REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Mohamed Khider – BISKRA
Faculté des Sciences Exactes, des Sciences de la Nature et de la Vie
Département d'informatique

N° d'ordre : RTIC22/M2/2019

Mémoire

Présenté pour obtenir le diplôme de master académique en

Informatique

Parcours : **Réseau et technologies de l'information et de la communication (RTIC)**

Gestion dynamique du spectre pour l'Internet des objets (IoT)

Par :

DJEFFAL LEILA

Soutenu le 11juillet 2019, devant le jury composé de :

Mr.BITAM Salim	**PROF**	**Président**
Mme. ZOUIOUCHE Amina	**MAB**	**Rapporteur**
Mr. AYAD Soheyb	**MCA**	**Examinateur**

~*Remerciements* ~

***A**louange appartient à ﷲje le loue et je le remercie pour m'avoir donné la force, la volonté et le Courage pour terminer ce modeste travail ;*

*Jetiens à remercier et à exprimer ma profonde gratitude à mon encadreur **M^me^ ZOUIOUCHE Amina** pour m'avoir fait confiance et accepter de m'encadrer au long de ce travail, poursa disponibilité toujours en j'offrant ses conseils, pour son écoute et ses encouragements qu'il m'afflués. Je remercie également les membres du jury qui ontaccepté de juger mon travail.*

Moninfinie reconnaissance s'adresse à ma familles qui ont su m'apporter, sans relâche leur soutien durant toutes ces longue années d'études.

Enfin jeremercie tous ceux qui ont contribués de près ou de loinà ce que ce modeste travail puisse voir le jour.

Leila. D

~*Dédicace* ~

A mes chers parents, pour tous leurs sacrifices, leur amour, leur tendresse,

Leur soutien et leurs prières tout au long de mes études.

A mes chères sœurs pour leurs encouragements permanents, et leur soutien moral.

A mon cher frère pour leur appui et leur encouragement.

A ma petite princesse « ***RANIM*** » la joie de ma vie

A mes chères amies et mes collègues.

A tous mes amis avec qui je partage des moments de ma vie au fil du temps.

A toute ma famille pour leur soutien tout au long de mon parcours universitaire.

Que ce travail soit l'accomplissement de vos vœux tant allégués, et le fuit de votre soutien infaillible,

Nous dédions ce modeste travail.

Merci d'être toujours là pour nos.

Leila. D

Résumé

L'internet des objets (IoT) en tant qu'une évolution de l'internet actuel permet une amélioration considérable de notre mode de vie et la façon dont les objets intelligents dans notre entourage interagissent entre eux et avec leurs utilisateurs.

IoT est un réseau sans fil à courte portée de périphériques interconnectés, tels que WiFi et Zigbee. Le WiFi et Zigbee se distinguent comme technologies de communication préférées pour les maisons intelligentes.

On sait que la rareté du spectre constitue le principal obstacle pour l'augmentation de la capacité des réseaux sans fil. Le partage du spectre est une solution à ce problème. La bande ISM sans licence est de plus en plus utilisée par les utilisateurs et les périphériques WLAN et WPAN.

Le partage du spectre au sein des périphériques d'un même réseau ne pose pas de problème. Mais la coexistence de WLAN et de WPAN (WiFi et Zigbee) est un problème difficile. Le partage du spectre entre ces réseaux améliorera certainement l'utilisation du spectre. WiFi et Zigbee utilisent une bande ISM de 2,4 GHz. WiseBee est un algorithme de gestion de spectre, qui permet une coexistence de Zigbee et WiFi en minimisant les interférences. Il utilise un seul récepteur d'antenne sans modifier les conceptions WiFi et Zigbee.

Mots clés

Gestion de spectre, WiFi, Zigbee, interférence, Coexistence, IoT, WiseBee.

Abstract

The internet of things (IoT) as an evolution of the current internet allows a considerable improvement of our way of life and the way in which smart objects in our environment interact with each other and with their users.

IoT is a short-range wireless network of interconnected devices, such as Wi-Fi and Zigbee. WiFi and Zigbee stand out as the preferred communication technologies for smart homes.

We know that spectrum scarcity is the biggest obstacle to increasing the capacity of wireless networks. Spectrum sharing is a solution to this problem. The unlicensed ISM band is being used more and more by WLAN and WPAN users and devices.

Spectrum sharing within devices on the same network is not a problem. But the coexistence of WLAN and WPAN (WiFi and Zigbee) is a difficult problem. Spectrum sharing between these networks will certainly improve the use of spectrum. Wifi and Zigbee use a 2.4 GHz ISM band. WiseBee is a spectrum management algorithm, which allows coexistence of Zigbee and WiFi by minimizing interference. It uses a single antenna receiver without modifying WiFi and ZigBee designs.

Keywords

Spectrum management, WiFi, Zigbee, Interference, Coexistence, IoT, WiseBee

Table de matières

.

Liste des abréviations

3GPP :	Third Generation Partnership Project
BSS :	Basic Service Set
CSMA/CA :	Carrier Sens Multiple Access/Collision Avoidance
DCF :	Distributed Coordination Function
DIFS :	DCF Inter-Frame Spacing)
DS :	Distribution System
DSSS :	Direct Sequence Spread Spectrum
ED :	End Divice
EIFS :	Extended Inter-Frame Spacing
eMTC :	Enhanced Machine Type Communication
ESS :	Extended Service Set
FFD :	Full Function Device
FHSS :	Frequency Hopping Spread Spectrum
GW :	GateWaye
IEEE :	Institute of Electrical and Electronics Engineers
IFS :	Inter-Frame Space
IoT :	Internet of Things
IP :	Internet Protocole
ISM :	Industrial Scientific Medical
LLC :	Logical Link Control
LPWAN :	Lower-Power Wide Area Networks
LTE :	Long Term Evolution
MAC :	Media Access Control
MmWave :	Onde Millimétrique
NAV :	Network Allocation Vector
NB-IoT :	Narrow-Band IoT
OFDM :	Orthogonal Frequency Division Multiplexing
PA :	Acess Point
PCF :	Point Coordination Function
PIFS :	PCF Inter-Frame Spacing
RC :	Radio Cognitive
RF :	Radio Frequency
RFID :	Radio Frequency Identification
SAP :	Service Access Point
SIFS :	Short Inter-Frame Spacing
TVWS :	TV White Space
UP :	Utilisateur Primaire
US :	Utilisateur Secondaire
WiFi :	Wireless Fidelity
WSD :	White Space Devices
ZC :	Zigbee Coordinator
ZDO :	Zigbee Divice Object
ZED :	Zigbee End-Device

Liste des figures

Liste des tableaux

Introduction générale

L'internet des objets (IoT) en tant qu'une évolution de l'internet actuel permet une amélioration considérable de notre mode de vie et la façon dont les objets intelligents dans notre entourage interagissent entre eux et avec leurs utilisateurs.

IoT est un réseau sans fil à courte portée de périphériques interconnectés, tels que WiFi et Zigbee. Le WiFi et Zigbee se distinguent comme technologies de communication préférées pour les maisons intelligentes.

Le WiFi est devenu très populaire, mais son application est limitée en raison de sa consommation d'énergie élevée et de l'absence de capacités de réseau maillé standard pour les appareils à faible consommation. Pour ces raisons, de nombreux fabricants ont choisi Zigbee pour développer des dispositifs de domotique sans fil.

Et avec la diversité de l'utilisation de réseaux sans fil dans la même bande 2.4GHz ISM (Industrial-Scientific-Medical). Cette diversité pourrait poser des problèmes de coexistence entre ces réseaux, un défi qui limite le déploiement à grande échelle de l'Internet des objets.

Par exemple, dans une maison intelligente, les appareils WiFi fournissent une connectivité Internet sans fil pour la navigation sur le Web et la lecture en continu de vidéos, tandis que les appareils Zigbee permettent une détection et un actionnement écoénergétiques pour la domotique. Il a été démontré que le trafic généré par un périphérique WiFi peut perturber gravement la communication périphérique Zigbee.

Dans ce projet, nous présentons la conception du système qui est basé sur l'algorithme WiseBee qui permet de gérer l'interférence entre le WiFi et le Zigbee. Où WiseBee est un nœud Zigbee dont la puissance d'émission est de 5 à 20 dB plus forte que le signal Zigbee en zone à risque d'interférence entre le WiFi et le Zigbee. Son rôle est d'écouter la communication dans le canal et de détecter une éventuelle interférence (collision) entre le signal Zigbee et le signal WiFi. Lorsque le WiseBee détecte une collision, il récupère l'ensemble des paquets transmis. Il annule ensuite les informations du WiFi et extrait la trame Zigbee et déterminer le meilleur canal adapté à la transmission.

Notre objectif est d'éviter l'interférence entre le WiFi et le Zigbee pour gérer le spectre de fréquence, afin d'avoir l'utilisation la plus efficace de ce dernier.

Notre mémoire se compose se cinq chapitres: dans le premier chapitre, nous définissions l'internet des objets et présentons une vue générale sur l'IoT avec leur caractéristiques, défis et domaines d'application.

Dans le deuxième chapitre, nous présentons la gestion du spectre et son intérêt ainsi que les techniques les plus utilisées dans le domaine de l'IoT pour la gestion du spectre.

Dans le troisième chapitre, nous présentons deux technologies WiFi et Zigbee, et Nous présentons la coexistence entre elles.

Le quatrième chapitre, représentera la conception de notre système qui sera basée sur l'algorithme de gestion de spectre WiseBee pour la coexistence des technologies Zigbee et Wifi.

Dans le cinquième chapitre, nous allons essayer d'implémenter l'algorithme WiseBee en utilisant MATLAB et l'intégrer dans notre système de simulation, analyser les résultats obtenus avec et sans l'algorithme pour pouvoir étudier son applicabilité dans le domaine de l'IoT.

Nous terminerons notre mémoire par une conclusion générale représentant une synthèse du travail.

Chapitre I
Internet des Objets
IoT

I.1 Introduction

Internet connait aujourd'hui une extension inédite avec le développement des objets connectés. Jusqu'alors, internet se concevait comme la capacité des personnes de communiquer à tout moment et en tout lieu; avec les objets connectés, le monde physique peut désormais communiquer, que ce soit pour des relations de personnes à personnes, de personnes à objets ou d'objets à objets. Partant, les importantes potentialités offertes par ce qu'il a été convenu d'appeler « l'internet des objets » ou « Internet of Things (IoT) » en anglais.

Dans ce chapitre, nous allons présenter une vue générale sur l'internet des objets avec leur caractéristiques, défis et domaines d'application.

I.2 Classification des objets

Nous commençons par la figure I-1 qui explique la mise en service des IoT, qui ne sont ni plus ni moins que des équipements connectés à un réseau de télécommunications.

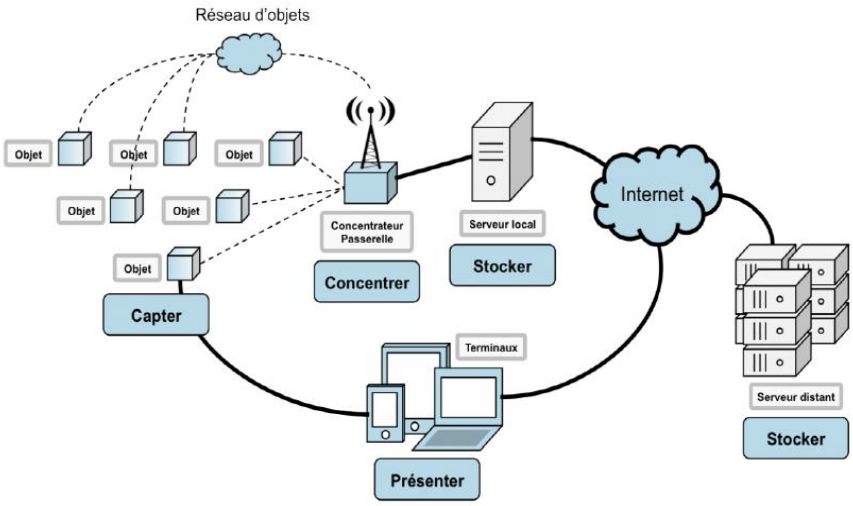


Figure I-1 : Mode d'opération des IoT[1].

Les objets sont des dispositifs matériels connectés à Internet et entre eux. Ils détectent et recueillent plus de données, deviennent sensibles au contexte et fournissent des informations plus concrètes pour aider les personnes et les machines. Il ya plusieurs type d'objet:

- ✓ **Electroniques:** comme les véhicules connectés en 4G pour optimiser lesperformances.
- ✓ **Electriques :** tout ce qui est de la domotique, allumage à distance etc...
- ✓ **Non électriques :** vêtements, animaux …
- ✓ **Capteurs environnementaux.**

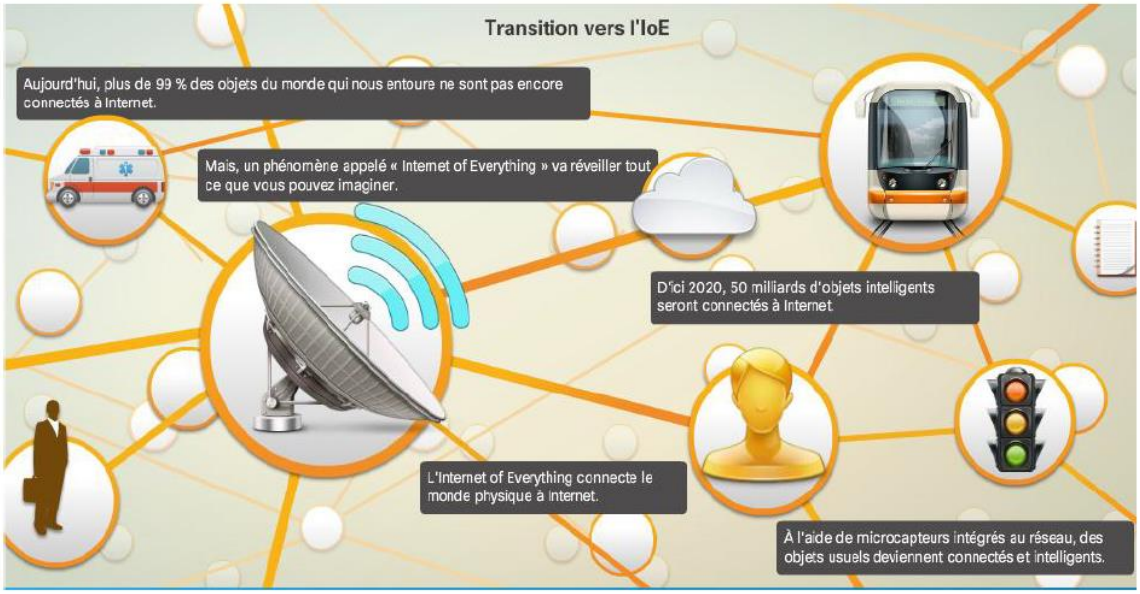


Figure I.2 : Application et systèmes connectés[1].

I.3 Définition de l'internet des objets (IoT)

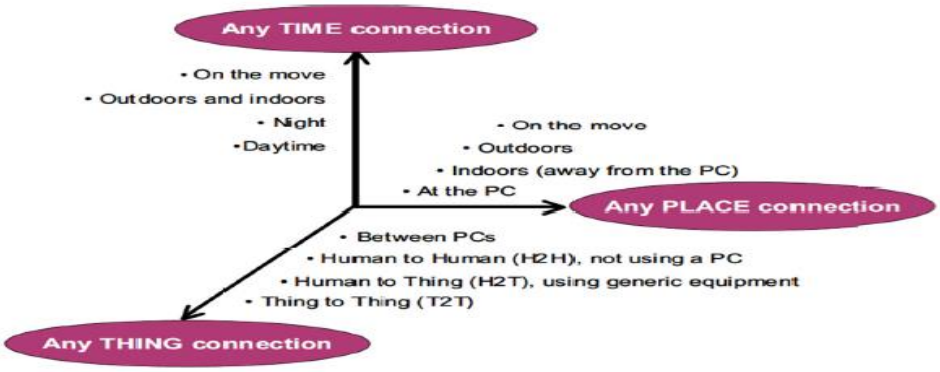
Il existe plusieurs définitions sur le concept de l'IoT.

- L'Internet des objets (IoT) est «un réseau qui relie et combine les objets avec l'Internet, en suivant les protocoles qui assurent leurs communication et échange d'informations à travers une variété de dispositifs»[2].

- L'IoT peut se définir aussi comme étant « un réseau de réseaux qui permet, via des systèmes d'identification électroniques normalisés et unifiés, et des dispositifs mobiles sans fil, d'identifier directement et sans ambiguïté des entités numériques et des objets physiques et ainsi, de pouvoir récupérer, stocker, transférer et traiter les données sans discontinuité entre les mondes physiques et virtuels »[2,3,7].

- La technologie IoT est considérée comme l'émergence de l'Internet du futur, certains la définissent comme des «objets ayant des identités et des personnalités virtuelles, opérant dans des espaces intelligents et utilisant des interfaces intelligentes pour se connecter et communiquer au sein de contextes d'usages variés» [30].

Ces définitions montrent les deux aspects de l'IoT: temporel et spatial qui permettent aux personnes de se connecter de n'importe où à n'importe quel moment à travers des objets connectés (Smartphone, tablettes, capteurs, caméras de vidéosurveillance, etc…). L'IoT doit être pensé pour un usage facile et une manipulation sécurisée pour éviter des menaces et risques potentiels, tout en masquant la complexité technologique sous-jacente.



FigureI.3 : Une nouvelle dimension pour IoT[4].

Alors les objets connectés se connectent eux-mêmes à l'internet. Les objets possèdent des puces électroniques qui leur permettent de se connecter les uns aux autres. Ils créent de la donnée et ils réagissent en fonction des paramètres que les utilisateurs ont mis en place.

I.4 Architecture des objets connectés

Les objets communiquent vers des Gateway, plusieurs Gateway peuvent capter les messages émis par les objets. Chaque Gateway remonte un message enrichi vers un Cloud opérateur qui gèrent les objets, le stockage des messages et communication avec les application métiers. Le Cloud opérateur pousse ensuite les messages bruts vers l'application métier : callback HTTP/S sous la forme d'une requête de type PUSH ou GET. Cette interface Cloud application métier est spécifique à chaque opérateur, chaque technologie.

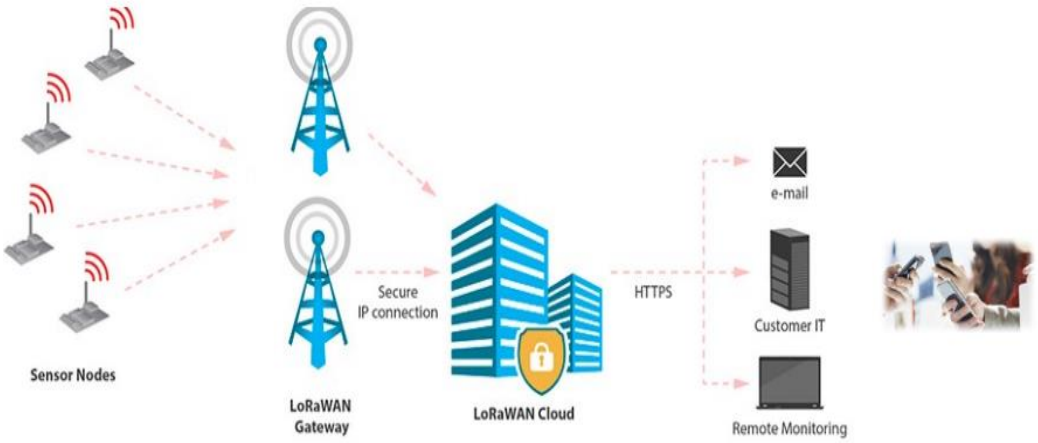


Figure I.4: Architecture des objets connectés[42].

I.5 Les Eléments IoT

Pour comprendre la structure de l'IoT, nous comprenons mieux la signification et les fonctions réelles de l'IoT. Nous montrons à la FigureI.5 les six éléments essentiels nécessaires pour fournir les fonctionnalités de l'IoT.

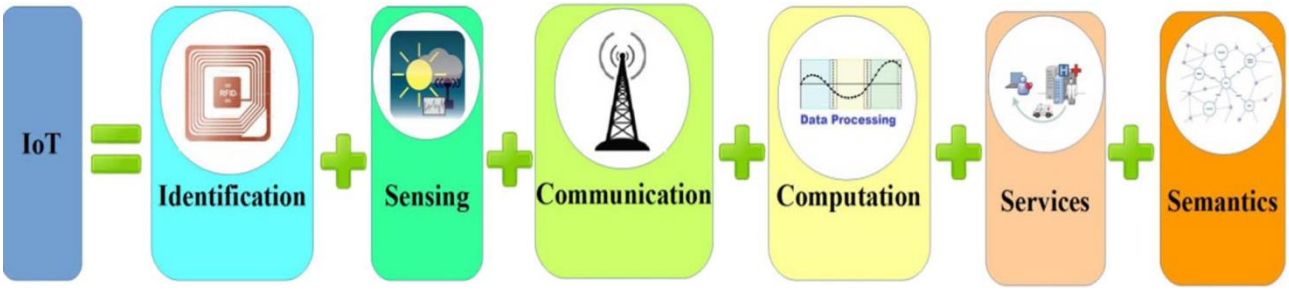


Figure I.5: Les éléments IoT.[5]

I.5.1 Identification : pour faire partie de l'IoT, les objets doivent pouvoir être désignés et avoir une adresse, tout comme les ordinateurs peuvent être localisés et identifiés grâce à leur adresse IP (protocole internet). En d'autres termes, les dispositifs intelligents ne sont d'aucune utilité s'ils ne peuvent être directement accessibles [31]. De nos jours, il existe une multitude d'identifiants pour les produits IoT, par exemple les identificateurs de ressources uniformes (URI), les codes produits électroniques (EPC), des codes universels et des adresses IP relevant du tout dernier protocole en vigueur (IPv6).[5]

I.5.2 Détection (Sensing): les capteurs permettent aux objets intelligents d'obtenir des données et donc d'interagir avec le monde physique. Les smartphones d'aujourd'hui en contiennent d'ailleurs une multitude, notamment, des détecteurs de proximité, des capteurs de lumière, des baromètres, des magnétomètres, des détecteurs de position, de vitesse et de courant, des accéléromètres, des gyroscopes, des thermomètres, des podomètres, des cardiofréquencemètres, des capteurs d'empreintes digitales et même des détecteurs de rayonnement. Les chercheurs tentent même de mettre au point des détecteurs de goûts et d'odeurs qui puissent un jour rivaliser avec le goût et l'odorat de l'utilisateur.[8]

I.5.3 Communication: il faut que les données récoltées par les capteurs soient transmises à un dispositif susceptible de les analyser puis d'y réagir. Les températures relevées par des thermostats intelligents doivent être envoyées aux éléments du réseau qui sont en mesure de répondre en conséquence (monter le chauffage ou enclencher la climatisation, etc…). Il existe une diversité de technologies filaires ou sans fil pouvant assurer ces communications. Par exemple, l'IoT reposait à ses débuts sur l'utilisation d'étiquettes RFID (radio-étiquettes) pour le suivi de marchandises à l'échelle nationale ou mondiale.

