 Kilo Watt et moins de 1000 Kilo Watt du MSU. Les informations du niveau d'énergie sont très importantes pour l'attaquant, il doit les utiliser afin de dévoyer les SU.

Une deuxième solution a été proposée pour se défendre contre l'attaque PUE c'est Localization Based Defense (LocDef) qui se résume en 3 étapes :

- Vérification des caractéristiques du signal.
- Mesure du niveau d'énergie du signal reçu.
- Localisation de la source du signal [10].

Cette méthode utilise RSS-Based localisation qui exploite la relation entre la force du signal et la position de l'utilisateur, quand la force du signal diminue cela veut dire que la distance entre l'émetteur et le récepteur est grand. Si un nœud assemble des données sur la puissance du signal à partir des nœuds distribués sur le réseau, il peut former un modèle de signal qu'il utilise pour connaitre la localisation de l'émetteur, et pour collecter les mesures RSS, un réseau capteur sous-jacent WSN (Wireless Sensor Network) est utilisé pour la collecte

des mesures RSS. Un autre objectif pour WSN, il contribue à la détection du spectre et donne des informations sur les opportunités du réseau [14].

L'empreinte digitale est la solution la plus efficace qui a été utilisée pour l'authentification [15], au début, une approche qui permet d'améliorer la sécurité dans les réseaux sans fil a été proposée. La technique RFF (Réseau Ferré de France) utilise un procédé unique dans un temps court où l'émetteur est présent dans les ondes et activé. RFF est classé dans : système de synthèse de fréquence, sous-système modulateur, des amplificateurs RF et les propriétés physiques de l'émetteur. RFF permet la surveillance et l'analyse du signal analogique d'un réseau sur la couche physique. Donc, l'identification de l'émetteur et le problème de sécurité peuvent être résolues, mais cette solution n'est pas optimale à cause des calculs lourds et les gros échantillons [15].

L'approche EMS (Signatures électromagnétiques) a été proposée pour résoudre le problème de l'optimisation. EMS permet la reconnaissance de motifs de signal de couche croisé. Le but de l'attaque PHY est de profiter de la simplicité, la flexibilité de la RC. EMS évite cette attaque car elle utilise l'identification des émetteurs, la détection, la collection des données et le test [10].

« EMS est un module de sécurité inter couche qui est capable de mettre en évidence les distinctions entre les dispositifs radio cognitifs. Il est conçu pour apprendre la caractéristique unique initiale à l'épreuve des dispositifs RC et le compare aux transmissions ultérieures pour validation et authentification » EMS authentifie la source de l'émetteur et donc elle diminue les attaques DoS et les attaques PUE [16], le fonctionnement de la technique de l'empreinte digitale est d'effacer la modulation des signaux reçus pour avoir un support avec bruit de phase. Les auteurs proposent l'empreinte digitale après une analyse et des statistiques logiques. Cette technique est la base de l'identification et contre les attaques PUE [17].

1.6.1.1.2 L'attaque de la fonction objective (Objective FunctionAttack)

« Cognitive radio is a smart radio that has the ability to sense the external environment, learn from the history, and make intelligent decisions to adjust its transmission parameters according to the current state of the environment » [18].

Le moteur cognitif adapte les paramètres radio telles que : la faible consommation d'énergie, le débit de données élevé, la haute sécurité, la fréquence centrale, la bande passante,

la puissance, le type de cryptage …etc. Les fonctions objectives sont utilisées pour calculer ces paramètres.

Par exemple : les paramètres radio qui maximisent le débit de données et minimisent la puissance. Le temps où le moteur cognitif est entrain de trouver les paramètres radio, un attaquant peut cibler ces paramètres pour que les résultats soient adaptés à son intérêt. Un exemple détaillé qui explique l'attaque de la fonction objective.

Cette attaque n'affecte que le type Learning radio, le scénario de l'attaque est qu'à chaque fois que le moteur cognitif tente d'utiliser un niveau élevé de sécurité, l'attaquant lance un brouillage sur la radio en réduisant le taux de transmission R et réduisant aussi la fonction objective F = w1.R+w2.S où S taux de sécurité et w1,w2 représente les poids de R et S, cette fonction objectif qui est utilisé par le moteur cognitif qui est responsable de l'ajustement des paramètres radio afin de répondre à des exigences spécifiques tel que la minimisation de la consommation d'énergie, le débit de données élevé et la haute sécurité. De cette façon l'attaquant force la radio à utiliser un niveau faible de sécurité [19].

Solution contre l'attaque de la fonction Objective : Que des suggestions ont été proposées pour se défendre contre l'attaquant parmi eux, définir des valeurs de seuil pour chaque paramètres radio, si les paramètres ne respectent pas les seuils la communication s'arrête, une autre suggestion a été présentée dans [12], c'est demander l'aide d'un système de détection d'intrusion IDS.

1.6.1.1.3-Jamming (L'attaque de Brouillage)

Le brouillage (Jamming) est une attaque qui cible les deux couches physique et MAC, l'objectif de l'attaque est d'envoyer des paquets de manière continue à des utilisateurs légitimes afin de saturer la bande spectrale, reporter la transmission des SU et causer des interférences, aussi avoir une situation DoS (Deny of Service) rendre le service indisponible, perturbation des communications…etc. Un Jammer peut bloquer le canal qui fait les échanges entre les réseaux radio cognitifs. La connaissance et l'écoute des données de contrôle par l'attaquant est très dangereux pour le réseau radio cognitif [20].

Le Jamming a quatre types de brouilleurs :

- **Jammer constant :** permet d'envoyer les paquets de données en continu sans faire une considération pour les protocoles de la couche Mac et sans attendre que le canal soit libre.

- **Jammer trompeur :** son but et de truquer les SU en envoyant des paquets de données excessive afin de les rendre en état reçu pendant une durée, il reste dans cet état lorsqu'il détecte un flux stable de données.
- **Jammer aléatoire :** il prend des pauses entre les signaux de brouillage, et il peut se comporter comme un Jammer constant ou trompeur.
- **Jammer réactif :** qui met le canal sous-surveillance et quand il détecte une communication sur le canal il commence le brouillage ce Jammer est le plus difficile à détecter car il ne transmet pas tout le temps [21].

Solution contre l'attaque Jamming : vu que le DoS peut être appliqué dans les deux couches liaison et physique, chaque couche a sa méthode de détection : Détection couche physique : les dispositifs légitimes utilisent une méthode de comparaison du bruit dans le réseau en recueillant suffisamment de données sur le niveau de bruit dans le canal et savoir si c'est normal ou anormal. LCC (Location Consistency Checks) a été proposée pour la détection des brouillages dont l'emplacement est intéressant et qui est établi par GPS et informé par chaque nœud. Cette technique vérifie la cohérence des emplacements par exemple : un nœud est brouillé si ses voisins reçoivent un nombre minimal de paquets. La cohérence d'un PDR d'un nœud sera vérifiée avec ses voisins. Détection couche Liaison : les dispositifs légitimes utilisent le protocole populaire d'accès au medium CSMA (Carrier Sensing Multiple Access), la détection d'un canal disponible sera faite par un périphérique, ce dernier ne transmet pas les données qu'après un délai de propagation. Si l'attaquant envoi les paquets et de manière continue le dispositif n'exécute jamais le protocole CSMA et il sera forcé de reculer, par conséquent le dispositif saura qu'il est victime d'un DoS. Une autre technique a été proposée, son principe est d'analyser la relation entre la force du signal SS (Signal Strength) et le rapport de livraison des paquets PDR (Packet Delivery Ratio). PDR est le rapport des paquets livrés (nombre de paquets envoyés par un émetteur). Par exemple, dans le cas où SS est élevé et le PDR est faible l'utilisateur suppose qu'il est brouillé si ses voisins n'ont pas un SS et un PDR élevé. Deux stratégies sont utilisées pour se préserver contre l'attaque Jamming (DoS) :

- **Channel Surfing** (déplacement des canaux ou changement de fréquence) : L'utilisation d'un canal différent lorsque l'attaque DoS est survenu.
- **Spatial Retreat** : L'emplacement des utilisateurs légitimes sera changé pour éviter les interférences de l'attaquant [22].

1.6.1.2 Les attaques de la couche liaison (Link Layer Attack)

1.6.1.2.1 Falsification des données de détection du spectre

SSDF (Spectrum Sensing Data Falsification) ou l'attaque Byzantine, consiste à envoyer des données fausses sur la détection du spectre. La figure suivante montre le mécanisme de l'attaque Byzantine [23] :

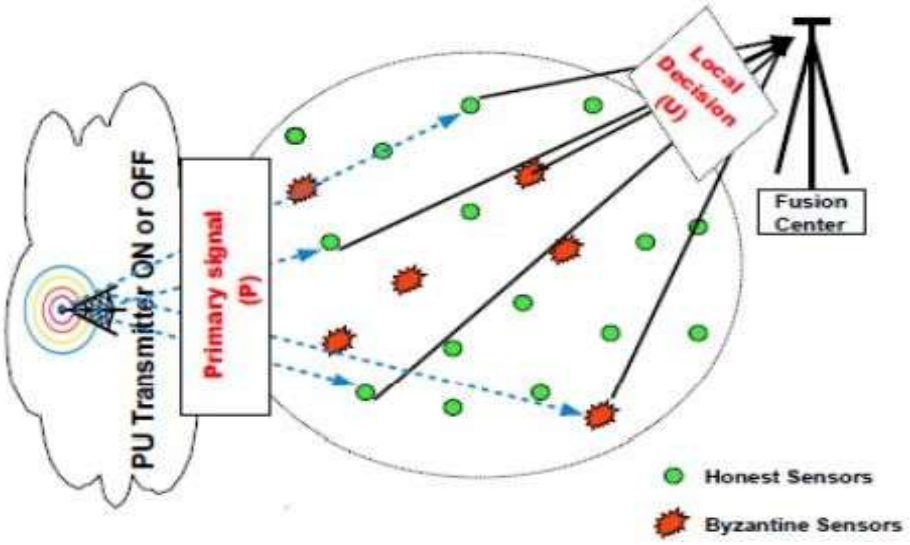


Figure I.12: L'attaque Byzantine [21].

Cette attaque cible les réseaux radio cognitifs centralisés et distribués.

- **RRC centralisé :** la collection des données détectées et l'allocation des bandes de fréquences sont faites par un centre d'intégration.

L'attaque SSDF (Byzantine) va tromper ce centre pour que les utilisateurs légitimes n'accèdent pas à des bandes de fréquences libres, ou ils peuvent accéder à des BS qui sont occupées.

- **RRC distribué :** la décision des bandes de fréquence est faite par la collaboration entre les réseaux radio cognitifs. SSDF est extrêmement malveillant dans les RRC distribués en raison de l'extension des données erronées.

Donc, dans le RRC centralisé l'effet de données malveillantes est moins diminué car le centre d'intégration compare les données reçues de la RC avec quelques techniques intelligentes pour bien connaitre RC légitime [24].

Une analyse sur l'attaque byzantine a été faite où ils ont utilisé les limites de performance en termes de la fraction des attaquants byzantins quand aucune approche de défense sera fonctionnelle [25].

Une étude a été faite pour bien analyser la performance du système RC en se basant sur la qualité de service QoS (Quality of Service) et la performance de détection des attaques et différentes contraintes sont traitées [26].

Solution contre SSDF : SDF (Several Data Fusion) est des stratégies pour se défendre contre SSDF (Byzantine).

Parmi les techniques suggérées : la Décision Fusion, qui permettent de regrouper les données de la détection du spectre. Une condition sur l'addition a été faite : si la somme est supérieure ou égale au seuil, donc le résultat est occupé, un signal est présenté. Sinon le résultat indique que la bande est libre. A cause des interférences une stratégie qui supporte de prendre un et un seul seuil, dans ce cas, la détection sera erronée c'est-à-dire elle indique la présence d'un signal sur le réseau alors que ce n'est pas vrai, la bande est disponible.

L'attaquant SSDF profite de cette stratégie puisqu'elle indique toujours la présence d'un signal sortant et le résultat est toujours occupé, et pour résoudre ce problème, la valeur du seuil sera augmentée cela conduit à un accroissement de la probabilité de détection de défauts [26].

WSRT (Weighted Sequential Ratio Test) est une stratégie qui a été suggérée pour se défendre contre les attaques SSDF.

Dans la structure Ad Hoc, les nœuds qui détectent le spectre vont rassembler les données et les rapports de détection des voisins.

Les deux étapes principales de cette technique sont :

- **Maintenance de la valeur :** chaque nœud a une valeur initiale égale à zéro, la valeur sera augmentée de 1 si le spectre est correct [13].
- **Hypothèse d'essai de WSPRT** : cette phase suppose le test de probabilité de séquence et la valeur du terminal. WSRT ressemble à la technique des réseaux de capteurs sans fils (WSN) [27].

Un dispositif a été suggéré pour l'identification des attaques Byzantins, permet de compter les décalages entre les décisions locales et les décisions globales, après la suppression des byzantins du processus. Cette technique est robuste contre les attaques SSDF [27].

Une autre technique a été proposée, algorithme de détection des utilisateurs malveillants qui permet de calculer le niveau suspect des SU par une stratégie qui calcule une valeur de confiance c'est avec cette valeur que la séparation entre SU légitime et SU malveillant peut être fait. Tous ces systèmes de défense qui ont été cités ci-dessus ont des techniques et des mécanismes robustes et sécurisées, mais toujours la dégradation des performances [28].

1.6.1.2.2 CCSD (Control Channel Saturation DoSAttack)

La négociation des canaux d'un processus RC est répartie, en utilisant un réseau radio cognitif multi hop. Pour la réservation du canal, des échanges de trame Mac seront faits dans cette étape de négociation. Dans le cas où tous les RRC communiquent en même temps, le canal supporte qu'un nombre limité des données, et donc l'attaquant profite de cette situation et il envoie des trames Mac truquées pour saturer le canal et diminuer les performances. Le fonctionnement de cette attaque est juste dans le RRC multi hop et non pas le centralisé car dans le centralisé les trames sont authentifiées par une station de base [11].

1.6.1.2.3 SCN (Selfish Channel Negociation)

Le RRC peut rejeter la transmission des données pour d'autres réseaux, et alors le nœud RC peut conserver son énergie et augmenter le débit. Un scénario similaire lorsque l'hôte égoïste peut modifier le comportement Mac d'un RC. Cette attaque dégrade le débit du RRC [10].

Solution contre CCS et SCN : afin de minimiser la gravité de ces deux attaques CCS et SCN, il faut adapter une architecture de confiance où tout hôte suspect RC sera surveillé et évalué par ses voisins. Un voisin peut alors effectuer une analyse séquentielle sur l'ensemble des données d'observation, et conclure une décision finale, qu'il s'agisse d'un mauvais comportement ou non.Le test de rapport de probabilité séquentiel peut être utilisé à cette fin, car il a prouvé son efficacité en termes de temps de détection [29].

1.6.1.3 Les attaques de la couche réseau (Network Attack Layer)

Le développement dans le RRC s'est concentré sur les deux couches Physique et Liaison ce qui a causé des problèmes de routage, le RRC avec ces trois architectures présente des vulnérabilités même aux anciennes attaques du réseau sans fils. Dans ce qui suit une discussion sur les deux attaques les plus pertinentes contre le RRC, l'attaque Sinkhole (les puits) et l'attaque Hello Flood (inondation Hello) [24] [1].

1.6.1.3.1 Attaque Sinkhole

Dans cette attaque, l'attaquant se présente comme le meilleur itinéraire vers une destination spécifique attirant les nœuds voisins et transmettant leurs paquets ; cette attaque peut être la clé d'une autre attaque vue que les données pourront être lues, modifiées et supprimées. L'attaque n'est efficace que sur les architectures avec infrastructure et maillées où le trafic passe par une station de base [24] [1].

Solution contre Sinkhole : l'attaque de puits peut être difficile à détecter car elle exploite la même conception du protocole de routage et de l'architecture réseau, cependant il existe des protocoles qui ont empêché cette attaque comme le protocole Géographique, le principe de ce protocole est de construire une topologie aux besoins, en utilisant uniquement des communications et des informations locales sans avoir besoin d'initiation à partir de la station de base [1].

1.6.1.3.2 Attaque Hello Flood

Cette attaque est plus défectueuse que celle décrite au-dessus, ici l'attaquant fait une diffusion à tous les nœuds du réseau avec une bonne qualité de service afin de les convaincre que c'est leurs voisins, par exemple un attaquant envoie un paquet publicitaire d'un lien de haute qualité vers une destination spécifique encouragera même les nœuds lointains à utiliser cette route et pourra les convaincre qu'il est leur voisin, toutefois leurs paquets seront perdus et si un nœud découvre l'attaque il sera laissé sans voisin à transmettre ses paquets car tous vont utiliser la même malice route [20].

Solution contre Hello Flood : pour se défendre contre cette attaque, l'idée c'est d'utiliser une clé symétrique, elle devrait être partagée avec une station base de confiance, la station de base servira de tierce partie de confiance comme dans Kerberos5 et facilitera l'établissement des clés de session entre les parties réseaux. Afin de protéger leurs communication cette clé peut être utilisée par les nœuds pour vérifier l'identité de chacun et pour authentifier et chiffrer le lien entre eux, le nombre de clé partagé doit être limité pour empêcher n'importe quels nœuds intrus de créer une clé avec chaque nœud du réseau, de plus un nœud prétendant être le voisin de tant de nœuds dans un réseau doit déclencher une alarme, les algorithmes de clés symétrique sont les plus suggérés car ils sont rapides.

En général pour se défendre contre les attaques de routage, il y a des protocoles de sécurité de routage tel qu'un protocole de routage ad hoc SEAD (Secure Efficient Ad hoc

Distance Vector) à vecteur de distance, ce protocole protège contre les attaques de DoS car il réalise une fonction de hachage unidirectionnel au lieu du cryptage asymétrique pour empêcher les attaquants de tenter de faire en sorte que d'autres nœuds utilisent plus de bande passante ou de temps de traitement [24] [20].

1.6.1.4 Les attaques de la couche transport (Transport Attack Layer)

La couche transport (Transport Layer) peut être attaquée de plusieurs attaques qui visent les réseaux Ad Hoc sans fil, par exemple, l'attaque Lion qui cible le réseau radio cognitif.

L'attaque Lion peut être considérée comme une attaque cross-layer (multicouche) effectuée sur la couche physique qui applique PUE (l'attaque d'émulation d'utilisateur principal) afin d'interrompre la connexion TCP où les SU seront forcés de faire un changement de fréquence comme solution à l'attaque PUE, ainsi le protocole TCP ne sera pas au courant de ce changement et continuera à créer des connexions logiques et à envoyer des paquets sans recevoir des acquittements, les segments TCP commencent alors à expirer et par conséquent TCP retransmet ces segments avec un timeout accrue et cela engendre une perte de paquets. De plus l'attaquant peut aussi interrompre les messages pendant le transfert de fréquence, cela conduit à une famine totale sur le réseau [23].

Solution contre Lion Attack : pour diminuer l'effet de l'attaque du Lion, les auteurs Hernandez Serrano et AL proposent une stratégie qui permet de rendre le protocole TCP sensoriel de ce qui passe dans la couche physique, en utilisant le partage de données entre les couches : Physique, liaison et transport [30].

Les mécanismes utilisés dans le RRC bloquent les paramètres de connexion TCP, pendant le changement de fréquence et les ajustent aux nouvelles conditions du réseau.

La gestion de clé de groupe GKM (group key management) a été utilisée pour que les données de contrôle soient fiables. Cette technique permet de crypter, décrypter et d'authentifier les membres du réseau radio cognitif. Aussi, un IDS (Système de Détection d'Intrusion) multicouches a été utilisé pour trouver la source d'attaque [23], comme indiqué dans la figure suivante :

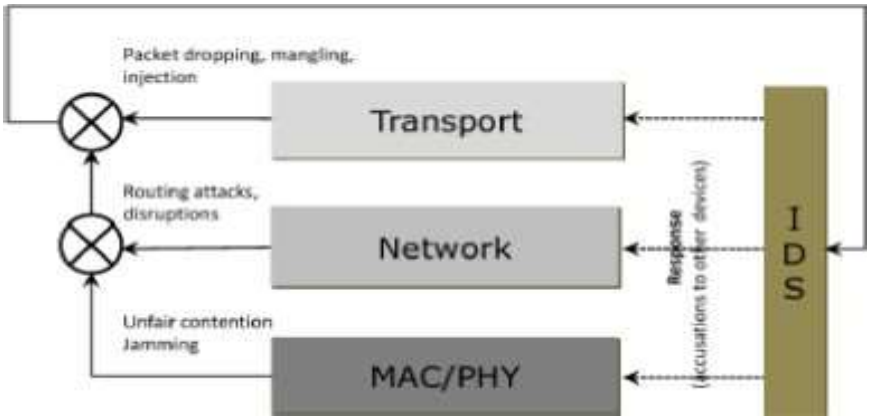


Figure I.13: IDS, Système de détection d'intrusion [23].

1.7 Domaine d'application de la Radio Cognitive

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

- **Les réseaux sans fil de prochaine génération :** La radio cognitive devrait être une technologie clé pour la prochaine génération de réseaux sans fil hétérogènes. La radio cognitive fournira des renseignements intelligents à la fois pour l'utilisateur et pour le fournisseur d'équipements. Pour l'utilisateur, un dispositif mobile avec des interfaces d'air multiples (WiFi, WiMAX, cellulaires) peut observer l'état des réseaux d'accès sans fil (la qualité de transmission, débit, délai) et prendre une décision sur la sélection de l'accès au réseau pour communiquer avec. Pour le fournisseur, les ressources radio de plusieurs réseaux peuvent être optimisées pour l'ensemble des utilisateurs de mobiles et de leurs exigences de QoS [2].
- **Coexistence de différentes technologies sans fil :** Les nouvelles technologies sans fil (IEEE 802.22) sont en cours d'élaboration pour la réutilisation des fréquences radio allouées à d'autres services sans fil (service TV). La radio cognitive est une solution qui fournit la coexistence de ces différentes technologies et services sans fil. Par exemple, IEEE 802.22, basée sur les utilisateurs WRAN peut utiliser efficacement la bande TV quand il n'y a pas d'utilisation du téléviseur à proximité ou quand une station de télévision ne diffuse pas [2].
- **Services de cyber santé (eHealth services):** Différents types de

technologies sans fil sont adoptés dans les services de santé pour améliorer l'efficacité de la prise en charge des patients et la gestion des soins de santé. Cependant, la plupart des dispositifs de soins utilisés sont sans fil et sont limités par les EMI (interférences électromagnétiques) et EMC (compatibilité électromagnétique). Depuis que les équipements médicaux et les capteurs bio signal sont sensibles aux EMI, la puissance d'émission des appareils sans fil doit être soigneusement contrôlée. En outre, différents dispositifs biomédicaux (équipement et appareils chirurgicaux, de diagnostic et de suivi) utilisent la transmission RF. L'utilisation du spectre de ces dispositifs doit être choisie avec soin pour éviter toute interférence avec l'autre. Dans ce cas, les concepts de la radio cognitive peuvent être appliqués. Par exemple, de nombreux capteurs médicaux sans fil sont conçus pour fonctionner dans les ISM (industriel, Scientifique et Médicale), et donc ils peuvent utiliser les concepts de la radio cognitive pour choisir les bandes de transmission permettant d'éviter les interférences [2].

- **Réseaux d'urgence :** les réseaux de sécurité publique et d'urgence peuvent profiter des concepts de la radio cognitive pour fournir la fiabilité et la flexibilité de communication sans fil. Par exemple, dans un scénario où il y a une catastrophe, l'infrastructure de communication standard peut ne pas être disponible, et par conséquent, un système de communication sans fil adaptatif (soit un réseau d'urgence) peut être nécessaire d'être créé pour soutenir la reprise après sinistre. Ce genre de réseau peut utiliser le concept de la radio cognitive pour permettre la transmission sans fil et la réception sur une large gamme du spectre radio [2].
- **Réseaux militaires :** Avec la radio cognitive, les paramètres de la communication sans fil peuvent être adaptés de manière dynamique en fonction du temps et de l'emplacement ainsi que de la mission des soldats. Par exemple, si certaines fréquences sont brouillées ou bruyantes, les dispositifs radio cognitifs (émetteurs/récepteurs) peuvent effectuer des recherches pour trouver des bandes de fréquence d'accès de rechange pour la communication [2].

1.8 Conclusion

La radio cognitive est un domaine technologique à la pointe des télécommunications et de l'intelligence artificielle. C'est d'abord un système radio qui, en plus de sa fonction principale (la communication), établit une "boucle cognitive" qui lui permet de comprendre son contexte et d'agir en conséquence. Cela offre aux utilisateurs un débit et une qualité de service plus élevés.

Nous avons présenté dans ce chapitre des notions importantes concernant la radio cognitive, ainsi que ses principes, en passant par une petite description de la radio logicielle jusqu'aux algorithmes intelligents utilisés dans le domaine de la radio cognitive.

Notre prochaine étude sera sur les systèmes multi-agent dont la technologie principale pour les futurs communications son fil qui la radio cognitive.

Chapitre 2
SMA et Algorithme d'Authentification dans les RRC

Sommaire

2.1 Introduction

À la différence de l'intelligence artificielle classique qui modélise le comportement intelligent d'un seul agent, les systèmes multi-agents s'intéressent à des comportements intelligents qui sont le produit de l'activité coopérative de plusieurs agents ou compétitive de chaque agent.

Le passage du comportement individuel aux comportements collectifs et considéré non seulement comme une extension mais aussi comme un enrichissement de l'intelligence artificielle, d'où émergent de nouvelles propriétés et de nouveaux comportements.

Les systèmes multi-agents (SMA) représentent actuellement un domaine très actif et largement appliqué notamment dans les réseaux radio cognitifs (RRC).