Il existe d'autres technologies d'étiquetage, notamment les codes QR (*Quick Response*) et le Bluetooth *LowEnergy*, ainsi que d'autres technologies de communication, comme la communication en champ proche (NFC pour *Near-Field Communication*), le wifi, Bluetooth ou Zigbee, ainsi que des technologies radio à bande étroite (reposant sur des services dédiés ou des systèmes de téléphonie mobile).

I.5.4 Informatisation: une fois les données récoltées et communiquées, elles doivent être informatisées, ce qui peut se faire de diverses façons. Certains produits IoT seront en mesure de traiter les données grâce à des microcontrôleurs. Il est fréquent qu'ils puissent aussi réagir aux informations qu'ils reçoivent grâce à des actionneurs. C'est ainsi qu'en l'absence de la famille, partie en vacances, des détecteurs de fumée intelligents peuvent au besoin directement appeler les pompiers. D'autres dispositifs vont toutefois envoyer leurs données à des smartphones ou à des ordinateurs situés à proximité. Dans d'autres configurations encore, il se pourrait que des réseaux informatiques locaux soient en mesure de traiter les données eux-mêmes ou qu'ils fassent office de passerelles vers des services d'informatique en nuage (*cloud computing*)[8].

I.5.5 Services: une fois les données arrivées à destination, les services entrent en jeu. Une solution domotique intelligente réglera la température, le flux d'air ou l'éclairage dans une habitation. Un système logistique intelligent saura à quel moment il doit commander de nouveaux composants pour une chaîne de montage ou ordonner l'expédition d'un conteneur qui vient juste d'être rempli. Un réseau électrique intelligent analysera les données émises par ses composants et optimisera ensuite la production d'énergie ou l'utilisation de celle-ci en conséquence. En définitive, la seule limite aux possibilités de services IoT est l'imagination de l'être humain (ou des machines).

I.5.6 Sémantique: la sémantique dans l'IoT qui «fournit un modèle commun permettant aux données d'être partagées - et réutilisées - entre plusieurs applications, entreprises et groupes d'utilisateurs ». Le web sémantique devrait pouvoir intégrer et fusionner les données provenant de nombreuses sources hétérogènes pour que les êtres humains ou les machines puissent trier les données disponibles de façon plus intuitive. La sémantique devient donc extrêmement utile dans l'environnement IoT. Un expert affirme même qu'elle est le « cerveau de l'IoT »[5].

.I.6 Technologies fondatrices de l'IoT

L'Internet des Objets (IoT) permet l'interconnexion des différents objets intelligents via l'Internet. Ainsi, pour son fonctionnement, plusieurs systèmes technologiques sont nécessaires. Citons quelques exemples de ces technologies.

« L'IoT désigne diverses solutions techniques (RFID, TCP/IP, technologies mobiles, etc…) qui permettent d'identifier des objets, de capter, stocker, traiter, et transférer des données dans les environnements physiques, mais aussi entre des contextes physiques et des univers virtuels»[2].

En effet, bien qu'il existe plusieurs technologies utilisées dans le fonctionnement de l'IoT. Ces technologies sont:

I.6.1 Radio Frequency Identification (RFID): Le terme RFID [3] englobe toutes les technologies qui utilisent les ondes radio pour identifier automatiquement des objets ou des personnes. C'est une technologie qui permet de mémoriser et de récupérer des informations à distance grâce à une étiquette qui émet des ondes radio[9]. Il s'agit d'une méthode utilisée pour transférer les données des étiquettes à des objets, ou pour identifier les objets à distance. L'étiquette contient des informations stockées électroniquement pouvant être lues à distance [10].

I.6.2 Wireless Sensor Network (WSN): C'est un ensemble de nœuds qui communiquent sans fil et qui sont organisés en un réseau coopératif. Chaque nœud possède une capacité de traitement et peut contenir différents types de mémoires, un émetteur-récepteur RF et une source d'alimentation, comme il peut aussi tenir compte des divers capteurs et des actionneurs[9]. Comme son nom l'indique, le WSN constitue alors un réseau de capteurs sans fil qui peut être une technologie nécessaire au fonctionnement de l'IoT[2].

I.6.3 Machine to Machine (M2M): C'est «l'association des technologies de l'information et de la communication avec des objets intelligents dans le but de donner à ces derniers les moyens d'interagir sans intervention humaine avec le système d'information d'une organisation ou d'une entreprise »[11].

I.6.4 Schémas d'adressage: La capacité d'identifier de manière unique les «choses» est essentielle au succès de l'internet des objets. Cela nous permettra non seulement d'identifier de manière unique des milliards d'appareils, mais également de contrôler des appareils distants via Internet. Les quelques caractéristiques les plus critiques de la création d'une adresse unique sont les suivantes: unicité, fiabilité, persistance et évolutivité. Chaque élément déjà connecté et ceux qui vont l'être doivent être identifiés par leur identification, emplacement et fonctionnalités uniques. L'IPv4 actuel peut prendre en charge dans une certaine mesure un groupe de capteurs en cohabitation pouvant être identifiés géographiquement, mais pas individuellement[6].

Les attributs de mobilité Internet dans l'IPv6 peuvent résoudre certains problèmes d'identification du périphérique; Cependant, la nature hétérogène des nœuds sans fil, les types de données variables, les opérations simultanées et la confluence des données des périphériques aggravent encore le problème. Le réseau persistant fonctionnant de manière à canaliser le trafic de données de manière omniprésente et implacable est un autre aspect de l'IoT. Bien que TCP/IP gère ce mécanisme en acheminant de manière plus fiable et efficace, de la source à la destination, l'IoT se

heurte à un goulot d'étranglement au niveau de l'interface entre la passerelle et les capteurs sans fil.

IPv6 offre également une très bonne option pour accéder aux ressources de manière unique et à distance. Un autre développement critique dans le domaine des adresses est le développement d'un IPv6 léger qui permettra d'adresser les appareils ménagers de manière unique. L'ensemble du réseau constitue désormais un réseau de connectivité allant des utilisateurs (de haut niveau) aux capteurs (de bas niveau), adressable (via URN (Uniform Resource Name), accessible (via URL) et contrôlable (via URC).

I.6.5 Stockage et analyse des données: l'un des résultats les plus importants de ce domaine émergent est la création d'une quantité de données sans précédent. Le stockage, la propriété et l'expiration des données deviennent des problèmes critiques. Internet consomme jusqu'à 5% de l'énergie totale générée aujourd'hui et, avec ce type de demandes, il va certainement augmenter encore plus. Par conséquent, les centres de données qui fonctionnent à partir de l'énergie récupérée et qui sont centralisés assureront efficacité énergétique et fiabilité. Les données doivent être stockées et utilisées intelligemment pour une surveillance et une activation intelligentes. Il est important de développer des algorithmes d'intelligence artificielle pouvant être centralisés ou distribués en fonction des besoins.

I.6.6 Visualisation: la visualisation est essentielle pour une application IoT, car elle permet une interaction de l'utilisateur avec l'environnement. Avec les progrès récents des technologies d'écran tactile, l'utilisation de tablettes et de téléphones intelligents est devenue très intuitive. Pour qu'un profane profite pleinement de la révolution de l'IoT, il faut créer une visualisation attrayante et facile à comprendre. Lorsque nous passons d'écrans 2D à 3D, davantage d'informations peuvent être fournies à l'utilisateur de manière significative pour les consommateurs. [6]

I.7 Domaines d'application de l'IoT

Nous constatons que le concept de l'Internet des Objets (IoT) est en pleine explosion vu que nous avons de plus en plus besoin dans la vie quotidienne d'objets intelligents capables de rendre l'atteinte de nos objectifs plus facile. Ainsi, les domaines d'applications de l'IoT peuvent être variés.

Plusieurs domaines d'application sont touchés par l'IoT :

1. Le domaine personnel ;
2. Le domaine du transport;
3. L'environnement ;
4. L'infrastructure et les services publics.

Comme le schéma ci-dessous le montre, on trouve alors l'IoT dans notre vie personnelle quotidienne et également dans les services publics offerts par le gouvernement.

Figure I.6: Les domaines d'Internet des Objets[11]

Nous pouvons affirmer que l'Internet peut être connecté à n'importe quel objet. Ainsi, les domaines d'applications de l'IoT sont multiples. On cite, à titre d'exemples, l'industrie, la santé, l'éducation et la recherche. Cependant, il sera possible dans le futur de trouver le concept de l'IoT n'importe où, n'importe quand et à la disposition de tout le monde.

L'IoT consiste en un monde de données (énormes), qui, si elles sont exploitées correctement, contribueront à répondre aux problèmes d'aujourd'hui, notamment dans les domaines suivants: aérospatial, aviation, automobile, télécommunications, construction, médical, autonomie des personnes handicapées, pharmaceutiques, logistiques, gestion des chaînes d'approvisionnements, fabrication et gestion du cycle de vie des produits, sécurité, sûreté, surveillance de l'environnement, traçabilité alimentaire, agriculture et élevage.[2]

❖ **La domotique (home automation)** : la domotique est l'ensemble des techniques permettant de centraliser le contrôle des différents systèmes d'une habitation. Le principe de la domotique est de faire en sorte qu'une maison devienne intelligente, indépendante et qu'elle réfléchisse par elle-même. Tous ces principes sont possibles grâce à l'IoT qui permet de connecter les dispositifs de la maison à un réseau et de les piloter à distance. La domotique a pour but d'améliorer le confort quotidien en automatisant ou en gérant à distance les tâches récurrentes.

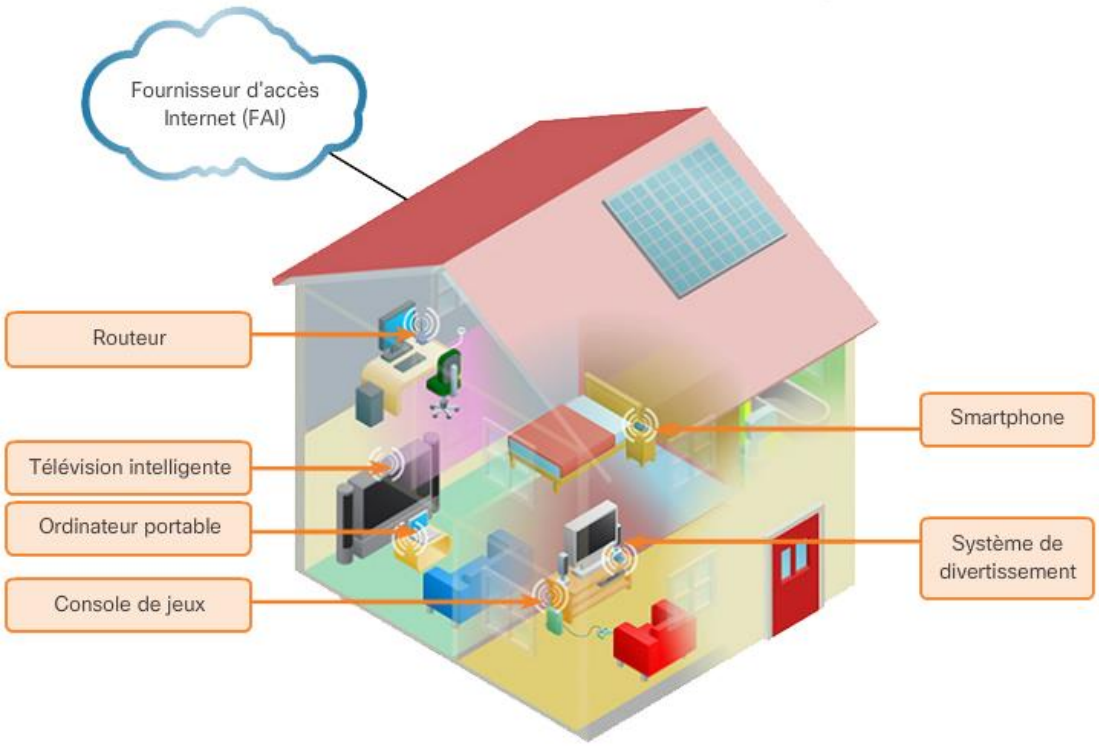


Figure I.7 Réseau local sans fil domestique [3].

Il existe aussi des villes intelligente (Smart Caties) est utiliser pour désigner l'écosystème cyber physique émergeant par le déploiement d'une infrastructure de communication avancée et de nouveaux services sur des scénarios à l'échelle de la ville. Grace à des services avancés, il est en effet possible d'optimiser l'utilisation des infrastructures physiques de la ville (par exemple, les réseaux routiers, le réseau électrique, etc…) et la qualité de vie des citoyens [9].

❖ **La Santé (Health):** les patients porteront des capteurs médicaux qui surveillent les constantes biologiques, telles que la température corporelle, la pression artérielle et l'activité respiratoire.

D'autres capteurs portables (accéléromètres, gyroscopes, etc.), ou fixes, seront utilisées pour recueillir les données permettant de surveiller les activités des patients dans leur milieu de vie. Ces données seront agrégées localement et transmises aux centres médicaux distants, qui pourront effectuer une surveillance à distance et seront capables de prendre des mesures rapides en cas de besoin [11].

❖ **Véhicule :** Le marché des transports a déjà anticipé l'arrivée des objets connectés. Parmi les enjeux les plus fréquents que ce domaine fait naitre on retrouve la réduction des accidents et des embouteillages, le partage de voitures, le développement des offres de VTC et de TAX ou encore la gestion des flots automobile [9].

❖ **La Sécurité :** Pour le cabinet en stratégie, ces entreprises vont rapidement se positionner comme des alliés des personnes qui résident dans leur domicile. En fournissant des données relatives à la consommation d'énergie aux foyers, ces groupes vont apparaitre comme des arguments contre le facteur EDF pour les fournisseurs d'énergie la précision sera difficile à tenir car ils seront probablement contraints d'accompagner leurs clients dans une baisse de leurs facteurs énergétique.

❖ **L'Industrie :** Le déploiement de L'IoT dans l'industrie sera certainement un grand support pour le développement de l'économie et le secteur des services, puisque L'IoT permettra d'assurer un suivi total des produits, de la chaine de production, jusqu'à la chaine logistique et de distribution en supervisant les conditions d'approvisionnements. Cette traçabilité de bout en bout facilitera la lutte contre la contrefaçon, la fraude et les crimes économiques transfrontaliers.

Certains éditeurs tels que SAP et CISCO montrant d'ores et déjà comment certaines zones industrielles comme le port d'Hambourg ont pu être équipés en puces et autres objets connectés. L'internet couvre un énorme nombre d'industries et utilise des cas qui s'étendent d'un seul dispositif contraint aux déploiements croisés de technologies intégrées de systèmes Cloud connectés en temps réel [9].

❖ **L'agriculture (agriculture)**: l'usage des objets connectés se démocratise dans l'agriculture. En effet, de nombreuses améliorations en découlent concernant la gestion des engins agricoles, la maîtrise de l'irrigation ou la gestion optimisée des intrants, la surveillance de la croissance des plantes ou encore la prévention des risques météo. De quoi renouveler en profondeur les pratiques de cette activité ancestrale grâce à l'analyse des données collectées [11].

❖ **Les chaussures de sport** fournissent le temps, la distance et la performance de celui qui les portent, une comparaison peut alors s'effectuer entre athlètes indépendamment de leurs localisations. Les capteurs enregistrent des données pour les communiquer aux utilisateurs. Très récemment, les chaussures de sport équipées de puces embarquées indiquent l'implication d'un athlète et ses performances[1].

❖ **Les usines intelligentes**: la technologie de l'IoT permet aujourd'hui aux usines de maximiser l'efficacité opérationnelle, d'optimiser la production, et d'augmenter la sécurité des travailleurs.

❖ **Commerces**: pour les commerçants, l'IoT offre des opportunités illimitées pour augmenter l'efficacité de la chaîne d'approvisionnement, développer des nouveaux services et réorganiser l'expérience du consommateur.

I.8 Les enjeux pour le déploiement de l'internet des objets

❖ **Connectivité et réseaux**: Il s'agit de favoriser le développement de réseaux adaptés aux besoins de l'internet des objets, et leur large disponibilité.

Il existe des typologies et technologies de réseaux variées : WiFi, Bluetooth, réseaux de téléphonie mobile, RFID, radio FM, etc. WiFi, Bluetooth, SigFox, haut ou bas débit, longue ou courte portée, etc. Cette diversité de l'offre répond à des besoins et usages multiples : mobiles, objets connectés, besoins industriels, etc...[43]

❖ **Ressources rares**: Il s'agit de s'assurer que les ressources notamment hertziennes mobilisables par ces réseaux permettent de répondre au besoin. Différentes réponses peuvent exister entre des bandes de fréquences soumises à un régime d'autorisation qui garantissent l'exclusivité de l'utilisation et des bandes de fréquences libres. Ces différents régimes d'utilisation peuvent répondre à différents besoins, dépendant de l'application souhaitée.

❖ **Ouverture**: C'est un sujet qui peut se décomposer en deux thèmes: la fluidité et l'interopérabilité. La problématique fondamentale de l'Internet des objets est de savoir comment tous les objets fonctionnent ensemble et communiquent entre eux. Il en résulte des enjeux majeurs d'interopérabilité: comment faire en sorte que deux objets se comprennent et qu'ils parlent le même langage ?

Les problèmes d'interopérabilité soulèvent aussi des questions d'écosystème, notamment de maîtrise de la chaîne de valeur. En effet, celui qui maîtrise le langage commun occupe une position centrale dans la chaîne de valeur, ce qui peut avoir un fort impact. C'est un point d'attention pour l'ARCEP. Une partie de ces questions d'interopérabilité sont relativement proches des enjeux que traitent le régulateur des télécoms sur les communications électroniques, mais une grande partie le dépasse largement, notamment les enjeux relatifs aux données, aux services et aux applications qui en sont faits, par exemple dans les réseaux énergétiques.

❖ **Confiance:** L'enjeu de la confiance englobe deux sujets d'attention: les données personnelles et la sécurité des réseaux. D'une part, les données sont au cœur de l'Internet des objets. Lorsqu'il s'agit de données personnelles, elles doivent être traitées dans le respect des obligations applicables; ce point sera essentiel pour la confiance des utilisateurs. Ainsi, l'ARCEP travaille en collaboration avec la CNIL sur cette question.

D'autre part, la sécurité des réseaux est un enjeu systémique. La multiplication des objets connectés peut multiplier les possibilités d'attaque. Si les réseaux soient conçus à l'origine avec des dimensions de sécurités relativement importantes, il faut sécuriser la chaîne de valeur de bout en bout et les premiers points d'attention portent peut-être plutôt sur les couches logicielles et la bonne mise à jour des politiques de sécurité (ex. gestion des mots de passe).

❖ **Mutation**: Le développement des objets connectés impacte les modes d'organisation, les besoins en compétences et les modèles d'affaire. Organiser un dialogue régulier avec l'écosystème apparaît important pour mieux comprendre anticiper ces évolutions. Ces sujets constituent des points de réflexion, notamment avec la DGE [43].

I.9 Les avantages et les inconvénients de l'IoT

I.9.1 Les avantage

- Accès ubiquitaire à l'information pour un monde plus intelligent et un mode vie sophistiqué et confortable.
- Amélioration de la qualité de service et de la télésurveillance dans différents domaines d'applications, à savoir le domaine industriel, médical, etc.
- Améliorer la productivité et l'expérience-client : les objets connectes envoient des rapports `a leurs constructeurs indiquant les préférences et les habitudes des clients aidant davantage les entreprises à agir de manière proactive et adaptée qui satisfait la demande et les exigences de la clientèle.
- Le gain du temps est un autre avantage de l'IoT. Les déplacements inutiles sont dès lors remplaces par une simple navigation sur le web pour commander des produits, contrôler l'état des objets et/ou endroits connectés.
- Dans certaines applications, l'IoT nous permet même de rationaliser nos dépenses et faire des économies car on ne consomme qu'en cas de besoin, que ça soit pour les achats ou la consommation énergétique (nécessaire pour l'éclairage ou la climatisation) ou autre.
- Possibilité d'exploitation des ressources géantes de l'Internet pour le stockage et le traitement des données écoulées de l'IoT.

I.9.2 Les inconvénients

- **Les risques pour la sécurité de l'information** : La mise en œuvre de l'IoT au sein d'une entreprise comporte un obstacle de taille qu'il importe de surmonter : la sécurité. Une atteinte à la sécurité pourrait avoir d'importantes répercussions sur la réputation et la crédibilité de l'entreprise, et se traduire par une perte de temps et d'argent, en plus d'avoir des conséquences juridiques.

- **L'IoT et la confidentialité** : Qu'il soit lié à l'IoT ou non, tout cyber-incident augmente considérablement les risques de vol, de divulgation ou d'altération de l'information. Ainsi, l'information concernant votre entreprise, vos employés et vos clients pourrait être détruite, altérée, volée ou publiée, ou même « retenue en otage » jusqu'au versement d'une rançon.

- Les appareils connectés collectent de grandes quantités de données, ce qui représente un motif de préoccupation pour la confidentialité et l'intégrité des données de l'entreprise.

- Quand un appareil connecté contrôle des biens matériels et des opérations, comme un véhicule intelligent ou une pompe à insuline, la menace que fait planer un cyber-incident éventuel ne se limite pas à une brèche dans la sécurité de l'information. L'utilisation non autorisée ou la prise de contrôle à distance d'un objet connecté pourraient endommager les données et l'équipement de votre entreprise ou causer des dommages physiques à des personnes. Ces dommages pourraient s'avérer coûteux, si vous devez réparer les systèmes et équipements de votre entreprise et rétablir sa réputation. Le rôle que jouent de nombreux objets est bien plus important que l'information qu'ils emmagasinent. Pensez aux conséquences juridiques et financières que pourraient entraîner la défaillance ou le piratage d'un appareil connecté, par exemple [5].

I.10 Conclusion

Dans ce chapitre nous avons présenté principalement, le fonctionnement, les technologies de base, les applications de l'IoT. Nous avons aussi mis en évidence les contraintes liées au déploiement de l'IoT et les avantages et les inconvénients d'IoT

L'Internet des objets en tant qu'une évolution de l'Internet actuel permet une amélioration considérable de notre mode de vie et la façon dont les objets intelligents dans notre entourage interagissent entre eux et avec leurs utilisateurs. Le plus gros problème rencontré par la déployer d'IoT est la rareté le spectre.

Dans le prochain chapitre, nous allons présenter les différentes méthodes de la gestion du spectre dans certaines technologies.

Chapitre II

Gestion du Spectre

II.1 Introduction

Où que nous allions, la plupart d'entre nous prenons pour acquis des possibilités jadis inimaginables. Nous pouvons non seulement parler, envoyer des SMS, Email, naviguer en ligne et se connecter à des médias sociaux en déplacement, nous suivons également nos pas, cartographions nos itinéraires et visionnons des vidéos et des longs métrages. Pendant tout ce temps, nous empruntons un chemin dont nous connaissons sérieusement l'existence, car il est invisible pour nous: c'est ce qu'on appelle le spectre.