Dans ce chapitre, nous parlerons d'abord du système multi-agent et des notions d'agent puis des différents algorithmes de chiffrement et de quelques notions d'authentification afin de protéger un agent contre le piratage ou toute perte d'informations en le renforçant par un algorithme de cryptage puissant et rapide.

2.2 Les systèmes multi-agents (SMA)

2.2.1 Qu'est-ce qu'un agent ?

On appelle « agent » une entité physique ou virtuelle :

- Qui est capable d'agir dans un environnement,
- Qui peut communiquer directement avec d'autres agents,
- Qui sont guidés par un ensemble de directions (sous forme d'objectifs individuels ou d'une fonction de satisfaction, qu'il cherche à améliorer),
- Qui possède des ressources propres,
- Qui est capable de percevoir (mais de manière limitée) son environnement,
- Qui ne dispose que d'une représentation partielle de cet environnement (et éventuellement aucune),
- Qui possède des compétences et offre des services,
- Qui peut éventuellement se reproduire,
- Dont le comportement tend à satisfaire ses objectifs, en tenant compte des ressources et des compétences dont elle dispose, et en fonction de sa perception, de ses représentations et des communications qu'elle reçoit.

Chacun des termes de cette définition est important. Une entité physique est quelque chose qui agit dans le monde réel : un robot, un avion ou une voiture sont des exemples d'entités physiques. En revanche, un composant logiciel, un module informatique sont des entités virtuelles, car elles n'existent pas physiquement.

Les agents sont capables d'agir, et non pas seulement de raisonner comme dans les systèmes d'IA classique.

L'action, qui est un concept fondamental pour les systèmes multi-agents, repose sur le fait que les agents accomplissent des actions qui vont modifier l'environnement des agents et donc leurs prises de décision futures.

Ils peuvent aussi communiquer entre eux, et c'est d'ailleurs l`a l'un des modes principaux d'interaction existant entre les agents.

Les agents n'ont qu'une représentation partielle de leur environnement, c'est-à-dire qu'ils n'ont pas de vision globale de tout ce qui se passe. C'est d'ailleurs ce qui se passe dans les réalisations humaines d'envergure (la fabrication d'un Airbus par exemple) dans lesquelles personne ne connaît tous les détails de la réalisation, chaque spécialiste n'ayant qu'une vue partielle correspondant à son domaine de compétence.

L'agent est ainsi une sorte "d'organisme vivant" dont le comportement, qui se résume à communiquer, à agir et, éventuellement, à se reproduire, vise à la satisfaction de ses besoins et de ses objectifs à partir de tous les autres éléments (Perceptions, représentations, actions, communications et ressources) dont il dispose [31].

2.2.1.1 l'agent purement communicant

Par comparaison avec la définition générale d'un agent donnée précédemment, on appelle agent purement communicant (ou agent logiciel) une entité informatique qui :

- Se trouve dans un système informatique ouvert (ensemble d'applications, de réseaux et de systèmes hétérogènes)
- Peut communiquer avec d'autres agents,
- Est mue par un ensemble d'objectifs propres,
- Possède des ressources propres,
- Ne dispose que d'une représentation partielle des autres agents,
- Possède des compétences (services) qu'elle peut offrir aux autres agents,
- A un comportement tendant à satisfaire ses objectifs, en tenant compte des ressources et des compétences dont elle dispose et en fonction de ses

représentations et des communications qu'elle reçoit.

Un agent purement communicant se distingue donc de la notion d'agent en général par le fait qu'il ne possède pas de perception des autres agents, que ses tendances prennent l'aspect d'objectifs, qu'il n'agit pas dans un environnement et que son contexte d'évolution est naturellement celui des réseaux informatiques [31].

2.2.1.2 l'agent purement situé

On appelle agent purement situé une entité physique (ou éventuellement informatique si on la simule) qui :

- Se trouve située dans un environnement,
- Est piloté par une fonction de survie
- Possède des ressources propres, sous la forme d'énergie et d'outils,
- Est capable de percevoir (mais de manière limitée) son environnement,
- Ne possède pratiquement aucune représentation de son environnement,
- Possède des compétences,
- Peut éventuellement se reproduire,
- A un comportement tendant à satisfaire sa fonction de survie, entenant compte des ressources, des perceptions et des compétences dont elle dispose.

Les agents purement situés sont donc à l'opposé des agents logiciels en ce qui concerne les capacités de représentations (quasiment nulles) et le fait que les communications ne s'effectuent généralement pas directement, mais indirectement par le biais des perceptions et de leurs actions dans l'environnement [31].

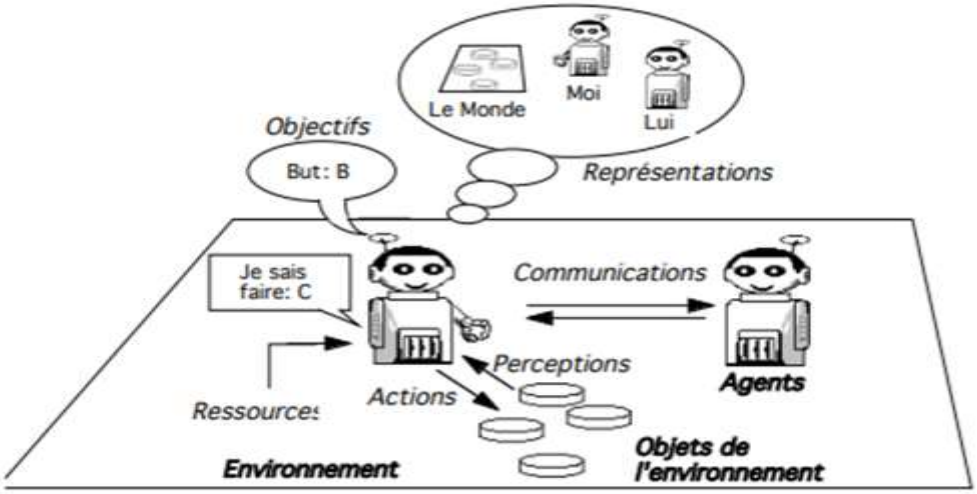


Figure II.1 : un agent en interaction avec son environnement et les autres agents [31]

2.2.2 Définition des systèmes multi-agent

On appelle système multi-agent (ou SMA), un système composé des éléments suivants :

- Un environnement E, c'est-à-dire un espace disposant généralement d'une métrique.
- Un ensemble d'objets O. Ces objets sont situés, c'est-à-dire que, pour tout objet, il est possible, à un moment donné, d'associer une position dans E. Ces objets sont passifs, c'est-à-dire qu'ils peuvent être perçus, créés, détruits et modifiés par les agents.
- Un ensemble A d'agents, qui sont des objets particuliers ($A \subseteq O$), lesquels représentent les entités actives du système.
- Un ensemble de relations R qui unissent des objets (et donc des agents) entre eux.
- Un ensemble d'opérations Op permettant aux agents de A de percevoir, produire, consommer, transformer et manipuler des objets de O.
- Des opérateurs chargés de représenter l'application de ces opérations et la réaction du monde à cette tentative de modification, que l'on appellera les lois de l'univers.

Par exemple, dans un univers de robots, les agents A sont les robots, E est l'espace géométrique euclidien dans lequel se déplacent les robots et O se compose évidemment des agents, mais aussi de l'ensemble des objets physiques placés ici et là, et que les robots doivent éviter, prendre ou manipuler. Les opérations Op sont les actions que les robots peuvent faire en se déplaçant, en bougeant les autres objets ou en communiquant, et R est l'ensemble des relations qui unissent certains agents à d'autres, telles que des relations d'accointances (certains agents en connaissent d'autres) et les relations de communicabilité (les agents peuvent communiquer avec certains agents mais pas nécessairement avec tous).

Il existe un cas particulier de systèmes dans lequel A = O, et E est égal à l'ensemble vide. Dans ce cas, les relations R définissent un réseau : chaque agent est lié directement à un ensemble d'autres agents, que l'on appelle ses accointances.

Ces systèmes, que l'on peut appeler SMA purement communicants sont très courants en intelligence artificielle distribuée. Leur domaine de prédilection est la coopération de modules logiciels dont la fonction est de résoudre un problème ou d'élaborer une expertise

(interprétation de signaux ou conception d'un produit par exemple) à partir de modules spécialisés [31].

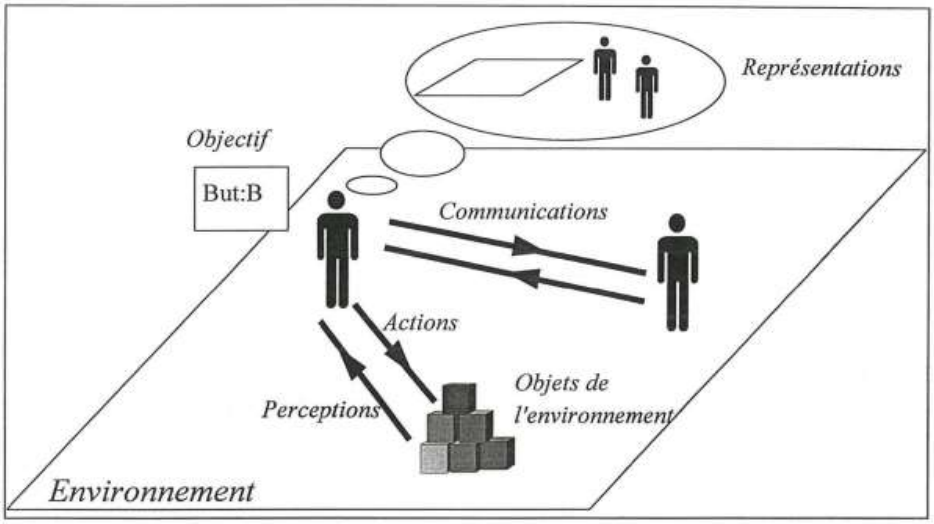


Figure II.2: représentation imagée d'un système multi-agent [31].

2.2.2.1 Catégories ou modèles d'agents dans le SMA

On peut établir une classification des agents selon deux critères : agents cognitifs ou réactifs d'une part, comportement téléonomique ou réflexe d'autre part.

La distinction que l'on peut faire entre cognitif et réactif tient essentiellement de la représentation du monde dont dispose l'agent. Si l'individu est doté d'une "représentation symbolique" du monde à partir de laquelle il est capable de formuler des raisonnements, on parlera d'agent cognitif tandis que s'il ne dispose que d'une "représentation sub-symbolique", c'est-à-dire limitée à ses perceptions, on parlera d'agent réactif. Cette distinction cognitif/réactif correspond à deux écoles de pensée des systèmes multi-agents. La première soutient une approche de famille d'agents "intelligents", avec une perspective plus sociologique. La deuxième étudie la possibilité de l'émergence d'un comportement "intelligent" d'un ensemble d'agents non-intelligents (type fourmis).

La seconde distinction entre comportement téléonomique ou réflexe sépare les comportements intentionnels (poursuite de buts explicites) des comportements liés à des perceptions. Les tendances des agents peuvent ainsi être exprimées explicitement dans les agents ou au contraire provenir de l'environnement. Les agents cognitifs sont la plupart du temps intentionnels, c'est-à-dire qu'ils ont des buts fixés qu'ils tentent d'accomplir. On peut

cependant trouver parfois des agents dits modules qui n'ont pas de buts précis, s'ils ont une représentation de leur univers. Ils pourraient servir par exemple à répondre à des interrogations des autres agents sur l'univers.

Les agents réactifs peuvent être séparés en agents pulsionnels et tropiques, un agent pulsionnel aura une mission fixée (par exemple, s'assurer qu'un réservoir reste toujours suffisamment rempli) et déclenchera un comportement s'il perçoit que l'environnement ne répond plus au but qui lui était affecté (le niveau du réservoir est trop bas), l'agent tropique, lui, ne réagit qu'à l'état local de l'environnement (il y a de la lumière, je fuis). La source de motivation est dans un cas interne (agents pulsionnels qui ont une "mission"), dans l'autre cas liée uniquement à l'environnement [31].

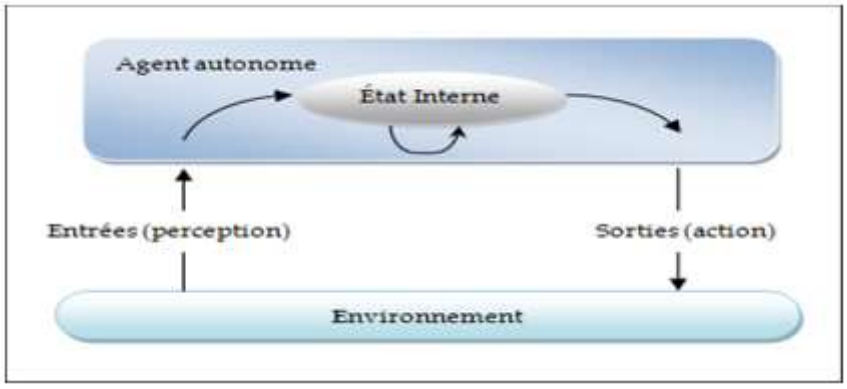


Figure II.3 : structure d'un agent réactif [33].

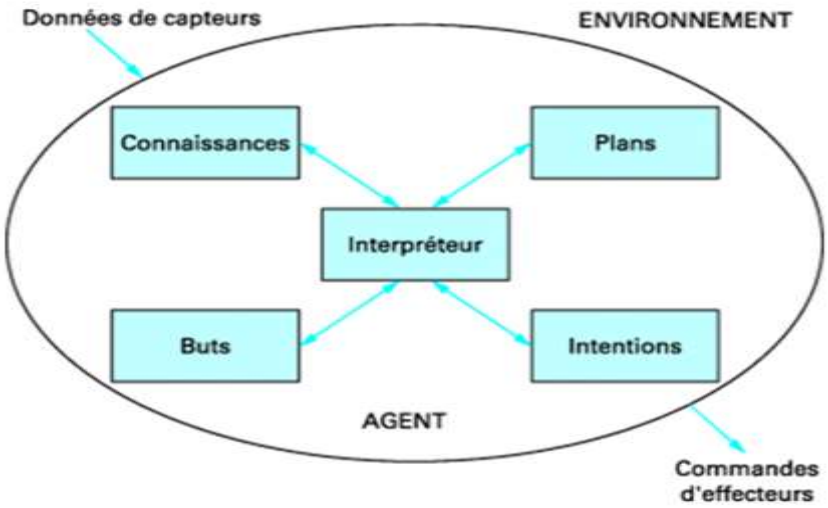


Figure II.4 : structure d'un agent cognitif [32].

2.2.2.2 La Communication entre agents

Un agent doit être capable de communiquer avec les autres agents, les agents doivent avoir des capacités à manipuler un langage commun.

Il y'a 2 types de communication :

- Communication indirecte : Partage d'informations via l'environnement.
- Communication directe : envoi de messages.

L'agent peut participer à un dialogue en étant passif ou actif.

- Un agent passif doit accepter les questions des autres agents et répondre à leurs questions.
- Un agent actif doit proposer et envoyer des interrogations.

Dans un dialogue les agents alternent des rôles actifs et passifs, et échangent des séries de messages en respectant des protocoles bien précis, ce sont les protocoles de coordination, de coopération et de négociation [59].

2.2.2.2.1 Les protocoles de coordination

Les protocoles de coordination aident les agents à gérer leurs engagements, ils lui permettent de gérer ces engagements dans le cas où les circonstances dans lesquelles ils ont été élaborés, évoluent.

Ils définissent aussi sous quelles conditions les engagements peuvent être revus et quelles sont alors les actions à prendre [59].

2.2.2.2.2 Les protocoles de coopération

La coopération entre les agents consiste à décomposer les tâches en sous-tâches puis à les répartir entre les différents agents, il existe plusieurs décompositions possibles, le processus de décomposition doit donc tenir compte des ressources disponibles et des compétences des agents [59].

2.2.2.2.3 La négociation

La négociation intervient lorsque des agents interagissent pour prendre des décisions communes, alors qu'ils poursuivent des buts différents. Les deux principales voies sur la négociation sont :

- Les langages de négociation : il s'agit d'étudier les primitives de

communication pour la négociation, leur sémantique et leur usage dans les protocoles.

- Le processus de négociation : il s'agit de proposer des modèles généraux de comportements des agents en situation de négociation.

Il y'a 2 techniques de négociation :

1. La négociation centrée sur l'environnement : adapter le contexte ou l'environnement à la négociation.
2. La négociation centrée sur l'agent : adapter le comportement de l'agent compte-tenu des propriétés du contexte donné.

Et il y'a 3 types de négociations :

1. One-to-one: agent – agent.
2. Many-to-one: multi agents- agent.
3. Many-to-many: multi agents - multi agents.

La communication inter-agent est fondamentale à la réalisation du paradigme agent, tout comme le développement du langage humain était la clé du développement de l'intelligence humaine et des sociétés.

Pour échanger les informations et les connaissances, les agents utilisent des ACL messages (Agent Communication Language). De nombreux langages de communications entre agents (ACL) se sont développés comme KQML (Knowledge Query and Manipulation Language) et FIPA-ACL (Foundation for Intelligent Physical Agents) [59].

2.2.2.3 L'architecture des systèmes multi-agents

Les agents doivent être dotés de systèmes de décisions et de planification à plusieurs. Les théories de la décision sont un domaine à part entière d'étude à ce sujet. Dans la catégorie des interactions avec l'environnement, un autre problème récurrent des systèmes d'agents est celui du pathfinding (avec son algorithme le plus connu, l'algorithme A*).

Les agents doivent être dotés d'un modèle cognitif : Là aussi, plusieurs modèles existent, l'un des plus classiques étant le modèle BDI (Beliefs-Desires-Intentions). Il considère d'une part l'ensemble de croyances (Beliefs) de l'agent sur son environnement, qui sont le résultat de ses connaissances et de ses perceptions, et d'autre part un ensemble d'objectifs (Desires). En croisant ces deux ensembles, on obtient un nouvel ensemble d'intentions (Intentions) qui peuvent ensuite se traduire directement en actions.

Les agents doivent être dotés d'un système de communication. Plusieurs langages spécialisés ont vu le jour à cette fin : le Knowledge Query and Manipulation Language (KQML), et plus récemment, le standard FIPA-ACL (ACL pour Agent Communication Language) créé par la Foundation for Intelligent Physical Agents FIPA. Ce dernier standard repose en particulier sur la théorie des actes de langage.

La problématique de l'adaptation est un sujet épineux, objet de recherches nombreuses à l'heure actuelle. On pourrait toutefois citer l'exemple de certains virus, aussi bien biologiques qu'informatiques, capables de s'adapter à leur environnement en mutant.

Enfin, l'implémentation effective du système multi-agents, si elle ne fait pas à proprement parler partie de l'architecture du système, mérite d'être évoquée à travers l'exemple des nombreux langages de programmation qui ont été développés à des fins de recherche en intelligence artificielle [31].

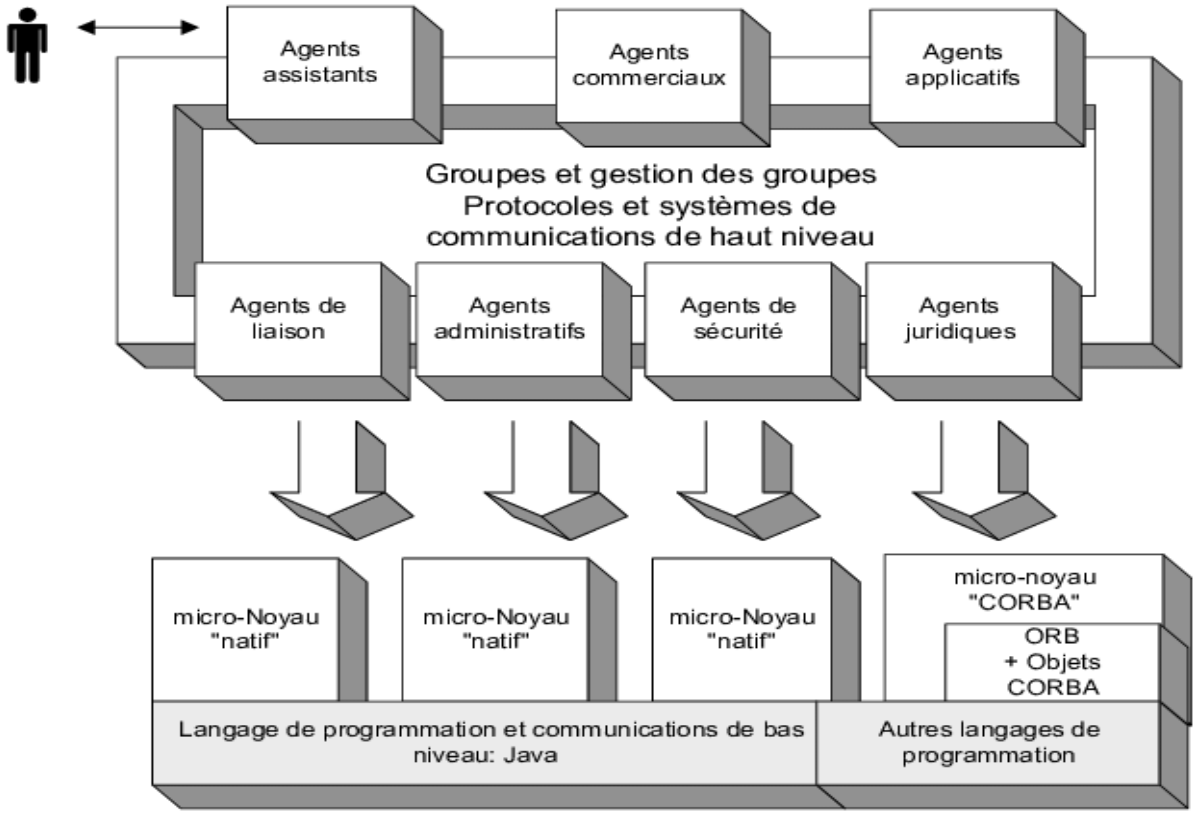


Figure II.5 : L'architecture d'un système multi-agent fonctionnant sur réseau [38]

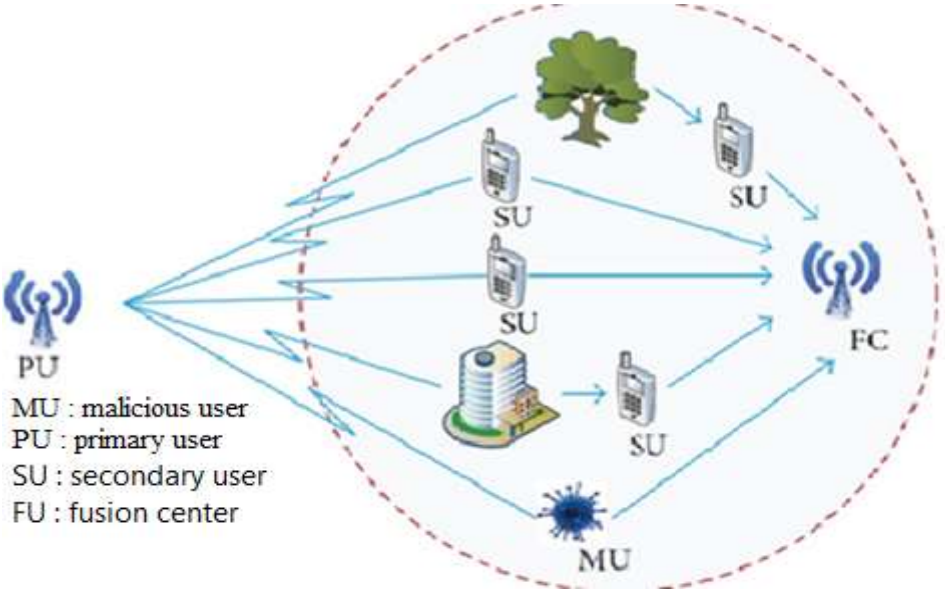


Figure II.6: Réseau radio cognitif [45].

2.2.2.4 Organisation des agents

Avec le développement des systèmes multi-agents, différents paradigmes organisationnels ont été développés. Ces organisations établissent un cadre pour les relations et interactions entre les agents. Nous allons présenter ici les principales organisations [34] :

Hiérarchies : Dans ce modèle, les agents sont hiérarchisés selon la structure d'un arbre, dans lequel chaque nœud représente un agent, et possède un lien d'autorité sur ses nœuds-fils. Ce modèle permet de décomposer la tâche globale du système.

Holarchies : L'holarchie se rapproche de la hiérarchie, mais il existe quand même une différence majeure. En effet, il n'y a pas de relation d'autorité entre un agent et son sous-groupe, mais les agents du sous-groupe constituent "physiquement" leur sur-agent. Pour illustrer cette notion, on peut prendre l'exemple d'une ville, constituée de bâtiments. Les bâtiments sont des agents, et la ville est un agent constitué de ces agents bâtiments. On peut également avoir, à l'échelle supérieure, un agent région qui sera constitué d'agents villes. De même, un banc de poissons ressemble parfois à un poisson plus gros que les poissons qui le composent, le banc comme les poissons sont alors des agents, organisés en holarchie [35].

Coalitions : Une coalition est une alliance temporaire d'agents qui s'unissent et collaborent car leurs intérêts individuels se rencontrent. La valeur de la coalition doit être supérieure à la somme des valeurs individuelles des agents la composant. Pour illustrer cette notion, imaginons que nous ayons des agents qui ont chacun besoin d'un gâteau. Le gâteau

individuel coûte 5 €, et le lot de 6 coûte 24 €. Si six agents forment une coalition pour acheter un lot, chacun pourra repartir avec son gâteau pour seulement 4 €. La coalition leur a donc permis d'optimiser leurs intérêts individuels.

Équipes : Les agents constituant l'équipe travaillent ensemble à la réalisation d'objectifs communs. À la différence des agents d'une coalition, les agents d'une équipe cherchent à maximiser les intérêts de l'équipe plutôt que leurs intérêts personnels.