Dans ce chapitre, nous allons présenter quelques techniques d'IoT et comment gérer le spectre afin d'éviter les interférences et obtenir d'excellents services.

II.2 Spectre

Le spectre est un composant essentiel des réseaux sans fil. Il constitue les «ondes» qui sous-tendent les services de communication que nous utilisons quotidiennement. Tels que mobile, Wifi et télévision où l'onde radio est un champ électromagnétique variable (c'est donc une onde électromagnétique), souvent périodique, produit par une antenne. Une onde électromagnétique est composée d'un champ électrique et d'un champ magnétique qui se propagent tous deux à la même vitesse [12].

.II.2.1 Spectre électromagnétique

Le spectre électromagnétique représente l'ensemble des rayonnements de différentes énergies qui se propagent sous forme d'ondes à la fois électriques et magnétiques. Lorsqu'un champ magnétique est généré, un champ électrique correspondant l'est aussi et vice versa. Les deux champs, qui se déplacent comme une onde, sont perpendiculaires. Le terme « rayonnement » désigne toute forme d'énergie qui se déplace dans l'espace.

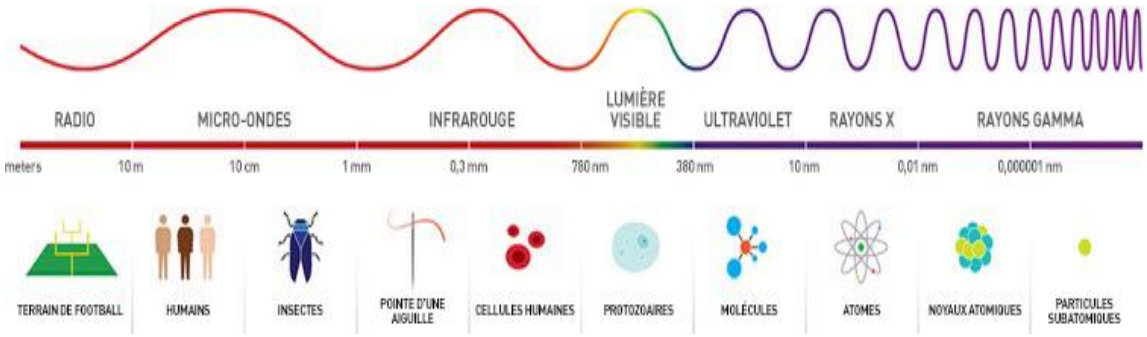


Figure II.1: Spectre électromagnétique [44].

Le rayonnement électromagnétique se déplace simultanément sous la forme d'ondes de différentes fréquences et de particules appelées « photons ». Les ondes radio ont une fréquence de seulement 10 000 hertz (1Hz = un cycle par seconde) et une

longueur d'à peine 1 000 mètres (m), tandis que les rayons gamma ont une très haute fréquence (1020 Hz) et une très courte longueur (10-12 m). La lumière visible constitue une forme de rayonnement électromagnétique de fréquence et de longueur intermédiaires. Plus la fréquence est élevée, plus grande sera la quantité d'énergie associée à chaque photon [44].

Des ondes radio qui transmettent de la musique et des conversations par téléphone mobile passent directement à travers votre corps. Les seules parties du spectre électromagnétique que nos sens peuvent détecter directement sont la chaleur radiante (l'infrarouge), la lumière visible et l'ultraviolet [44].

II.2.2 Spectre de fréquence

Le spectre de fréquence est la partie du spectre électromagnétique qui achemine les ondes radio. Il est subdivise en neuf bandes de fréquences, désignées par des nombres entiers consécutifs conformément au tableau ci-après :

Numéro de la bande	Symboles	Gamme de fréquence	Subdivision métrique correspondance
4	VLF	3 à 30 KHZ	ondes myriamétrique
5	LF	30 à 300 KHZ	ondes kilométrique
6	MF	300 à 3000 KHZ	ondes hectométrique
7	HF	3 à 30 MHZ	ondes décamétrique
8	VHF	30 à 300MHZ	ondes métrique
9	UHF	300 à 3000MHZ	ondes déciétrique
10	SHF	3 à 30 GHZ	ondes centimétrique
11	EHF	30 à 300 GHZ	ondes millimétrique
12	...	300 à 3000 GHZ	ondes décimillimétrique

Table II.1: Le spectre de fréquence [12,13].

II.2.3 Gestion d'un spectre

Les principales préoccupations de la gestion du spectre (promouvoir l'accès au spectre et son utilisation efficace, résoudre les demandes conflictuelles, gérer le changement, améliorer la coordination et éviter les interférences, favoriser la communication et la consultation et garantir le partage des données et des informations) nécessitent une vision plus large du développement des capacités.

La gestion d'un spectre signifié le processus qui détermine le mode et les conditions d'exploitation du spectre par certains systèmes. Ces conditions varient selon la couverture radioélectrique du système, qui dépend de :

- La situation de l'émetteur (dans un bâtiment, dans la rue, sur un point haut, en orbite. . .).
- La directivité de l'émission (émission omnidirectionnelle ou sectorielle) et de la puissance du signal émis.
- La puissance électrique de l'émetteur.

- Caractéristiques du système antennaire.
- Caractéristiques de propagation des bandes utilisées qui ne sont pas homogènes selon les gammes de fréquences: en vue directe, les bandes basses subissent moins sujettes aux réflexions sur l'ionosphère et aux atténuations atmosphériques.

II.2.4 Objectifs de la gestion du spectre

- L'objectif principal de la gestion du spectre consiste à obtenir un taux maximum de l'exploitation globale du spectre radio et ceci en autorisant l'accès aux utilisateurs efficaces autant que possible tout en garantissant que les interférences entre différents utilisateurs restent gérables.
- Garantir une plus grande facilité d'utilisation du spectre.
- Rationaliser l'usage du spectre, même dans un environnement où la fréquence n'est pas encore une ressource rare.
- Garantir la disponibilité des fréquences.
- Répondre au besoin de développement des télécommunications et des radiocommunications nationales.
- Répondre aux besoins de la sécurité et de la défense nationale.

La croissance continue de la demande de spectre, aussi bien pour les services existants que pour les nouveaux services radio, exerce des contraintes de plus en plus fortes sur cette ressource notamment en ce qui concerne l'équilibre entre l'offre et la demande; cette ressource doit être gérée d'une manière efficace afin que l'on puisse en retirer un maximum d'avantages sur les plans économiques et sociales. Plus le spectre radioélectrique est encombré, plus il est difficile à gérer, et plus l'outil nécessaire pour bien le gérer doit être performant.

Il faut donc des méthodes novatrices pour le gérer de manière dynamique afin qu'elle puisse être disponible pour les nouveaux services. Sa gestion permet également d'éviter les brouillages de signaux (interférences).

II.3 Radio Cognitive

II.3.1 Définition: La radio cognitive (RC) est une technologie émergente en matière d'accès sans fil, visant à améliorer considérablement l'utilisation du spectre radio en permettant d'y accéder de manière opportuniste [14]**.** Dans laquelle un émetteur/récepteur conçu pour utiliser les meilleurs canaux de communication dans son voisinage. Cette radio ayant la capacité de reconnaître son cadre d'utilisation et de détecter automatiquement les canaux qui sont disponibles et ceux qui ne le sont pas dans le spectre. L'utilisation des fréquences radio du spectre permet de minimiser les interférences entre les terminaux [15].

Le paradigme de la radio cognitive a été un moyen essentiel pour une utilisation plus efficace du spectre radioélectrique. La radio cognitive obtient une efficacité d'utilisation du spectre supérieure grâce à un accès opportuniste au spectre qui n'est pas utilisé par un service primaire sous licence à un endroit et à un moment

déterminés[16]. Les technologies basées sur la radio cognitive peuvent détecter et surveiller en temps réel le spectre radioélectrique environnant, apprendre de l'environnement et prendre des décisions intelligentes pour établir la communication en utilisant les meilleures ressources spectrales disponibles, avec un minimum d'interférences et une puissance rayonnée optimale.

Le principe de la RC, repris dans la norme IEEE 802.22 et IEE 802.16h[17] nécessite une gestion alternative du spectre qui est la suivante: un utilisateur dit secondaire pourra à tout moment accéder à des bandes de fréquence qu'il trouve libres, c'est-à-dire, non occupées par l'utilisateur dit primaire possédant une licence sur cette bande. L'utilisateur secondaire (US) devra les céder une fois le service terminé ou une fois qu'un utilisateur primaire (PU) aura montré des velléités de connexion.

II.3.2 Fonctions de la radio cognitive

Les principales fonctions de la radio cognitive sont les suivants:

II.3.2.1 Détection du spectre (Spectrum sensing): C'est la fonctionnalité de base, détection des portions du spectre vides par détection de signaux d'utilisateurs sous licence [17], elle consiste à :

- Détecter le spectre non utilisé ;
- Partager le spectre sans interférence avec d'autre utilisateur.

L'objectif de cette fonction est de détecter des interférences pour obtenir l'état du spectre (libre/occupé) par US.

II.3.2.2 Gestion du spectre (Spectrum management): Capturer la bande de fréquence disponible pour répondre aux besoins de communication des utilisateurs [29] avec des fonctions classées comme suit :

- **Analyse du spectre:** Analyser les résultats de la détection du spectre pour estimer la qualité du spectre (la disponibilité des espaces blancs du spectre, durée moyenne)[15]. Des algorithmes d'apprentissage de l'Intelligence Artificielle sont des techniques qui peuvent être employées par les utilisateurs de la RC pour l'analyse du spectre.

- **Décision sur le spectre:** Prise de la décision pour l'accès au spectre dépend des résultats de l'analyse du spectre. Partage des portions du spectre détecté avec d'autres utilisateurs ou coexistant [29] avec eux sur la même bande par des techniques comme d'optimisation stochastique. Dans un système RC coopératifs/non coopératifs, il existe deux utilisateurs (UP et US) qui peuvent être influé sur l'accès au spectre.

Dans un environnement multi utilisateur distribué, pour un accès non-coopératif au spectre, chaque utilisateur parvient à une décision optimale de façon indépendante en observant le comportement (historique/action) des autres utilisateurs du système. Par conséquent, un algorithme distribué est nécessaire pour un US pour prendre la décision sur l'accès au spectre de manière autonome[17].

II.3.2.3 Mobilité du spectre (Spectrum mobility): La mobilité des terminaux de la radio cognitive permettant à changer sa bande de fréquence, donc l'utilisation du spectre de manière dynamique [29].

- Recherche des meilleures bandes de fréquence disponible ;
- Auto-coexistence et synchronisation ;

Laissant la partie du spectre lorsque l'utilisateur sous licence d'héritage veut l'utiliser de façon isolée, sinon un utilisateur primaire peut partager la fréquence avec un utilisateur secondaire avec une certaine contrainte comme la durée.

II.3.3 Techniques d'accès dynamique au spectre

II.3.3.1 Les enchères: La théorie des enchères est basée sur des règles simples, qui permettent de faciliter la répartition dans les bandes de fréquence à tous les utilisateurs (UP et US) [18]. Il existe plusieurs formes d'enchères, notamment :

- Enchères anglaises : enchère publique au premier prix ascendante.
- Enchères hollandaises : enchère publique au premier prix descendante.
- Enchères scellée au premier prix.
- Enchères scellée au second prix : (Vickrey).

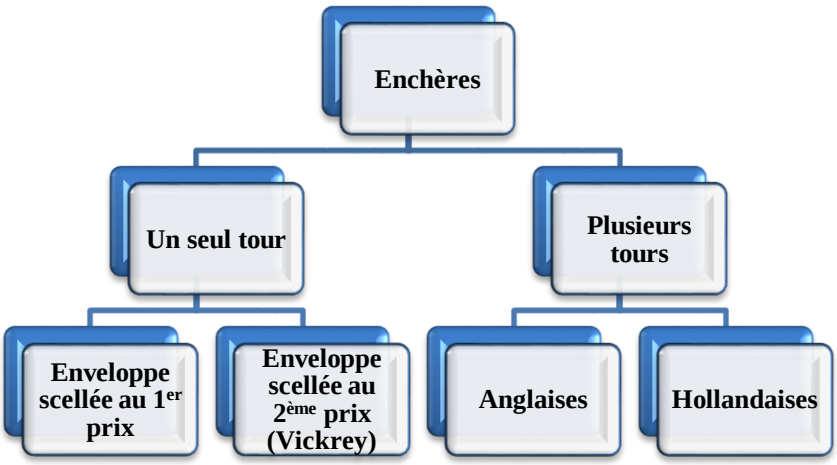


Figure II.2 : Organigramme représentant les types d'enchères[18].

Le but principal de l'utilisation des enchères dans les réseaux RC est de fournir une motivation aux USs pour maximiser leur utilisation du spectre et aux UPs afin de maximiser leur gain. Afin d'utiliser pleinement le spectre, l'allocation dynamique du spectre utilisant les enchères est devenue une approche prometteuse qui permet aux utilisateurs secondaires de louer des bandes inutilisées par les utilisateurs primaires[17].

II.3.3.2 La théorie des jeux: Les jeux sont généralement divisés en deux types: jeux compétitifs et jeux coopératifs [15].

- **Jeux compétitifs:** tous les joueurs sont préoccupés par tous les gains globaux et ils ne sont pas très inquiets de leur gain personnel.

- **Jeux coopératifs:** chaque utilisateur est principalement préoccupé par son gain personnel et donc toutes ses décisions sont prises de manière compétitive et égoïste. Dans la littérature existante, nous avons constaté que les concepts théoriques du jeu ont été largement utilisés pour des attributions de fréquences dans les réseaux RC, où lorsque les UPs et les USs participent à un jeu, ils ont un comportement rationnel pour choisir les stratégies qui maximisent leurs propres gains.

II.3.3.3 Les approche de Markov: Les approches de la théorie des jeux ne modélisent pas l'interaction entre lesUS et les UP pour l'accès au spectre. Cette modélisation peut être réalisée en utilisant efficacement les chaines de Markov [29]. Une chaine de Markov est une suite de variables aléatoires qui permet de modéliser l'évolution dynamique d'un système aléatoire. La propriété fondamentale des chaines de Markov est que son évolution future ne dépend du passé qu'au travers de sa valeur actuelle. Autrement, dans le cas de la RC, cette méthode ne se contente pas du résultat seulement comme les autres méthodes mais permet également de modéliser l'interaction entre les utilisateurs (UP et US) [15].

II.3.3.4 Les Systèmes Multi Agents: L'approche classique de l'intelligence artificielle (IA), modélise le comportement intelligent d'un seul agent. Le passage du comportement individuel au comportement social pour combler les limites de l'I.A. classique à résoudre des problèmes complexes. Pour cela, nécessité de distribuer l'intelligence sur plusieurs agents.

Un Système Multi-Agents (SMA) est un système distribué composé d'un ensemble d'entités réactifs ou cognitifs, qui interagissent les uns avec les autres, situé dans un environnement commun.

L'association des SMA avec la RC assure un futur remarquable pour la gestion optimale des fréquences. Dans le cas de l'utilisation des bandes sans licence, le terminal RC doit coordonner et coopérer pour un usage meilleur du spectre sans causer d'interférences[15].

On utilise algorithme de gestion du handover spectral pour un nœud radio cognitive mobile. Cet algorithme présente une approche décentralisée qui utilise les systèmes multi agents. Nous exploitons également des algorithmes de négociation et de coopération issus du domaine multi-agents afin d'assurer une répartition plus efficace du spectre. La gestion du handover dans un réseau radio cognitive en assurant une utilisation optimale du spectre.

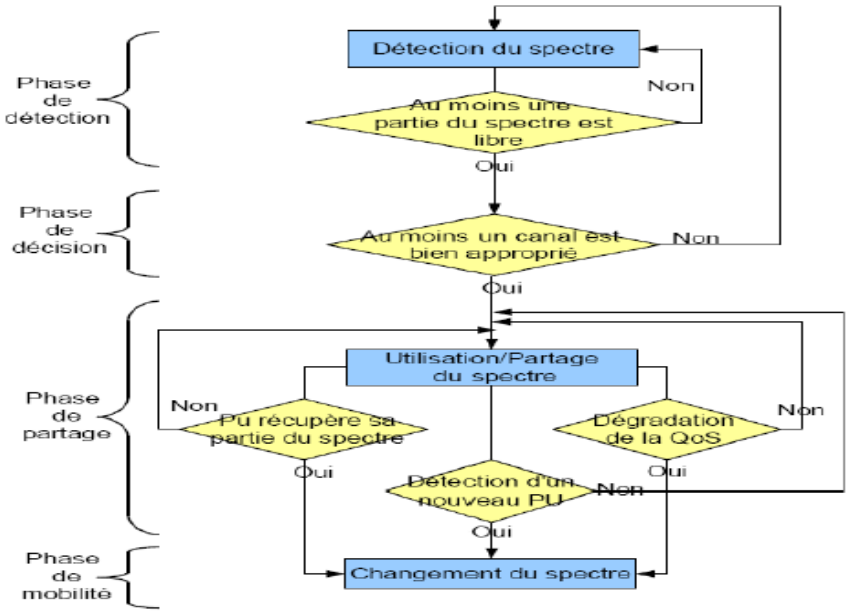


Figure II.3: Organigramme de fonctionnement d'un nœud radio cognitive[14].

II.3.4 Avantage et Inconvénients des Techniques d'Accès au Spectre

Technique	Avantages	Inconvénients
Théorie des Enchères	- Simplicité - Equitables et transparentes	- Parfois coûteuse
Théorie des jeux	- Lecture aisée des issues des stratégies - Modélise le comportement d'un agent face à des situations de choix	- Coût important - Ne permet pas de faire un choix rationnel
Modèles de Markov	- Modélisation des processus	- Ne prennent pas en compte les états caches - Ne peut pas prendre en charge un très grand nombre d'états
Systèmes Multi Agents	- Modularité - Rapidité - Fiabilité et flexibilité	- Coût élevé - Manque de support logiciel - Manque de méthodes

Tableau II.1: Avantage et Inconvénients des Techniques d'Accès au Spectre[17]

Plusieurs normes basées sur des techniques de radio cognitive ont été développées. Par exemple, IEEE 802.22b et IEEE 802.11af implémentent des techniques de radio cognitive permettant d'accéder de manière dynamique aux bandes VHF (Very High Frequency) et UHF (Ultra-High Frequency)[16].

La plupart des ressources du spectre sont généralement attribuées à la radiodiffusion TV numérique en tant que service autorisé principal. Les attributions de spectre de la bande TV qui ne sont pas utilisées à un endroit et à une heure donnée sont appelées espaces blancs TV (TVWS).

II.4 Espaces Blancs TV (TV White Space) TVWS

II.4.1 Définition TVWS: est première mise en œuvre et test d'approches d'accès dynamique au spectre étaient des TVWS. L'innovation était principal objectif politique lors de la mise au point de cette nouvelle méthode d'autorisation de l'accès aux parties inutilisées du précieux spectre de fréquences basses dans la bande 470 à 790 MHz. La mise en œuvre une approche dynamique à plusieurs niveaux permettant aux appareils TVWS exemptés de licence, qui répondent à une spécification technique minimale et sont autorisés ou contrôlés par une base de données, de tirer parti du spectre inutilisé. Cette approche répond à l'objectif de permettre à de nouveaux acteurs d'innover et à une utilisation partagée du spectre [19].

II.4.2 Gestion du spectre dans TVWS

Afin d'éviter tout brouillage préjudiciable aux services primaires et d'atteindre une qualité de service moyenne dans TVWS, les WSD (White Space Devices) doivent avoir une connaissance du statut d'occupation du spectre [20].

L'approche de la base de données de géo-localisation a déjà fait l'objet de discussions approfondies dans le contexte des principales évolutions réglementaires récentes. L'approche par base de données pose des défis pour protéger les utilisateurs autorisés de la DTT (Digital Terrestrial Television) et des acteurs non enregistrés de la production de programmes et des événements spéciaux PMSE (Programme Making and Special Events) dans les scénarios de villes urbaines, et pour détecter le PMSE sans licence coexistant à proximité [16].

Afin de réaliser la gestion dynamique du spectre sur TVWS, le banc d'essai TD-LTE activé par CR, avec capacité de détection du spectre et modification de la pile des protocoles. L'algorithme de détection du spectre utilisé dans le banc d'essai est d'abord présenté. En outre, la modification de protocole proposée pour le banc d'essai est présentée.

En tant que clé pour une utilisation efficace du spectre dans TVWS, le Cognitive eNodeB (CeNB) a été proposé pour exploiter la détection du spectre dans le système TD-LTE activé par la CR, ce qui présente deux avantages. Premièrement, il est possible de minimiser le temps occupé par le spectre et la surcharge de signalisation pour l'échange d'informations entre utilisateurs CR et CeNB. Deuxièmement, la consommation d'énergie pour la détection du spectre par les utilisateurs CR peut être économisée [20].

Cette méthode de détection des caractéristiques permet également de réduire le bruit et la durée d'échantillonnage, ce qui donne de bonnes performances dans les conditions de faible rapport signal / bruit (SNR « Signal-to-Noise Ratio »)[20].

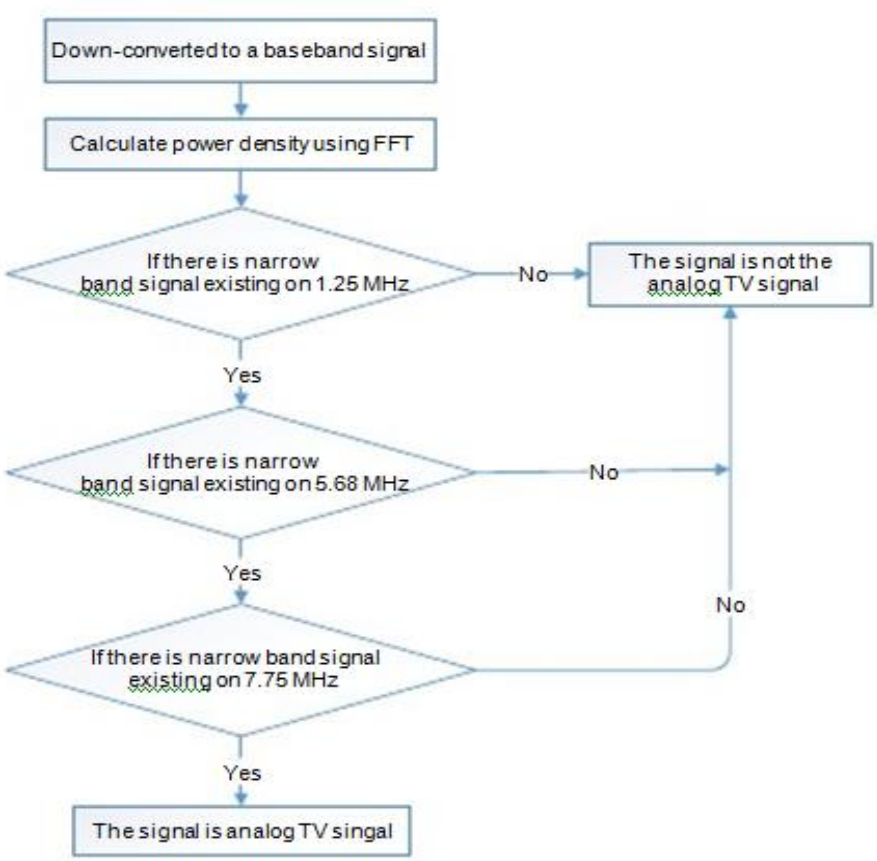


Figure II.4: Procédure de la méthode de détection des caractéristiques pour les signaux de TV analogiques[20].