Congrégations : Les congrégations sont assez similaires aux coalitions et aux équipes. Cependant, elles sont destinées à être permanentes et ont généralement plusieurs objectifs à réaliser. De plus, les agents peuvent entrer et sortir des congrégations, et appartenir à plusieurs congrégations en même temps [36].

Sociétés : La société est un ensemble d'agents variés, qui interagissent et communiquent. Ils possèdent différents objectifs, n'ont pas le même niveau de rationalité, ni les mêmes capacités, mais sont tous soumis à des lois communes (normes).

Fédérations : Les agents d'une fédération cèdent une partie de leur autonomie au délégué de leur groupe. Les agents d'un groupe n'interagissent qu'avec leur délégué, qui lui-même interagit avec les délégués des autres groupes.

Marchés : Des agents vendeurs proposent des objets à la vente, sur lesquels des agents acheteurs peuvent enchérir. Ce genre d'organisation permet, par exemple, de simuler des marchés réels et/ou de comparer différentes stratégies de négociation.

Matrices : Les agents d'une organisation en matrices sont hiérarchisés. Cependant, à la différence de la hiérarchie présentée plus haut, où un agent n'était soumis qu'à l'autorité d'au plus un seul autre agent, les agents dans une organisation matricielle peuvent être soumis à plusieurs autres agents.

Combinaisons : Une organisation combinée mélange plusieurs des styles présentés ci-dessus (ou d'autres qui auraient été oubliés dans cette liste). Cela peut être, par exemple, une fédération de coalitions ou une hiérarchie d'équipes [37].

2.2.2.5 Applications des systèmes multi-agents

Les domaines d'application des systèmes multi-agents sont particulièrement riches. Nous en citerons seulement les principales directions, toute recherche d'exhaustivité étant a priori incompatible dans le cadre d'un domaine de recherche en pleine évolution. On peut

considérer qu'il existe, pour l'instant, trois grandes catégories d'applications des systèmes multi-agents : la conception de systèmes complexes ouverts ou génie logiciel multi-agent, la simulation multi-agent et la robotique distribuée [38].

2.2.2.5.1 Génie logiciel multi-agent

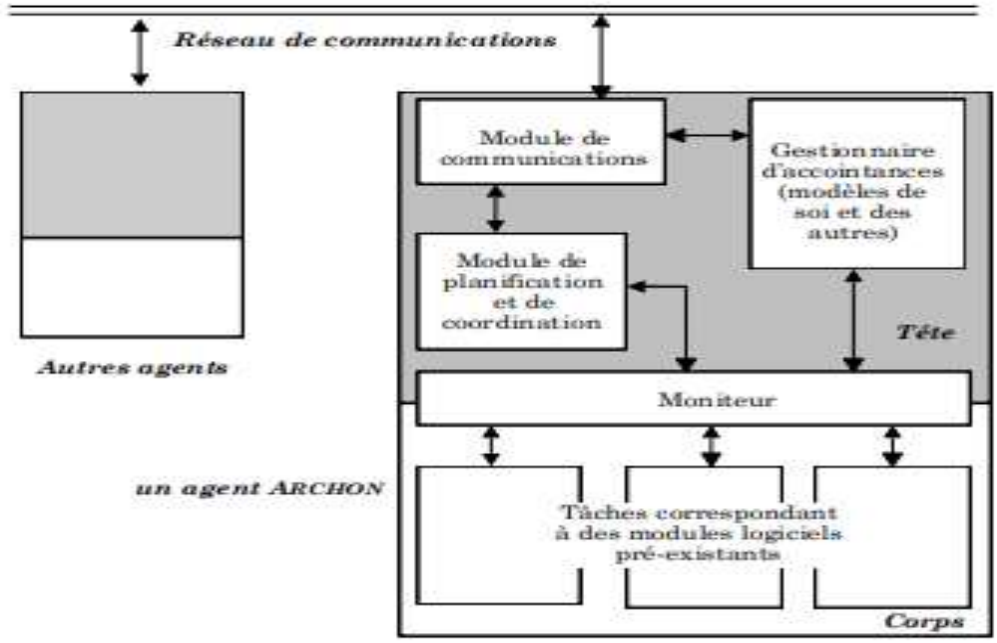
Les SMA proposent une nouvelle technologie de construction de logiciels à partir des concepts d'agent et d'interaction, en considérant que chaque unité de programme peut prendre la forme d'un agent qui dispose de sa propre autonomie, de ses propres objectifs et « vit » sur le réseau comme un animal dans un écosystème naturel, coopère ou négocie avec d'autres unités de même nature. L'un des systèmes les plus connus en Europe pour avoir tenté de donner un cadre opérationnel à ces idées est le système ARCHON (Architecture for Cooperating Heterogeneous On-line Systems), issu d'un projet ESPRIT qui propose une architecture générale de SMA pour intégrer différents programmes devant coopérer ensemble [38].

2.2.2.5.1.1 Niveau cognitif

Le niveau cognitif est composé de la connaissance et des processus. Il introduit la capacité de fonctionnalisation et fait de l'agent un agent cognitif, susceptible de satisfaire les critères d'évaluation [61].

Lorsqu'on parle de SMA d'un point de vue Génie logiciel, il est vrai à dire qu'agent est équivalent à un thread et c'est pour cela que le cycle de vie d'un agent ressemble beaucoup à celui d'un thread. En fusionnant le cycle de vie de la radio cognitive et celui d'un agent dans une plateforme multi-agents [61].

Un thread ou fil d'exécution ou tâche, est similaire à un processus car tous deux représentent l'exécution d'un ensemble d'instructions du langage machine d'un processeur [62].



Figçoure II.7: L'architecture générale du système ARCHON [38].

2.2.2.5.2 Les télécommunications

La plus grande gamme d'applications intéressantes pour les systèmes multi agents dans le cadre de réseaux de télécommunications semble être celle de l'intégration de services et le développement du marché électronique. Il s'agit de mettre en commun des clients et des fournisseurs de services dans une architecture totalement ouverte, clients et fournisseurs étant des agents électroniques qui négocient entre eux des échanges de services. Le système multi-agent constitue alors une sorte de « place de marché électronique », dans lequel les clients émettent des demandes et les fournisseurs envoient des propositions de services. Finalement des contrats sont établis entre clients et fournisseurs, et tout cela de manière automatique ou en tous cas avec une intervention humaine réduite [38].

2.2.2.6 Les problématiques des SMA

On peut relever cinq problématiques principales lors de la création de systèmes multi-agents :

- D'abord, la problématique de l'action : comment un ensemble d'agents peut agir de manière simultanée dans un environnement partagé, et comment cet environnement interagit en retour avec les agents ? Les questions sous-jacentes sont entre autres celles de la représentation de l'environnement par

les agents, de la collaboration entre agents, de la planification multi-agent.

- Ensuite la problématique de l'agent et de sa relation au monde, qui est représentée par le modèle cognitif dont dispose l'agent. L'individu d'une société multi-agent doit être capable de mettre en œuvre les actions qui répondent au mieux à ses objectifs. Cette capacité à la décision est liée à un "état mental" qui reflète les perceptions, les représentations, les croyances et un certain nombre de paramètres "psychiques" (désirs, tendances…) de l'agent. La problématique de l'individu et de sa relation au monde couvre aussi la notion d'engagement de l'agent vis-à-vis d'un agent tiers.
- Les systèmes multi-agents passent aussi par l'étude de la nature des interactions, comme source de possibilités d'une part et de contraintes d'autre part. La problématique de l'interaction s'intéresse aux moyens de l'interaction (quel langage ? quel support ?), et à l'analyse et la conception des formes d'interactions entre agents. Les notions de collaboration et coopération (en prenant coopération comme collaboration + coordination d'actions + résolution de conflits) sont ici centrales.
- On peut évoquer ensuite la problématique de l'adaptation en termes d'adaptation individuelle ou apprentissage d'une part et d'adaptation collective ou évolution d'autre part.
- Enfin, il reste la question de la réalisation effective et de l'implémentation des SMA, en structurant notamment les langages de programmation en plusieurs types allant du langage de type L5, ou langage de formalisation et de spécification, au langage de type L1 qui est le langage d'implémentation effective. Entre les deux, on retrouve le langage de communication entre agents, de description des lois de l'environnement et de représentation des connaissances [31].

2.3 La sécurité dans les SMA dédier au RRC

La sécurité c'est d'assurer un certain nombre d'exigences à travers l'authentification et l'autorisation tout en prenant en compte les ressources limitées des utilisateurs :

- Faire en sorte qu'un utilisateur non autorisé qu'on appellera adversaire ou attaquant dans la suite, ne réussisse pas à intégrer ou à utiliser les services du réseau.

- Les utilisateurs autorisés ne doivent pas traiter ou recevoir des données corrompues.
- L'accès au réseau ne doit pas être interdit aux utilisateurs légitimes.

Le mécanisme doit également prendre en compte les exigences des utilisateurs en termes de capacité de stockage, de calcul et de transmission. Ainsi, le mécanisme de contrôle d'accès doit minimiser le stockage des clés et utiliser des algorithmes cryptographiques moins coûteux en calcul.

- Il faut des protocoles de contrôle d'accès qui minimisent le temps de transmission.
- Pour assurer l'authentification, les utilisateurs doivent déchiffrer puis chiffrer les messages reçus, cela nécessite beaucoup de calculs et une augmentation du temps de traitement. Ce qui ne répond pas aux exigences de certaines applications comme le cas d'une application temps réel [44].

2.3.1 L'authentification

L'authentification est la fonction de sécurité qui consiste à apporter et à contrôler la preuve de l'identité d'une personne, de l'émetteur d'un message, d'un logiciel, d'un serveur logique ou d'un équipement.

En ce qui concerne l'authentification des personnes, la terminologie est la suivante :

- S'identifier consiste à donner/délivrer son identité.
- Identifier une personne consiste à demander et obtenir son identité.
- S'authentifier consiste à apporter/délivrer la preuve de son identité.
- Authentifier consiste à vérifier l'identité d'une personne en lui demandant une preuve tangible de son identité puis en validant ou en invalidant cette preuve.

Il existe des notions connexes à l'authentification qui doivent être comprises pour ne pas entraîner de confusion.

L'autorisation correspond à l'allocation des droits d'accès aux ressources du système d'information aux utilisateurs authentifiés au préalable [60].

2.3.2 La cryptographie

La cryptographie est sans doute la technique la plus utilisée dans le cadre des réseaux filaires et des réseaux sans fil traditionnels disposant d'une capacité de calcul et de mémoire conséquente. Les solutions de cryptographie sont réputées comme des solutions sures qui

répondent à l'ensemble des problèmes liés à la sécurité des données. Les spécificités des réseaux de capteurs, à savoir une faible puissance de calcul et une mémoire limitée auxquelles se rajoute la problématique de préservation de l'énergie, sont des freins considérables à l'utilisation des systèmes cryptographiques courant réputés sûrs (SSL, RSA, ˆ etc.).

Les travaux de recherche actuels s'attachent à trouver des solutions dites de cryptographie légère [39]. Ces solutions consistent à adapter les algorithmes de cryptographie classiques pour les réseaux de capteurs, ou à en trouver de nouveau tout aussi efficaces en termes de sécurité, de temps d'exécution et de consommation énergétique. On distingue deux types de cryptographie : la cryptographie symétrique à clé secrète et la cryptographie asymétrique ou à clé publique [44].

2.3.2.1 La cryptographie symétrique

Un algorithme de chiffrement symétrique transforme un message en clair P avec une clé secrète K. Le résultat est un message chiffré C. La fonction de chiffrement doit être inversible [52].

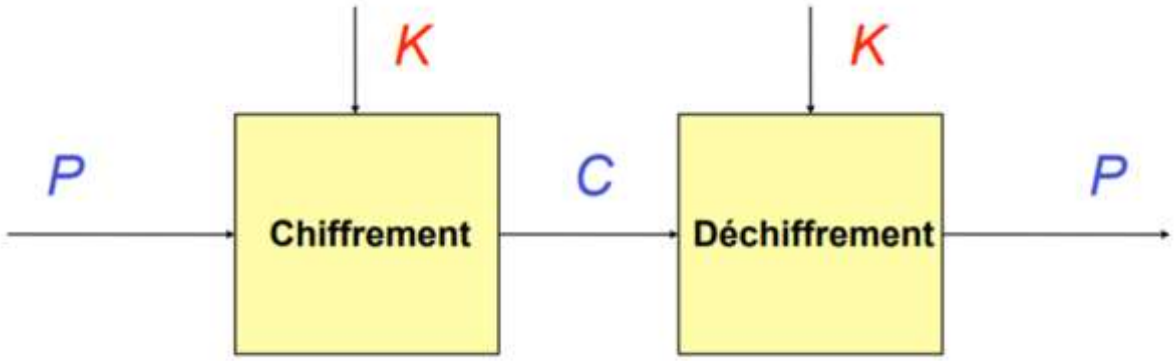


Figure II.8 : La cryptographie symétrique [52].

2.3.2.1.1 Algorithme de chiffrement DES

Il s'agit d'un système de chiffrement symétrique par blocs de 64 bits, dont 8 bits (un octet) servent de test de parité (pour vérifier l'intégrité de la clé). Chaque bit de parité de la clé (1 tous les 8 bits) sert à tester un des octets de la clé par parité impaire, c'est-à-dire que chacun des bits de parité est ajusté de façon à avoir un nombre impair de '1' dans l'octet à qui il appartient. La clé possède donc une longueur « utile » de 56 bits, ce qui signifie que seuls 56 bits servent réellement dans l'algorithme.

L'algorithme consiste à effectuer des combinaisons, des substitutions et des permutations entre le texte à chiffrer et la clé, en faisant en sorte que les opérations puissent se faire dans les deux sens (pour le déchiffrement). La combinaison entre substitutions et permutations est appelée code produit.

La clé est codée sur 64 bits et formée de 16 blocs de 4 bits, généralement notés k1 à k16. Etant donné que « seuls » 56 bits servent effectivement à chiffrer, il peut exister 256 (soit 7.2*1016) clés différentes [53].

2.3.2.1.2 Algorithme de chiffrement 3DES

Le Triple DES (aussi appelé 3DES ou TDES) est un algorithme de chiffrement symétrique par bloc, enchaînant 3 applications successives de l'algorithme DES sur le même bloc de données de 64 bits, avec 2 ou 3 clés DES différentes [54].

Cette utilisation de trois chiffrements DES a été développée par IBM, présenté en 1998 (sous la référence de ANSI X9.52) puis publié en 1999. Il existe en effet d'autres manières d'employer trois fois DES mais elles ne sont pas forcément sûres. Cette version utilise un chiffrement, suivi d'un déchiffrement pour se conclure à nouveau par un chiffrement [55].

Le Triple DES est généralement utilisé avec seulement deux clés différentes. Le mode d'usage standard est de l'utiliser en mode EDE (Encryption, Decryption, Encryption, c'est-à-dire Chiffrement, Déchiffrement, Chiffrement) ce qui le rend compatible avec DES quand on utilise trois fois la même clé. Dans le cas d'une implémentation matérielle cela permet d'utiliser le même composant pour respecter le standard DES et le standard Triple DES [55].

2.3.2.1.3 Algorithme de chiffrement AES

AES (Advanced Encryption Standard), il s'agit d'un système de chiffrement symétrique par blocs. On peut aussi le nommer Rijndael qui est le nom du créateur.

C'est un chiffrement par bloc, L'algorithme prend en entrée un bloc de 128 bits (16 octets),192 bits ou 256 bits, et la clé fait 128, 192 ou 256 bits.
AES est implémenté dans des logiciels et du matériel à travers le monde pour chiffrer les données sensibles, Il est essentiel pour la sécurité informatique, la cyber sécurité et la protection des données électroniques mais on le trouve de plus en plus tous les jours, pour le chiffrement de base de données ou de stockage de données, par exemple, on utilise AES pour chiffrer un fichier ou disque dur ou le stockage de mot de passe comme les gestionnaires de mots de passe,

la protection par mot de passe de fichiers PDF ou de fichiers ZIP.

En effet, les applications telles que WhatsApp, Signal, VeraCrypt ou 7-zip et WinZip utilisent AES pour chiffrer (crypter) les communications ou le contenu en clair donc, AES est très utilise pour protéger ses données [51].

Le chiffrement par blocs AES a été proposé comme algorithme de chiffrement dans le standard IEEE 802.15.4 pour sécuriser au niveau de la couche MAC les données transitant sur des réseaux de capteurs sans fil. Le temps d'exécution de cet algorithme de chiffrement donne d'assez bons résultats (de l'ordre de plusieurs microsecondes) et limite le surcoût énergétique du chiffrement de données [40].

2.3.2.2 La cryptographie asymétrique

Un chiffrement asymétrique est un cryptage où l'algorithme de chiffrement n'est pas le même que celui de déchiffrement, et où les clés utilisées sont différentes.

L'intérêt est énorme : il n'y a plus besoin de transmettre la clé à son destinataire, il suffit de publier librement les clés de cryptage. N'importe qui peut alors crypter un message, mais seul son destinataire, qui possède la clé de décodage, pourra le lire [58]

La cryptographie asymétrique, ou cryptographie à clef publique est un domaine relativement récent de la cryptographie. Elle permet d'assurer la confidentialité d'une communication, ou d'authentifier les participants, sans que cela repose sur une donnée secrète partagée entre ceux-ci, contrairement à la cryptographie symétrique qui nécessite ce secret partagé préalable.

La cryptographie asymétrique peut être illustrée avec l'exemple du chiffrement à clef publique et privée, dont le but, comme tout chiffrement, est de garantir la confidentialité d'une donnée lors d'une transmission de celle-ci. Le terme asymétrique s'explique par le fait qu'il utilise deux clefs différentes, l'une, la clef publique, pour chiffrer, l'autre, la clef privée, pour déchiffrer. L'utilisateur qui souhaite recevoir des messages engendre un tel couple de clefs. Il ne transmet à personne la clef privée alors que la clef publique est transmissible sans restriction [57].

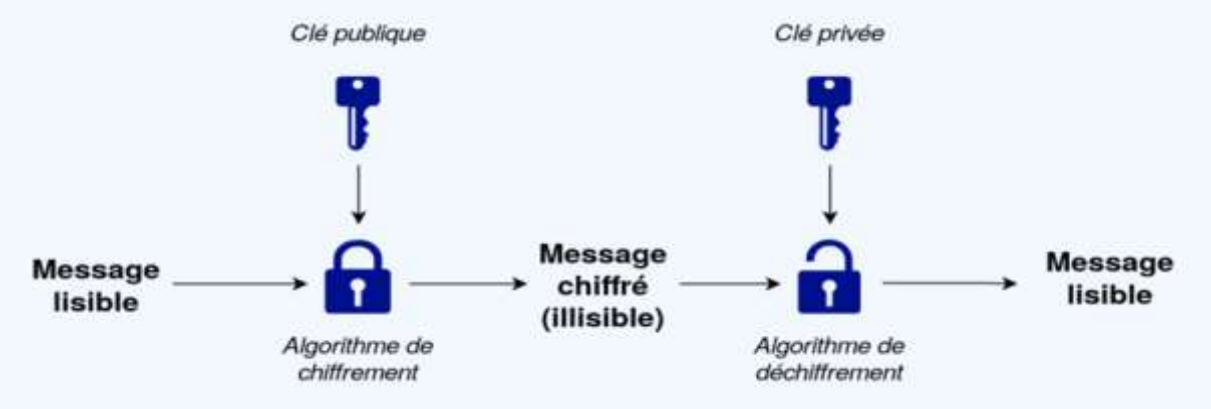


Figure II.9 : LA CRYPTOGRAPHIE ASYMÉTRIQUE [59].

2.3.2.2.1 La signature numérique (ou digitale)

La cryptographie à clé publique permet de s'affranchir du problème de l'échange de la clé, facilitant le travail de l'expéditeur. Mais comment s'assurer de l'authenticité de l'envoi ? Comment être sûr que personne n'usurpe l'identité d'Alice pour vous envoyer un message ? Comment être sûr qu'Alice ne va pas nier vous avoir envoyé ce message ?

La norme (ISO 7498-2) définit la signature numérique comme des "données ajoutées à une unité de données, ou transformation cryptographique d'une unité de données, permettant à un destinataire de prouver la source et l'intégrité de l'unité de données et protégeant contre la contrefaçon (par le destinataire, par exemple)". La mention "protégeant contre la contrefaçon" implique que seul l'expéditeur doit être capable de générer la signature.

Une signature numérique fournit donc les services d'authentification de l'origine des données, d'intégrité des données et de non répudiation. Ce dernier point la différencie des codes d'authentification de message, et a pour conséquence que la plupart des algorithmes de signature utilisent la cryptographie à clef publique [65].

2.3.2.2.1.1 Signature et Fonctions de hachage

Les procédés de signatures ne permettant designer que des petits messages (128ou160bits). Que se passera-t-il lorsqu'on veut signer des messages beaucoup plus longs ? On peut découper le message en blocs, et signer chacun d'entre eux, cette approche est très lente, et elle ne garantit pas contre un réarrangement des blocs qui peut changer la signification du message.

Une solution consiste à compresser le message en utilisant une fonction de hachage,

cette fonction doit être rapide à calculer, transforme un message de longueur arbitraire en une empreinte numérique de longueur fixe. Ensuite on signe l'empreinte pour authentifier le message [64].

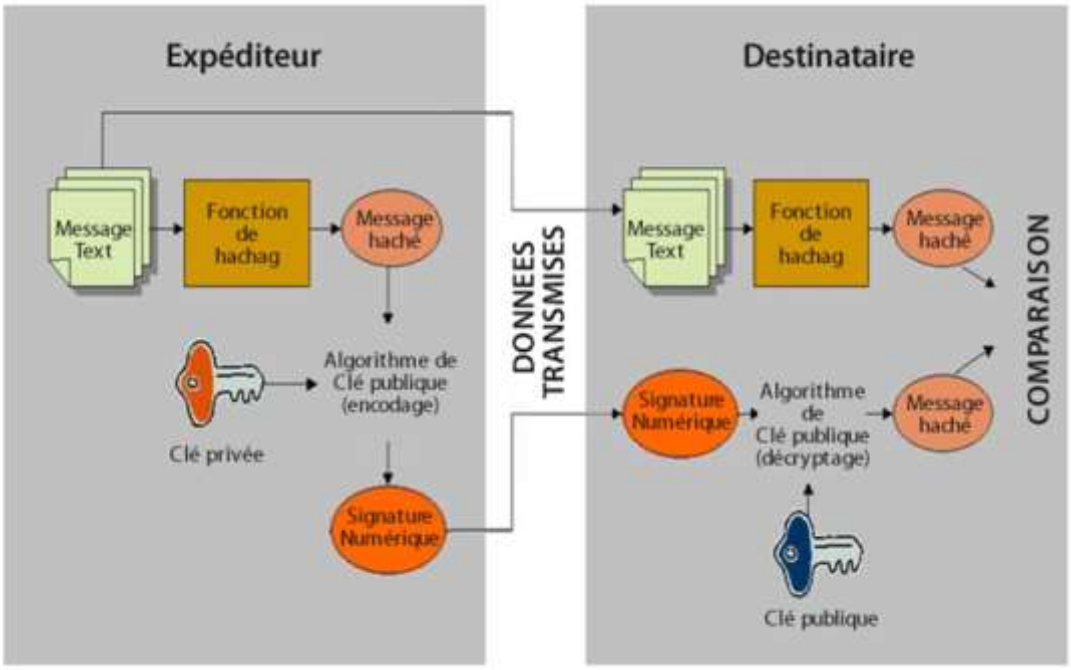


Figure II.10: Signature électronique **[63].**

2.3.2.2.2Le système RSA

Le cryptage RSA, du nom de ses concepteurs, Ron Rivest, Adi Shamir et Leonard Adleman, est le premier algorithme de chiffrement asymétrique. Il a été découvert en 1977 au Massachusetts Institute of Technology.

LE RSA s'est imposé pour le cryptage comme pour l'authentification et a progressivement supplanté son concurrent, le RSA, il est basé sur la théorie des nombres premiers, et sa robustesse tient du faitqu'il n'existe aucun algorithme de décomposition d'un nombre en facteurs premiers. Alors qu'il est facile de multiplier deux nombres premiers, il est très difficile de retrouver ces deux entiers si l'on en connaît le produit [58].

2.3.2.2.3 Les courbes elliptiques

Les courbes elliptiques existent depuis le 3ème siècle pour résoudre des problèmes arithmétiques anciens. Leur étude en algèbre géométrique date du milieu du 19ème siècle.

La description en 1984 par Hendrik Lenstra d'un algorithme de factorisation polynomiale sur ces structures a motivé certains chercheurs à s'investir dans l'aspect

cryptographique des courbes elliptiques et dans le calcul théorique des nombres [46, 47]. Leur intérêt particulier s'explique essentiellement par leur niveau de sécurité très élevé. Comparées au système RSA, on s'aperçoit que pour un même niveau de sécurité, les courbes elliptiques en cryptographie utilisent des clés de plus petites tailles. Il a été démontré qu'une clé de courbe elliptique de 160 bits fournit le même niveau de sécurité qu'une clé de 1024 bits de RSA [48, 49]. Cette qualité rend les ECCs plus attractifs pour les dispositifs aux ressources limitées telles que la capacité de calcul, de transmission/réception et de stockage mémoire qui peuvent impacter fortement sur la consommation énergétique dans le cas des capteurs [44].

Les courbes elliptiques sont les courbes les plus simples après les droites et les coniques. On peut considérer une courbe elliptique sur un corps fini F, elle intervient ainsi dans certains protocoles cryptographiques. On peut définir une courbe elliptique E sur un corps fini F noté E(F) par son équation à la forme de Weierstrass [50] :

$$E : y^2 + a_1.x.y+a_3.y=x^3 +\alpha_2.x^2+a_4.x+a_6 \qquad (\mathbf{II}.1)$$

Où a_1, a_2, a_3, a_4 et $a_6 \in F$.

Les corps sont des systèmes de nombres bien connus tels que les nombres rationnels Q ou les nombres réels R et les nombres complexes C. Un corps est un ensemble F possédant deux opérations élémentaires, l'addition (notée +) et la multiplication (notée.), satisfaisant les propriétés arithmétiques suivantes :

- (F, +) est un groupe abélien (avec l'addition) et l'élément neutre est 0.

- (F*, .) est un groupe abélien (avec la multiplication) et l'élément neutre est 1.

La distributivité est respectée : (a+b).c=a.c+ b.c pour tout a, b, c ∈ F. Un corps est fini quand il contient un nombre fini d'éléments, autrement dit l'ensemble F est fini. II existe trois grands types de corps finis qui sont utilisables pour l'implémentation de la cryptographie pour les courbes elliptiques : les corps premiers, les corps binaires et les corps d'extension. L'ordre d'un corps fini est le nombre d'éléments présents dans le corps. Compter le nombre de points d'une courbe elliptique définie sur un corps fini fait partie des problématiques essentielles dans la recherche des courbes cryptographiquement sûres. La communauté des mathématiciens s'en est notamment intéressé, c'est Hasse en 1922 qui démontra le résultat sur ce nombre également appelé ordre du groupe des points d'une courbe elliptique sur un corps fini :

$$E(Fp)-p-1\leq 2\sqrt{P} \qquad (\mathbf{II}.2)$$

Les corps premiers notés par F, où p= q^m et q un nombre premier (appelé la caractéristique de F_p) sont généralement utilisés en cryptographie. Si m=1 alors F, est appelé un corps premier. Si m ≥ 2 alors F, est appelé un corps d'extension. Les corps binaires sont des corps finis d'ordre 2 à coefficient dans (0,1). Dans cette thèse, nous avons travaillé avec les corps premiers F_p, où p >3. Pour ces corps premiers, si la caractéristique est supérieure à 3, l'équation de Weierstrass pour une courbe elliptique sur un corps fini premier noté E(F) peut être représentée par :

$$E : y^2=x^3+a.x+b \qquad (\mathbf{II}.3)$$

Où a et b ∈ F_p

Pour être utilisée en cryptographie, la condition nécessaire est que le discriminant du polynôme soit égal à 0. Cette condition garantie que, pour tout point de la courbe elliptique, passe une et une seule tangente.

$$F(x) = x^2 + a.x + b$$

$$\triangle=4a^3+27b^2 \neq 0 \qquad (\mathbf{II}.4)$$

L'ensemble des points (x, y), dont les coordonnées x, y vérifient l'équation 1.1 et le point à l'infini noté ∞ sont sur la courbe et forment un groupe abélien additif

$$(E(Fp).+):(E(F_p), +) = \{x, y\} \in F_p.F_p : y^2 – x^3 - a_x - b = 0 \cup \{\infty\} \qquad (\mathbf{II}.5)$$

Ce groupe est principalement constitue de deux opérations de base : le doublement de point (2P) et l'addition de points (P+Q) où P et Q sont deux points différents de la courbe. Etant donnes P= (x_p, y_p) et Q=(x_q,y_q) deux points ($\neq \infty$) d'une courbe elliptique sur un corps fini Fp noté E (Fp). Géométriquement, l'addition de point (P + Q) avec P, Q consiste à prendre le symétrique du troisième point (P*Q) d'intersection de la droite PQ avec la courbe elliptique. Le doublement d'un point est le cas particulier d'addition ou P = Q, on prend alors le symétrique du point d'intersection de la tangente en P avec la courbe elliptique. Si P et Q sont symétriques par rapport à l'axe des x, dans ce cas la droite PQ coupe la courbe au point à l'infini (qui est le zéro du groupe) et donc Q = -P.

L'addition de points P+Q= (x_{pq}, y_{pq}) ou le doublement de point 2P=P+Q= (x_{pq}, y_{pq}) si P = Q peuvent être calculés à travers les équations (**II**.6) et (**II**.7) :

$$\begin{cases} xpq = \lambda 2 - xp - x \\ ypq = \lambda(xp - xpq) - yp \end{cases} \qquad (\mathbf{II}.6)$$

$$\begin{cases} \lambda = \frac{(yq - yp)}{(xq - xp)} \text{ si } P \neq Q \\ \lambda = \frac{(3xp2 + a)}{(2yp)} \text{ si } P = Q \end{cases} \quad \textbf{(II.7)}$$

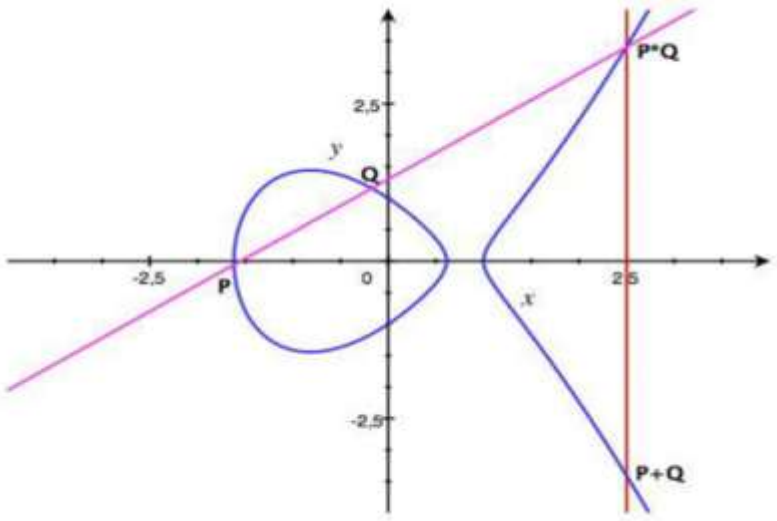


Figure II.11: Addition de points [44].

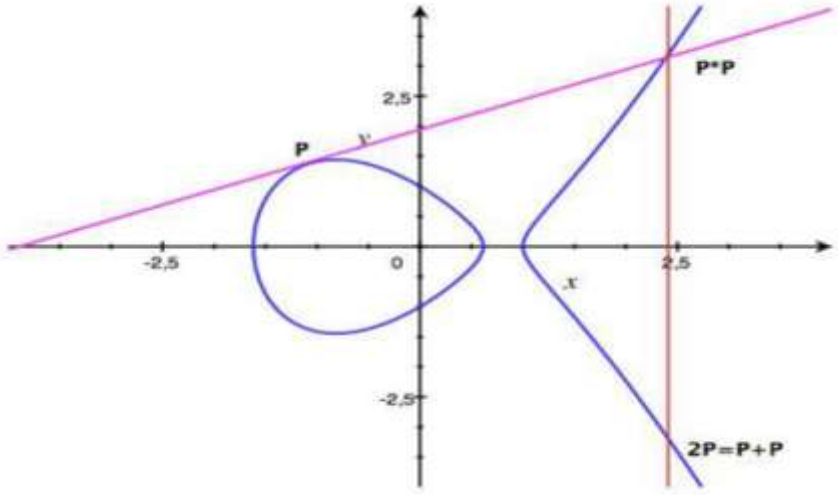


Figure II.12: Doublement de point [44].

Les équations : (**II**.1), (**II**.2), (**II**.3), (**II**.4) (**II**.5) (**II**.6) (**II**.7) (**II**.8) sont référencier en [44].

2.3.2.2.3.1 Protocoles cryptographiques basés sur ECC

2.3.2.2.3.1.1 ECC ElGamal

ElGamal propose un protocole de chiffrement et de signature numérique basé sur le protocole d'échange de clé Diffie-Hellman [66]. Dans le protocole Diffie-Hellman, A et B veulent partager un secret entre eux, et chacun détient une clé privée appelé respectivement x_A et x_B, p est un grand nombre premier, et α est la racine primitive modulo p (le générateur). A calcule $y_A \equiv \alpha^{xA} (\text{mod } p)$ et l'envoie à B, et dans l'autre sens, B calcule $y_B \equiv \alpha^{xB} (\text{mod } p)$ et l'envoie à A . Le secret partagé KAB est donc

$$KAB \equiv \alpha^{xAxB} (\text{mod } p)$$

$$\equiv y_A{}^{xB} (\text{mod } p)$$

$$\equiv y_B{}^{xA} (\text{mod } p) \qquad \textbf{(II}.8)$$

Grâce à la difficulté pour résoudre le problème du logarithme discret, A et B peuvent s'envoyer y_A et y_B sans risque, car il est extrêmement difficile de calculer les valeurs x_A et x_B. Une fois le secret partagé établi entre A et B, ils peuvent sécuriser la communication entre eux avec un algorithme de cryptographie symétrique qui est moins lourd à gérer [68].

2.3.2.2.3.1.1.1 Chiffrement et déchiffrement

Un algorithme de chiffrement et déchiffrement à clé public est aussi proposé dans [67]. Si A veut envoyer un message m à B où $m \in [0, p-1]$. A choisit d'abord un nombre entier k $\in [0, p-1]$ et on calcule

$$K \equiv y^k_B (\text{mod } p) \qquad \textbf{(II}.9)$$

Où $y_B \equiv \alpha^{xB} (\text{mod } p)$ est en effet la clé publique de B. Pour chiffrer le message, A calcule

$$c_1 \equiv \alpha^k (\text{mod } p) \qquad c_2 \equiv K_m (\text{mod } p) \qquad \textbf{(II}.10)$$

Et envoie c1 et c2 à B. Pour déchiffrer le message, B calcule dans un premier temps la valeur de $K \equiv (\alpha^k)^{xB} \equiv c_1{}^{xB} (\text{mod } p)$, car x_B est la clé privée de B, ensuite B divise c_2 par K pour récupérer le message m.

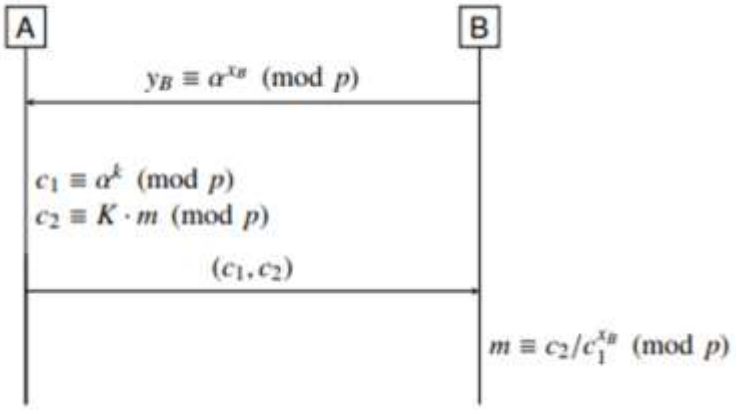


Figure II.12 Protocole de chiffrement d'ElGamal **[68].**

Cet algorithme peut aussi être appliqué sur les courbes elliptiques. Supposons que G soit le point générateur sur une courbe définie dans un corps premier fini, notée E(Fp). A et B disposent chacun d'une clé privée, x_A et x_B avec lesquelles ils peuvent calculer leurs clés publiques P_A et P_B.

$$P_A = x_A.G \text{ et } P_B = x_B.G \qquad \textbf{(II}.11)$$

Lorsque A veut envoyer un message m à B, il convertit d'abord m en un point, noté M, sur la courbe E(Fp), et prendre un nombre entier aléatoire $k \in [0, p-1]$, ensuite il commence à chiffrer le message en calculant

$$M_1 = k.G \qquad M_2 = M + k.P_B \qquad \textbf{(II}.12)$$

Enfin le couple (M1, M2) est envoyé à B qui peut déchiffrer le message de la manière suivante [68].

$$M = M_2 - x_B.M_1 = M + k.P_B - x_B.k.G = M + (k.P_B - k.P_B) \qquad \textbf{(II}.13)$$

Les équations : (**II**.8), (**II**.9), (**II**.10), (**II**.11) (**II**.12) (**II**.13) sont référencier en [68].

2.3.2.2.3.1.2 Elliptic Curve Integrated Encryption Scheme (ECIES)

Le protocole d'Elgamal est rarement utilisé directement avec les courbes elliptiques. Avant de chiffrer un message, il faut d'abord le convertir à un point sur la courbe elliptique utilisée. Il y a différentes techniques qui existent, mais la conversion nécessite plus de calcul. Généralement on utilise les courbes elliptiques pour établir une clé partagée entre les 2 parties d'une conversation, ensuite nous pouvons utiliser un algorithme de cryptographie symétrique

pour sécuriser la communication entre elles. Le protocole ECIES est en effet une variante d'Elgamal standardisée. Supposons qu'Alice désire envoyer un message M à Bob d'une manière sécurisée, ils doivent d'abord disposer de toutes les informations suivantes :

– KDF (Key Derivation Function) : Une fonction de dérivation de clé qui permet de générer plusieurs clés à partir d'une valeur secrète de référence.

– MAC (Message Authentification Code) : Code transmis avec les données dans le but d'assurer l'intégrité de ces dernières.

– S Y M : Algorithme de chiffrement symétrique.

– E(Fp) : La courbe elliptique utilisée avec le point de générateur G dont ordp(G) = n.

– K_B : La clé publique de Bob $K_B = k_B.G$ où $k_B \in [1, n-1]$ est sa clé privée.

Pour chiffrer le message M, Alice doit effectuer des opérations suivantes :

1. Choisir un nombre entier $k \in [1, n-1]$ et calculer $R = k.G$.

2. Calculer $Z = k.K_B$.

3. Générer les clés (k_1, k_2) = KDF (abscisse(Z), R).

4. Chiffrer le message C = S Y M (k_1, M).

5. Générer le code MAC t = MAC (k_2, C).

6. Envoyer (R, C, t) à Bob.

Pour déchiffrer le message (R,C, t), Bob doit effectuer des calculs ci-dessous :

1. Rejeter le message si $R \neq E(Fp)$.

2. Calculer $Z = k_B.R = k_B.k.G = k.KB$.

3. Générer les clés (k_1, k_2) = KDF (abscisse(Z), R).

4. Générer le code MAC $t' = MAC (k_2,C)$.

5. Rejeter le message si $t \neq t$.

6. Déchiffrer le message $M = S Y M^{-1} (k_1, C)$ [68].

2.3.2.2.3.1.3 Elliptic Curve Digital Signature Algorithm (ECDSA)

Le protocole ECDSA est proposé par Johnson, il est une variante de DSA qui utilise les techniques de cryptographie sur les courbes elliptiques. Le protocole DSA signifie Digital

Signature Algorithme en Anglais, c'est un algorithme de signature numérique standardisé par le NIST aux États-Unis [68].

Le protocole est basé sur l'idée du protocole de signature d'Elgamal. Nous supposons qu'Alice et Bob utilisent la même courbe elliptique E(Fp) pour sécuriser la communication entre eux. Nous supposons que la clé publique d'Alice est KA = k_A.G où kA est sa clé privée et G est le point de générateur de l'ordre n. Pour signer un message M, Alice doit suivre les opérations suivantes [68] :

1. Choisir un nombre aléatoire k ∈ [1, n − 1].

2. Calculer R = k.G.

3. Calculer r ≡ abscisse(R) (mod n). Si r = 0, retourner à l'étape 1.

4. Calculer $s \equiv k^{-1} (H(M) + k_A r) \pmod n$ où H est une fonction de hachage. Si s = 0, retourner à l'étape 1.

5. Envoyer (r, s) à Bob

Après avoir reçu le message signé, Bob vérifie la signature du message :

1. Vérifier si $K_A \neq \infty$ (point à l'infini) et $K_A \in E(Fp)$.

2. Vérifier si $n.K_A = \infty$ car $n.K_A = n.k_A.G$ et ordp(G) = n.

3. Vérifier si (r, s) ∈ [1, n − 1].

4. Calculer $R = (H (M) s^{-1} \bmod n) G + (rs-1 \bmod n) K_A$.

5. Vérifier si r ≡ abscisse(R) (mod n).

$R = (H (M) s^{-1}) G + (rs-1) K_A \pmod n$

$= (H (M) s^{-1}) G + (rs-1) k_A G \pmod n$

$= s^{-1} G (H (M) + rk_A) \pmod n$

$= k (H (M) + k_A r)^{-1} G(H (M) + rk_A) \pmod n = k_G$

2.3.2.2.3.1.4 Elliptic Curve Menezes Qu Vanstone (ECMQV)

ECMQV est un protocole d'échange de clés authentifié proposé dans, car en utilisant Diffie-Hellman, nous ne pouvons pas assurer l'authentification des participants Nous supposons que $R(x_R, y_R)$ est un point sur une courbe elliptique, et P est le point de générateur dont ord(P) =n. Nous calculons $R^{-} = (x_R \bmod 2L) + 2 L$ où $L = \lceil \lfloor (\log_2 n \rfloor + 1) / 2 \rceil$, alors R^{-}

est en effet les premier L bits de la coordonnée abscisse de R. En outre, (q_A, Q_A) et (q_B, Q_B) sont respectivement la clé privée et la clé publique d'Alice et Bob [68].

2.3.2.2.3.1.5 Elliptic Curve MASSEY-OMURA (EC MASSEY-OMURA)

En cryptographie, le protocole à trois passes, permet à Alice d'envoyer un message chiffré à Bob sans avoir besoin d'échanger ou de distribuer des clés. Le premier protocole à trois passes était celui développé par Shamir en 1980. Il est aussi appelé Shamir No-Key Protocol, car l'émetteur et le récepteur n'ont pas besoin d'échanger des clés. Le protocole nécessite néanmoins deux clés privées pour crypter et décrypter les messages.

James Masey et Jim K. Omura ont proposé une amélioration du protocole de Shamir en 1982. La méthode de Massey-Omura utilise l'exponentiation dans le corps de Galois GF (2n). Le message chiffré est M^e et le message déchiffré est M^d. Les calculs sont effectués dans le corps de Galois. Quel que soit le nombre entier e utilisé pour chiffrer le message avec $0 < e < 2^n - 1$ et PGCD $(e, 2^b - 1) = 1$, le nombre entier d permettant de déchiffrer le message est tel que $de \equiv 1 \pmod{2n - 1}$. Comme le groupe multiplicatif associé au corps de Galois GF (2n) est de l'ordre $2^n - 1$, le théorème de Lagrange implique que $m^{de} = m$ pour tout m dans GF $(2n)^*$ [68].

2.3.2.2.3.2 Comparaisons de performance entre ECC et RSA

ECC peut avoir le même niveau de sécurité que RSA avec une clé beaucoup plus courte. Les longueurs qui se situent dans la même colonne sont censées pouvoir fournir le même niveau de robustesse. D'ailleurs, l'algorithme de signature utilisé pour ECC est ECDSA, une variante de DSA conçue pour les courbes elliptiques, et un texte de longueur 100 Ko est utilisé pour tester la signature.

Pour atteindre le même niveau de sécurité, premièrement, la consommation de mémoire est beaucoup moins importante avec ECC, car nous utilisons des clés plus courtes. Deuxièmement, les calculs de la génération de clé et de la signature de message sont plus rapide avec ECC. La vérification de signature est plus rapide avec RSA, car il suffit d'effectuer une exponentiation modulaire.

ECC était plus avantageux en termes de consommation de mémoire et vitesse de calcul. C'est la raison principale pour laquelle ECC devient de plus en plus le choix préféré pour les systèmes embarqués qui disposent d'une mémoire et d'une puissance de calcul très limitée. Actuellement RSA demeure toujours le crypto système asymétrique le plus largement utilisé, car il est sorti beaucoup plus tôt par rapport à ECC. RSA est publié en 1978 et standardisé en 1993, tandis que ECC est proposé dans les années 80 et standardisé vers la fin des années 90.

Les 2 crypto systèmes sont initialement protégés par des brevets. Du fait que le brevet de RSA a expiré depuis 2000, il peut être utilisé librement par tout le monde, mais celui de ECC est toujours valable.

Une autre raison qui limite l'utilisation de ECC est que mathématiquement RSA est relativement plus simple. De nombreuse spécifications de ECC existent, mais les implémentations sont souvent incomplètes, c'est-à-dire que seulement quelques courbes décrites dans les spécifications sont implémentées [68].

Clés RSA (bits)	Clés ECC (bits)
1024	160
2048	224
3072	256
7680	384
5360	521

Tableau II.1 : Comparaison entre ECC et RSA [44].

2.4 Conclusion

Nous avons évoqué dans ce chapitre les différentes facettes des systèmes multi-agents à savoir les types d'agents, la façon dont les agents communiquent et les méthodes de sécurité que nous voulons utiliser pour protéger les RRC.

Notre objectif est de protéger les RRC de toute intrusion ou piratage pour la sécurité des informations et des données en optimisant le système cognitif par une architecture améliorer ainsi que des algorithmes d'authentification et de chiffrement robustes, dont ils feront l'objectif du prochain chapitre.

Chapitre 3
Architecture et Protocole d’authentification utilisé

Sommaire

3.1 Introduction

La sécurité des réseaux mobiles est devenue un nécessité absolu pour les réseaux de future génération, divers protocoles et algorithme sont proposées pour renforcer la sécurité et d'authentifier les utilisateurs afin de séparer l'honnête du malicieux. Dans les réseaux radio cognitive nous cherchons à améliorer l'authenticité des utilisateurs afin de protéger les utilisateurs secondaires des fausses bandes de fréquences libre. L'idée est de joindre au message une signature électronique, l'équivalent de l'autographe dans le monde physique, qui certifie au destinataire l'identité de l'expéditeur.

Dans ce chapitre, nous allons décrire plusieurs algorithmes (d'authentification, de chiffrement et à multicritère) pour garantir la confidentialité, l'authenticité et l'intégrité des messages en détaillant l'algorithme à base des courbes elliptiques qui est le présent et probablement le futur meilleur algorithme de cryptographie asymétrique. Nous allons aussi décrire l'approche proposée pour assurer le partage sécurisé du bout en bout de l'utilisateur secondaire avec le meilleur utilisateur primaire.

3.2 Le crypto système de Diffie-Hellman DH

Ce système est inventé par Diffie-Hellman il permet à deux personnes qui n'ont jamais communiqué ensemble auparavant d'engendrer une clé secrète en utilisant le logarithme discret [66].

3.2.1 Description de Diffie-Hellman

L'émetteur et le destinataire se mettent d'accord sur un nombre premier p et un élément g de IF^*_P qu'ils rendent publiques, ensuite :

- L'émetteur choisit un nombre $x \in IF_q$ et le destinataire un nombre $y \in IF_q$ les nombres x et y sont respectivement les clés secrètes de l'émetteur et du destinataire.
- L'émetteur envoie $X = g^x \bmod (p)$ au destinataire et le destinataire envoie $Y = g^y \bmod (p)$ à l'émetteur [66].
- L'émetteur calcule la clé $K = Y^x \bmod (p)$ et le destinataire calcule

$$\mathbf{K' = X^y \bmod p = X^y \bmod p.} \qquad \textbf{(III. 1)}$$

3.2.2 Fonctionnement de Diffe-Hellman

L'émetteur et le récepteur ont bien la même clé car :

$$K = Y^{x} \bmod (p)$$

$$= (g^{y})^{x} \bmod (p)$$

$$= g^{xy} \bmod (p)$$

$$= (g^{x})^{y} \bmod (p)$$

$$= X^{y} \bmod (p)$$

$$= K' \qquad \textbf{(III.2)}$$

3.3 Algorithme d'authentification asymétrique utilisé

3.3.1 Elliptic Curve Diffie-Hellman ECDH

Ce protocole est une nouvelle variante du protocole Diffie-Hellman utilisant la courbe elliptique cryptographique ECC. Il est décrit dans le rapport CARICOM Research.

Cet algorithme est exécuté comme suit :

1. Alice et Bob sélectionnent une courbe elliptique E définie sur Fp Le nombre de points dans E(Fp) doit être divisible par un grand nombre premier n
2. Ils sélectionnent un point $P \in E(Fp)$ d'ordre n.
3. Alice sélectionne un nombre entier statistiquement unique et imprévisible a dans l'intervalle [1, n-1], Bob choisit l'entier b sur [1, n-1].
4. Alice calcule le point $C = a \times P$ et l'envoie à Bob.
5. Bob calcule le point $D = b \times P$ et l'envoie à Alice.
6. Alice et Bob peuvent maintenant calculer un point commun $K \in E(Fp)$:

$$K = a \times D = a \times (b \times P) = (a \times b) \times P = b \times (a \times P) = b \times C \qquad \textbf{(III. 3)}$$

Les équations (III.1), (III.2) et (III.3) sont référencier en [66]

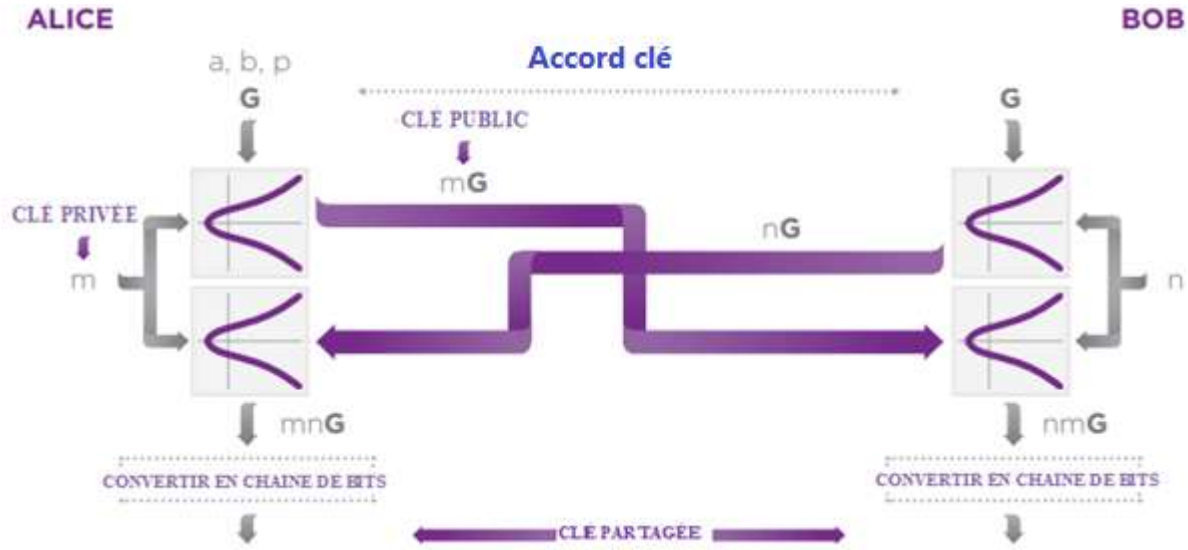


Figure III .1 : Partage de clé par ECDH

3.3.2 Description of ECDH

La courbe elliptique Diffie Hellman (ECDH) se distingue du Diffie Hellman général (DH) dans la mesure où elle est basée sur le problème du logarithme discret de la courbe elliptique (ECDLP) au lieu du problème du logarithme discret (DLP). ECDH est un protocole d'accord de clé anonyme qui permet à deux parties, A et B, d'établir une clé secrète partagée sur un canal non sécurisé, où chacune des parties dispose d'une paire de clés publique-privée à courbe elliptique.