Les services IoT peuvent être déployés à l'aide de toute une gamme de technologies de communication, câblées et sans fil. Cependant, nombre de ces services nécessiteront la flexibilité ou la mobilité des réseaux sans fil et dépendront donc de la disponibilité du spectre pour prendre en charge leur connectivité.

La gestion du spectre et octroi des licences est un important pour garantir la disponibilité et la capacité des communications IoT. Les dispositifs IoT communiquent en utilisant une gamme de protocoles différents, en fonction de leurs exigences de connectivité et des contraintes de ressources.

À partir de maintenant, la plupart des systèmes IoT fonctionnent dans des fréquences radio sans licence, notamment dans les bandes ISM à faible bande passante et utilisent toute une gamme de normes de connectivité sans fil telles que Bluetooth, ZigBee, Z-Wave et Wi-Fi (802.11 Standards), qui ont tous été conçus pour fonctionner dans des bandes de spectre internationales non autorisées par ISM, telles que l'utilisation de capteurs connectés sans fil pour une agriculture intelligente; systèmes

intelligents de gestion du trafic; et énergie intelligente: systèmes de surveillance vidéo et de contrôle d'accès; communications en champ proche (NFC/ISO/IEC 14443 et ISO/IEC 18000-3) pour les paiements mobiles; et code de produit électronique (EPC) et identification par radiofréquence (RFID)[21].

En plus de, LPWAN (Lower-Power Wide Area Networks) à faible débit pour les dispositifs. Exemple d'applications IoT via la connectivité LPWAN: systèmes de surveillance à distance Systèmes d'alarme à distance, agriculture intelligente, réseaux de capteurs, capteurs à piles[21].

Réseaux mobiles sous licence (application nécessitant des opérations sur de plus longues distances), exemples d'applications IoT via une connectivité de réseau mobile sous licence: logistique (suivi des actifs pour la gestion de flotte), transport (technologie de voiture intelligente et systèmes de verrouillage sans clé). L'utilisation des réseaux existants permet de conserver certains des principaux avantages:

- Assurée la qualité de service QoS ;
- Forte sécurité ;
- Excellente couverture ;
- Capacités d'itinérance ;
- La connectivité est maintenant capable de s'étendre dans des lieux souterrains et de pénétrer dans les murs et les sols.

En réalité, les opérateurs de téléphonie mobile sont enclins à exploiter les normes et infrastructures existantes des réseaux cellulaires actuels et à déployer l'IoT dans le spectre cellulaire sous licence. Les sociétés propriétaires préfèrent toutefois déployer l'IoT dans un spectre sans licence afin d'éviter tout frais de licence.

Il a été utilisé les technologies IoT déployées dans le spectre cellulaire, c'est-à-dire la communication de type machine améliorée (enhanced machine type communication) eMTC et l'IoT à bande étroite (narrow-band IoT)NB-IoT. Et technologies IoT Bluetooth et Zigbee, LoRaWAN et SigFox.

II.5 Les Technologies l'eMTC et le NB-IoT

L'eMTC et le NB-IoT sont des technologies IoT représentatives déployées dans le spectre cellulaire sous licence. En particulier, eMTC et NB-IoT sont normalisés dans la version LTP (Long Term Evolution)13/14 par le 3GPP, qui établit l'IoT en exploitant autant que possible les solutions normalisées des réseaux cellulaires et des infrastructures existantes. Les technologies eMTC et NB-IoT sont essentiellement conçues pour offrir des coûts matériels réduits, des consommations d'énergie faibles, des couvertures étendues et des connexions massives[22].

II.5.1 Les Technologies eMTC

eMTC est une évolution du LTE optimisée pour l'IoT. Il a introduit un ensemble de fonctionnalités de couche physique visant à réduire les coûts et la consommation d'énergie tout en élargissant la couverture. Les périphériques eMTC fonctionnent avec une bande passante de 1,08 MHz (6 blocs de ressources physiques LTE) pour la transmission et la réception de canaux et de signaux physiques [23].

La liaison descendante de l'eMTC est basée sur un schéma de multiplexage par répartition en fréquence orthogonale (OFDM) avec un espacement de sous-porteuse de 15 kHz comme dans le LTE. En liaison montante, eMTC utilise également la même numérologie que LTE. La transmission est basée sur un accès multiple par division de fréquence de porteuse (SC-FDMA) avec un espacement de sous-porteuse de 15 kHz.

II.5.2 Les Technologies NB-IoT

NB-IoT est une nouvelle technologie d'accès radio 3GPP construite à partir des fonctionnalités LTE. Il n'est pas rétro-compatible avec les périphériques 3GPP existants. Il est néanmoins conçu pour coexister avec le LTE. NB-IoT occupe une bande de fréquences de 180 kHz, qui est encore diminuée par rapport à l'eMTC et correspond à un PRB dans la transmission LTE. Cette bande passante étroite permet de réduire davantage la complexité du périphérique aux dépens d'un débit de données plus faible. La liaison descendante de NB-IoT est basée sur OFDM avec un espacement de sous-porteuses de 15 kHz comme dans le LTE (le PRB contient 12 sous-porteuses) [23].

En liaison montante, NB-IoT utilise également la même numérologie que LTE, mais NB-IoT prend en charge non seulement les transmissions à plusieurs tonalités, mais également les monotones. Une transmission à tonalité prend en charge l'espacement des sous-porteuses de 3,75kHz et 15 kHz. La numérologie 3,75kHz utilise une durée de fente de 2 ms au lieu de 0,5 ms, et le PRB contient 48 sous-porteuses au lieu de 12 sous-porteuses pour rester compatible avec la numérologie LTE[23].

Pour NB-IoT, nous considérons un déploiement conjoint avec une infrastructure LTE BS, en considérant le mode intra-bande. NB-IoT utilise la modulation QPSK permettant un débit binaire de 204,8 kbps sur la liaison montante, nécessitant un rapport signal sur bruit de 3 dB, sur la base d'une perte de couplage maximale théorique de 145 dB. Pour la liaison montante, les terminaux peuvent utiliser le mode d'amélioration de la couverture. Ce mode utilise une modulation BPSK et une tonalité unique de 15 kHz permettant un rapport signal / bruit aussi bas que -12,6 dB. Néanmoins, le débit de données est aussi bas que 20 b/s[16].

II.5.3 Caractéristiques d'eMTC et NB-IoT

L'eMTC et NB-IoT héritent tous deux du système LTE, notamment en ce qui concerne la numérologie, le codage de canal, la correspondance de débit, l'entrelacement, etc. Cet héritage peut accélérer le déploiement des spécifications techniques, le développement et le déploiement des produits IoT. Dans le même temps, les protocoles eMTC et NB-IoT simplifient le protocole LTE pour le rendre conforme aux nouveaux modèles de trafic et aux nouvelles exigences de l'IoT.

II.5.4 Différentes Caractéristiques entre l'eMTC et le NB-IoT

Le spectre cible constitue une différence majeure entre le eMTC et le NB-IoT: le eMTC exploite le spectre LTE et le NB-IoT exploite à la fois le spectre LTE et les autres spectres cellulaires régénérés. En particulier, les largeurs de bande des technologies eMTC et NB-IoT sont de 1,08 MHz et 180 kHz, respectivement. Notez que la bande passante de chaque porteuse GSM est de 200 kHz et la bande passante de chaque bloc de ressources physiques en LTE est de 180 kHz.

Ainsi, la bande passante de l'eMTC couvre six blocs de ressources physiques de LTE dans le domaine des fréquences, tandis que la bande passante de NB-IoT lui permet de coexister parfaitement avec les technologies GSM et LTE. Une autre différence réside dans la transmission sur la liaison montante. En particulier, seul le SC-FDMA multi-tonalités (avec un espacement de tonalité de 15 kHz) est pris en charge dans eMTC, tandis que les deux mono- ton (avec espacement de 3,75 kHz ou 15 kHz) et multi-tonalité SC-FDMA (avec espacement de 15 kHz) sont utilisés pour NB-IoT. Cette différence permet à NB-IoT d'utiliser le spectre plus efficacement et de programmer davantage de DE avec un débit de données réduit par rapport à eMTC[22].

II.5.5 Partage du Spectre

L'eMTC vise à partager le spectre LTE, et NB-IoT vise à partager à la fois le spectre LTE et les autres fréquences cellulaires réaménagées. Cette différence conduit à des modes de déploiement distincts d'eMTC et de NB-IoT. En particulier, l'eMTC ne peut être déployé que dans le spectre LTE, alors que NB-IoT dispose de trois modes de déploiement: fonctionnement autonome, fonctionnement dans la bande et fonctionnement en bande de garde. En mode autonome, on s'attend à ce que NB-IoT utilise le spectre cellulaire libre régénéré à partir de systèmes cellulaires actuels, par exemple, GSM / CDMA.

Dans l'exploitation en bande, NB-IoT est déployé au sein des opérateurs LTE et utilise les mêmes PRB que le LTE. En mode bande de garde, NB-IoT est déployé dans les bandes de garde des porteuses LTE. Cela est réalisable car environ 10% de la bande passante d'une porteuse LTE (5% de chaque côté) est généralement réservée pour éviter les brouillages entre porteuses. Il convient de noter que, puisque eMTC et NB-IoT partagent le spectre avec les réseaux cellulaires actuels, les opérateurs de téléphonie mobile peuvent gérer le spectre de manière centralisée. En attribuant un spectre orthogonal à des liaisons cellulaires / IoT, les opérateurs de téléphonie mobile peuvent

éviter les interférences entre les réseaux cellulaires actuels et les réseaux eMTC / NB-IoT[22].

II.6 Technologies Bluetooth et Zigbee

Bluetooth et Zigbee sont tous deux en mesure de fournir des coûts matériels réduits et une consommation énergétique réduite au niveau des services d'éducation. En conséquence, Bluetooth et ZigBee ont été largement appliqués dans des scénarios pratiques, notamment les commandes sans fil et les réseaux de capteurs sans fil.

II.6.1 Bluetooth

Le Bluetooth classique était destiné aux dispositifs de faible portée et à faible consommation d'énergie et était principalement utilisé pour la transmission audio, comme les casques mains libres pour téléphones mobiles et pour la connexion à des haut-parleurs sans fil. La limitation de 8 dispositifs actifs par (pico) cellule limite considérablement la facilité d'utilisation dans les installations de production. Avec l'introduction de la technologie Bluetooth LowEnergy (LE) et de la structure maillée, Bluetooth prend désormais en charge jusqu'à 32767 appareils par cellule. Avec les capacités de maillage, un grand nombre de points d'accès n'est pas nécessaire[24].

L'inconvénient est que les batteries des nœuds proches des points d'accès peuvent être rapidement épuisées en relayant les messages de la communication multi-sauts. L'avantage de la vaste gamme de topologies de réseau prises en charge est la possibilité d'organiser les nœuds en fonction des besoins sans avoir besoin de points d'accès supplémentaires. En raison de son application dans l'électronique grand public, la réputation de Bluetooth n'est pas très bonne et l'acceptation dans l'industrie n'est donc pas très élevée. De plus, le support pour les basses énergies et le maillage n'est pas encore très répandu et la fourchette n'est pas très élevée.

L'utilisation de la bande 2,4 GHz ISM est un autre inconvénient de Bluetooth. En raison de la prolifération des communications sans fil, le spectre sans licence limitée peut être saturé et le trafic régulier dans les bureaux Wi-Fis peut interférer avec le réseau Bluetooth de l'usine.

- **Partage du Spectre de Bluetooth**

Bluetooth fonctionne dans la bande 2,4 GHz ISM (de 2,4 à 2,4835 GHz). Étant donné que la bande ISM 2,4 GHz est globalement sans licence et libre d'accès, Bluetooth est globalement compatible et souffre d'un grave problème d'interférences. Pour faciliter le partage du spectre sur la bande ISM 2,4 GHz, Bluetooth adopte une approche à spectre étalé à sauts de fréquence (FHSS).

En particulier, le système FHSS est capable de tirer parti des diversités de fréquence et de réaliser le partage du spectre sans planification, et est donc largement utilisé pour le partage du spectre sans licence. Par exemple, dans le protocole Bluetooth classique, le spectre compris entre 2,4 GHz et 2,4835 GHz est divisé en 79 canaux Bluetooth de 1 MHz. Si nous définissons un jeu de saut comme l'ensemble des canaux

utilisés pour le saut, un jeu de saut peut être partiel ou la totalité des 79 canaux Bluetooth. De plus, les données transmises sont divisées en plusieurs paquets et chaque paquet est transmis sur l'un des 79 canaux Bluetooth en fonction d'un ordre prédéterminé.

Pour éviter de graves interférences d'une transmission Bluetooth avec d'autres transmissions, il est réglementé que l'occupation de chaque canal ne soit pas supérieure à 0,4 seconde.

Néanmoins, les dispositifs Bluetooth peuvent subir deux types d'interférences: les interférences fréquence-statique et les interférences dynamique en fréquence. En particulier, l'interférence de fréquence statique se produit lorsqu'une paire d'émetteur-récepteur Bluetooth saute sur un canal occupé par d'autres transmissions.

Le brouillage dynamique en fréquence provient d'un piconet colocalisé, qui utilise des canaux identiques. Pour lutter contre les interférences de fréquence statique, Bluetooth adopte un schéma FHSS adaptatif, à savoir AFHSS. L'idée principale du système AFHSS est la suivante: le nœud maître surveille la qualité du canal dans un ensemble de saut initial pendant un certain intervalle de temps et classe les canaux dans le groupe de saut initial comme «bons» ou «mauvais». En supprimant les canaux défectueux du hopset initial, il est probable que seule une faible interférence statique de fréquence existe sur les canaux restants du hopset.

Spécifiquement, l'axe des temps est d'abord divisé en intervalles de temps orthogonaux de durée identique. Ensuite, les ensembles de sauts de plusieurs piconets sont soigneusement conçus de manière collaborative, de sorte que les canaux des différents ensembles de sauts soient orthogonaux entre eux dans chaque intervalle de temps. Notez que la synchronisation de l'heure entre différents piconets est requise dans ce schéma. Sinon, le non synchronisation peut entraîner la non-orthogonalité des canaux dans différents ensembles de sauts et entraîner inévitablement une interférence dynamique en fréquence [22].

II.6.2 ZigBee

ZigBee est un protocole destiné aux appareils intégrés à faible consommation d'énergie et à faible coût. Dans la bande de fréquences 2,4 GHz, les débits de données peuvent atteindre 250 Kb/s, tandis que dans la bande de fréquences 868 MHz, il n'a que 20 Kb/s. Les topologies supportées par ZigBee sont les topologies étoile, arbre et maillage, ce qui le rend très flexible. Avec une plage nominale plus élevée que Bluetooth, le nombre de points d'accès peut être inférieur. La plage nominale plus élevée nécessite en outre moins de sauts pour la même distance, ce qui réduit la charge des batteries des stations qui autrement transmet des messages. La prise en charge de 65 536 appareils par cellule est la plus haute des technologies actuelles que nous avons examinées.

Comme la bande de fréquences de 2,4 GHz est très encombrée et peut donc entraîner des interférences, alors que la bande de fréquences moins utilisée de 868 MHz a un débit binaire très bas par rapport aux autres technologies[24].

- **Partage de Spectre de Zigbee**

La plupart des périphériques Zigbee commerciaux partagent la bande ISM 2,4 GHz et fonctionnent sur 16 canaux de 2 MHz. Pour faire face au brouillage causé à la bande ISM 2,4 GHz, Zigbee adopte une technique de spectre étalé à séquence directe (DSSS) et un mécanisme d'accès à accès multiple / évitement de collision (CSMA / CA) à détection de porteuse. En particulier, en adoptant la technique DSSS, Zigbee étale un signal à bande étroite sur un canal à large bande avec des séquences d'étalement conçues. Ensuite, le signal DSSS a des propriétés similaires à celles du bruit et résiste donc aux interférences de bande étroite. En outre, le DSSS permet à plusieurs DE d'accéder simultanément à un coordinateur / routeur commun. Bien que plusieurs signaux puissent interférer les uns avec les autres au niveau d'un coordinateur / routeur, la propriété de corrélation des séquences étalées permet au coordinateur / routeur d'extraire correctement le signal requis de plusieurs signaux.

De plus, en utilisant le mécanisme d'accès CSMA/CA, le dispositif Zigbee détecte d'abord le canal cible et ne passe à la transmission de données que si le canal cible est détecté comme étant inactif. En fait, le CSMA/CA est un mécanisme efficace d'accès aux canaux lorsque les canaux cibles ne sont pas encombrés.

II.7 Technologies LoRaWAN et SigFox

LoRaWAN et SigFox sont respectivement proposés par LoRa Alliance et la société SigFox, qui visent tous deux à déployer l'IoT dans le spectre ISM libre et à réduire les coûts de déploiement [22].

II.7.1 LoRaWAN

LoRa est une modulation sans fil basée sur le spectre étalé en modulation de fréquence, qui offre de grandes distances de communication tout en maintenant les caractéristiques de faible puissance de la modulation par déplacement de fréquence (FSK). Par conséquent, LoRa n'est pas une pile LPWAN ou de protocole complète, mais un composant sans fil de couche physique propriétaire (PHY).

LoRaWAN est le reste de la pile de protocoles de LoRa, composée principalement du MAC et de certains éléments de la couche réseau, qui repose sur le schéma de modulation LoRa. Dans LoRaWAN, les STA ne sont pas associées à un GW spécifique, car les paquets de liaison montante, transmis sur des canaux de fréquence et des débits de données différents (de 300 à 50 kbit/s), sont généralement reçus par plusieurs GW, qui les transmettent ensuite à un serveur basé sur un nuage. Afin de prolonger la durée de vie des batteries des STA, un serveur de réseau définit le débit de données et la puissance de sortie de chaque STA du LPWAN à l'aide d'un schéma de débit de données adaptatif.

Il existe trois classes de STA dans LoRaWAN: A, B et C. En classe A, la communication est initiée par les STA de telle sorte que les transmissions en liaison montante déclenchent deux courtes fenêtres en liaison descendante. Les créneaux de transmission sont programmés par les STA chaque fois qu'elles souhaitent transmettre dans un protocole basé sur ALOHA. Les STA de classe A consomment le moins d'énergie. Les STA de classe B ouvrent des fenêtres de réception programmées supplémentaires via une balise de synchronisation, ce qui permet au serveur d'identifier à quel moment les STA écoutent le canal. Enfin, les STA de classe C sont toujours à l'écoute avec des fenêtres de réception ouvertes en permanence qui ne sont fermées que lors de la transmission, ce qui permet une latence plus faible mais une consommation d'énergie plus élevée.

II.7.2 SigFox

Cette technologie s'appuie sur des antennes BS installées sur des tours d'opérateurs de réseau tels que Cellnex Telecom en Espagne ou Nettrotter en Italie, fournissant une solution de bout en bout incluant le réseau LPWAN, c'est-à-dire des STA avec un modem certifié (ou GW), et la plate-forme de gestion en nuage dorsale pour la configuration des rappels afin de recevoir et d'envoyer des messages. SIGFOX fonctionne à 868 MHz dans l'Union européenne et à 902 MHz aux États-Unis, divisant le spectre en 400 canaux de 100Hz (de 868,180 à 868,220 MHz dans le premier cas).

Les paquets dans SigFox sont très petits (respectivement 12 et 8 octets en liaison montante et en liaison descendante) et sont transmis à faible débit (100 bps) à l'aide d'une clé de décalage de phase binaire (BPSK) à bande ultra-étroite (UNB). Les STA peuvent envoyer jusqu'à 140 messages par jour, tandis que le GW est autorisé à ne transmettre que 4 messages.

Dans SigFox, aucune signalisation, ni aucune poignée de main entre les STA et les GW n'est requise, ce qui conduit à une couche réseau simple et robuste. En ce qui concerne la communication en liaison montante, les STA désireuses de transmettre un paquet sélectionnent un canal de fréquence pseudo-aléatoire et les transmettent directement au GW. Pour la liaison descendante, les STA doivent spécifiquement demander des mises à jour du réseau, ce qui leur permet d'être dans des états de faible puissance et d'économiser de l'énergie la plupart du temps[25].

II.7.3 Caractéristiques de LoRaWAN et de SigFox

II.7.3.1 Caractéristique de LoRaWAN

Pour réduire la consommation d'énergie des ED, LoRaWAN divise les ED en trois catégories en fonction de l'exigence de latence de liaison descendante: Classe A, Classe B et Classe C. En particulier, les ED de Classe A sont insensibles, à la latence de liaison descendante. Ces ED ouvrent les liaisons descendantes ne reçoivent les fenêtres qu'après une transmission en liaison montante. En d'autres termes, la plupart des fonctionnalités de ces disques peuvent être désactivées pour économiser de l'énergie s'il n'y a pas de transmission sur la liaison montante. Les ED de la classe B ont des

exigences limitées sur la latence de la liaison descendante. Ces ED sont programmés pour ouvrir périodiquement les fenêtres de réception en liaison descendante[22].

Les ED de la classe C ont des exigences strictes sur le temps de latence de la liaison descendante. Ces ED doivent toujours garder les fenêtres de réception ouvertes et ne les fermer que pour les transmissions montantes. De plus, LoRaWAN adopte un mécanisme d'accès ALOHA pour simplifier les opérations aux US. Cela signifie qu'un DE transmet ses données directement sans vérifier l'état du canal et retransmet les données en cas de collision.

Pour améliorer les chances de décoder correctement le signal requis au point d'accès, LoRaWAN adopte un mécanisme de retransmission avec un nombre de retransmission maximal de huit. Pour atteindre une large couverture, LoRaWAN modifie de manière adaptative le débit de données. LoRaWAN propose en particulier six classes de débits de données allant de 0,3 kbps à 37,5 kbps en fonction de différents facteurs d'étalement et de largeurs de bande de canaux. En particulier, un petit débit correspond à une large couverture et inversement.

II.7.3.2 Caractéristique de SigFox

Deux caractéristiques hautement reconnaissables de SigFox sont la bande passante ultra-étroite, c'est-à-dire 100 Hz, et la fonctionnalité cognitive de chaque AP. En utilisant notamment la bande passante ultra-étroite, SigFox réduit la puissance de bruit de fond à la fois des points d'accès et des points de vue. Cela permet d'économiser la puissance d'émission des ED et d'étendre la couverture de l'AP de 160 dB environ avec un MCL.