L'ECDH fonctionne comme suit. A et B sont d'accord sur le groupe de courbes elliptiques E d'ordre n et un élément primitif P dans E, qui a alors aussi l'ordre n.m. E, n et P sont supposés connus de l'adversaire. L'ECDLP, dont l'ECDH est le siège sur, est défini comme le calcul de l'entier k étant donné P et Q tels que Q = [k] P [67].

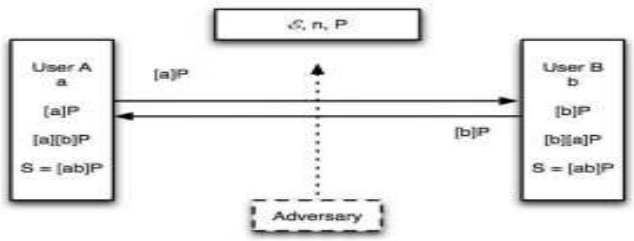


Figure III .2 Méthode d'échange de clé ECDH [67].

3.3.3 Security for ECDH

La courbe elliptique computationnelle Diffie-Hellman problème (ECDHP) est le

problème d'essayer de trouver S= [a×b mod (n)] ×P, étant donné E, n, P et les deux points Q= [a] P et R= [b] P sont le problème que l'adversaire va essayer de résoudre pour obtenir la clé secrète S, et la capacité de vaincre ce type d'attaques est une partie importante de la sécurité de l'ECDH.

Si l'ECDLP dans < P > peut être efficacement résolu, alors l'ECDHP dans < P > peut également être résolu efficacement en trouvant a à partir de (P, Q) puis calculer S = [a] ×R. En d'autres termes, l'ECDHP n'est pas plus difficile que l'ECDLP. C'est inconnu si la dureté de l'ECDHP est égale à la dureté de l'ECDLP. Quoi qu'il en soit, pour que l'ECDHP avoir un haut degré de sécurité, il est essentiel que l'ECDLP correspondant à un degré élevé de sécurité [68].

3.3.4 Comparaison entre le ECDH et DH

Durlanik fait des tests expérimentaux pour comparer entre ECDH et DH Il a rapporté que outre les tailles de clé, on peut dire que ECDH est plus rapide que DH en termes de temps d'exécution et de statistiques d'utilisation de la mémoire selon les comparaisons Par exemple, le temps nécessaire pour générer les paramètres de domaine de courbe elliptique avec un nombre premier de 256 bits est bien inférieur à celui nécessaire pour les paramètres de domaine DH avec 512 bits (0,0676 seconde pour ECDH-256 et 0,5783 seconde pour DH-512)[69].

3.4 Algorithme d'authentification symétrique utilisé

3.4.1 Le mode ECB (Electronic Code Book)

Le carnet de codage électronique, en anglais "Electronic Code Book" (ECB), est le mode opératoire le plus simple. Il consiste à chiffrer chaque bloc de texte en clair en un bloc de texte chiffré. Son nom provient du fait qu'un texte en clair donné est transformé à chaque fois dans le même texte chiffré à condition d'utiliser toujours la même clé pour l'encoder. On pourrait donc théoriquement construire un carnet comportant tous les textes en clair et les textes chiffrés correspondants pour une clé donnée. Mais cela fait par exemple 264 paires de blocs par clé dans le cas du DES et il existe 256 clés différent. Ce n'est donc pas faisable pour les algorithmes de chiffrement dont les clés ont une longueur suffisante. Pour un texte en mode ECB, on effectue donc les opérations suivantes :

$$\mathbf{C[n] = E\,(M[n]),\ pour\ n \geq 1} \qquad \textbf{(III. 4)}$$

Pour déchiffrer un texte en mode ECB, on effectue les opérations suivantes :

$$\mathbf{M[n] = D\,(C[n]),\ pour\ n \geq 1} \qquad \textbf{(III. 5)}$$

Les équations (III.4), (III.5) sur la référence [70]

M[n] c'est le n-ième bloc du texte en clair. La taille du bloc dépend du mode opératoire et du procédé de chiffrement.

C[n] c'est le n-ième bloc du texte chiffré, la taille du bloc dépend du mode opératoire et du procédé de chiffrement

E(M) c'est la fonction de chiffrement.

D(M) c'est la fonction de déchiffrement [70].

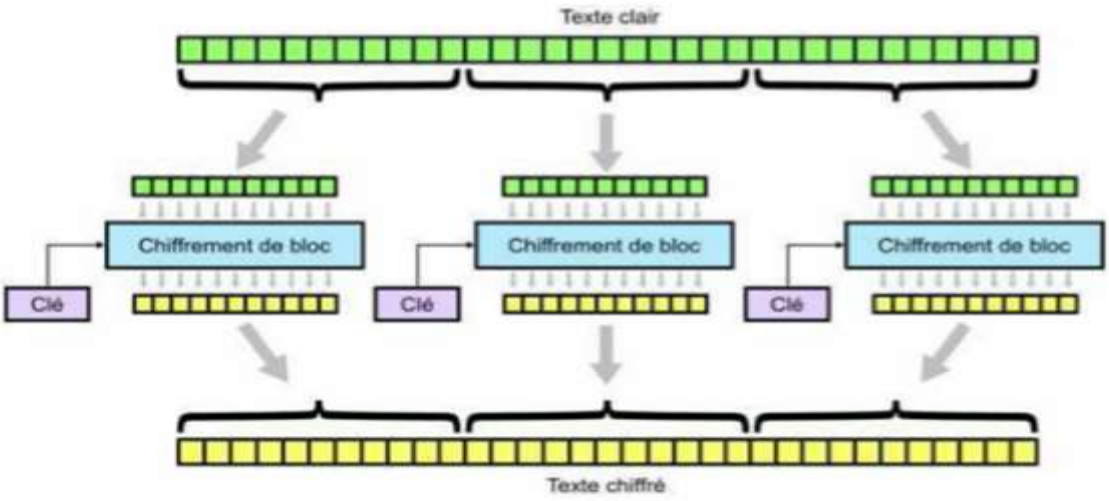


Figure III.3 Le mode ECB [71].

Ce mode souffre de plusieurs défauts de sécurité :

- Deux blocs clairs identiques sont chiffrés de la même façon. Ceci facilite les attaques statistiques, notamment cela permet de repérer les blocs clairs utilisés les plus fréquemment.
- Le mode ECB ne respecte pas l'intégrité des données. Un attaquant peut remplacer certains blocs chiffrés par d'autres blocs chiffrés du message, ou permuter deux blocs, sans que le destinataire s'en aperçoive. Imaginons que le message chiffré soit le montant d'une transaction électronique, et que l'attaquant arrive à permuter deux chiffres.

Ce mode, dictionnaire de codes, est le plus simple des modes. Il revient à crypter un bloc indépendamment des autres ; cela permet entre autres de crypter suivant un ordre aléatoire (bases de données, etc..) mais en contrepartie, ce mode est très vulnérable aux attaques. On peut aussi l'utiliser pour pipeline du hardware.

ECB a d'autres effets négatifs sur l'intégrité et la protection des données. Ce mode est sensible à des « attaques par répétition » : elles consistent à réinjecter dans le système des données identiques à celles interceptées auparavant. Le but est de modifier le comportement du système ou répéter des actions. Ce mode est pour ces raisons fortement déconseillé dans toute application cryptographique. Le seul avantage qu'il peut procurer est un accès rapide à une zone quelconque du texte chiffré et la possibilité de déchiffrer une partie seulement des données [72].

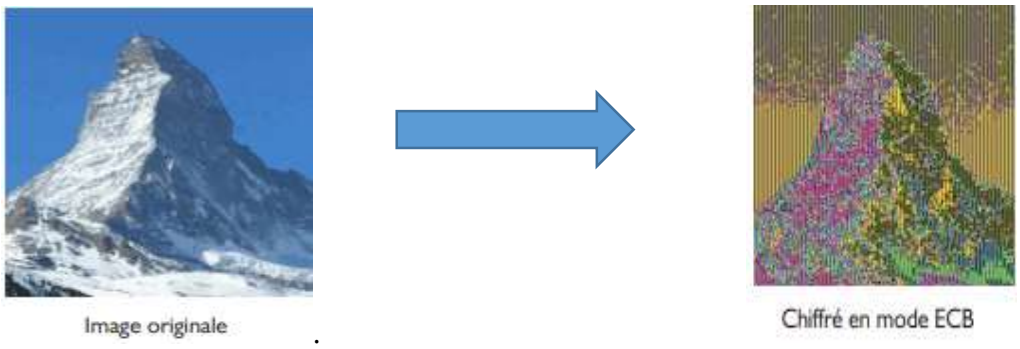


Figure III.4 : chiffrement ECB [72].

3.4.2 Le mode ECB optimisé

La partie essentielle dans notre étude est l'optimisation de mode ECB (l'optimisation de code est la pratique consistant à améliorer l'efficacité d'un programme). Ces améliorations permettent généralement au programme résultant de s'exécuter plus rapidement, de prendre moins de place en mémoire, de limiter sa consommation de ressources (par exemple les fichiers).

La vulnérabilité de l'ECB est encore plus flagrante sur une image. En effet, les images sont constituées de nombreuses redondances dont les blocs sont chiffrés de la même manière. ECB a d'autres effets négatifs sur l'intégrité et la protection des données. Ce mode est sensible à des « attaques par répétition » : elles consistent à réinjecter dans le système des données identiques à celles interceptées auparavant. Le but est de modifier le comportement du système ou répéter des actions [73].

Donc lorsqu'on déchiffre un seul bloc de donnée on peut déchiffrer tout le message chiffré dans le ECB normal, c'est pour cette raison on a proposé d'optimiser ce mode par le chiffrement de chaque bloc de message en utilisant sa propre clé, donc chaque bloc à une clé indépendante des autres blocs, la figure III.5 nous montre un exemple qu'on va l'étudier par la suite dans le chapitre suivant et l'implémenter dans Xilinx et voir le résultat de cryptage de ce

mode optimisé. Notre travail consiste a chiffré un message de 1024 bits en utilisant le ECC à 1024 bits, dans ce cas-là on subdivise le message en claire en des blocs de 256 bits et crypter chaque bloc par une clé de 256 bits.

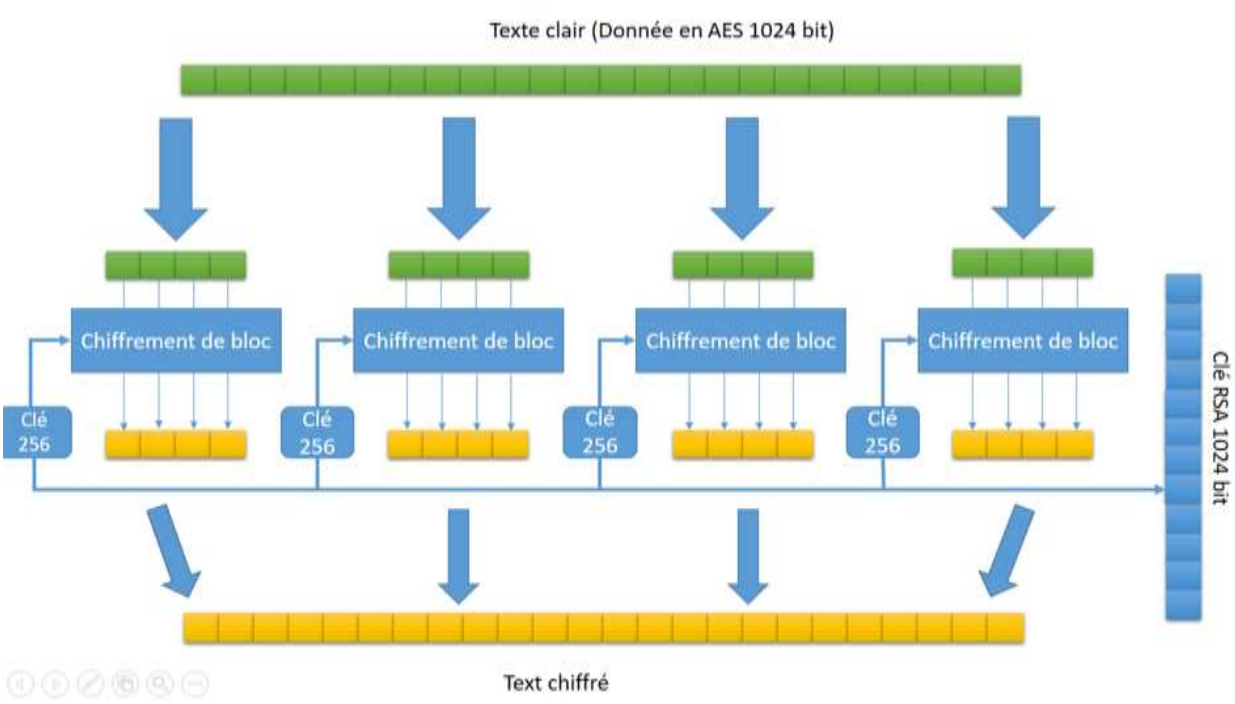


Figure III.5 : Le mode ECB optimisé par l'AES à 256 bits [73].

Dans le deuxième cas, on chiffre aussi un message de 1024 bits en utilisant le ECC 1024 dans ce cas-là on subdivise le message en claire en des blocs de 128 bits et crypter chaque bloc par une clé de128 bits :

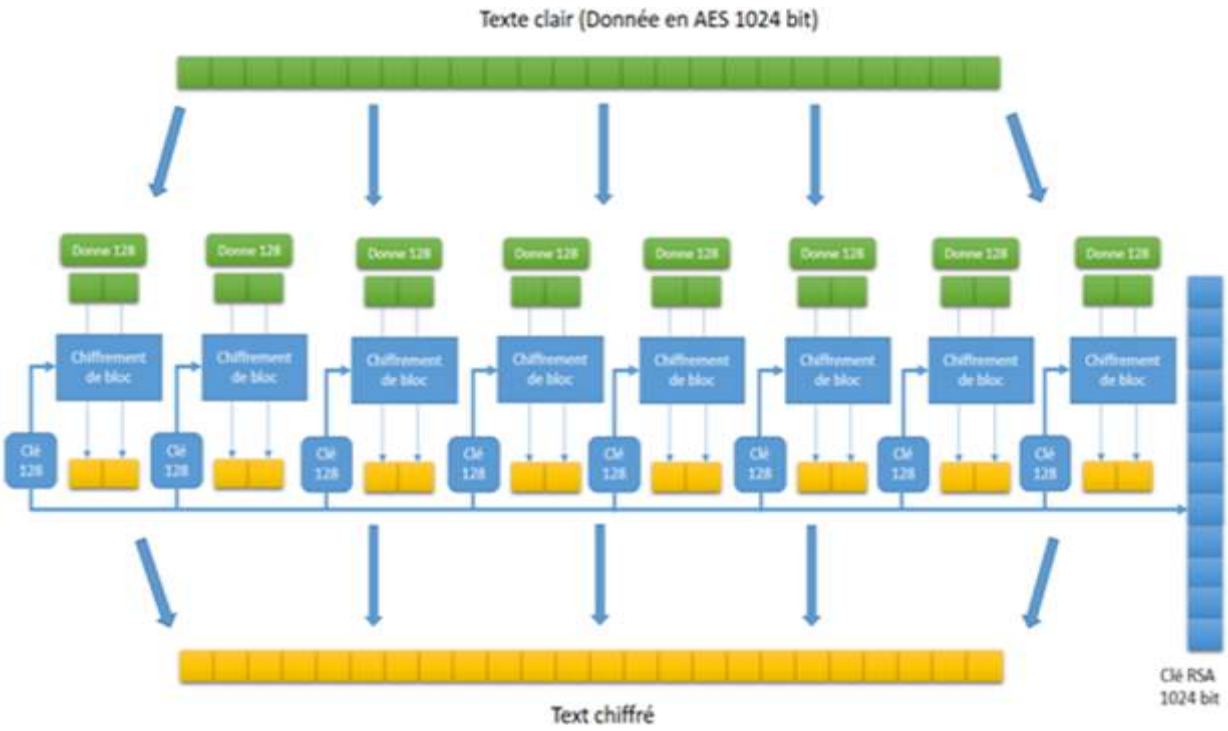


Figure III.6 Le mode ECB optimisé par l'AES à 128 bits [73].

Dans le troisième cas, on chiffre aussi un message de 1024 bits en utilisant le ECC 1024 bits dans ce cas-là on subdivise le message en claire en des blocs d'AES de 128,192 et 256 bits et crypter chaque bloc par propre clé :

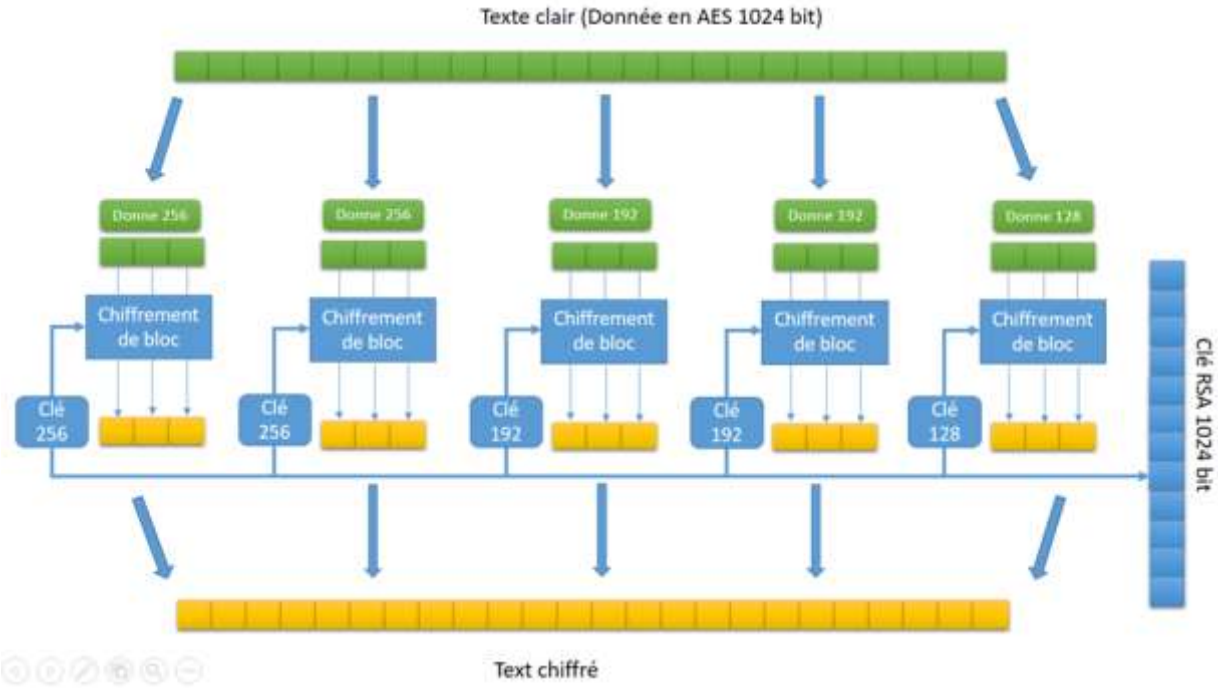


Figure III.7 : Le mode ECB optimisé (AES 128, 192 et à 256 bits) [73].

3.4.3 Comparaison entre le ECB normal et ECB optimisé

Le but essentiel de notre étude est d'optimiser le mode ECB afin de rendre notre crypto système robuste, plus rapide et difficile à l'hacker, le tableau ci-dessus est un tableau comparatif entre les deux modes (ECB normal et ECB optimisé) :

	ECB normal	**ECB optimisé**
Avantages	Ce mode permet le chiffrement en parallèle des différents blocs composant un message. -plus rapide	-plus sécurisé et difficile pour un attaquant de déduire la clé utilisée pour déchiffrer le message crypté -si l'attaquant peut déchiffrer un bloc ça ne veut pas dire qu'il peut déchiffrer tous le message (chaque bloc est chiffré par sa propre clé)
Inconvénient	Un attaquant actif pourra facilement déchiffrer le message en déduisant la clé répétitive utilisé pour chaque bloc.	Prendre un peu plus de temps pour la génération des clés pour chaque bloc de données par rapport à ECB normal (qui utilise une seule clé pour tous les blocs).

Tableau III.1 : Comparaison des deux modes (ECB normale et optimisé) [73].

Basé sur des études vues précédemment, nous avons opté à utiliser le mode de chiffrement ECB optimisé de l'algorithme AES afin de garder la rapidité de chiffrement des blocs en toute sécurité et en transmettant la clé secrète de l'AES avec l'algorithme asymétrique ECDH.

3.5 Algorithme TOPSIS

3.5.1 Définition

TOPSIS (Technique for Order Preference by Similarity to Idéale Solution) est l'une des méthodes classiques de résolution de certains problèmes de décision MADM (Multiple Attribute Decision Making), proposée pour la première fois par Hwang et Yoon en 1981 [74].

Son principe consiste à choisir une solution qui se rapproche le plus de la solution idéale et de s'éloigner le plus possible de la solution anti idéale (la pire). La solution idéale correspond à une alternative dont les valeurs de performances de chaque critère sont les meilleures par rapport à n'importe quelle autre alternative. Par contre, la pire des solutions représente une alternative dont les critères détiennent les pires valeurs de performances. En effet, la méthode calcule la distance euclidienne entre chaque alternative et les deux solutions l'idéale et la pire. La solution choisie par TOPSIS doit avoir la distance la plus courte de la solution idéale et la distance la plus longue de la solution pire [75].

En pratique, TOPSIS a été avec succès appliqué pour résoudre des problèmes de sélection, évaluation avec un nombre fini d'alternatives parce que c'est intuitif et facile de comprendre et exécuter. En outre, TOPSIS a une logique solide qui représente l'exposé raisonné de choix humain et a été prouvée pour être une des meilleures méthodes dans le fait d'adresser l'édition de renversement de grade [76].

3.5.2 Principe de fonctionnement

Son principe consiste à déterminer pour chaque alternative un coefficient compris entre 0 et 1 sur la base des distances (euclidiennes) entre chaque alternative d'une part et les solutions idéales favorable et défavorable. Nous allons voir ci-dessous en détail les étapes à suivre pas à pas.

Une alternative est dite idéale favorable si elle est la plus loin de la pire alternative et la plus proche de la meilleure alternative, une alternative est dite idéale défavorable si elle est la plus proche de la pire alternative et là plus loin de la meilleure alternative [77].

L'idée principale de TOPSIS est choisie l'action ayant :

- La plus petite distance à l'action dite « idéale » (positive-ideal solution)
- La plus grande distance à l'action dite « anti-idéale » (negative-ideal solution) [78].

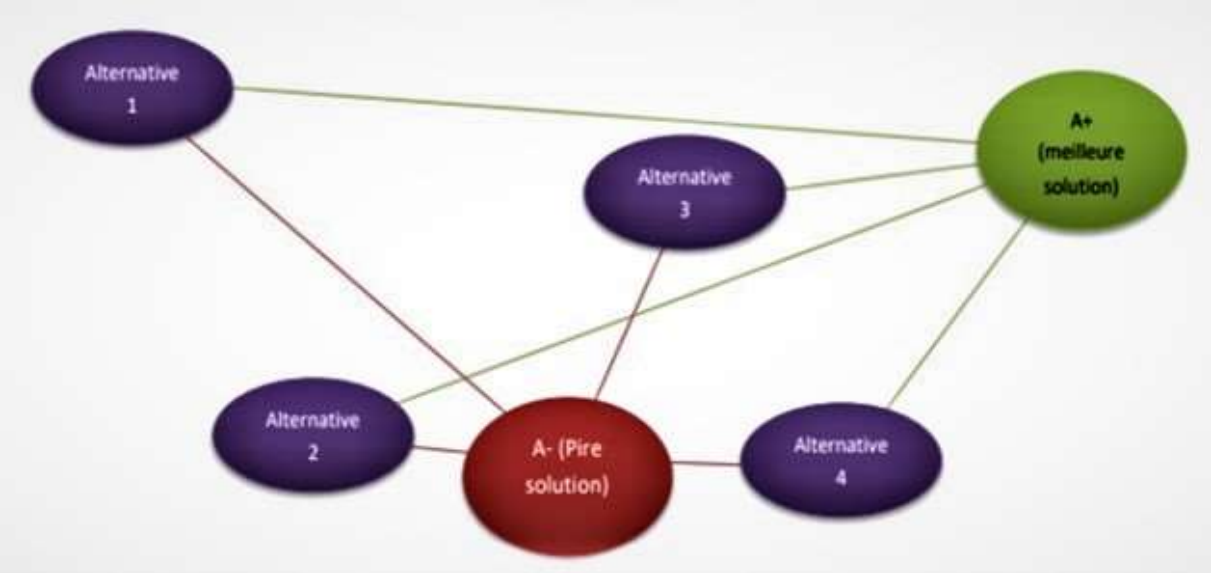


Figure III.8 Principe de méthode TOPSIS [79].