Par ailleurs, largeur de bande ultra-étroite signifie une faible exigence en matière de capacité de traitement du signal et réduit ainsi le coût en matériel (par exemple, un CNA et un CAN) à chaque ED. Cependant, la bande passante ultra-étroite conduit également à un débit de données réalisable aussi bas que 100 bps. Avec la fonctionnalité cognitive, chaque AP est capable d'identifier automatiquement le canal utilisé par un ED. Ensuite, il est inutile d'échanger des signaux de sélection de canal, ce qui permet d'économiser à la fois de l'énergie et des ressources de spectre. Semblable à LoRaWAN, SigFox adopte également un mécanisme d'accès ALOHA pour les transmissions montantes. Toutefois, SigFox ne prend pas en charge l'accusé de réception pour chaque transmission montante. En d'autres termes, un ED ne peut pas être informé d'une défaillance de la transmission sur la liaison montante. Pour faire face au problème, SigFox permet à un ED de transmettre chaque signal trois fois et améliore les chances de décoder correctement le signal requis au niveau du point d'accès[22].

II.7.4 Partage du Spectre de LoRaWAN et de SigFox

II.7.4.1 Partage du Spectre de LoRaWAN

LoRaWAN fonctionne sur diverses bandes ISM inférieures au GHz dans différents pays / régions. LoRaWAN fonctionne notamment sur les fréquences 433MHz et 868 MHz en Europe, 915 MHz aux États-Unis et 430 MHz en Asie. Pour se conformer à la réglementation en matière de spectre et éviter toute interférence importante avec d'autres appareils électroniques se trouvant sur le même spectre / canal, LoRaWAN est autorisé à utiliser un cycle de service inférieur à 1%. De plus, LoRaWAN adopte une technique CSS exclusive et diffuse un signal à bande étroite sur un canal à large bande. Ensuite, le LoRaWAN résiste aux interférences de bande étroite.

En outre, LoRaWAN a une topologie en étoile, dans laquelle chaque UE est connectée à plusieurs points d'accès et chaque point d'accès est également connecté à plusieurs ED. En d'autres termes, un signal transmis par un ED peut être reçu par plusieurs points d'accès. En combinant les signaux reçus dans plusieurs AP, LoRaWAN augmente les chances de décoder le signal et crée un gain de diversité en réception.

II.7.4.2 Partage du Spectre de LoRaWAN

Semblable au LoRaWAN, SigFox fonctionne également sur les bandes ISM inférieures au GHz. En particulier, SigFox fonctionne sur 868 MHz en Europe et 902 MHz aux États-Unis. Pour se conformer à la réglementation du spectre et éviter d'importantes interférences avec d'autres appareils électroniques se trouvant sur le même spectre / canal, SigFox est autorisé à:

- Travailler avec un cycle de travail ne dépassant pas 1%. SigFox peut notamment transmettre 140 messages de 12 octets par jour sur la liaison montante et 4 messages de 8 octets par jour sur la liaison descendante. En outre, SigFox permet à un DE de transmettre plusieurs copies d'un signal sur différents canaux et combine ces copies au niveau du point d'accès en présence d'interférences. Cela améliore les chances de décoder correctement le signal requis au niveau du point d'accès et tire parti d'un gain en diversité de réception[22].

II.8 Nouvelles Technologies de l'IoT

Les petites cellules peuvent avoir un rôle important à future, beaucoup d'entre elles s'attendant à s'appuyer sur des réseaux hétérogènes pour fournir une connectivité plus répandue.

II.8.1 L'Onde Millimétrique

L'onde millimétrique (mmWave) (également la bande millimétrique) est la bande de spectre comprise entre 30 GHz et 300 GHz. C'est une bande de spectre non développée qui peut être utilisée dans une large gamme de produits et services sur les réseaux mobiles et sans fil, car elle permet des débits de données plus élevés jusqu'à 10 Gbps, tels que les réseaux locaux sans fil à haut débit (WLAN) et accès haut débit[21].

❖ **Caractéristique de mmWave**

- Les ondes millimétriques ont une courte portée d'environ un kilomètre (les bandes de mmWave ne vont pas sur de longues distances) ;
- Très haut débit;
- Faible coût;
- Longue portée (jusqu'à 10 mètres), la flexibilité des câbles ;
- Les liaisons de communication point à point à large bande passante sont utilisées sur les mmWave allant de 71 GHz à 76 GHz, de 81 GHz à 86 GHz et de 92 GHz à 95 GHz ;
- Nécessite une licence de nombreuses autorités de réglementation internationales ;
- Fournir des services plus rapides et de meilleure qualité ;
- Le mmWave permet l'utilisation d'un grand nombre d'antennes dans une configuration multi-in multiple-out (MIMO);
- Efficacité spectrale élevée et la capacité globale seront multipliées par 10 environ par rapport à l'utilisation d'une seule antenne.

Le terme mmWave représente une technologie de communication efficace à courte portée et à haut débit, qui peut être utilisée dans certains scénarios IoT. Néanmoins, le partage du spectre sur l'onde millimétrique est difficile, car son modèle d'interférence est très différent des technologies IoT existantes. Il est donc nécessaire d'explorer davantage de ressources spectrales pour les utilisations IoT et d'analyser les solutions de partage de spectre correspondantes[22].

Les fréquences plus élevées telles que mmWave, dont les bandes de fréquences sont supérieures à 24 GHz, ont été recommandées pour les futures applications IoT 5G car une bande passante plus importante pourrait être envisagée pour améliorer la capacité et permettre aux utilisateurs d'utiliser des débits très élevés applications à courte portée. La bande de fréquences de 24 à 28 GHz a été exploitée comme l'une des bandes considérées pour les applications 5G-IoT [26].

II.8.2 La Cinquième Génération 5G

La 5G est la prochaine génération de technologies mobiles. Elle est conçue pour offrir une plus grande capacité de réseaux sans fil, une fiabilité accrue et des débits de données extrêmement rapides, permettant ainsi de nouveaux services innovants dans différents secteurs de l'industrie. La première vague de produits commerciaux devrait être disponibles en 2020 [27].

II.8.2.1 L'objectif de la 5 G

L'objectif des ces réseaux est d'offrir une qualité de fonctionnement élevée dans différents scénarios, par exemple en zone urbaine très peuplée, pour des points d'accès publics en intérieur ou en zone rurale. Plusieurs pays ont débuté les tests 5G et les résultats sont en cours d'évaluation, de nombreuses entreprises ayant mené à bien des essais spécifiques à petite échelle.

Comme les générations précédentes de réseaux large bande mobiles, les réseaux 5G utiliseront le spectre des fréquences radioélectriques. Celui-ci est divisé en bandes de fréquences, qui sont attribuées aux services de radiocommunication de telle sorte que chaque bande ne puisse être utilisée que par des services pouvant coexister. La prise en charge d'un trafic accru et d'un débit plus élevé dont la 5G a impérativement besoin nécessitera des technologies beaucoup plus efficaces sur le plan spectral, ainsi que des fréquences en bien plus grand nombre que ce que la 3G et la 4G utilisent actuellement.

Ces fréquences seront pour la plupart situées dans des bandes au-dessus de 24 GHz, lesquelles posent des problèmes considérables en termes de propagation radioélectrique et sont par ailleurs utilisées par plusieurs services de radiocommunication, notamment pour les communications par satellite, les prévisions météorologiques et la surveillance des ressources terrestres et des changements climatiques [45].

II.8.2.2 Les avantages de la 5G

Les avantages de la 5G sont nombreux:

- Grande capacité de bande passante (jusqu'à 10 gigabits par seconde) ;
- Faible latence (moins de 5 millisecondes) ;
- Consommation énergétique raisonnable et capacité à opérer plusieurs types de réseaux sans fils existants, du Wifi à la 4G ;
- Précisément, l'avenir de l'IoT pourrait nécessiter un réseau mobile pouvant assurer à la fois le transit de quantités massives de données, dans des délais parfois très courts (relations entre voitures connectées pour prévenir les accidents; vidéo de haute définition; réalité augmentée), nécessite de très hauts débits.
- En outre, la 5G serait en mesure, grâce à sa faible consommation énergétique, de concurrencer directement les réseaux bas débit [28].
- La 5G sera le moteur de croissance et source de revenus pour tous les pays où elle sera déployée. Afin de pouvoir optimiser les réseaux de prochaine génération, il est nécessaire d'adopter une approche de prochaine génération pour l'allocation et la gestion du spectre.

II.9 Conclusion

Afin de profiter pleinement des bandes de fréquences disponibles, il faut déployer des technologies efficaces après avoir consolidé les ressources du réseau radio existant. En outre, l'octroi de licences est un sujet crucial. En effet, aujourd'hui, les fournisseurs de services qui ont déjà acheté la licence d'une certaine bande de fréquence peuvent continuer à l'utiliser exclusivement à condition qu'ils assurent une couverture complète du réseau et qu'ils respectent le pourcentage de spectre qui lui est alloué.

Satellites, aéronefs, navires, stations de télévision ou de radio, dispositifs mobiles, radars de défense, de trafic aérien ou maritime, tous utilisent une bande de fréquences données conformément aux dispositions du règlement des radiocommunications. L'attribution des bandes de fréquences au niveau mondial par l'UIT permet à tous les services de radiocommunication de coexister sans interférences.

Dans ce chapitre nous avons présenté la gestion du spectre et leur objectif et aussi présenté comment quelque technique de l'internet des objets gère le spectre. Nous connaissons les caractéristiques de chaque technique

Dans le prochain chapitre nous allons présenter deux technologies WiFi et Zigbee.

Chapitre III

Coexistence Zigbee-WiFi pour la gestion du Spectre

III.1 Introduction

Zigbee est une norme sans fil ouverte conçue pour fournir la base de l'IoT en permettant aux objets quotidiens de fonctionner ensemble. Zigbee est souvent choisi comme une technologie permettant de connecter des objets en raison de caractéristiques telles que la résilience des réseaux, l'interopérabilité et une faible consommation d'énergie. Les objets utilisant Zigbee sont interopérables, car la norme spécifie la manière dont les objets interagissent en plus de la manière dont ils communiquent. De plus, Zigbee permet un réseau à faible consommation capable de prendre en charge plus de 65 000 périphériques sur un seul réseau, ce qui en fait un excellent choix pour connecter des objets.

Cependant, ces dernières années, nous avons assisté à la prolifération de dispositifs intelligents utilisant les technologies Wifi ou Zigbee, qui fonctionnent dans la même bande de fréquence. Lors du déploiement de WiFi et de Zigbee dans les mêmes environnements, une planification minutieuse doit être effectuée pour s'assurer qu'ils n'interfèrent pas les uns avec les autres.

Dans ce chapitre nous allons détaillons deux technologies WiFi et Zigbee, et présenter la coexistence entre aux.

III.2 La norme IEEE 802.11

Le WiFi est un ensemble de protocoles de communications sans fils régis par les normes du groupe IEEE 802.11. WiFi a été créé pour permettre aux dispositifs mobiles, tels que les ordinateurs portables, les téléphones et les tablettes de se connecter sans fil à Internet, mais ces équipements impliquent évidemment une interface utilisateur avec écran et clavier. Ces éléments simplifient dans une large mesure l'établissement de la connexion initiale à un dispositif ou une station sans fil et sa sécurisation. Toutefois, ce procédé relève du défi pour les produits IoT comme les capteurs, qui n'ont pas une telle interface utilisateur.

.III.2.1 Généralités sur le WiFi

- **Le Wi-Fi Alliance** est une association créée en 1999 pour permettre l'adoption d'une norme pour les réseaux locaux sans fil. Elle assure l'interopérabilité du matériel répondant à la norme 802.11.
- La norme IEEE 802.11 (ISO/IEC 8802-11) est un standard international décrivant les caractéristiques d'un réseau local sans fil (*WLAN*)[32].
- Le nom **WiFi** (contraction de *Wireless Fidelity*) [33] correspond initialement au nom donné à la certification délivrée par la WiFi Alliance.
- Le WiFi est utilisé largement dans tous les domaines: le bureau, la résidence, le restaurant, pour n'en nommer que quelques-uns. En tant que moyen de communication sans-fil populaire.

- Le WiFi est caractérisé par haut débit de transfert de données, ainsi que sa sécurité et stabilité de connexion très élevées [34].

III.2.2 Normes IEEE 802.11 (WiFi)

Normes	Débit max	Fréquence	Date	Description
802.11	1à 2 Mb/s	2,4 Ghz	1997	-Première norme WiFi
802.11a	54 Mb/s	5 Ghz	1999	-Haut débit sur 8 canaux -De 50Mbsjusqu 'à 70 m
802.11b	11 Mb/s	2,4 Ghz	1999	-Fixe un débit moyen maximum à 11 Mb/s théorique -Portée de 50m en intérieur à 300m en extérieur -Spécifie 3 canaux radio (1, 6 et 11)
802.11g	54 Mb/s	2,4 Ghz	2001	-Fixe un débit moyen maximum à 54 Mb/s théorique -Portée de 25m en intérieur à 75m en extérieur -Spécifie 3 canaux radio (1, 6 et 11)
802.11i			2004	Améliore la sécurité (authentification, cryptage et distribution des clés) en s'appuyant sur la norme Advanced Encryption Standard.
802.11n	1à 2 Mb/s	2,4 Ghz ou 5 Ghz	2009	-Regroupement des canaux -Rgrégation des paquets de données
802.11s	1 Gb/s	5 Ghz	2012	-En cours de normalisation -Améliore 802.11n
802.11ac	1,3 Gb/s	5 Ghz	2014	-Jusqu'à 1 300 Mbit/s de débit théorique
802.11ah	4 Mb/s	900 Mhz	2017	-Consommation d'énergie réduite

Tableau III.1: Normes IEEE 802.11[32,37]

III.2.3 Composants d'un réseau WiFi

Les points d'accès ou des cartes clientes possèdent le même type d'éléments actifs WiFi; leur fonction principale est de convertir les données numériques provenant d'un réseau Ethernet en signaux analogiques destinés à l'antenne.

C'est à son niveau que les protocoles de modulation/démodulation des signaux interviennent. En réception, il effectue le processus inverse consistant à décoder les signaux transmis par l'antenne en données IP pour le réseau.

Les caractéristiques principales d'un élément actif sont sa puissance d'émission et sa sensibilité en réception, toutes deux exprimées en mW ou dBm.

III.2.3.1 Points d'accès (AP)

Le rôle des points d'accès est similaire à celui que tient les hubs dans les réseaux traditionnels. Il permet aux stations équipées de cartes WiFi d'obtenir une connexion au réseau.

Figure III.1: point d'accès [32].

III.2.3.2 Adaptateurs Wifi USB

- Plus facile à installer
- Plus petite antenne que les WNIC donc moins fiable

III.2.3.3 Carte WiFi

Ce terme désigne les périphériques actifs Wi-Fi/antenne directement branchés à un ordinateur client. Ils jouent exactement le même rôle que les cartes réseaux traditionnelles à la différence près qu'on ne branche pas de câble dessus, puisque la liaison est assurée par radio [33].

III.2.3.4 Les Antennes

Une antenne peut être définie comme un système de conducteurs utilise pour rayonner de l'énergie électromagnétique ou la récolter. Pour transmettre un signal, l'énergie électrique du transmetteur est convertie en une énergie électromagnétique par l'antenne et est rayonnée dans l'environnement l'entourant (espace, eau, atmosphère).

La caractéristique la plus importante d'une antenne est son gain où le gain d'une antenne s'exprime en décibels isotropes (dBi).

Figure III.2 : antenne[32].

III.2.4 La topologie de WiFi

Il existe deux modèles de déploiement d'un réseau WiFi: ad hoc et infrastructure.

III.2.4.1 Le mode infrastructure

Le réseau à infrastructure comprend des points d'accès (AP) qui gèrent l'ensemble des communications dans une même zone géographique sous la forme de cellule [36]. Chaque cellule appelée BSS (Basic Service Set) est contrôlée par une station de base (AP). Chaque BSS est identifié par un BSSID (Basic Service Set Identifier), un identifiant de 6 octets (48 bits). Dans le mode infrastructure, le BSSID correspond à l'adresse MAC du point d'accès [37].

Afin d'étendre la zone de couverture, de multiples BSS sont utilisées avec des points d'accès qui sont reliés par un réseau filaire central appelé système de distribution. L'ensemble des BSSs interconnectés et leur système de distribution forment un réseau qui est appelé ESS (Extended Service Set). Identifié par un nom ESSID de 32 caractères maximum, appelé simplement SSID (**Service Set Identifier)** (ex:DJAWEB,…).

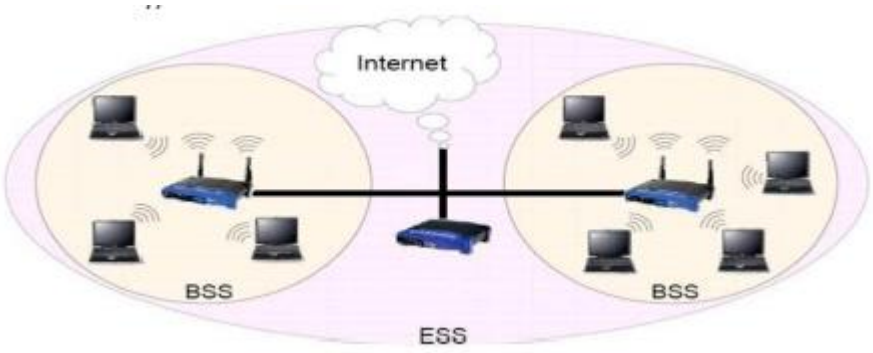


Figure III.3: Wifi en mode infrastructure [38].

III.2.4.2 Le mode sans infrastructure (IBSS) Ad-Hoc

IBSS : Independent Basic Service Set [36], c'est-à dire mode point à point

- pas de points d'accès.
- Routage dynamique selon la localisation desstations et leur zone de couverture.

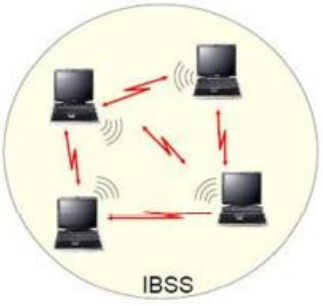


Figure III.4 : WiFi en mode Ad-Hoc[38].

III.2.5 L'Architecture du WiFi

La norme IEEE 802.11 s'attache à définir les couches basses du modèle OSI pour une liaison sans fil utilisant des ondes électromagnétiques, c'est-à-dire :

- **La couche physique**, proposant trois types de codages de l'information.
- **La couche liaison de donnée**s, constitué de deux sous-couches [35]: le contrôle de la liaison logique (***Logical Link Control***, *ou* ***LLC***) et le contrôle d'accès au support (***Media Access Control***, *ou* ***MAC***)[33].

Le WiFi définit les deux premières couches (basses) du modèle OSI, à savoir la couche physique et la couche liaison de données. Elle introduit des modifications sur la couche basse du niveau lien (donc niveau MAC) et sur le niveau physique avec le support de plusieurs méthodes d'accès radio et les règles de communication entre les différentes stations. Il est à noter que la nouvelle couche MAC est commune à toutes les couches physiques. La figure III.5 illustre l'architecture en couches de la norme IEEE 802.11.

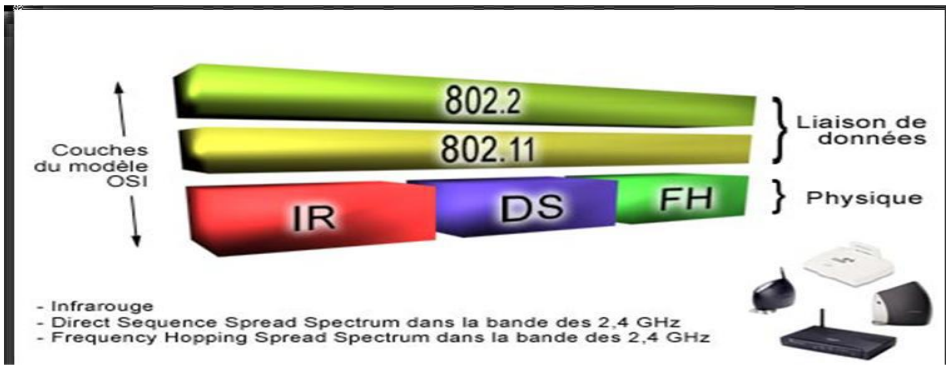


Figure III.5 : L'architecture en couches de la norme IEEE 802.11 [32].

La couche physique définit la modulation des ondes radioélectriques et les caractéristiques de la signalisation pour la transmission de données, tandis que la couche liaison de données définit l'interface entre le bus de la machine et la couche physique, notamment une méthode d'accès proche de celle utilisée dans le standard Ethernet et les règles de communication entre les différentes stations.

III.2.5.1 La couche physique

La norme IEEE 802.11 définit deux sous-couches physiques :

- **PMD** (Physical Media Dependant): gère l'encodage des données et la modulation.
- **PLCP** (Physical Layer Convergence Procedure): s'occupe de l'écoute du support et est directement reliée à la couche MAC pour lui signifier que le support de transmission est libre [37].

Le standard 802.11 d'origine a défini trois couches physiques de base, FHSS, DSSS, IR, auxquelles ont été rajoutées trois nouvelles couches physiques Wifi (avec deux variantes au sein de la solution 802.11b) et Wi-Fi5 (802.11a/g).la figure suivante illustre ça :

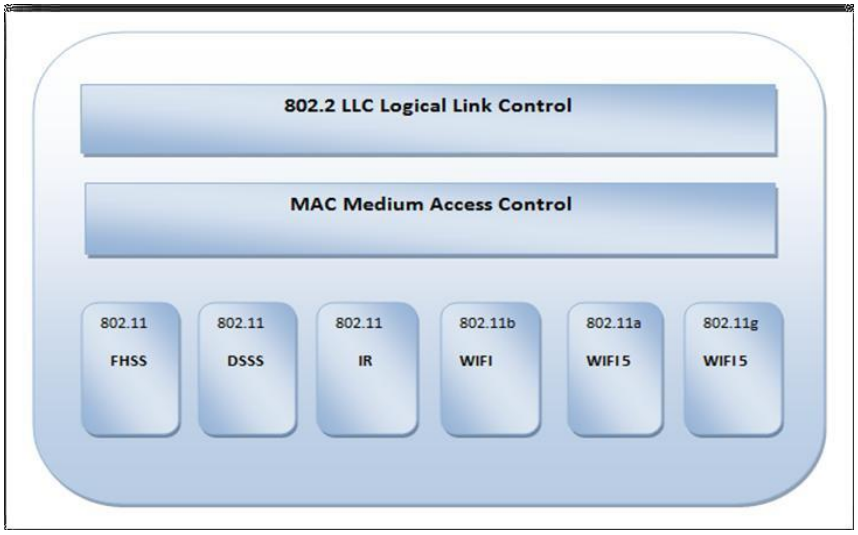


Figure III.6 : Les couches physiques du standard 802.11 [32].