Les résultats de TOPSIS sont basés sur le calcule de deux solutions, l'une au cercle vert est la solution positive c'est la meilleure solution sur tous les critères, l'autre au cercle rouge est la solution négative c'est la pire solution, puis le calcul des distances euclidiennes correspondants de chaque alternative à la meilleure et à la pire solution, après le classement des alternatives telle que :

La meilleure alternative : est la plus proche à la meilleure solution, et la plus loin de la pire Solution

La mauvaise alternative : est la plus loin à la meilleure solution, et la plus proche de la pire solution

3.5.3 Les étapes TOPSIS

Figure III.9 Etapes d'algorithme TOPSIS [80]

Les étapes de la résolution par la méthode TOPSIS se présentent comme suit :

3.5.3.1 Etape 1 : Construire la matrice d'entrée (décision)

Consiste à construire la matrice de décision originale en considérant un nombre d'alternative **m** et un nombre de critère **n** [79], les critères pris dans notre étude sont le nombre des canaux, le temps de réponse, le prix et la technologie utilisée, avec des priorités variables. Les valeurs de cette matrice sont obtenues par l'évaluation des alternatives (PUs) par rapport aux critères.

3.5.3.2 Etape 2 : Normalisation de la matrice d'entrée

Il s'agit de normaliser la matrice de décision originale, en divisant chaque nombre de la colonne de la matrice originale par la racine carrée de la somme des carrées des nombres de la même colonne de cette matrice [79].

3.5.3.3 Etape 3 : Pondération de la matrice

Pondération de la matrice, tel que les poids wi sont donnés par le décideur pour représenter les préférences entre les critères. Pour cela, on multiplie chaque élément de la matrice normalisé par le poids w_i correspondant à chaque critère [79].

3.5.3.4 Etape 4 : Définition de l'idéal positif $\boldsymbol{A}^{+\mathrm{i}}$ et l'idéal négatif $\boldsymbol{A}^{-}$

A cette étape, on considère deux alternatives : l'idéal positif (meilleure sur tous les critères) et l'idéal négatif (la pire solution) [79].

3.5.3.5 Etape 5 : L'distance euclidienne par rapport à la meilleure et la pire solution

A cette étape on considère deux vecteurs E^{+} expriment la distance euclidienne de chaque alternative de la meilleure solution, et E^{-} expriment la distance euclidienne de chaque alternative de la pire solution, telle que [79]

$$S_i^+ = \sqrt{\sum_{j=1}^{n}(V_j^+ - V_{ij})^2} \qquad \textbf{(III. 6)}$$

$$S_i^- = \sqrt{\sum_{j=1}^{n}(V_j^- - V_{ij})^2} \qquad \textbf{(III. 7)}$$

3.5.3.6 Etape 6 : Calcul de degré de proximité au positif idéal Dj +

Pour cela, on divise chaque élément de la ligne de la matrice obtenue, par la somme de la même ligne de cette matrice (par la somme des distances euclidiennes par rapport à l'idéal positif et l'idéal négatif de la même ligne), tel que [79] :

$$P_i^* = \frac{S_i^-}{S_i^- + S_i^+} \qquad \textbf{(III. 8)}$$

Les équations (III.6), (III.7) et (III. 8) sont référencier en [79]

3.5.3.7 Etape 7 : Triage des solutions par rapport à *Dj* +

Cette étape consiste à choisir les meilleures alternatives les plus proches de l'idéal positif et les plus loin de l'idéal négatif [79].

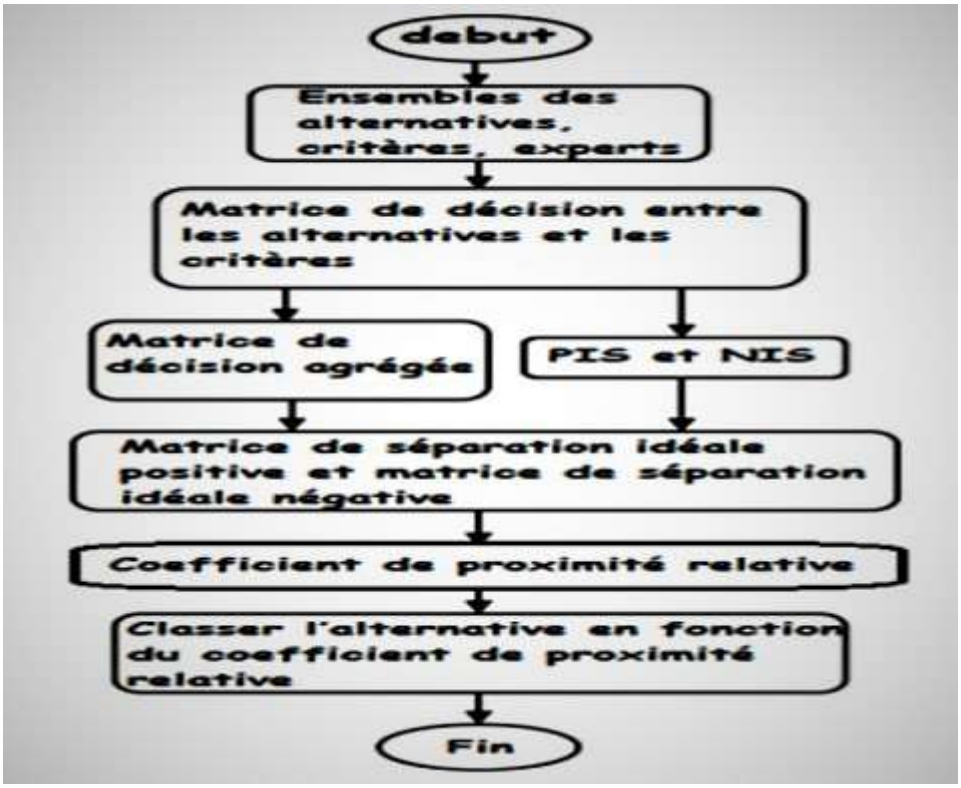


Figure III.10 Organigramme de l'Algorithme TOPSIS [81]

3.6 Architecture proposé

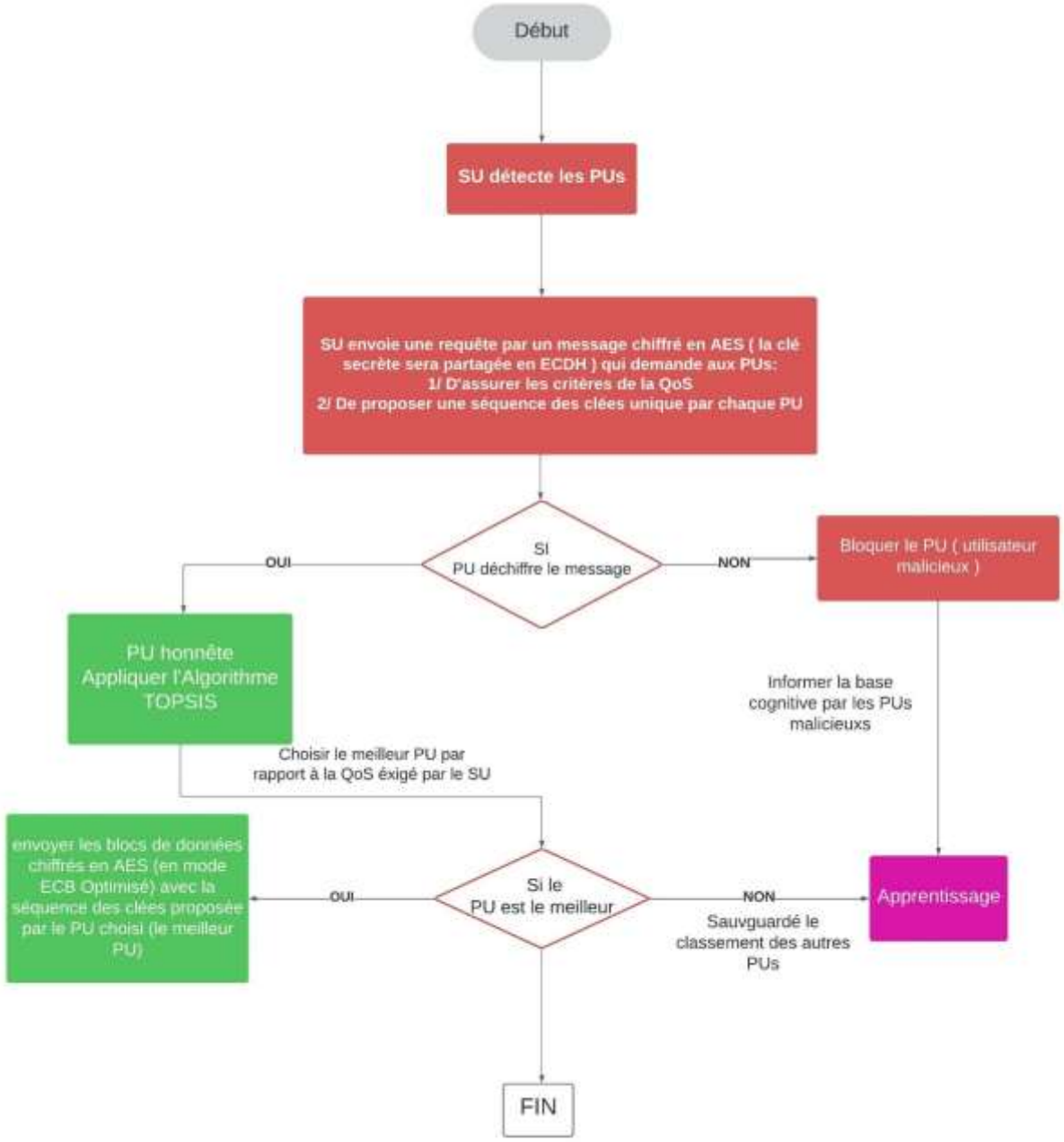


Figure III.11 scénario proposé

Dans la figure III.11, Le SU cherche à détecter des PUs dans son environnement, dès qu'il détecte un certain nombre de PUs, il envoie à chaque PU une requête qui contient un message chiffré en ECC (avec l'algorithme ECDH) demandant les critères de la QoS (Qualité de Service exigé par le SU) et une séquence de différentes tailles de clés symétrique de l'algorithme AES proposée par chaque PU.

Si le PU n'envoie pas un message chiffré contenant les offres demandées, il sera considéré comme un utilisateur malveillant et le SU bloquera tous les utilisateurs qui ne sont pas en mesure de déchiffrer le message ou de retarder la réponse à la demande.

Si le PU déchiffre le message et envoie une offre au SU, il est considéré comme un utilisateur honnête et ses offres seront traiter avec les autres offres à d'autres PUs par l'algorithme multicritères TOPSIS. Ce dernier choisira le meilleur PU parmi les PUs honnêtes, ce choix est basé sur 4 critères : la durée de l'allocation, le prix de l'allocation des canaux, la technologie et la bande passante utiliser.

Les autres PUs non retenues seront classés et archiver par le SU dans une base de données en cas ou le PU choisie sera non disponible à des fins diverses.

En dernier lieu le PU choisi, sera celui qui recevra des données crypter par notre utilisateur secondaire en toute sécurité en utilisant le mode ECB optimisé décrit précédemment avec la séquence des tailles de clés proposé par le PU choisie.

3.7 Conclusion

Dans ce chapitre, nous avons présenté l'algorithme choisi des courbes elliptiques dans la cryptographie pour l'authentification des données qui est basé sur la multiplication scalaire, et sa sécurité repose sur le problème du logarithme discret, nous avons aussi expliquer l'algorithme TOPSIS et son fonctionnement ainsi que le mode de chiffrement ECB optimisé présenter dans une précédente étude. Nous avons essayé de proposer une approche rassemblent tous ces critères afin de sécuriser les réseaux radio cognitive contre des utilisateurs malicieux.

Dans le dernier chapitre, nous allons voir les résultats de simulation de cette approche proposée avec une plateforme qui se rapproche le plus de l'environnement radio cognitif idéal.

Chapitre 4

Résultats des allocations dynamiques et sécurisées des réseaux RC

Sommaire

4.1 Introduction

Un réseau RC est un environnement ou il y a deux types d'utilisateurs, les utilisateurs primaires (PUs), ils s'appellent aussi les propriétaires originaux des bandes de fréquences, et des utilisateurs secondaires (cognitives), qui n'ont pas l'accès aux bandes de fréquences sauf à travers ces propriétaires. Et comme il y a un nombre important des utilisateurs primaires, les utilisateurs secondaires basés sur l'intelligence artificiel doit être adapté à choisir le meilleur offre et en cas d'une récupération temporaire ou permanente de la bande fréquentielle du meilleur PU le SU doit être aussi adapté à réserver des plans alternatifs.

Dans le cadre de ce chapitre, nous allons présenter le logiciel utiliser ainsi que la plateforme de simulation ensuite nous présenterons les résultats de simulations de l'approche proposée ainsi que des comparaisons de notre contribution avec ceux de la littérature.

4.2 EDI NETBEANS

4.2.1 Définition

NetBeans est un environnement de développement intégré (EDI), placé en "open source" par Sun en juin 2000 sous licence CDDL (Common Development and Distribution License) et GPLv2. En plus de Java, NetBeans permet la prise en charge native de divers langages tels que le Language C, C++, JavaScript, XML, PHP et HTML, ou d'autres. Il offre toutes les facilités d'un IDE moderne.

Compilé en Java, NetBeans est disponible sous Windows, Linux, Solaris (sur x86 et SPARC), Mac OS X ou sous une version indépendante des systèmes d'exploitation (requérant une machine virtuelle Java). Un environnement (Java Development Kit) JDK est requis pour les développements en Java.

NetBeans constitue par ailleurs une plateforme qui permet le développement d'applications spécifiques (bibliothèque Swing (Java)). L'IDE NetBeans s'appuie sur cette plateforme [85].

4.2.2 Principaux langages de programmation

Le monde de l'informatique est en constante évolution et l'émergence continue des langages de programmation en est un bon exemple. Les langages de programmation les plus utilisés dans le monde sont les suivants :

1) JavaScript	7) C#	13) Objective-C	19) Lua
2) Python	8) Shell	14) Swift	20) Matlab
3) Java	9) Go	15) Kotlin	21) Power Shell
4) C++	10) Type Script	16) R	22) Coffee Script
5) C	11) Ruby	17) Scala	23) Perl
6) PHP	18) Rust	24) Groovy [86]	

4.2.3 Plateforme JADE

JADE (Java Agent Developpement Framework) est une plateforme multi-agents développée en Java par le laboratoire TILAB (Groupe de recherche de Gruppo Telecom, Italie) qui a pour but la construction des systèmes multi-agents et la réalisation d'applications conformes à la norme FIPA (Foundation for Intelligent Physical Agents). JADE comprend deux composantes de base : une plate-forme agents compatible FIPA et un paquet logiciel pour le développement des agents Java [87].

Cette plateforme est considérée la plus théorique pour la technologie de Radio Cognitive grâce à ses caractéristiques.

Nous avons choisi d'utiliser JADE car d'une part elle gère l'interopérabilité et d'autre part elle est plus souple et plus flexible que les autres plateformes multi-agents sous JAVA. En effet, la plateforme multi-agents JADE peut être distribuée sur plusieurs machines (pas nécessairement le même système d'exploitation) et les configurations peuvent être modifiées au démarrage des agents en les déplaçant d'une machine à une autre, ce qui permet une très grande portabilité des agents.

JADE, un middleware qui facilite le développement des SMA, contient :

- Un environnement d'exécution : l'environnement où les agents peuvent vivre, cet environnement doit être activé pour pouvoir lancer les agents.
- Une librairie de classes : que les développeurs utilisent pour leurs agents.
- Une suite d'outils graphiques : qui facilitent la gestion et la supervision de la plateforme des agents.

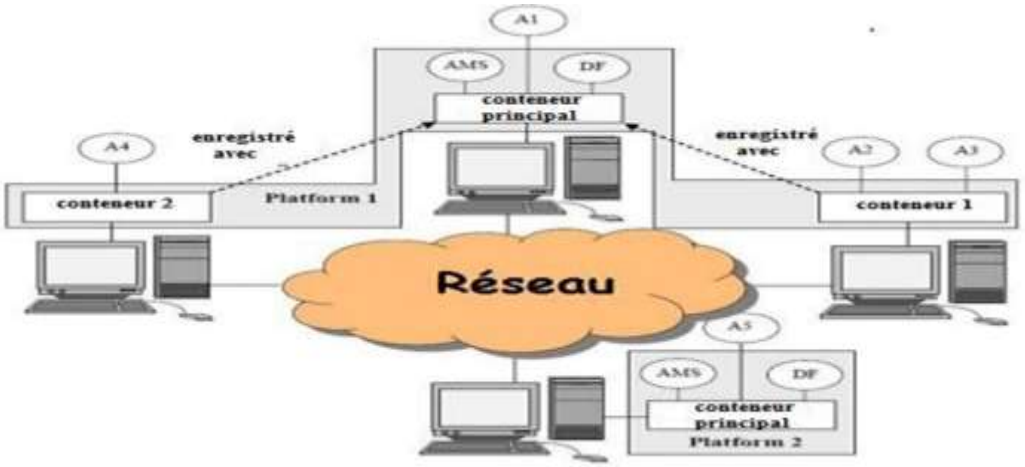


Figure IV.1 : Architecture logicielle de la plateforme JADE [88].

Chaque instance de JADE est appelée conteneur et peut contenir plusieurs agents, ainsi, un ensemble de conteneurs constitue une plateforme et chaque plateforme doit contenir un conteneur spécial appelé main-container et tous les autres conteneurs s'enregistrent auprès de celui-là dès leur lancement. Le main-container se distingue des autres conteneurs car il contient toujours deux agents spéciaux appelés AMS (Agent Management System) et DF (Director Facilitor) qui se lancent automatiquement avec le main-container. La plateforme contient également d'autres modules tels que le Dummy Agent, le Sniffer Agent et l'Introspector Agent qui sont très utiles pour tracer l'exécution de l'application [88]. La figure suivante nous montre l'interface de JADE après le lancement du main- container.

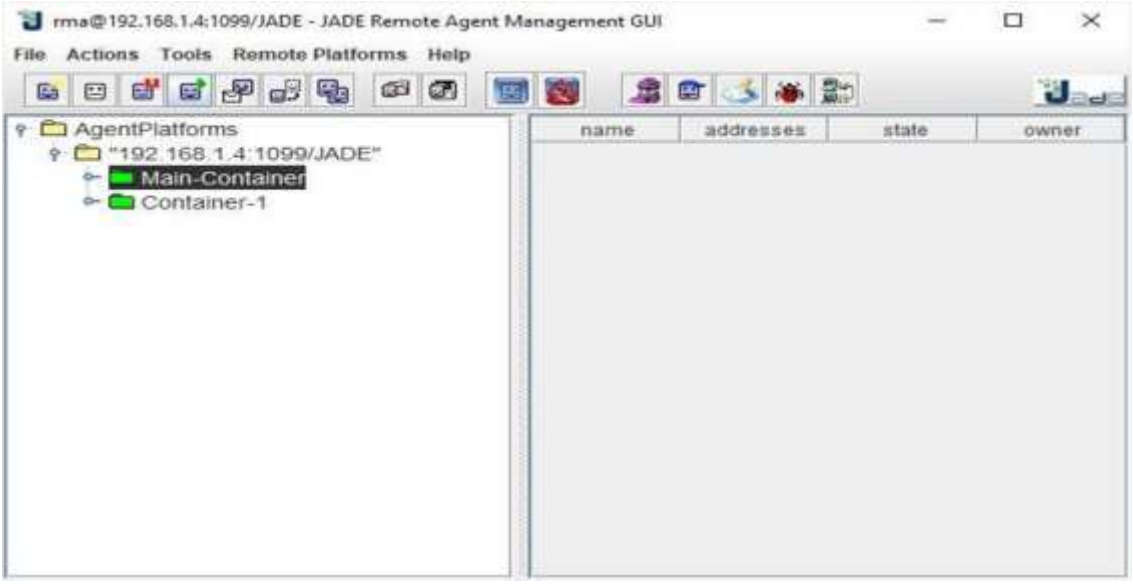


Figure IV.2 : Plateforme JADE

4.2.4 Les composants de JADE

Pour supporter la tâche difficile du débogage des applications multi-agents, des outils ont été développés dans la plate-forme JADE. Chaque outil est empaqueté comme un agent, obéissant aux mêmes règles, aux mêmes possibilités de communication et aux mêmes cycles de vie d'un agent générique [89].

4.2.4.1 Agent RMA

Le RMA permet de contrôler le cycle de vie de la plate-forme et tous les agents la composant. L'architecture répartie de JADE permet le contrôle à distance d'une autre plateforme. Plusieurs RMA peuvent être lancés sur la même plate-forme du moment qu'ils ont des noms distincts [88], comme le montre la figure IV.3 :

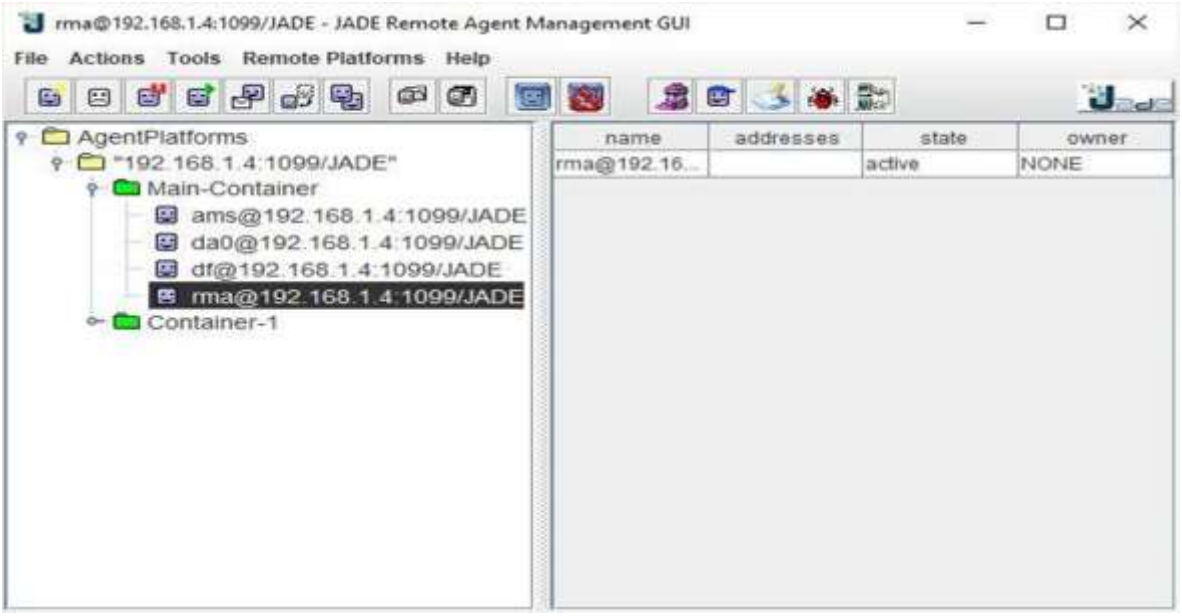


Figure IV.3 : Interface agent RMA

4.2.4.2 Agent Dummy

L'outil Dummy Agent permet aux utilisateurs d'interagir avec les agents JADE d'une façon particulière. L'interface permet la composition et l'envoi de messages ACL et maintient une liste de messages ACL envoyés et reçus. Cette liste peut être examinée par l'utilisateur et chaque message peut être vu en détail ou même édité. Plus encore, le message peut être sauvegardé sur le disque et renvoyé plus tard [89].

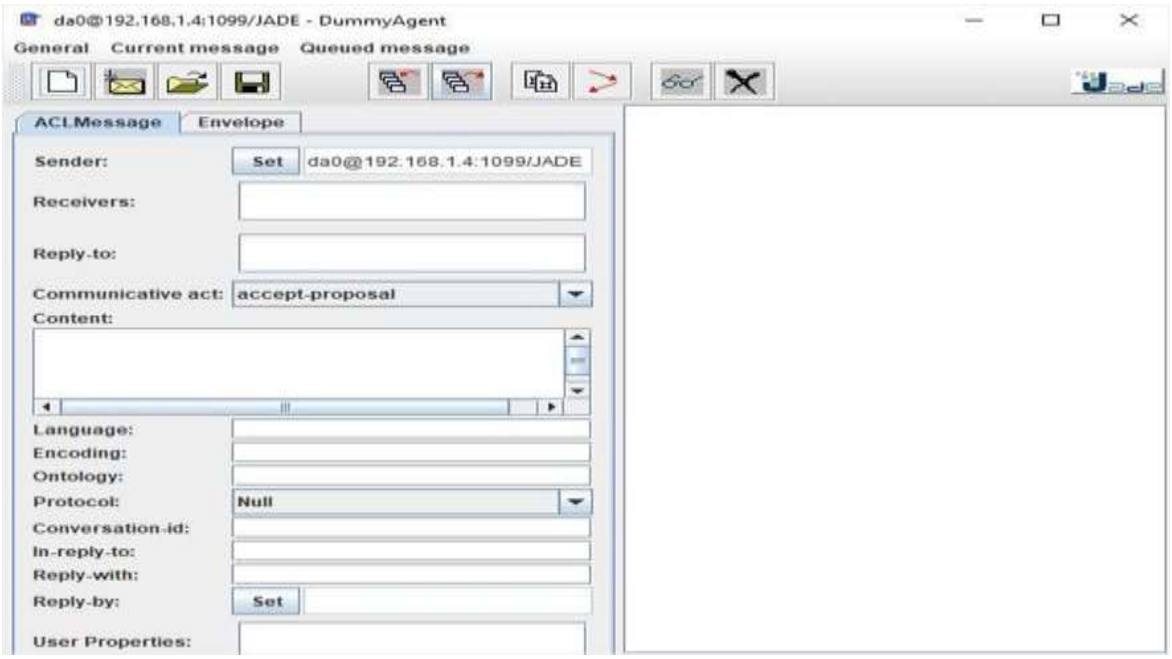


Figure IV.4 : Interface Agent Dummy.