III.2.5.1.1 Les technologies de transmission

La technique utilisée à l'origine pour les transmissions radio est appelé transmission en bande étroite, elle consiste à passer les différentes communications sur des canaux différents. Les transmissions radio sont toutefois soumises à de nombreuses contraintes rendant ce type de transmission non suffisantes. Ces contraintes sont notamment :

Le partage de la bande passante entre les différentes stations présentes dans une même cellule.

La propagation par des chemins multiples d'une onde radio. Une onde radio peut en effet se propager dans différentes direction et éventuellement être réfléchie ou réfractés par des objets de l'environnement physique, si bien qu'un récepteur peut être amené recevoir à quelques instants d'intervalles deux mêmes informations ayant emprunté des cheminements différents par réflexions successives.

III.2.5.1.1.1 Les techniques d'étalement de spectre

La norme IEEE 802.11 propose deux techniques de modulation de fréquence pour la transmission de données issues des technologies militaires. Ces techniques, appelées étalement de spectre (*en anglais spread spectrum*) consistent à utiliser une bande de fréquence large pour transmettre des données à faible puissance. On distingue deux techniques d'étalement de spectre :

- La technique de l'étalement de spectre à saut de fréquence,
- La technique de l'étalement de spectre à séquence directe

➢ **La technique de l'étalement de spectre à saut de fréquence *(Frequency Hopping Spread Spectrum* FHSS)** [47]: La technique FHSS consiste à découper la large bande de fréquence en un minimum de 75 canaux (*hops ou sauts d'une largeur de 1MHz*)[36,35], puis de transmettre en utilisant une combinaison de canaux connue de toutes les stations de la cellule.

Dans la norme 802.11, la bande de fréquence 2.4 - 2.4835 GHz permet de créer 79 canaux de 1 MHz [22]. La transmission se fait ainsi en émettant successivement sur un canal puis sur un autre pendant une courte période de temps (*d'environ 400 ms*), ce qui permet à un instant donné de transmettre un signal plus facilement reconnaissable sur une fréquence donnée.

Aujourd'hui les réseaux locaux utilisant cette technologie sont standards ce qui signifie que la séquence de fréquences utilisées est connue de tous, FHSS n'assure donc plus cette fonction de sécurisation des échanges. En contrepartie, le FHSS est désormais utilisé dans le standard 802.11 de telle manière à réduire les interférences entre les transmissions des diverses stations d'une cellule.

➢ **La technique de l'étalement de spectre à séquence directe (*Direct Sequence Spread Spectrum DSSS*)***:* La technique DSSS, consiste à transmettre pour chaque bit une séquence Barker (*parfois appelée bruit pseudo-aléatoire ou en anglais pseudo-random noise, noté PN*)[47] de bits. Ainsi chaque bit valant 1 est remplacé par une séquence de bits et chaque bit valant 0 par son complément.

La couche physique de la norme 802.11 définit une séquence de 11 bits (10110111000) pour représenter un 1 et son complément (01001000111) pour coder un 0 [35]. On appelle chip ou chipping code (*en français puce*) chaque bit encodé à l'aide de la séquence. Cette technique (*appelée chipping*) revient donc à moduler chaque bit avec la séquence barker. Grâce au chipping de l'information redondante est transmise, ce qui permet d'effectuer des contrôles d'erreurs sur les transmissions.

Toutefois, pour une transmission de 11 Mbps correcte il est nécessaire de transmettre sur une bande de 22 MHz car, d'après le théorème de Shannon, la fréquence d'échantillonnage doit être au minimum égale au double du signal à numériser [37]. Ainsi certains canaux recouvrent partiellement les canaux adjacents, c'est la raison pour laquelle des canaux isolés (*les canaux 1, 6 et 11*) distants les uns des autres de 25 MHz sont généralement utilisés.

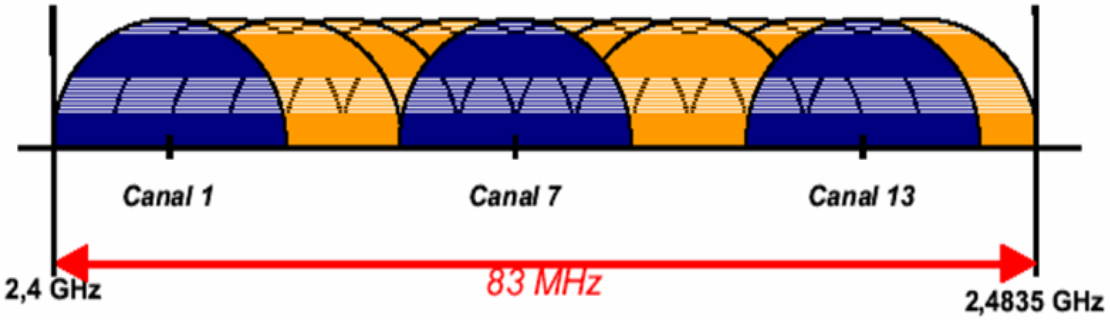


Figure III.7 : Décomposition de la bande ISM en sous canaux [36].

Lorsqu'un canal est sélectionné, le spectre du signal occupe une bande comprise entre 10 et 15 MHz de chaque coté de la fréquence centrale. La valeur 15 MHz provient de la décroissance non idéale des lobes secondaires de la modulation utilisée. Il n'est donc pas possible d'utiliser dans la même zone géographique les canaux adjacents à ce canal. Pour permettre à plusieurs réseaux d'émettre sur une même cellule, il faut allouer à chacun d'eux des canaux appropriés, qui ne se recouvrent pas.

Par exemple, considérons deux réseaux utilisant DSSS. Si l'un d'eux utilise le canal 6, le canal 5 et 7 ne peut pas être utilisé par le deuxième réseau, car trop proche. Il en va de malheureusement de même pour les canaux 2, 3,4, 8, 9 et 10, qui ne peuvent non plus être alloués du fait de l'étalement de la bande passante du canal 6. Les canaux qui peuvent être utilisés sont les canaux 1, 11, 12, 13 et 14. Sachant que la largeur de bande n'est que de 83.5 MHz, il ne peut donc y avoir au maximum que trois réseaux 802.11 DSSS émettant sur une même cellule sans risque d'interférences.

III.2.5.1.1.2 La modulation

- **PSK (Phase Shift Keying:** cette technique est utilisée par la norme 802.11b[F]. Chaque bit produit une rotation de phase. Une rotation de 180° permet de transmettre des débits peu élevés (technique appelée BPSK) tandis qu'une série de quatre rotations de 90° (technique appelée QPSK) permet des débits deux fois plus élevés grâce à l'optimisation de l'utilisation de la bande radio.

- **OFDM (Orthogonal Frequency Division Multiplexing):** OFDM est une méthode de codage appliquée aux normes 802.11a et g qui permet d'obtenir une meilleure bande passante. De ce fait, OFDM divise la bande de fréquence en bandes secondaires [36] qui transmettent simultanément des fractions de données. Plus le nombre de canaux est élevé, plus les données transmises en parallèle sont nombreuses, plus la bande passante est élevée. Selon les conditions de bande passante, OFDM peut utiliser des méthodes de modulation de phase et d'amplitude.

OFDM est plus efficace que DSSS à savoir: en fonctionnant avec une même bande de fréquences (2,4000 - 2,4835 GHz), 802.11g a une bande passante de 54 Mbps[F] avec OFDM, alors que 802.11b monte seulement jusqu'à 11 Mbps avec DSSS.

III.2.5.2 La couche liaison de données

La couche Liaison de données de la norme 802.11 est composée de deux sous-couches: la couche de contrôle de la liaison logique (LLC) et la couche de contrôle d'accès au support (MAC). En plus des fonctions habituellement rendues par la couche MAC, la couche MAC 802.11 offre d'autres fonctions qui sont normalement confiées aux protocoles supérieurs, comme:

- La fragmentation et le réassemblage des trames ;
- Le contrôle d'accès au support ;
- L'adressage et le formatage des trames [37] ;
- Le contrôle d'erreur sur la trame, à partir d'un CRC (Cyclic Redundancy Chek) ;
- La gestion de l'énergie et la gestion de la mobilité ;

- La qualité de service et la sécurité.

Le contrôle d'accès au support est une fonctionnalité qui nous intéresse ici particulièrement, se fait suivant deux méthodes (DCF et PCF) qui seront étudiées ultérieurement.

A) La sous-couche LLC

Le rôle de cette couche est, entre autres, d'adapter les données venant des couches supérieures à la couche physique. Il est ainsi tout à fait possible de connecter un réseau WLAN à tout autre réseau IEEE 802, filaire ou non [37]. La trame LLC contient comme en-tête une adresse et en fin une zone de détection d'erreurs, ce qui lui donne l'avantage de pouvoir contrôler le flux et corriger les erreurs détectées [35].

B) La sous couche MAC

La sous couche MAC assure la gestion d'accès de plusieurs stations à un support partagé d'où chaque station vérifie le canal (support) et fait la transmission dans le cas d'un canal libère.

La norme a défini 3 types de trames MAC: 1) Les trames de données: pour véhiculer les données à transmettre. 2) Les trames de contrôle : utiles dans la procédure d'accès au canal (RTS, CTS, ACK). 3) Les trames de gestion : contiennent des informations de gestion et ne sont pas remontées au niveau OSI supérieur (trames Beacon contenant les informations de synchronisation).

III.2.5.3 Méthodes d'accès au support de la norme IEEE 802.11

Comme mentionné plus haut, la principale fonctionnalité de la couche MAC 802.11 est de définir les mécanismes d'accès au support physique. Le standard définit deux méthodes d'accès au support: DCF et PCF.

- **Le Distributed Coordination Function (DCF):** la technique DCF est basée sur le mécanisme CSMA/CA (Carrier Sens Multiple Access/Collision Avoidance) [37] ou méthode d'accès multiple à détection de porteuse et évitement de collision. Cet algorithme distribué est exécuté localement sur chaque station afin de déterminer les périodes d'accès au médium.

Le CSMA/CA est une technique d'accès aléatoire avec écoute de la porteuse, qui permet d'écouter le support de transmission avant d'émettre. Le CSMA évite ainsi qu'une transmission ne soit faite que lorsque le support est libre. Cela réduit le risque de collision, mais ne permet pas de l'éviter complètement.

- **Description générale du mécanisme DCF**

Avant chaque émission, la station désirant émettre écoute le support. S'il est libre pendant une certaine durée DIFS (démontrer plus bas), la transmission est possible. Si le support est occupé, une procédure de *Backoff* est enclenchée.

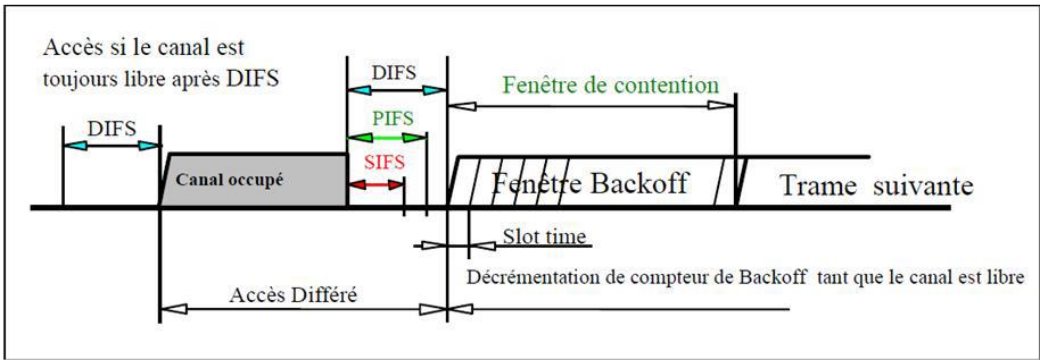


Figure III.8: Accès au médium en mode DCF[32].

Une station ayant correctement reçu un paquet, renvoie un accusé de réception (ACK) à la station émettrice. L'ACK indique à l'émetteur qu'aucune collision n'a eu lieu. Par contre, si l'émetteur ne reçoit pas d'acquittement au bout d'un certain temps, le fragment est retransmis jusqu'à réception d'un acquittement par le récepteur. Enfin, si après un nombre défini de retransmissions, aucun accusé de réception n'est reçu, l'émission est abandonnée.

Un espace **IFS (Inter-Frame Space)** est la durée pendant laquelle une station doit attendre avant de transmettre sur le canal. **SIFS (Short Inter-Frame Spacing)** est utilisé pour séparer les différentes trames transmises au sein d'un même dialogue (par exemple entre question et réponse). Le **PIFS** (**PCF Inter-Frame Spacing**) est le temps que doivent attendre les autres stations avant d'émettre un paquet en mode PCF. L'**EIFS (Extended Inter-Frame Spacing**) est le plus long des IFS que doit attendre une station tentant de transmettre sans succès pour abandonner Enfin, Le **DIFS** (**DCF Inter-Frame Spacing) e**st le temps que doivent attendre les autres stations avant d'émettre un paquet en mode DCF. La valeur du DIFS est égale à celle d'un SIFS augmentée de deux times slot.

.L'algorithme de Backoff

La procédure de Backoff est un mécanisme simple, basé sur le calcul d'un temporisateur gérant les transmissions et les retransmissions. Il permet de réduire la probabilité de collision sur le canal en essayant de minimiser les chances d'avoir plusieurs stations qui accèdent au support en même temps.

- **Déroulement** Une station S désirant envoyer des données attend pendant une période DIFS. Si après cette durée le canal est libre, la station accède directement au canal. Dans le cas contraire, la station déclenche le mécanisme de Backoff qui se déroule en 3 étapes [35] :

1. La station calcule son temporisateur Backoff_Timer :

Avec *Backoff _ Timer = Random() _ TS (time slot)*

- ***Random ( )***: nombre pseudo-aléatoire choisi ente 0 et CW-1 ; où CW est la taille de la fenêtre de contention qui sera détaillée plus loin. ***TS*** : durée d'un time-slot définie comme étant l'intervalle de temps nécessaire pour une station pour savoir si une autre a accédé au canal au début du time-slot précédant.

2. Décrémenter le time slot après un DIFS de libération du canal.

3. Pouvoir envoyer dans le cas d'un Backoff _Timer nul, deux stations ne peuvent pas envoyer au même temps, lors de la décrémentation, la station qui termine la première est celle qui est autorisée à envoyer dont l'autre est bloquée.

Pour une taille CWmin de la fenêtre de contention, la transmission est soit réussie ou elle sera un échec dans le cas de l'existence d'une collision lors de la transmission. Pour minimiser la probabilité de collision, il faut incrémenter la fenêtre de contention pour la mettre à *(CWnew = 2*CW+1).*

Lorsque CWmax est atteinte, la transmission sera souvent un échec car il est impossible d'incrémenter au delà de CWmax.

- **Gramme de fonctionnement**

La figure résume le fonctionnement de la procédure CSMA/CA et de l'algorithme de Backoff.

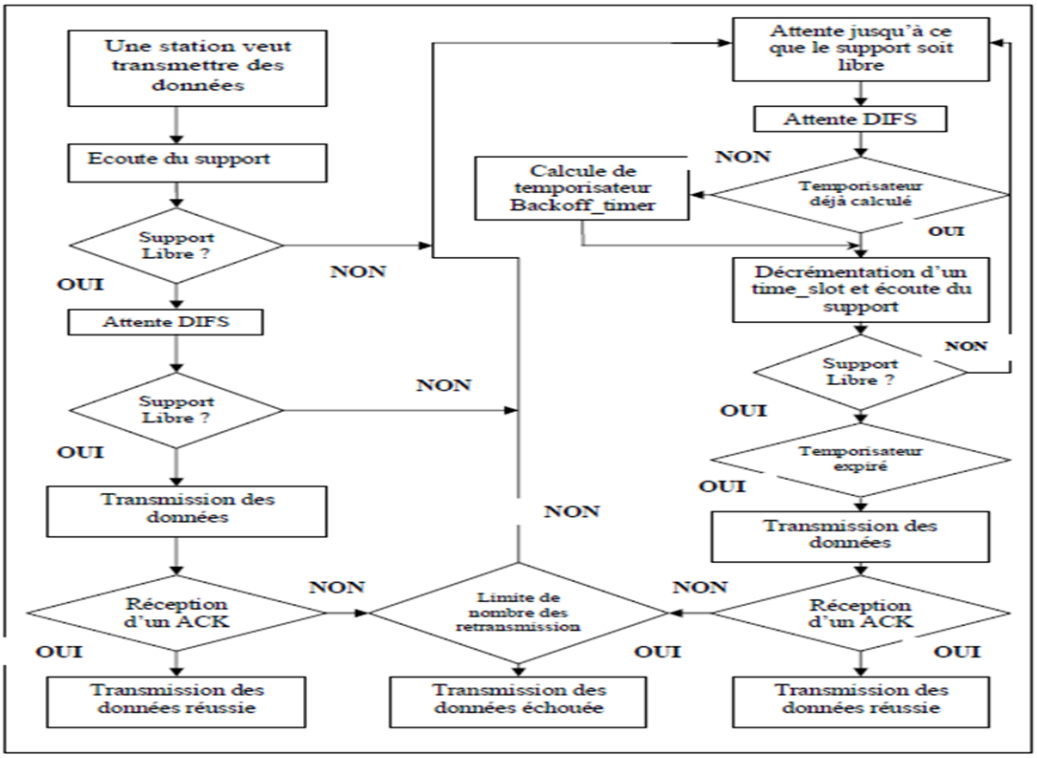


Figure III.9: Algorithme de CSMA/CA et Backoff [35].

➢ **Description générale du mécanisme PCF :** la PCF est une méthode qui ne fonctionne qu'en mode infrastructure, elle utilise une station avec un point d'accès (AP) et peut être implémentée avec la DCF. En faisant appel au protocole PLCP (Physical Layer Convergence Protocol), il écoute le support et autorise ou non l'émission de la station et un point de Coordination (PC) qui est installé sur l'AP.

Comme il est illustré sur la figure III.16, une trame est composée de deux parties appelés la CP et la CFP. La CP est faite pour écouter le canal avant d'effectuer une communication. Au début du CFP la transmission de toutes les stations doit être bloquée par un timer NAV (Network Allocation Vector) qui est calculé pour chaque station. Lorsqu'une station est autorisée par la CFP à émettre et durant une période PIFS dont le canal est libre, le PC envoie un beacon qui indique le début de la super trame et après un temps SIFS le PC envoie la trame de données qui contient le message de polling.

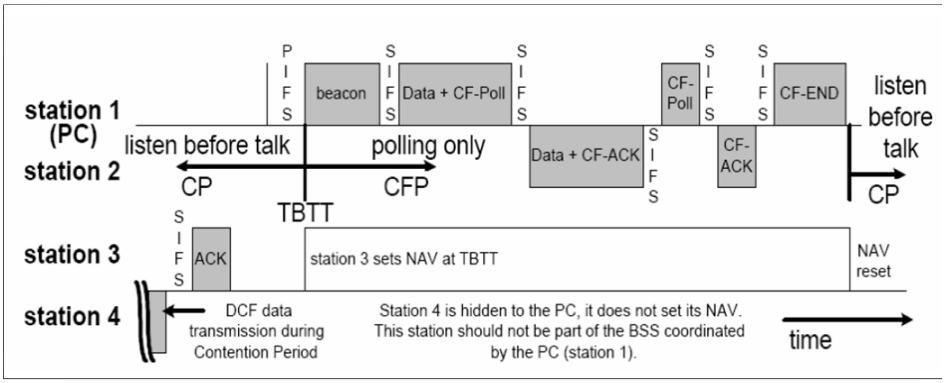


Figure III.10 : Principe du fonctionnement du PCF[32].

III.2.6 Les avantages et les inconvénients de WiFi

III.2.6.1 Les avantage

- **Mobilité**: La connexion au réseau sans fil permet de se déplacer librement dans le rayon disponible sans avoir à brancher/débrancher quoi que ce soit.
- **Facilité**: Un réseau WiFi bien configuré permet de se connecter très facilement, à condition de posséder une autorisation. Il suffit généralement de se trouver dans la zone de couverture pour être connecté.
- **Souplesse**: La souplesse d'installation du WiFi permet d'adapter facilement la zone d'action en fonction des besoins. Si le point d'accès est trop faible, on ajoute des répéteurs pour étendre la couverture.
- **Coût**: La plupart des éléments du réseau WiFi (point d'accès, répéteurs, antennes…) peuvent être simplement posés. L'installation peut donc parfois se faire sans le moindre outillage, ce qui réduit les coûts de main-d'œuvre. Le budget de fonctionnement est similaire à un réseau filaire.
- **Evolutivité**: La facilité d'extension ou de restriction du réseau permet d'avoir toujours une couverture WiFi correspondant aux besoins réels.

III.2.6.2 Les inconvénients

- Qualité et continuité du signal: ces notions ne sont pas garanties du fait des problèmes pouvant venir des interférences, du matériel et de l'environnement.
- Portée limitée.
- Consommation énergétique importante.
- Sécurité: Le WiFi étant un réseau sans fil, il est possible de s'y connecter sans intervention matérielle. Cela veut dire qu'il faut particulièrement étudier la sécurisation du réseau si l'on veut éviter la présence d'indésirables ou la fuite d'informations.

III.3 La norme IEEE 802.15.4

III.3.1 Généralités sur Zigbee

Un des soucis majeurs traités dans les communications sans fils, c'est la bande-passante, le type de message et la portée de la communication. Tous ça une relation de coût minimisant. Dans ce contexte, l'alliance Zigbee est née : c'est une association de compagnies travaillant ensemble pour développer un standard global et ouvert pour les communications sans fils avec un coût réduit et une basse consommation de l'énergie.

Zigbee est une norme qui définit un ensemble de protocoles de communication pour les réseaux sans fil à courte portée et à faible débit de données [38]. C'est le seul standard reconnu par la norme IEEE802.15.4 Personal-Area Network (PAN)[34], en matière de connectivité sans fil. Les périphériques sans fil basés sur Zigbee fonctionnent dans les bandes de fréquences 868 MHz, 915 MHz et 2,4 GHz. Le débit de données maximal est de 250Kbps.

Zigbee est principalement destiné aux applications alimentées par batterie, où les principales exigences sont un faible débit de données, un faible coût et une longue durée de vie de la batterie. Dans de nombreuses applications Zigbee, la durée totale d'activité d'un périphérique sans fil est très limitée. L'appareil passe le plus clair de son temps en mode d'économie d'énergie, également appelé mode veille. En conséquence, les appareils Zigbee enabled sont capables de fonctionner pendant plusieurs années avant que leurs batteries ne doivent être remplacées [38].

La communication entre les équipements Zigbee repose sur la définition de profils qui se décompose en deux types : privés et publics. Chaque profil public possède un identifiant (ID) allant de 0x0000 à 0x7FFF et 0xBF00 à 0xFFFF pour les profils privés.

III.3.2 Le type des applications

➢ **Home automation**: Zigbee est parfaitement adapté au contrôle à distance d'appareils ménagers tels que la commande de système d'éclairage, le contrôle d'appareils, le contrôle de systèmes de chauffage et de refroidissement, le fonctionnement et le contrôle d'équipements de sécurité, la surveillance, ventilation, air conditionné, etc.