4.2.4.3 Agent Direcory Facilitator

L'interface du DF peut être lancée à partir du menu du RMA. Cette action est en fait implantée par l'envoi d'un message ACL au DF lui demandant de charger son interface graphique. L'interface peut être juste vue sur l'hôte où la plate-forme est exécutée. En utilisant cette interface, l'utilisateur peut interagir avec le DF [89].

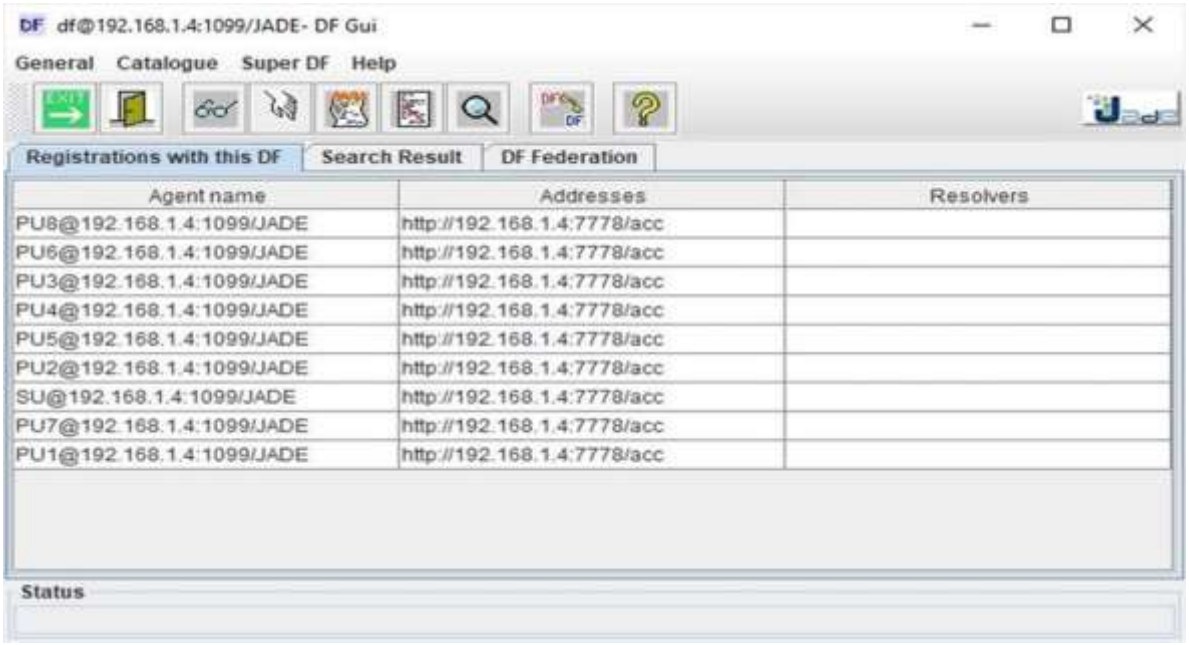


Figure IV.5 : Interface Agent DF [89].

4.2.4.4 Agent Sniffer

Quand un utilisateur décide d'épier un agent ou un groupe d'agents, il utilise un agent sniffer. Chaque message partant ou allant vers ce groupe est capté et affiché sur l'interface du sniffer. L'utilisateur peut voir et enregistrer tous les messages, pour éventuellement les analyser plus tard. L'agent peut être lancé du menu du RMA [86].

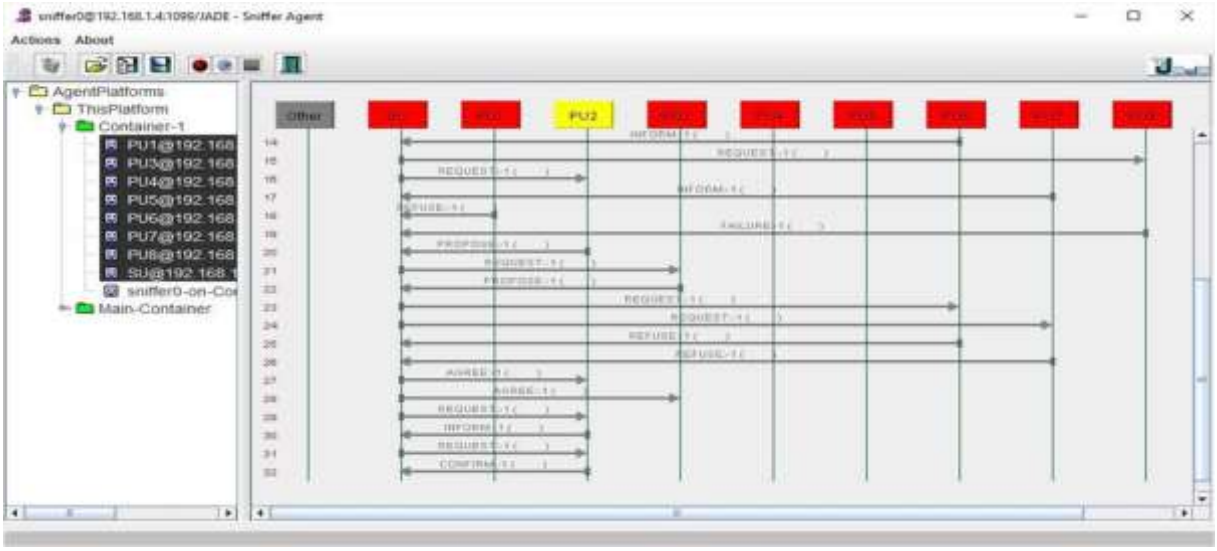


Figure IV.6 : Interface Agent Sniffer [89].

4.2.5 Avantage de JADE

Nous avons choisi de simuler notre scénario dans la plateforme JADE (Java Agent Developpement Framework) pour les raisons suivantes :

- Facilité d'installation.
- Documentation détaillée.
- Utilisation d'un langage puissant et stable (JAVA)
- Intégration avec d'autres outils de développement (Intégration dans Eclipse via les plugins EJIP et EJADE).
- Licence libre (LGPL : (pour GNU Lesser General Public License), c'est une licence utilisée par certains logiciels libres) .
- Plateforme qui a les caractéristiques pour la représentation de l'environnement radio cognitive dans le cas idéal (c'est-à-dire sans la présence des perturbations extérieures).

4.3 Simulation de notre contribution

La partie qui suit est consacrée pour représenter l'étude du scénario cité dans le chapitre précédent, dont on a une communication d'un SU avec des PUs, par rapport aux études faite l'année précédente [91]. Nous avons opté de faire notre étude sur 8 utilisateurs secondaires interagissant avec un utilisateur primaire afin de comparer notre travail avec des études précédentes. En ajoutant l'étape d'authentification en premier lieu, qui permet de garantir la fiabilité des PUs et sécurisée les données échangées entre le SU et le PU choisi après le classement de l'algorithme TOPSIS et en rajoutant un cinquième critère intitulé le taux de fiabilité. Dans ce cadre nous avons commencé par une pré simulation pour connaitre les PUs fiables de ceux qui sont malicieux.

Cette partie nous servira à sélectionner le PU le plus favorable et fiable pour notre contribution. La communication se déroulera comme suit :

Le SU envoie des requêtes contenant des messages cryptés vers les huit (8) PUs, et selon ces réponses le SU va décider qui seront les PUs honnêtes et qui seront malhonnêtes tels que :

Les PUs qui décryptent le message envoyé par le SU et qui répondent par des messages sensés sont des PUs honnêtes, les autres sont considérés comme des PUs malhonnêtes. A chaque tentative on va incrémenter par 1 les PUs fiables et un 0 au PUs non fiables et sur cent tentatives on va récupérer le pourcentage de fiabilité de chaque PU, pour classer le taux d'honnêteté et de malveillance.

Dans les études suivantes, nous utiliserons l'algorithme d'authentification ECDH et l'algorithme TOPSIS.

4.3.1 Etude 1 : Taux de Fiabilité

Dans cette étude de 100 tentatives nous calculons un taux de malveillance et d'honnêteté de 8 PUs en donnant la valeur 0 au PU honnête et la valeur 1 au PU malveillant, la somme des valeurs obtenues pour chaque PU sera le taux de malveillance et le pourcentage d'honnêteté sera (100 - le taux de malveillance), de sorte que la somme des 2 derniers soit égale à 100%.

Les résultats de pourcentages de taux de fiabilité de chaque PU avec le SU et présenter dans les tableaux et les figures suivants :

PUs	Taux de malveillance %	Taux de d'honnêteté %
PU1	12	88
PU2	12	88
PU3	20	80
PU4	5	95
PU5	5	95
PU6	11	89
PU7	14	86
PU8	5	95

Tableau IV.1 : Résultats de taux de malveillance / d'honnêteté pour chaque PU.

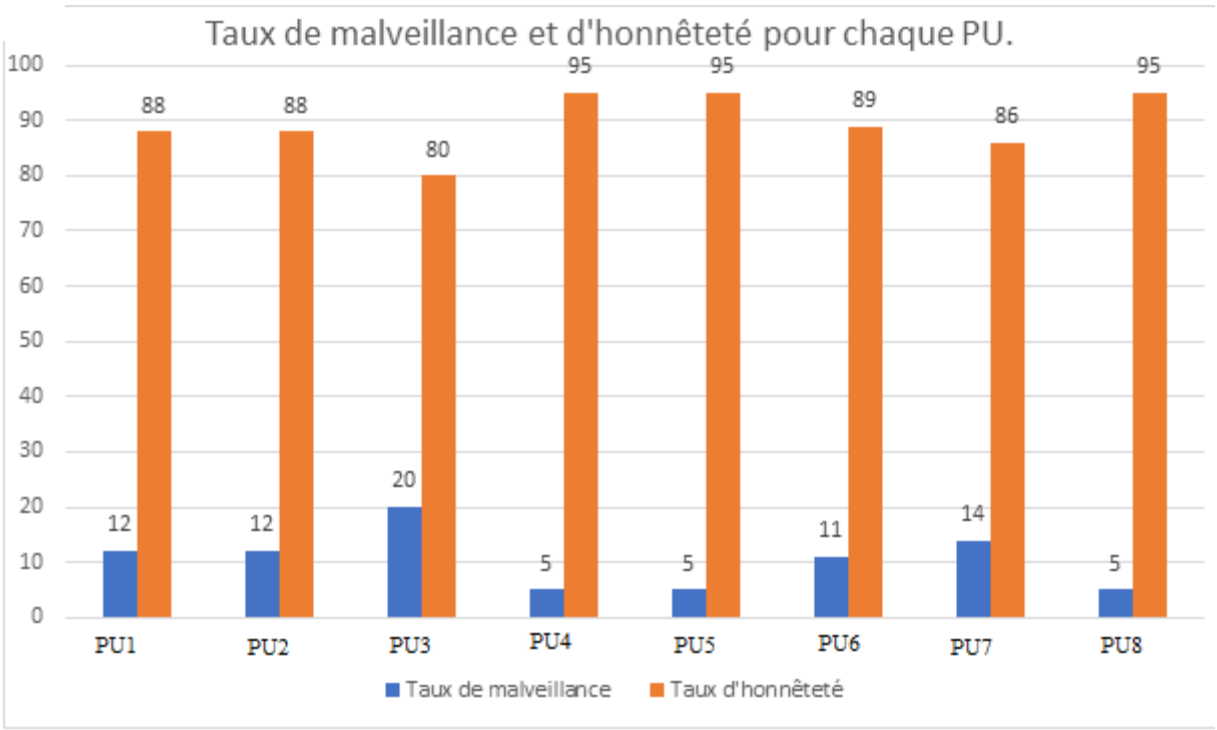


Figure IV.7 : Taux de fiabilité pour chaque PU.

Le graphe ci-dessus nous montre que PU4, PU5 et PU8 ont le taux d'honnêteté le plus élevé de 95% et automatiquement ils ont le taux de malveillance le plus bas de 5%.

C'est-à-dire qu'après 100 tentatives PU4, PU5 et PU8 étaient 95 fois honnêtes et 5 fois malveillants.

PU3 a le taux de malveillance le plus haut à 20 % et c'est normal qu'il ait le taux d'honnêteté le plus bas avec 80%.

Pus	**Classement par rapport le taux d'honnêteté et de malveillance**
PU1	4
PU2	4
PU3	5
PU4	1
PU5	1
PU6	2
PU7	3
PU8	1

Tableau IV.2 : Classement des PUs par rapport le taux de malveillance et d'honnêteté.

4.3.2 Etude 2 : Temps de convergence

Dans cette étude, nous allons calculer le temps de convergence qui est le temps de tout le processus depuis le début de l'authentification jusqu'à la fin de la négociation de chaque PU, sachant que si le PU est malicieux ou il n'a pas le nombre de canaux exigés son temps de convergence n'est pas pris en compte.

Les tableaux et les figures suivants représentent les résultats de temps de convergence pour chaque PUs.

Pus	Temps de convergence (ms)
PU1	91.24
PU2	87.09
PU3	98.10
PU4	99.95
PU5	96.46
PU6	98.49
PU7	97.2
PU8	107.04

Tableau IV.3 : Moyenne de temps de convergence pour chaque PU

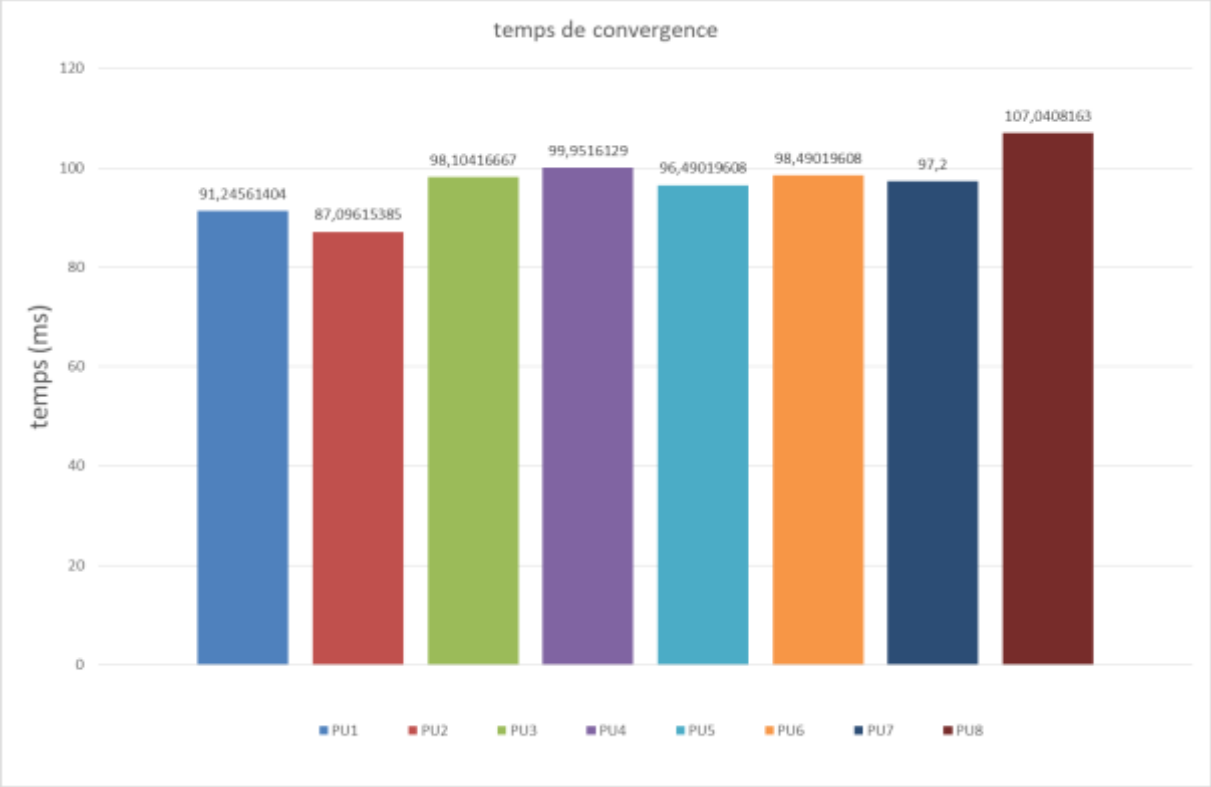


Figure IV.8 : Comparaison entre les PUs par rapport au temps de convergence

Les résultats ont montré que PU2 est le plus rapide avec un temps de convergence égale à 87,09 ms, et PU8 est le plus lent avec un temps de convergence égale à 107,04 ms.

Pus	**Classement par rapport le temps de convergence**
PU2	1
PU1	2
PU5	3
PU7	4
PU3	5
PU6	6
PU4	7
PU8	8

Tableau IV.4 : Classement des PUs par rapport au temps de convergence.

4.3.2.1 Comparaison avec les études précédentes

Nous avons pu comparer notre contribution avec l'article [91] ou on a ajouté une partie d'authentification et de sécurisation des données pour tester la fiabilité des agents cognitifs, ce qui aidera les utilisateurs secondaires de mieux partagés ses données en toutes sécurité dans des bandes de fréquences licenciées et sécurisées. Dans cette partie nous allons faire une comparaison entre nos résultats et ceux des travaux réalisés en [91] en termes de temps de convergence pour la qualité de service de la vidéo conférence.

Par rapport à cette dernière étude, le temps de convergence a augmenté car nous avons ajouté un nouveau processus, c'est le processus d'authentification ECDH qui permet de filtrer les utilisateurs malveillants. Donc notre algorithme comporte trois étapes, l'étape d'authentification (avec l'ECDH), l'étape de la négociation à multicritères (avec le TOPSIS) et l'étape de chiffrement (avec l'algorithme AES).

	Sécurité et Authentification	**Sécurité renforcée avec cryptage (AES+ECC)**	**Nombre de critère avec TOPSIS**	**Meilleur PU**	**Moyenne de convergence de meilleur PU (ms)**	**Pire PU**	**Moyenne de temps de convergence de pire PU**	**Moyenne générale de temps de convergence (ms)**
Travaux de [90]	**OUI**	**NON**	**5**	**PU3**	**70.25**	**PU8**	**88.70**	**78.38**
Travaux de notre approche	**OUI**	**OUI**	**5**	**PU2**	**87.09**	**PU8**	**107.04**	**96.94**

Tableau IV.5 : Comparaison entre les temps de convergences

Le tableau IV.1 nous montre les résultats de comparaison entre le temps de convergence de notre contribution avec ceux de la littérature [91]. On a un écart de 16.84 ms à la moyenne de temps de convergence du meilleur PU, et un écart de 18.34 pour le pire PU, en gros un écart ΔT de 18.56 à la moyenne générale de temps de convergence à cause de la présence de l'étape de sécurité renforcée avec cryptage (AES + ECC) des données. Néanmoins la qualité de service de la vidéo conférence est assurée puisque le temps est inférieur à 250 ms.

$$\Delta T = 96.94 - 78.38 = 18.56 \text{ ms}$$

La figure représente une comparaison entre nos résultats et les résultats des travaux précédents sur le temps de convergence d'une communication pour la vidéo conférence (4 canaux).

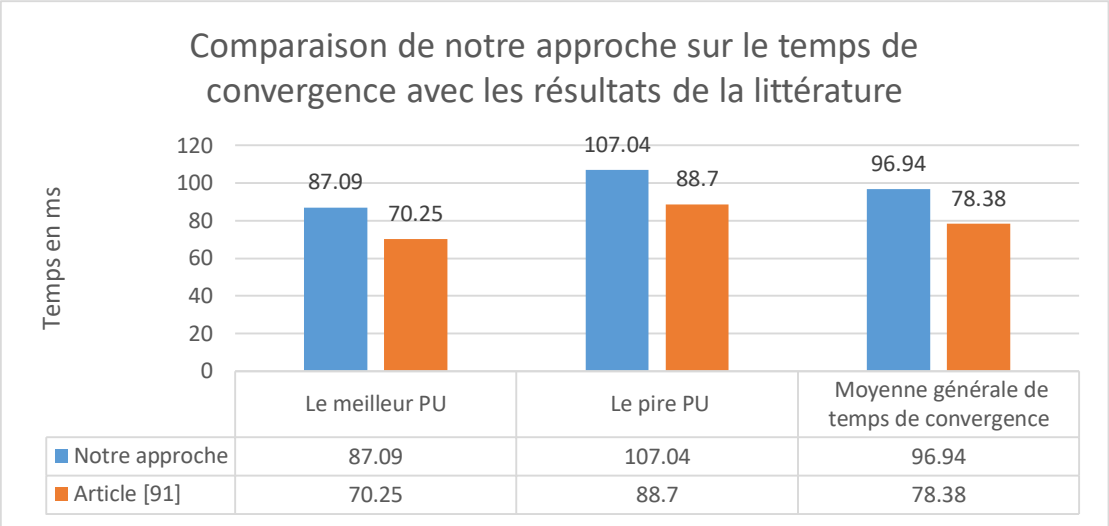


Figure IV.9 : Comparaison de notre approche sur le temps de convergence avec les résultats de la littérature.

4.3.3 Etude 3 : Le meilleur PU (the best)

Dans cette étude de 100 tentatives, nous essaierons d'authentifier le meilleur PU parmi les 8 PUs en donnant à chaque tentative le rang 8 au meilleur PU choisi par l'algorithme TOPSIS, 7 au deuxième PU, 6 au troisième. Ensuite, on fait la somme des rangs de chaque PU et on divise sur 800.

Les tableaux et les figures suivants représentent les résultats du taux du meilleurs PU sur 100 tentatives pour chaque PUs.

Pus	**Taux du meilleur PU (%)**
PU1	45.125
PU2	37.652
PU3	37.875
PU4	46.625
PU5	39.125
PU6	38,125
PU7	39,875
PU8	38,75

Tableau IV.6 : Résultats du meilleur PU sur 100 tentatives.

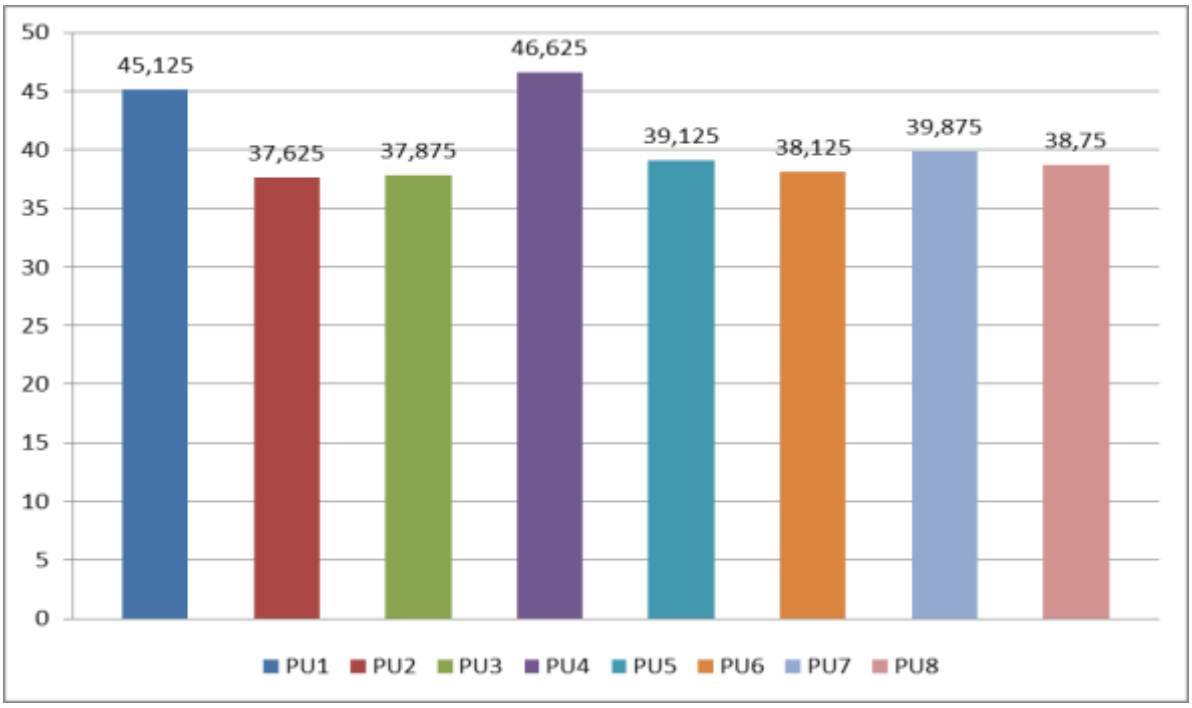


Figure IV.10 : Taux du meilleur PU en Pourcentage

Les résultats ont montré que PU4 est le meilleur PU avec un rang de 46.625% puis PU1 avec 45.125%, alors que PU2 a le pire rang avec 37.625 %.

Pus	Classement des meilleur PUs
PU4	1
PU1	2
PU7	3
PU5	4
PU8	5
PU6	6
PU3	7
PU2	8

Tableau IV.7 : Classement des meilleurs PUs

4.3.4 Etude 4 : Le pire PU (the worst)

Dans cette étude, nous allons calculer le pourcentage du pire PU en donnant :

- La valeur **0** au meilleur PU.
- La valeur **0.25** au PU honnête mais pas le meilleur.
- La valeur **0.75** au PU honnête mais n'a pas le nombre de canaux exigés par le SU.
- La valeur **1** au PU malicieux.

Les tableaux et les figures suivants représentent les résultats du pire PU.

Pus	**Taux du pire PU**
PU1	51.25 %
PU2	20.5 %
PU3	20.5 %
PU4	30 %
PU5	48.25 %
PU6	47,5 %
PU7	47,5 %
PU8	48,25 %

Tableau IV.8 : Résultats du pire PU.

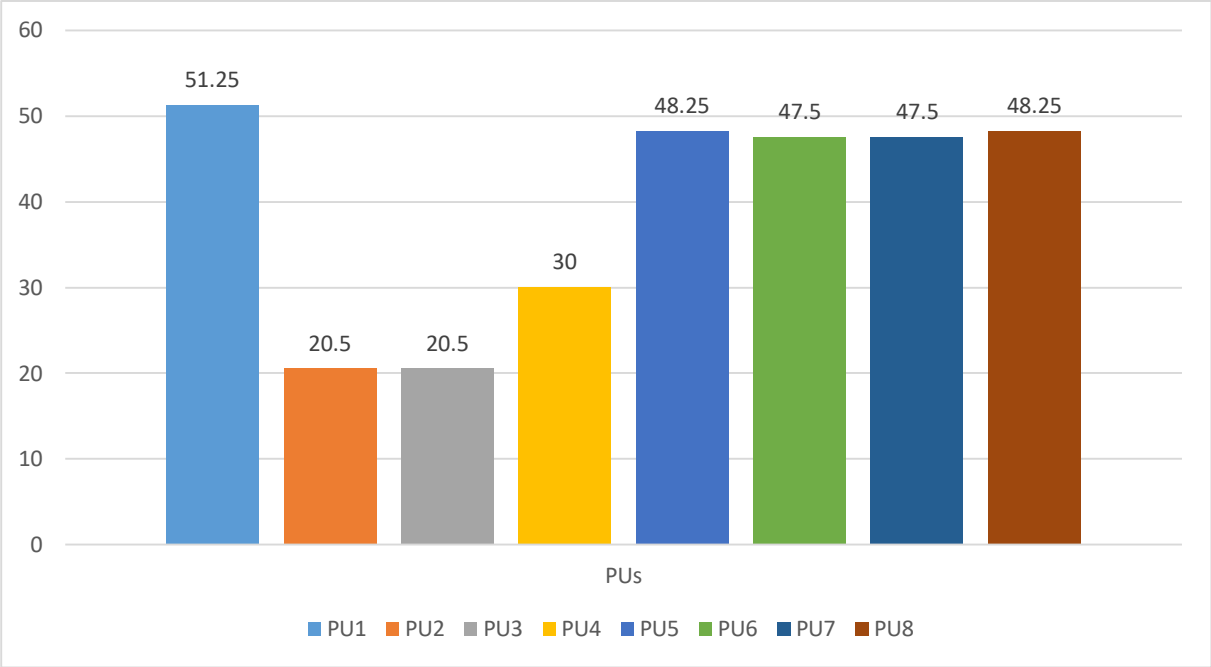
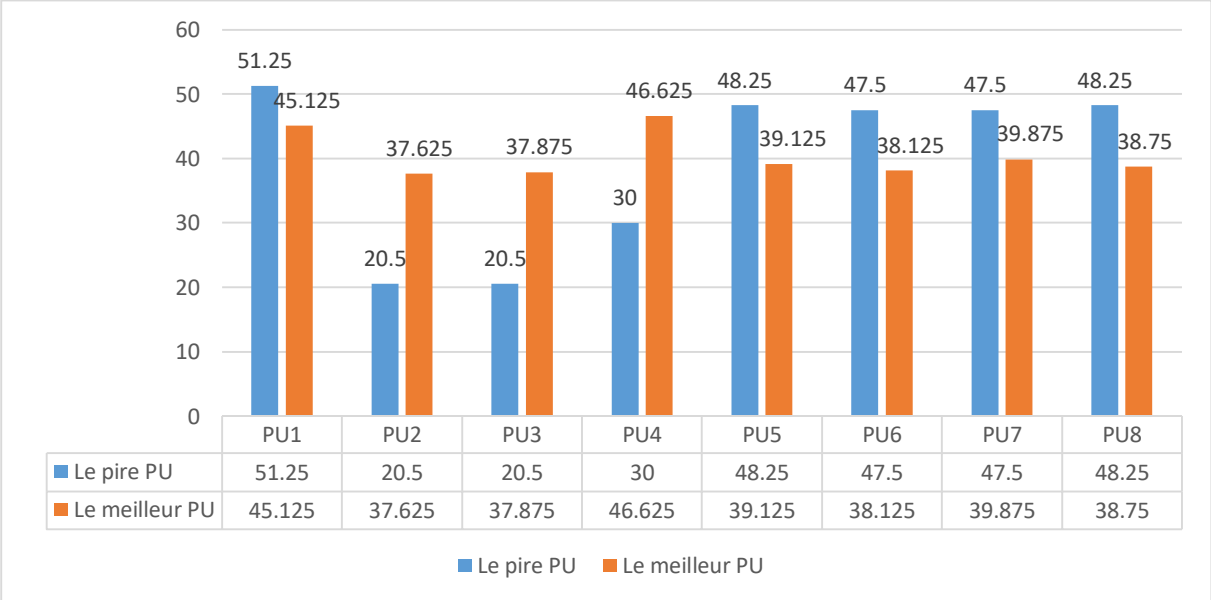


Figure IV.11 : Le pire PU

Les résultats ont montré que PU1 est le pire PU avec un pourcentage de 51.25 %, PU5 avec un pourcentage de 48.25 %, puis PU2 qui est le moins pire rang avec 20.5%.

La figure suivante représente une comparaison entre être le meilleur et être le pire pour chaque PU :



	PU1	PU2	PU3	PU4	PU5	PU6	PU7	PU8
Le pire PU	51.25	20.5	20.5	30	48.25	47.5	47.5	48.25
Le meilleur PU	45.125	37.625	37.875	46.625	39.125	38.125	39.875	38.75

Figure IV.12 : Comparaison entre être le meilleur et être le pire pour chaque PU

PU	Taux être le meilleur (Si+)	Taux être le pire (Si-)	La moyenne (Pi)	Classement
PU1	45,125	51,25	0.468	4
PU2	37,625	20,5	0,647	2
PU3	37,875	20,5	0.648	1
PU4	46,625	30	0.608	3
PU5	39,125	48,25	0.447	6
PU6	38,125	47,5	0.4452	8
PU7	39,875	47,5	0.456	5
PU8	38,75	48,25	0.4454	7

Tableau IV.9 : Classement de PU par rapport le taux être le **meilleur /pire** pour chaque PU

Après classement de la moyenne Pi représentée en (IV.1), nous avons trouvé que PU3 possède les caractéristiques les plus fiables et de qualité pour être partagé avec le SU tandis que PU6 et PU8 sont les utilisateurs les moins fiables pour être partagé avec le SU.

La moyenne $$\mathbf{Pi} = \frac{\mathbf{Si+}}{(\mathbf{Si+})+(\mathbf{Si-})} \qquad \textbf{(IV.1)}$$

Interprétation des résultats

Dans le cadre de notre étude, nous avons essayé de créer un protocole d'authentification dédier à la détection des utilisateurs malveillants dans les réseaux radio cognitifs et au-delà de ça nous avons complémentés notre travail avec des études précédentes afin de comparer et de valoriser notre approche jusqu'à la sécurisation avec chiffrement de toute la procédure de partage du spectre d'un utilisateur réseaux dites de la radio cognitive.

Le résultat obtenu est très satisfaisant puisque le temps de convergence pour une qualité de service d'utiliser une vidéo conférence est respectée (< 250 ms) et le taux de fiabilité (Honnête/ malicieux) peut être suggéré à d'autres SU afin de minimiser le contact avec des utilisateurs malveillants ainsi que le meilleur/pire PU sera connu de façon à l'utiliser le plus ou le moins souvent.

4.4 Conclusion

La plupart des technologies récentes cherchent à améliorer la bonne gestion et la sécurisation du spectre radio. Les réseaux de radio cognitifs ont ouvert la voie à des perspectives d'avenir très prometteuses pour les scientifiques et chercheurs de ce domaine, afin d'en assurer la meilleure utilisation possible.

Dans ce dernier chapitre, nous avons choisi d'englober et de continuer nos recherches complémentaires des travaux précédents tout en assurant l'authentification et la sécurité des réseaux radio cognitifs, où nous avons obtenu d'excellents résultats en termes de temps de convergence malgré l'ajout de plusieurs étapes de sécurisation et d'authentification des données, avec l'utilisation d'un algorithme d'authentification ECDH. Un autre pour le multicritère TOPSIS et un algorithme de chiffrement AES pour l'envoie et la réception des données en assurant une sécurité accrue à notre contribution.

Conclusion générale

La radio cognitive a apporté de nombreuses solutions aux problèmes de congestion du spectre radio, en particulier l'indépendance complète qu'elle donne aux utilisateurs primaires et secondaires et étant une technologie intelligente qui s'appuie principalement sur l'intelligence artificielle pour créer un environnement virtuel qui facilite la négociation entre les utilisateurs primaires (PU) et les utilisateurs secondaires (SU).

Pour assurer les résultats souhaités en termes de gestion et d'optimisation du spectre radio, nous avons proposé un système de sécurité qui donne une touche optimale à cette technologie, incluant la fiabilité des agents et assurant la confidentialité de ces données.

Dans ce PFE, nous avons pu mettre en place un système de sécurité pour approuver la sécurité des utilisateurs et assurer le bon déroulement du processus de négociation entre les utilisateurs primaires et secondaires en supprimant tous les utilisateurs malveillants de la négociation à l'aide d'un algorithme d'authentification ECDH qui filtre les utilisateurs malveillants.

Dans le premier chapitre, nous avons cité les différents réseaux sans fil et mobiles, et nous avons détaillé la technologie radio cognitive avec l'aspect de la sécurité dans ses réseaux.

Dans le deuxième chapitre, nous avons abordé les systèmes multi-agents, ainsi que la sécurité dans les réseaux radio cognitifs et le concept de chiffrement et de déchiffrement et les différents protocoles d'authentification qui nous ont permis de renforcer les systèmes radio cognitifs.

Dans le troisième chapitre, nous avons décrit les algorithmes utilisés pour notre approche, à savoir ceux d'authentification, de choix multicritère et de mode de chiffrement, ainsi que l'organigramme proposé.

Enfin, le dernier chapitre représente la simulation de notre contribution, où nous avons réalisé trois études pour comparer les utilisateurs primaires selon des critères tels que le temps de convergence, le taux d’honnêteté et de malveillance ou le classement sur 100 tentatives des meilleurs et des pires utilisateurs primaires.

Bibliographie

[1] El-Hajj Wassim, Haidar Safa, and Mohsen Guizani. "Survey of security issues in cognitive radio networks" Journal of Internet Technology 12, no. 2, P: 181-198, (2011).

[2] Benmammar, Badr, and Asma Amraoui. "R\'eseaux de radio cognitive: Allocation des

[3] Allio, S. (2007). Méthodes avancées pour une ingénierie WLAN multi-standards (Doctoral dissertation, INSTITUT NATIONAL DES SCIENCES APPLIQUÉES DE RENNES).

[4] El-Bendary, Mohsen AM. "Developing security tools of WSN and WBAN networks applications". Springer Japan, 2015

[5] Fabrice MFUAMBA, ''Etude portant sur l'implantation d'un réseau sans fil (wifi)'', institut supérieur des techniques appliquées de Kinshasa - Ingénieur technicien en électronique, 2012

[6] BENGHABRIT Nawel, ''Allocation des ressources dans les réseaux radio cognitifs'', 2019.

[7] ALLAL Mohammed Anes, "Utilisation du deep learning dans la radio cognitive", Université Abou Bakr Belkaid – Tlemcen, 2018

[8] Feng Wang, Student Member, IEEE, "Cognitive Radio Networks and Security: A Survey", IEEE Journal of selected topics in signal processing 5.1, June 2013.

[9] Chen, Ruiliang, and Jung-Min Park. "Ensuring trustworthy spectrum sensing in cognitive radio networks" In 2006 1st IEEE Workshop on Networking Technologies for Software Defined Radio Networks, pp. 110-119. IEEE, 2006.

[10] FASLA, Ouassini, and Samira BOULANOUAR. "Instauration d'un algorithme de sécurité pour l'accès dynamique au spectre dans un réseau radio cognitif" PhD diss., 11-01- 2018.

[11] El-Hajj Wassim, Haidar Safa, and Mohsen Guizani. "Survey of security issues in cognitive radio networks" Journal of Internet Technology 12, no. 2, P: 181-198, (2011).

[12] León, Olga, Juan Hernández-Serrano, and Miguel Soriano. "Securing cognitive radio networks" international journal of communication systems 23, no.5, p 633-652, (2010).

[13] Chen, Ruiliang, Jung-Min Park, Y. Thomas Hou, and Jeffrey H. Reed. "Toward secure distributed spectrum sensing in cognitive radio networks" IEEE Communications Magazine 46, no. 4, P: 50-55 (2008)

[14] Chen, Ruiliang, Jung-Min Park, and Jeffrey H. Reed. "Defense against primary user emulation attacks in cognitive radio networks." IEEE Journal on selected areas in communications 26, no. 1, P : 25-37,(2008).

[15] Ureten, Oktay, and Nur Serinken. "Wireless security through RF fingerprinting" Canadian Journal of Electrical and Computer Engineering 32, no. 1, P: 27- 33 (2007)

[16] Afolabi, O. Richard, Kiseon Kim, and Aftab Ahmad. "On secure spectrum sensing in cognitive radio networks using emitters electromagnetic signature" In 2009 Proceedings of 18th International Conference on Computer Communications and Networks, pp. 1-5. IEEE, 2009.
[17] Zhao, Caidan, Wumei Wang, Lianfen Huang, and Yan Yao. "Anti-PUE attack base on the transmitter fingerprint identification in cognitive radio" In 2009 5th International Conference on Wireless Communications, Networking and Mobile Computing, pp. 1-5. IEEE, 2009.
[18] Mahmoud, Qusay H. "Cognitive networks." John Wiley& Sons Ltd, P: 57-71 (2007)
[19] Clancy, T. Charles, and Nathan Goergen "Security in cognitive radio networks: Threats and mitigation" In 2008 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom 2008), pp. 1-8. IEEE, 2008.
[20] Zhang, Yuan, Gaochao Xu, and Xiaozhong Geng. "Security threats in cognitive radio networks" In 2008 10th IEEE International Conference on High Performance Computing and Communications, pp. 1036-1041. IEEE, 2008
[21] Xu, Wenyuan, Wade Trappe, Yanyong Zhang, and Timothy Wood. "The feasibility of launching and detecting jamming attacks in wireless networks" In Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing, pp. 46-57. 2005.
[22] Xu, Wenyuan, Timothy Wood, Wade Trappe, and Yanyong Zhang. "Channel surfing and spatial retreats: defenses against wireless denial of service" In Proceedings of the 3rd ACM workshop on Wireless security, pp. 80-89. 2004.
[23] Leon, Olga, Juan Hernandez-Serrano, and Miguel Soriano, "A new cross-layer attack to TCP in cognitive radio networks" In 2009 Second International Workshop on Cross Layer Design, pp. 1-5. IEEE, 2009.
[24] Karlof, Chris, and David Wagner. "Secure routing in wireless sensor networks: Attacks and countermeasures" Ad hoc networks 1, no. 2-3, P: 293-315 (2003).
[25] P. Anand, A. S. Rawat, H. Chen, et P. K. Varshney, « Collaborative spectrum sensing in the presence of byzantine attacks in cognitive radio networks », in Communication Systems and Networks (COMSNETS), 2010 Second International Conference on, p: 1–9, 2010.
[26] Wang, Huahui, Leonard Lightfoot, and Tongtong Li. "On phy-layer security of cognitive radio: Collaborative sensing under malicious attacks" In 2010 44th Annual Conference on Information Sciences and Systems (CISS), pp. 1-6. IEEE, 2010.92
[27] Shei, Yeelin, and Yu T. Su. "A sequential test based cooperative spectrum sensing scheme for cognitive radios" In 2008 IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications, pp. 1-5. IEEE, 2008.

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

[29] Bian, Kaigui, and Jung-Min Park. "MAC-layer misbehaviors in multi-hop cognitive radio networks" In 2006 US-Korea Conference on Science, Technology, and Entrepreneurship (UKC2006), pp. 228-248. 2006.

[30] Hernandez-Serrano, Juan, Olga León, and Miguel Soriano. "Modeling the lion attack in cognitive radio networks." EURASIP Journal on Wireless Communications and Networking 2011, P: 1-10 (2011).

[31] Jacques Ferber, Les Systèmes multi-agents : Vers une intelligence collective, Inter Editions, 1995, 522 p. (ISBN 2-7296-0665-3)

[32]https://www.techniques-ingenieur.fr/actualite/articles/intelligence-artificielle-et-systemes-multi-agents-55468/ visité le 15 mars 2022

[33] Mémoire de fin d'études arrousi sana CONCEPTION ET REALISATION D'UNE PLATE-FORME MULTI-AGENTS MINIMALE Septembre 2009

[34] Bryan Horling and Victor Lesser, "A Survey of Multi-Agent Organizational Paradigms," The Knowledge Engineering Review, vol. 19, No. 4, December 2004

[35] Klaus Fischer, Michael Schillo et JörgSiekmann, « Holonic Multiagent Systems: A Foundation for the Organisation of Multiagent Systems », Lecture Notes in Computer Science, vol. 2744, 2003

[36] Christopher H. Brooks, Edmund H. Durfee et Aaron Armstrong, « An Introduction to Congregating in Multiagent Systems », Proceedings Fourth International Conference on MultiAgent Systems,juillet 2000, p. 79-86

[37] Anthony Chavez et Pattie Maes, « Kasbah: An agent marketplace for buying and selling goods », AAAI, 1996

[38] Ferber, Jacques , Les systèmes multi-agents : un aperçu général.

[39] Thomas Eisenbarth, Sandeep Kumar, Christof Paar, Axel Poschmann, and Leif Uhsadel. Asurvey of lightweight-cryptography implementations. IEEE Design & Test of Computers,24(6) :522–533, 2007.

[40] Michael Healy, Thomas Newe, and Elfed Lewis. Analysis of hardware encryption versus software encryption on wireless sensor network motes. In Smart Sensors and Sensing Technology, pages 3–14. Springer, 2008.

[41] Yee Wei Law, Jeroen Doumen, and Pieter Hartel. Survey and benchmark of block ciphers for wireless sensor networks. ACM Transactions on Sensor Networks (TOSN), 2(1) :65–93, 2006.

[42] Haodong Wang and Qun Li. Efficient implementation of public key cryptosystems on mote sensors (short paper). In Information and Communications Security, pages 519–528. Springer, 2006

[43] Darrel Hankerson, Scott Vanstone, and Alfred J Menezes. Guide to elliptic curve cryptography. Springer, 2004

[44] Youssou Faye , Algorithmes d'authentification et de cryptographie efficaces pour les réseaux de capteurs sans fil, Mars 2015

[45] Rishabh Hastu, Parag Jagtap Abhishek, Shukla, Security in Cognitive Radio Networks University of Mumbai,April 2014

[46] Hendrik W Lenstra et al. Elliptic curves and number-theoretic algorithms. University van Amsterdam, Mathematisch Instituut, 1986.

[47] Hendrik W Lenstra Jr. Factoring integers with elliptic curves. Annals of mathematics, pages 649–673, 1987.

[48] Darrel Hankerson, Scott Vanstone, and Alfred J Menezes. Guide to elliptic curve cryptography. Springer, 2004.

[49] Nils Gura, Arun Patel, Arvinderpal Wander, Hans Eberle, and Sheueling Chang Shantz. Comparing elliptic curve cryptography and rsa on 8-bit cpus. In Cryptographic Hardware and Embedded Systems-CHES 2004, pages 119–132. Springer, 2004.

[50] Ross Anderson, Haowen Chan, and Adrian Perrig. Key infection: Smart trust for smart dust. In Network Protocols, 2004. ICNP 2004. Proceedings of the 12th IEEE International Conference on, pages 206–215. IEEE, 2004.

[51] malekal.com, INFORMATIQUE EN GÉNÉRAL, 14 AVRIL 2022.

[52] Pierre-Alain Fouque, Algorithmes de chiffrement symétrique par bloc (DES et AES)

[53] https://web.maths.unsw.edu.au/~lafaye/CCM/crypto/des.htm visité le 14/05/2022

[54] https://community.cisco.com/t5/security-documents/3des/ta-p/3113951 visité le 16 mai 2022 (DES), 25 octobre 1999

[56] Article Himanshu Tyagi et Shun Watanabe "A Bound for Multiparty Secret Key Agreement and Implications for a Problem of Secure Computing"

[57] https://www.gnupg.org/gph/fr/manual.html (consulté le 18 mars 2021)

[58] DESTREE Lucile, MARCHAL Mickaël, Mini-RSA Programme d'initiation au chiffrement RSA

[59] https://www.univ-tlemcen.dz/~benmammar/IA3.pdf visité le 165/05/2022,visité le 15/05/2022

[60] www.techniques-ingenieur.fr visité le 13/05/2022

[61] Asma AMRAOUI, Badr BENMAMMAR, Radio Cognitive et Accès Dynamique au Spectre, 18 Avril 2012

[62] Gérard Leblanc, C# et .NET : Version 1 à 4, Editions Eyrolles, 7 juillet 2011

[63] tfig.unece.org visité le 04/06/2022

[64] FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, "Digital Signature Standard (DSS)", FIPS PUB 186, 19 Mai 1994.

[65] El Khier DEHMECHE, ETUDE ET COMPARAISON DES PRINCIPAUX SYSTEMES DE CRYPTAGE, diplôme de magister en informatique, université M'sila, 2006.

[66] Whitfield Diffie and Martin Hellman. New directions in cryptography. Information Theory, IEEE Transactions on, 22(6) :644–654, 1976.

[67] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In Advances in Cryptology, pages 10–18. Springer, 1985.

[68] Yanbo Shou, Cryptographie sur les courbes elliptiques et tolérance aux pannes dans les réseaux de capteurs, 1 Dec 2014

[69] Jean-louis Poss. Introduction à la cryptographie. Ecole Nationale Supérieure d'Arts et Métiers, Aix.en-Provence, octobre 2000.

[70] Elliptic Curve Diffie-Hellman Available [68] [10] T. El Gamal, A public key crypto-system and signature scheme based on discrete logarithms. IEEE Transactions on Information Theory IT-31, 496-473,1976.

[71] Hankerson et. al. (2004) Guide Elliptic Curve Cryptography University of Waterloo, Springer-Verlag, New York [70] [18] FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, "Digital Signature Standard (DSS)", FIPS PUB 186, 19 Mai 1994

[72] D. Hankerson, A. Menezes & S. Vanstone. Guide to elliptic curve cryptography. Springer-Verlag New York, Inc, 2004.

[73] Thèse de Doctorat, Youssou Faye, « Algorithmes d'authentification et de cryptographie efficaces pour les réseaux de capteurs sans fil », Mars 2015

[74] Jang Schiltz, Les modes opératoires de la cryptographie symétrique 2003.
[75] NaimaHadj-Said, AddaAli-Pacha, MohamedSadekAli-Pacha – AekHaouas, « Nouveau Mode Opératoire pour la Cryptographie ».
[76] M. Z. BABA AHMED. « Conception d'un crypto système pour les transmissions d'images chiffrées en télécommunication ».Projet de fin d'études pour l'obtention du diplôme d'ingénieur d'état. Université Abou Bak Belkaid–Tlemcen. 2010.
[77] O. Boissier, S. Gitton, P. Glize, "Caractéristiques des Systèmes et des Applications", dans Systèmes Multi-Agents, vol. 29, pp. 25-54, Editions TEC & DOC, 2004
[78] Wang, Y., and al."Generalizing topsis for fuzzy multiple-criteria group decisionmaking." International Journal computers and mathematics with applications 53(11) (2007), 1762–1772.
[79] Sarraf, Amin Zadeh, Ali Mohaghar, and Hossein Bazargani. "Developing TOPSIS method using statistical normalization for selecting Knowledge management strategies." Journal of industrial engineering and management 6, no. 4 (2013): 860-875.
[80] Yezza, A. "La méthode TOPSIS expliquée pas à pas" Sopra Steria Group (2015)
[81] Martel, Jean-Marc, and Bernard Roy. "Analyse de la signifiance de diverses procédures d'agrégation multicritère." INFOR : Information Systems and Operational Research 43, no. 3, p : 221-245. (2005).
[82] HADJADJ, Nour El Houda, and Khaoula ABDI. "Investigation autour de la localisation optimale des stations d'épuration : cas du groupement urbain de Tlemcen." PhD diss.
[83] M. Benmammar Badr, "Allocation de ressources dans un réseau de radio cognitive en utilisant JADE" Rapport de recherche en Télécommunication, Université Tlemcen, juillet 2015.
[84] Parida, P. K. "A General View of TOPSIS Method Involving Multi-Attribute Decision Making Problems.",(2019).
[85] https://fr.wikipedia.org/wiki/NetBeans (dernière consultation le 25/06/2021)
[86]https://www.developpez.com/actu/185087/Quels-sont-les-langages-de-programmationles-plus-utilises-par-les-developpeurs-Une-analyse-des-evenements-publics-sur-GitHub/ (dernière consultation le 25/06/2021)
[87] Poslad, Stefan. "Specifying protocols for multi-agent systems interaction" ACM Transactions on Autonomous and Adaptive Systems (TAAS) 2, no. 4 (2007): 15-es.
[88] Bellifemine, Fabio Luigi, Giovanni Caire, and Dominic Greenwood. "Developing multiagent systems with JADE" Vol. 7. John Wiley & Sons, 2007.

[89] Mr ELANDALOUSSI SIDAHMED, "Développement d'un WEB-MAS pour la conception et fabrication assistées par ordinateur : application à un atelier de pièces mécaniques" Thèse de Magister en informatique, Université d'Oran, 2012/2013.
[90] Łatuszyńska, Anna. "Multiple-criteria decision analysis using TOPSIS method for interval data in research into the level of information society development." Folia Oeconomica Stetinensia 13, no. 2 (2014): 63-76.
[91] Mémoire de fin d'études : Khellafi, Abdelguerfi « Sécurisation des Données d'un Réseau de Radio Cognitif pour des Utilisateurs Secondaires à Multicritères »