- **Industrielles**: Détection de situation d'urgence, contrôle de machines
- **Automotive**: Contrôle de la pression des pneus, etc.;
- **Agriculture**: Mesure de l'humidité du sol, détection de situations pour l'usage des intrants, mesure de la salinité du sol, etc.
- **Autres** : Contrôle d'équipement électronique, communication entre PC et périphériques, etc.

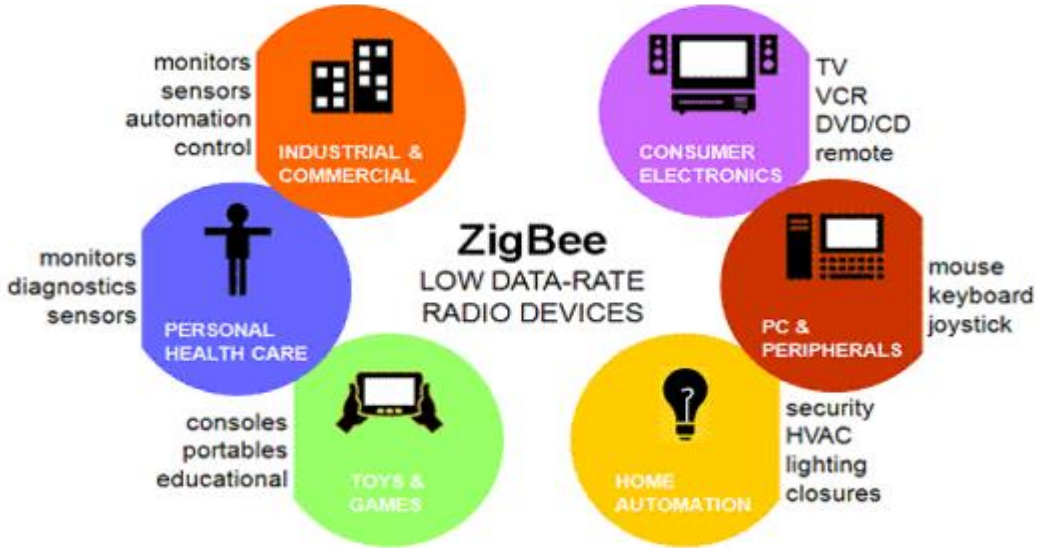


Figure III.11: Applications de Zigbee [48]

III.3.3 Les objectifs de Zigbee

Les objectifs visés par Zigbee peuvent être résumés dans les points suivants

- Usage sans restrictions (contrainte) géographiques ;
- Pénétration à travers les murs et plafonds ;
- Installation automatique/semi-automatique ;
- Possibilité de rajouter/retirer des dispositifs ;
- Coût avantageux.

III.3.4 La structure du système Zigbee

La structure du système Zigbee comprend trois types différents de périphériques, tels que le coordinateur Zigbee, le routeur et le périphérique final. Chaque réseau Zigbee doit comporter au moins un coordinateur qui agit en tant que racine et pont du réseau. Le coordinateur est responsable du traitement et du stockage des informations lors des opérations de réception et de transmission des données. Les routeurs Zigbee agissent comme des périphériques intermédiaires qui permettent aux données de les transmettre à d'autres périphériques.

Les périphériques finaux ont une fonctionnalité limitée pour communiquer avec les nœuds parents, de sorte que la batterie est économisée, comme indiqué sur la figure. Le nombre de routeurs, de coordinateurs et d'appareils finaux dépend du type de réseau, tel que les réseaux en étoile, en arbre et maillé.

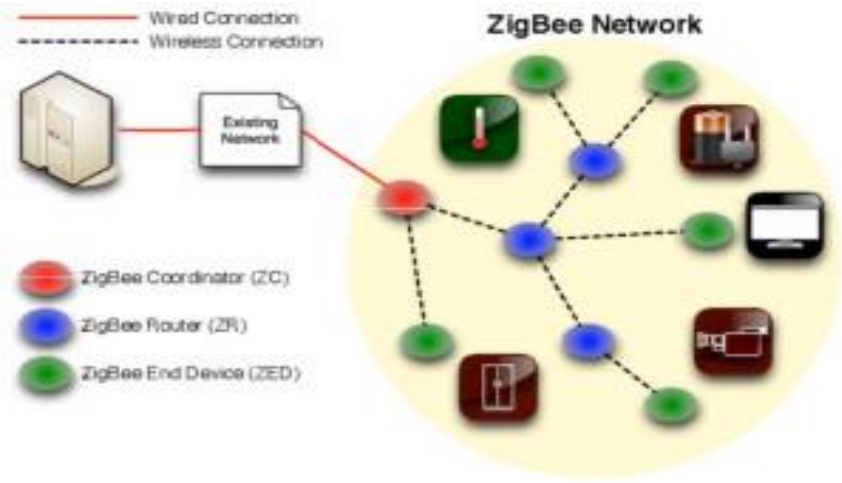


Figure III.12 : Structure du système Zigbee[34].

III.3.5 Les modes de fonctionnement de Zigbee

Les données bi-directionnelles Zigbee sont transférées dans deux modes: le mode non-balise et le mode balise. En mode balise, les coordinateurs et les routeurs surveillent en permanence l'état actif des données entrantes, ce qui permet de consommer plus d'énergie. Dans ce mode, les routeurs et les coordinateurs ne se mettent pas en veille car tout nœud peut se réveiller et communiquer. Cependant, il nécessite plus d'alimentation et sa consommation d'énergie est faible car la plupart des périphériques sont inactifs pendant de longues périodes sur le réseau.

En mode balise, en l'absence de communication de données à partir des périphériques finaux, les routeurs et les coordinateurs entrent en état de veille. Périodiquement, ce coordinateur se réveille et transmet les balises aux routeurs du réseau. Ces réseaux de balises fonctionnent pendant des créneaux horaires, c'est-à-dire qu'ils fonctionnent lorsque la communication requise réduit les cycles de travail et allonge la durée de vie de la batterie. Les modes balises et non balises de Zigbee peuvent gérer des types de données périodiques (données de capteurs), intermittentes (commutateurs d'éclairage) et répétitives.

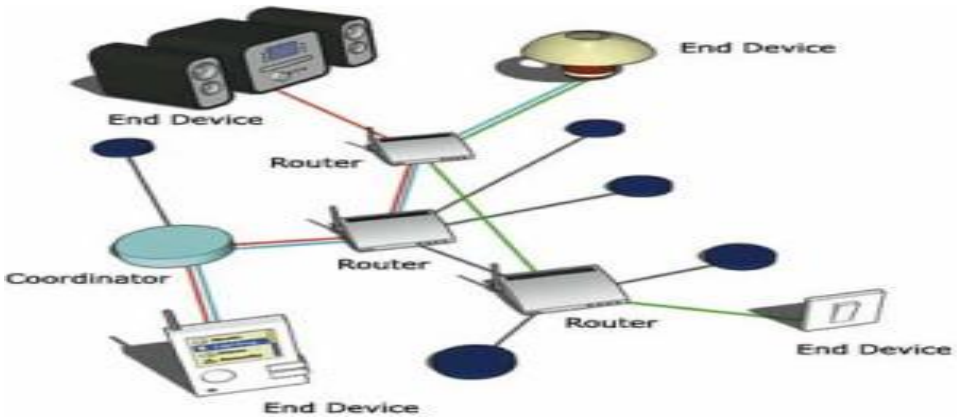


Figure III.13 : Opération de communication Zigbee [49]

III.3.6 La topologie de Zigbee

Zigbee prend en charge plusieurs topologies de réseau; Cependant, les configurations les plus couramment utilisées sont les topologies en étoile, en maillage et en grappes. Toute topologie consiste en un ou plusieurs coordinateurs.

Dans une topologie en étoile[39], le réseau est constitué d'un coordinateur chargé d'initialiser et de gérer les périphériques sur le réseau. Tous les autres appareils sont appelés appareils terminaux qui communiquent directement avec le coordinateur. Cette solution est utilisée dans les industries où tous les périphériques d'extrémité sont nécessaires pour communiquer avec le contrôleur central. Cette topologie est simple et facile à déployer.

Dans les topologies maillées et arborescentes [49], le réseau Zigbee est étendu avec plusieurs routeurs où le coordinateur est responsable de leur observation. Ces structures permettent à tout périphérique de communiquer avec tout autre nœud adjacent pour fournir une redondance aux données.

En cas de défaillance d'un nœud, les informations sont automatiquement acheminées vers un autre périphérique par ces topologies. Dans un réseau d'arborescence de grappes, chaque grappe est constituée d'un coordinateur avec des nœuds d'extrémité. Ces coordinateurs sont connectés au coordinateur parent qui initialise l'ensemble du réseau.

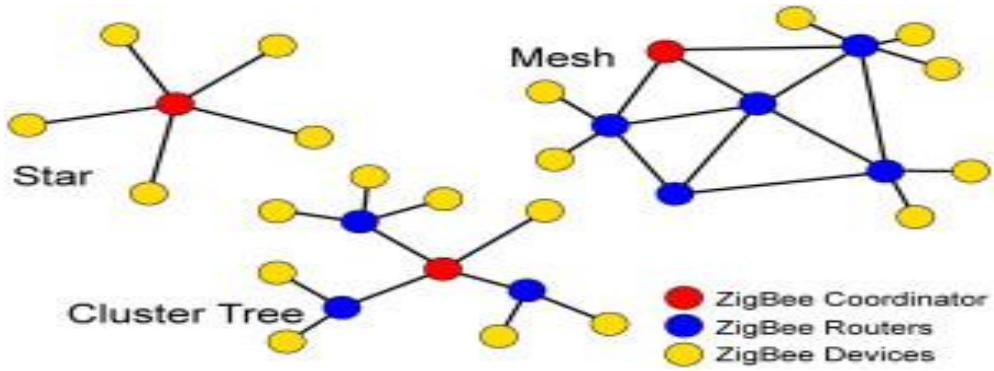


Figure III.14 : Topologies de Zigbee [49]

III.3.7 L'architecture de la norme IEEE 802.15.4

L'architecture du protocole Zigbee consiste en une pile de diverses couches, la pile du protocole Zigbee se compose de quatre couches: couche physique (PRY), couche de contrôle d'accès au support (MAC), couche de réseau (NWK), cette couche s'occupent de la création et de l'entretien du réseau, elles garantissent théoriquement le débit de transmission de données jusqu'à 250kbps, et couche d'application (APL) qui est responsable de la communication entre les dispositifs[34].

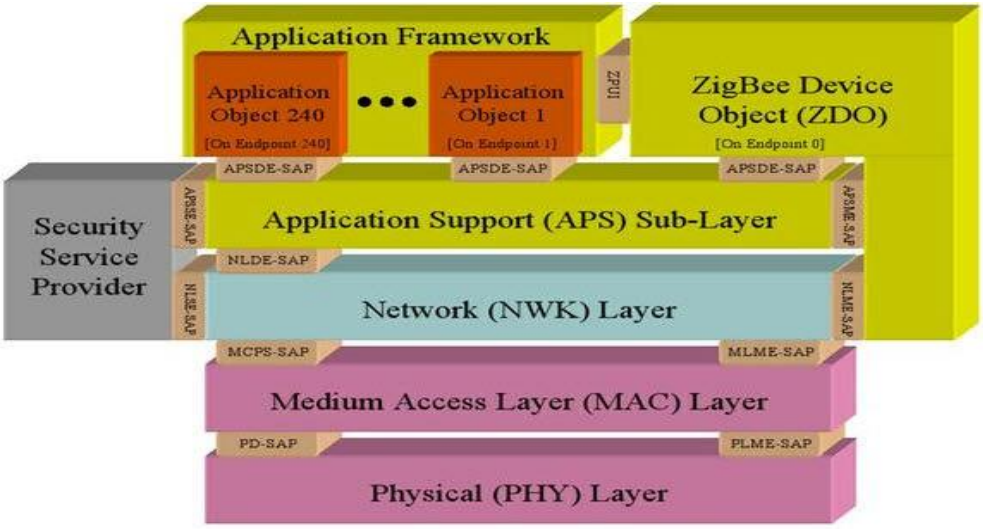


Figure III.15 : Architecture du 802.15.4 [49].

- **Couche physique** : cette couche effectue les opérations de modulation et de démodulation sur les signaux d'émission et de réception, respectivement. La fréquence [39], le débit et le nombre de canaux de cette couche sont indiqués ci-dessous.

Les trois premières couches (pYH, MAC, et NWK) s'occupent de la création et de l'entretien du réseau, elles garantissent théoriquement le débit de transmission de données jusqu'à 250kbps.

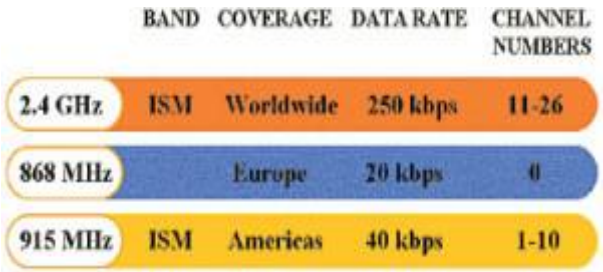


Figure III.16 : Couche physique du protocole Zigbee [34].

- **Couche MAC** : cette couche est responsable de la transmission fiable des données en accédant à différents réseaux avec l'évitement de collision d'accès multiple par le sens de porteuse (CSMA). Cela transmet également les trames de balise pour la synchronisation de la communication.

- **Couche réseau** : cette couche s'occupe de toutes les opérations liées au réseau telles que la configuration du réseau, la connexion et la déconnexion du périphérique final au réseau, le routage, la configuration des périphériques, etc...

- **Sous-couche de support d'application**: cette couche permet aux services nécessaires aux objets de périphérique Zigbee et aux objets d'application d'interagir avec les couches réseau pour les services de gestion de données. Cette couche est chargée de faire correspondre deux périphériques en fonction de leurs services et de leurs besoins.

- **Cadre d'application** : Il fournit deux types de services de données: paire de valeurs clés et services de messagerie génériques. Le message générique est une structure définie par le développeur, alors que la paire clé / valeur est utilisée pour obtenir des attributs dans les objets de l'application. ZDO (Zigbee Divice Object) fournit une interface entre les objets d'application et la couche APS des périphériques Zigbee. Il est responsable de la détection, de l'initialisation et de la liaison d'autres périphériques au réseau.

III.3.8 Les technologies de transmission

La norme IEEE 802.15.4 partagent la bande ISM 2,4 GHz et fonctionnent sur 16 canaux de 2 MHz [22]. Pour faire face au brouillage causé à la bande ISM 2,4 GHz, Zigbee adopte une technique de spectre étalé à séquence directe [38] et un mécanisme d'accès à accès multiple / évitement de collision (CSMA / CA) à détection de porteuse [39]. En particulier, en adoptant la technique DSSS, Zigbee étale un signal à bande étroite sur un canal à large bande avec des séquences d'étalement conçues. Ensuite, le signal DSSS a des propriétés similaires à celles du bruit et résiste donc aux interférences de bande étroite. En outre, le DSSS permet à plusieurs DE d'accéder simultanément à un coordinateur / routeur commun. Bien que plusieurs signaux puissent interférer les uns avec les autres au niveau d'un coordinateur / routeur, la propriété de corrélation des séquences étalées permet au coordinateur / routeur d'extraire correctement le signal requis de plusieurs signaux.

De plus, en utilisant le mécanisme d'accès CSMA/CA, le dispositif Zigbee détecte d'abord le canal cible et ne passe à la transmission de données que si le canal cible est détecté comme étant inactif. En fait, le CSMA/CA est un mécanisme efficace d'accès aux canaux lorsque les canaux cibles ne sont pas encombrés.

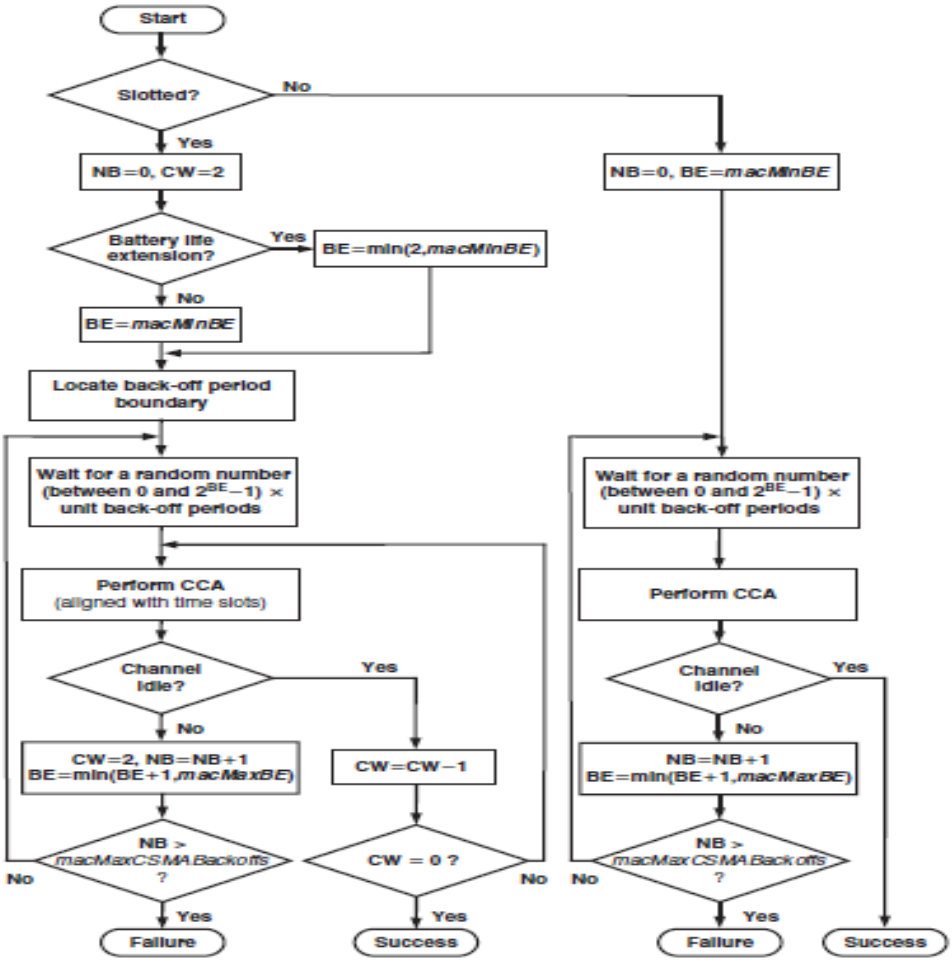


Figure III.17 : Algorithme de CSMA/CA [38]

III.3.9 La Pile

Zigbee est structuré en 4 couches : couche physique , couche MAC, couche réseau et couche application.

❖ La couche physique supporte la gestion des fréquences d'émission et de réception, le débit des données envoyées ou reçues, le type de modulation et le codage numérique des informations.

❖ La couche d'accès au médium ou MAC (Medium Access Control) s'appuie sur les ressources de la couche physique. C'est la couche principale pour les aspects logiciels qui définit la façon dont un nœud du réseau pourra dialoguer (transmettre ou recevoir)[40].

❖ La couche « Network » (NWK) est responsable de la topologie maillée (mesh networking) permettant à un nœud de communiquer à un autre grâce à un routage automatique. Elle fournit des mécanismes pour joindre, quitter et former un réseau, sécuriser le routage et la transmission des trames, identifier les chemins entre les

équipements connectés, découvrir le voisinage réseau, la gestion des types de services applicatifs, etc. Les paquets de la couche réseau peuvent être envoyés en unicast, broadcast ou encore multicast ;

❖ La couche « Application » (APL) est associée à plusieurs éléments :

- La sous-couche Application Support Sub-Layer (APS) assure l'interface entre la couche de réseau et la couche d'application à travers un ensemble de services. Elle gère le maintien des tables de routage, le transfert des messages entre les appareils reliés, le management des adresses, le mapping des adresses étendues de 64 bits en adresse de 16 bits pour la couche NWK, la fragmentation et réassemblage des paquets, ou encore dispose d'un mécanisme de multiplexage (cas de plusieurs applications sur la même adresse);

- L'Application Framework (AF) qui accueille les différents profils d'application. Elle propose également des API pour les développeurs. Chaque application dispose d'une adresse sur le nœud Zigbee comprise entre *0* et *255* ;

- Le module Security Service Provider (SSP) qui s'occupe de fournir des services de sécurité aux couches NWK et APS ;

- Le module Zigbee Device Object (ZDO) qui est responsable du management des équipements notamment pour la définition du rôle (coordinateur, routeur), de la découverte ou encore des services d'applications du dispositif qui seront fournis.

La figure suivante montre l'empilement de protocoles de Zigbee, réparties sur les couches précédemment décrites :

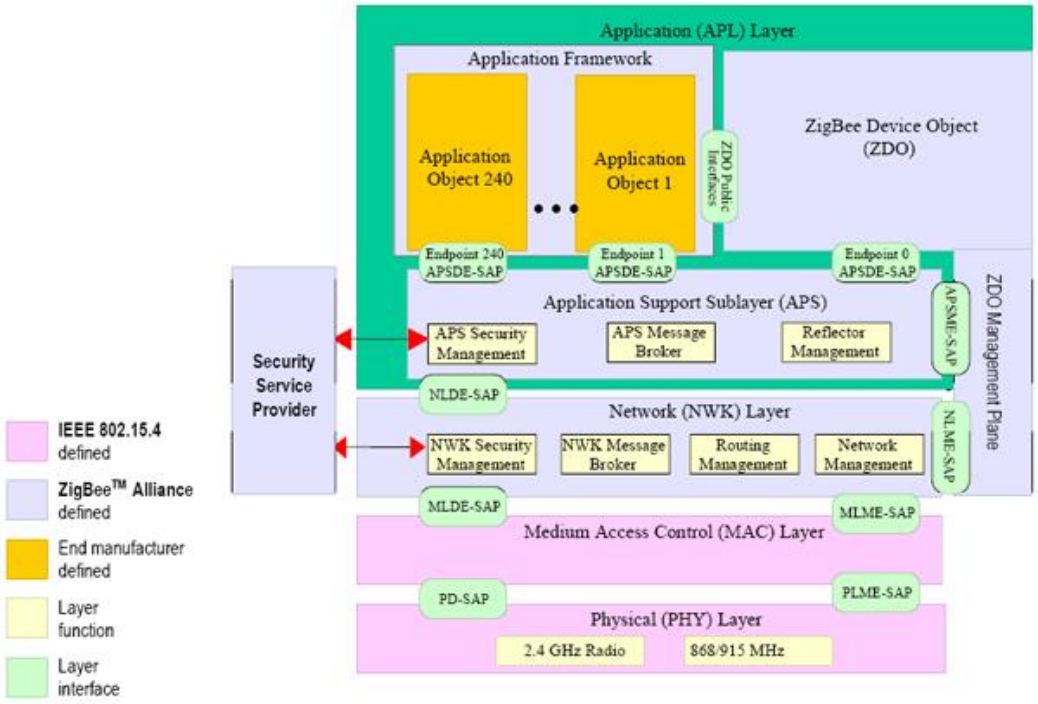


Figure III.18 : Pile Zigbee détaillée[34].

Chaque couche expose un certain nombre de services pour la couche supérieure et chaque service fournit une interface à la couche supérieure au travers d'un Service Access Point (SAP). Ces SAP offrent les API pour permettre aux couches de communiquer tout en isolant le travail interne à chacune des couches.

Le protocole Zigbee prévoit deux types d'objets :

- Les FFD (Full Function Device) implémentent toutes les spécifications du protocole. Ces derniers ont trois rôles possibles: coordinateurs (Zigbee Coordinator- ZC), routeurs (Zigbee Router- ZR) ou équipements finaux (Zigbee End-Device - ZED);

- Les RFD (Reduce Function Device) sont des équipements allégés qui sont peu gourmands tant au niveau énergétique qu e sur l'utilisation mémoire du microcontrôleur. Les équipements RFD sont donc des équipements finaux et ne peuvent être des coordinateurs ou routeurs.

III.3.10 Création d'un réseau

Dans un premier temps, le coordinateur cherche un canal utilisable qui n'interférera pas avec les fréquences en cours d'utilisation puis il envoie en broadcast via un message d'annonce (beacon) le numéro de PAN-ID choisi sur le canal sélectionné. Ce dernier doit être unique par canal pour les réseaux non capables de changements de canaux dynamiques et unique sur tous les canaux. Le coordinateur doit également inclure dans sa requête un numéro de PAN-ID étendu (EPID sur 8 octets) en supplément à l'ID-PAN afin de faciliter la sélection d'un réseau spécifique pour les nœuds qui vont s'y joindre.

III.3.11 Les avantages et les incontinents de Zigbee

III.3.11.1 Les avantage

- La configuration du réseau est très simple et facile, il ne possède pas de contrôleur central et les charges sont réparties uniformément sur le réseau ;
- Le protocole Zigbee est capable d'organiser (reconfigurer) le réseau automatiquement ;
- Il est facile de surveiller et de contrôler les appareils ménagers à distance ;
- Facilitant l'intégration des équipements entre eux ;
- Il remplacera les dispositifs basés sur la technologie infrarouge existants. Cela permettra de réduire les coûts de remplacement de la batterie, car Zigbee utilise une batterie au lithium qui dure longtemps ;
- Le réseau est évolutif et il est facile d'ajouter un dispositif final Zigbee / distant au réseau ;
- Consommation électrique très faible, ce qui permet aux appareils qui ont sources par batterie: capteur, moniteur, contrôleur, etc., de durer plus longtemps [34] ;

- Supporte un nombre élevé de nœuds (plus que 65000 nœuds peuvent coexister dans un réseau Zigbee, ce qui suffit à une grande maison avec plein d'appareil et capteurs Zigbee) ;
- Grande autonomie (parfois mesurable en mois ou en années) ;
- Faible coût ;
- Le temps de latence de Zigbee est court, environ 15 ms à 30 ms, ce qui garantit la transmission de donnée pour une gestion en temps-réel.

III.3.11.2 Les inconvénients

- La couverture est limitée et ne peut donc pas être utilisée comme système de communication sans fil extérieur. Il peut être utilisé dans les applications sans fil intérieures ;
- Faible débit de transmission de donnée (maximum 250 Kbps avec 2,4GHz) ;
- Faible portée ;
- La majorité des appareils Zigbee ne sont pas compatibles avec les autres protocoles de communication.

III.4 WiFi Vs Zigbee

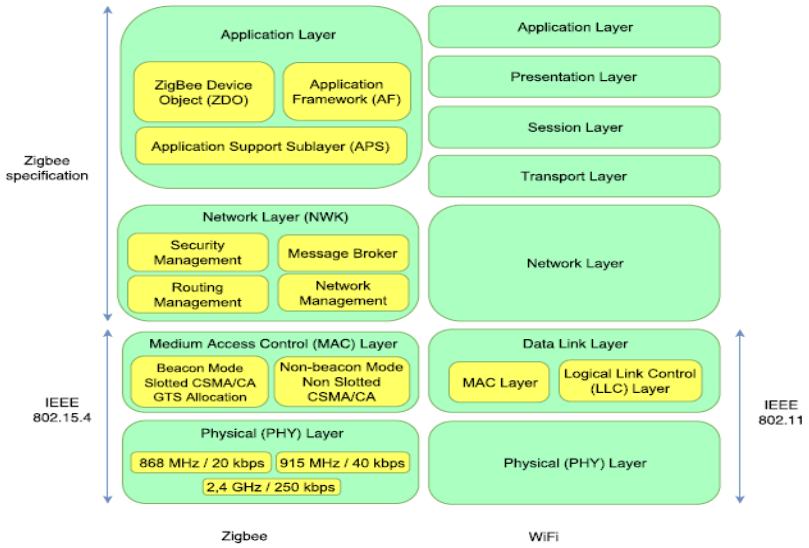


Figure III.19 : Zigbee versus WiFi protocol[49].

Comme on peut le constater sur la Figure III.19, la pile de protocoles de Zigbee diffère de celle utilisée par le WiFi. En réalité, les nœuds Zigbee utilisent les couches physiques (PHY) et de contrôle d'accès moyen (MAC) définies par le standard IEEE 802.15.4, tandis que les couches réseau et application sont couvertes par les spécifications données par Zigbee Alliance [32]. En revanche, le terme WiFi fait généralement référence aux technologies LAN (réseau local), englobant ainsi toutes les couches de la pile.

	Wifi	Zigbee
IEEE	802.11.(a/b/g/n …)	802.15.4
Mémoire	4-32 KB	+ 1 MB
Autonomie de la pile	Heures	1 Année (jusqu'à 2 ans duré de vie de batterie standard Alkaline)
Nombre de nœuds	32 nœuds	-Jusqu'à 65 000 nœuds par réseau -Jusqu'à 100 réseaux co-localisés (cluster)
Vitesses de transmission	Très haut (+Mb/s)	Moyen (250 kb/s)
Portée	Courte (300 m)	Courte (10-100 m)
Fréquence	2,4 GHz et 5 GHz	2,4 GHz
Sécurité	Authentication SSID, WEP	AES 128 bits et couche d'application définis par l'utilisateur
Avantage	Très Haut débit, qualité du signal assurée, connexion simple et rapide à la passerelle	Technologie peu consommatrice en énergie et s'intègre à bas coût dans les équipements
Inconvénients	Non adapté aux objets uniquement alimentés par batterie. Couverture réseau limitée à une faible zone autour de la passerelle. Une passerelle WiFi mal configurée expose le réseau à des failles de sécurité (man in the middle).	Couverture réseau limitée à une faible zone autour de la passerelle. Achat d'appareils spécifiques car la technologie n'est pas disponible dans les smartphones et ordinateurs.
applications	Adapté aux applications de domotique, au contexte indoor.	Adapté aux applications de contrôle de commandes dans les contextes bureautique et domotique.

Tableau III.2 : Comparaison entre WiFi et Zigbee[50,51]

La comparaison entre les technologies sans-fil va concerner d'autres aspects canaux de radio et fréquence.

- Les protocoles WiFi et Zigbee emploient les technologies à « spectre étalé » dans la bande 2.4 GHz, où le Wi-Fi utilise le DSSS à 14 canaux RF et 22 MHz de bande passante et le FHSS à 79 canaux et 1 MHz de bande passante, tandis que Zigbee emploi le DSSS à 16 canaux et 2 MHz de bande passante ;
- Le WiFi supporte le débit de transmission de 2Mbps à 600Mbps, la couverture est jusqu'à 100 m. Le Zigbee à différents débits de transmission pour les deux fréquences. Il est limité à20Kbps avec la portée maximale de 75 m en Europe, en attendant, aux États-Unis, le débit de données est jusqu'à 250Kbps pour approximativement 100 m ;
- Le protocole Zigbee soutient le réseau maillé, il a le nombre le plus élevé de nœuds maximaux qui dépassent 65 000. Le réseau WiFi, avec 32 nœuds ;
- Pour la sécurité, le wifi utilisé la méthode WPA2-PSK(AES) par contre le Zigbee utilisé la méthode AES-128 qui est un chiffrement par bloc à haute sécurité ;

➢ Le WiFi est conçu pour la communication à longue distance, en conséquence, une communication par WiFi consume plus d'énergie. Par contre Zigbee est conçu pour la communication à courte distance, il aun faible de consommation d'énergie [34].

III.5 Coexistence entre Zigbee et WiFi

Le WiFi et Zigbee se distinguent comme technologies de communication préférées pour les maisons intelligentes. Le WiFi est devenu très populaire, mais son application est limitée en raison de sa consommation d'énergie élevée et de l'absence de capacités de réseau maillé standard pour les appareils à faible consommation. Pour ces raisons, de nombreux fabricants ont choisi Zigbee pour développer des dispositifs de domotique sans fil. En conséquence, ces technologies peuvent coexister dans la bande des 2,4 GHz.

Lors du déploiement de WiFi et de Zigbee dans les mêmes environnements, une planification minutieuse doit être effectuée pour s'assurer qu'ils n'interfèrent pas les uns avec les autres.

La rareté du spectre est le principal obstacle à l'augmentation de la capacité des réseaux sans fil. Le partage du spectre est une solution à ce problème. Le spectre ISM est tellement encombré qu'il est partagé par différents réseaux sans fil. Le partage du spectre entre ces réseaux améliorera sûrement l'utilisation du spectre. Cependant, cela crée également un grand défi, en particulier la coexistence de protocoles MAC / PHY incompatibles.

Peut-être est-il essentiel que ces technologies coexistent avec un effet d'interférence minimal les unes sur les autres. Les canaux qui sont sujets à des interférence entre 802.11 et 802.15.4 sont illustrés à la figure III.20. cette figure montre que les canaux 15, 20, 25 et 26 ont une interférence minimale.

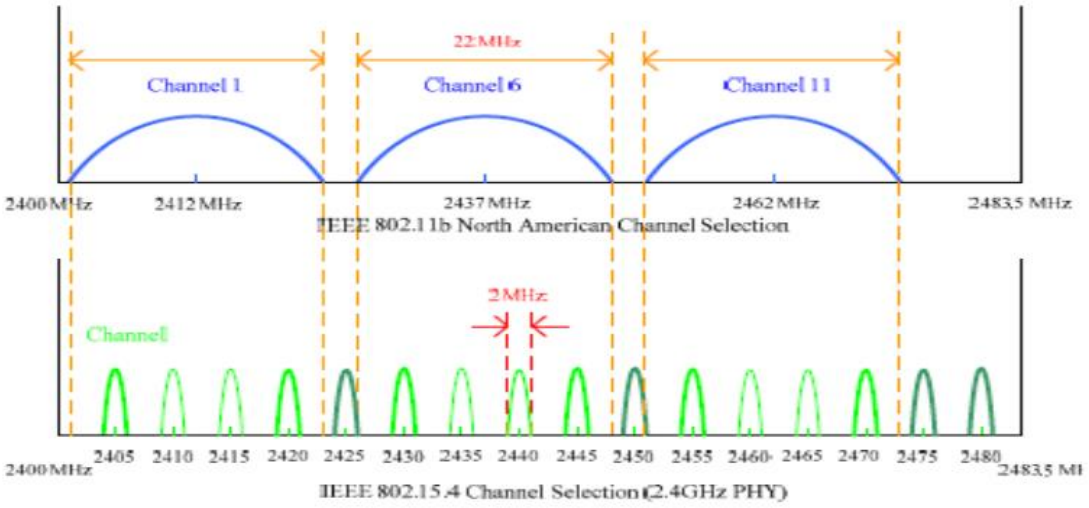


Figure III.20 : Les canaux WiFi et Zigbee dans la bande 2,4 GHz[41].

III.6 Conclusion

Les réseaux de capteurs sans fil sont utilisés pour la communication de données et sont généralement intégrés à des actionneurs pour mettre en œuvre les actions de commande à distance. Les technologies sans fil telles que Zigbee pour l'automatisation et le WiFi pour Internet fonctionnent dans la bande 2,4 GHz. La coexistence de différentes technologies sans fil fonctionnant dans la zone commune est inévitable.

Dans le prochain chapitre, nous allons étudier un des algorithmes de gestion de spectre dans la coexistence Zigbee et Wifi et l'intégrer dans un système de simulation en étudiant son applicabilité dans le domaine de la domotique.

Chapitre IV

Conception

IV.1 Introduction

Avec l'existence des réseaux de communication sans fil et leur demande croissante de transfert de données sans fil, la concurrence pour des ressources de spectre rares et la gestion des interférences devient un problème important.

En particulier, il est important de garantir que différentes technologies, ainsi que différentes applications prises en charge par la même technologie, coexistent et peuvent simultanément fonctionner de manière efficace.

Dans ce chapitre nous allons étudier la cohabitation des technologies WiFi et Zigbee à travers notre simulation basée principalement sur l'algorithme de gestion des interférences WiseBee et son application dans le domaine de la domotique.

IV.2 La conception globale

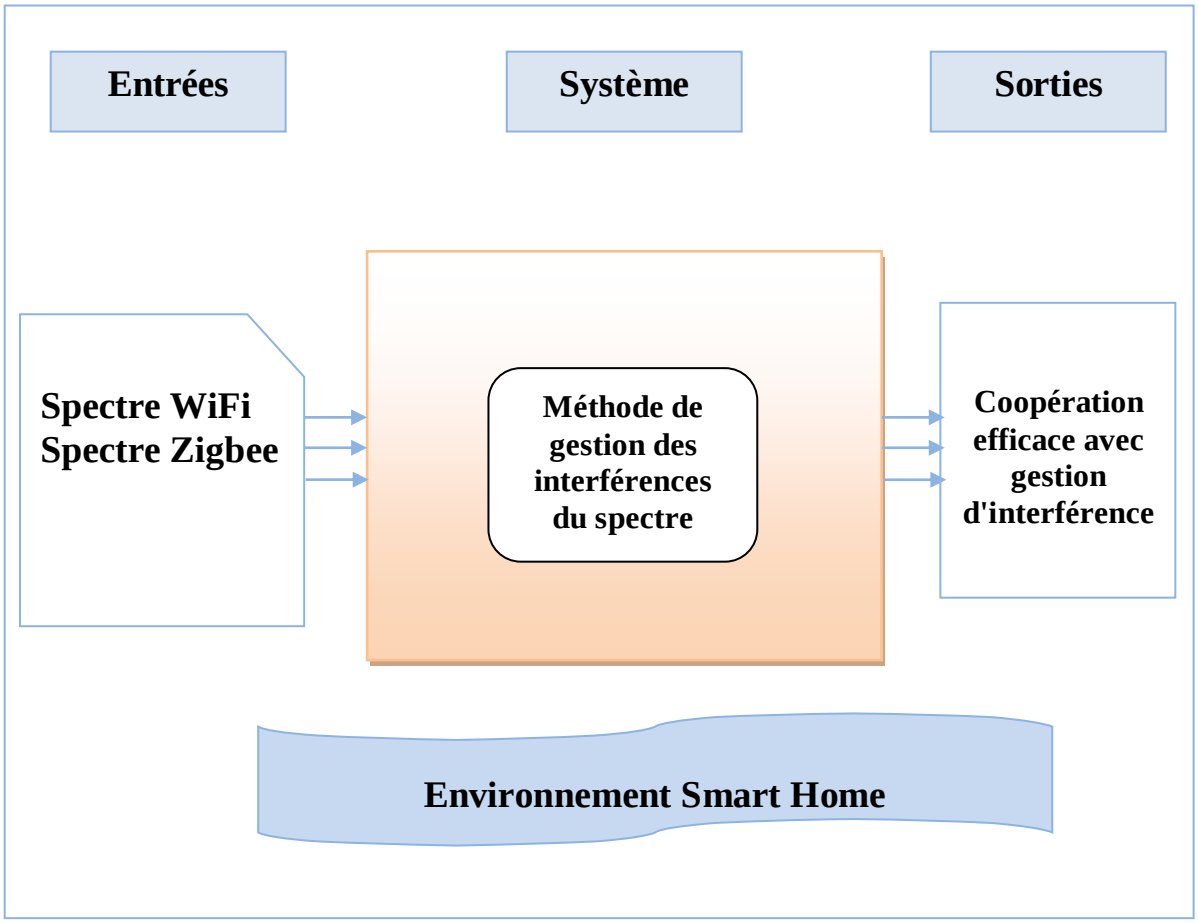


Figure IV.1 : Architecture globale du système.

IV.3 Conception Détaillée

IV.3.1 Entrées du système

L'entrée de notre système représente une simulation du spectre Zigbee et du spectre Wifi avec interférences cette simulation sera réalisée avec le logiciel de modélisation système multi-physique **simulink**.

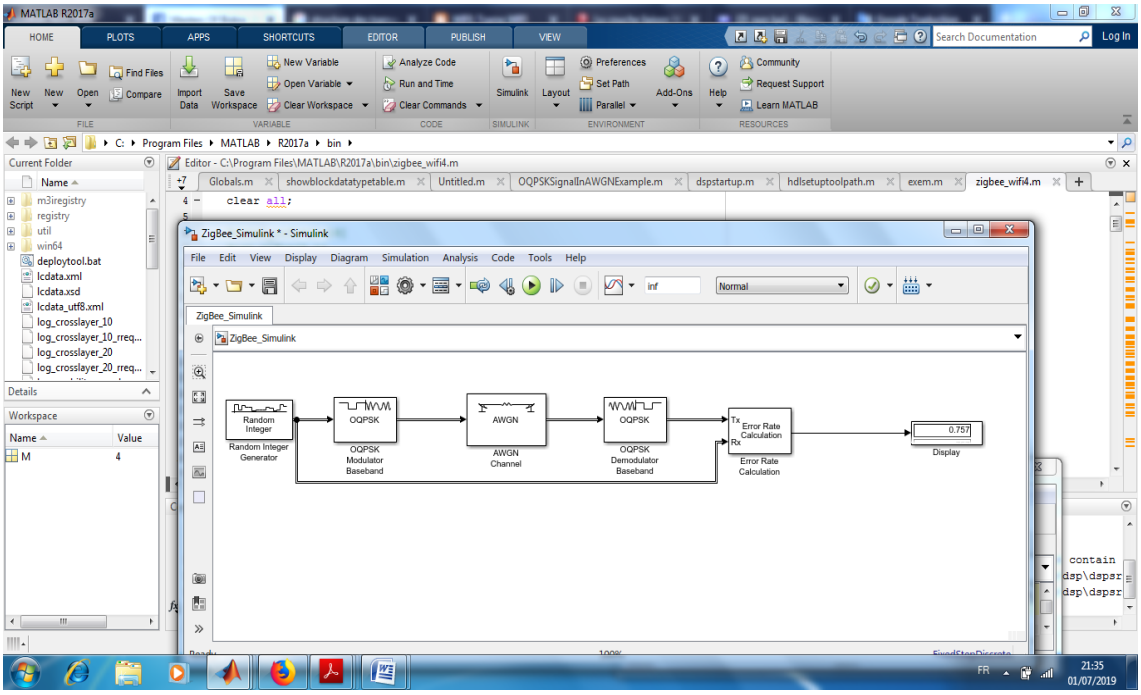


Figure IV.2 Simulink block for Zigbee.

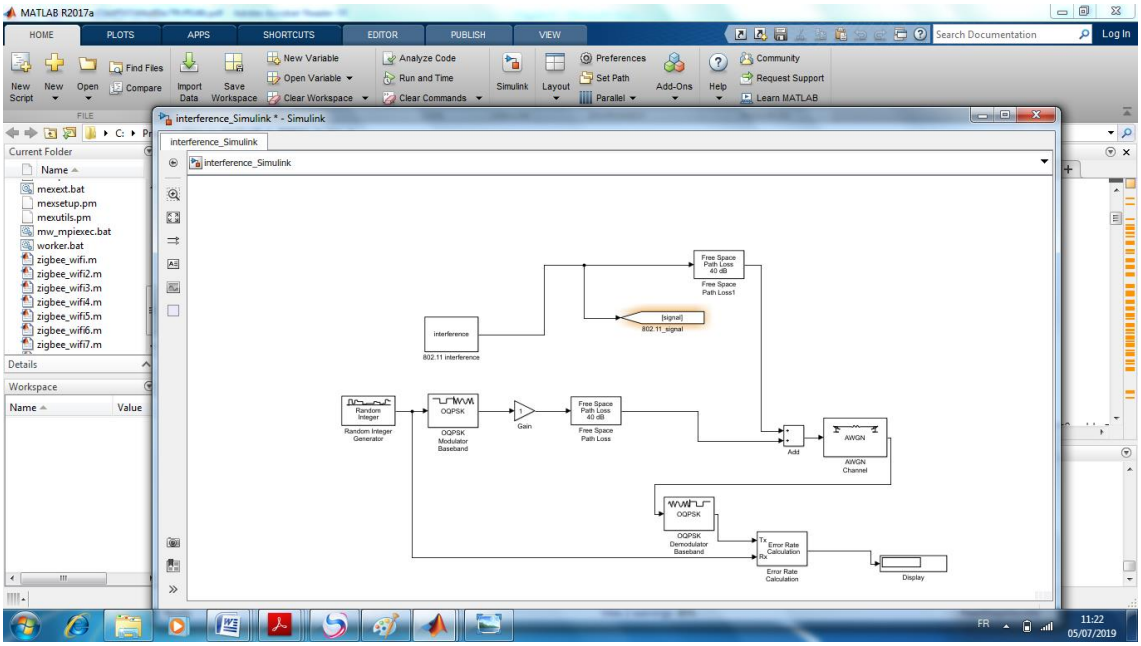


Figure IV.3 Simulink block for ZigBee with WiFi as interference.

IV.3.2 Module principal du système

Le module principal de notre système représente l'algorithme de gestion des interférences entre le WIFI (802.11) et Zigbee (802.15.4) WiseBee proposé dans les travaux de [54].

Presentation de l'Algorithme WiseBee

WizeBee est un noeud ZigBee dont la puissance d'émission est de 5 à 20 dB plus forte que le signal ZigBee en zone à risque d'interférence entre le WiFi et le ZigBee. Son rôle est d'écouter la communication dans le canal et de détecter une éventuelle interférence (collision) entre le signal ZigBee et le signal WiFi. Lorsque le WiseBee détecte une collision, il récupère l'ensemble des paquets transmis. Il annule ensuite les informations du WiFi et extrait la trame ZigBee. Enfin, il remet en forme les paquets ZigBee puis les retransmet sur le réseau.

f : décalage de fréquence.
$canal_w$: canal WwiFi
$canal_z$: canal Zigbee
Mn : auto corrélation
$X_w(t)$: valeur du signal WiFi
X_z (t): valeur du signal Zigbee
H_w : coefficient de canal WiFi
H_z : coefficient de canal Zigbee

```
Début
        Calcule_signal ()
        Detecter_inerference ()
        Si interference alors
                Detecter_WiFi()
                Démodulation _ WiFi()
                Annuler_inerference()
                Trouver_Zigbee()

            Transmettre le paquet Zigbee dans le canal
        Finsi

    Transmettre le paquet WiF dans le canal
    Transmettre le paquet Zigbee dans le canal
Fin
```

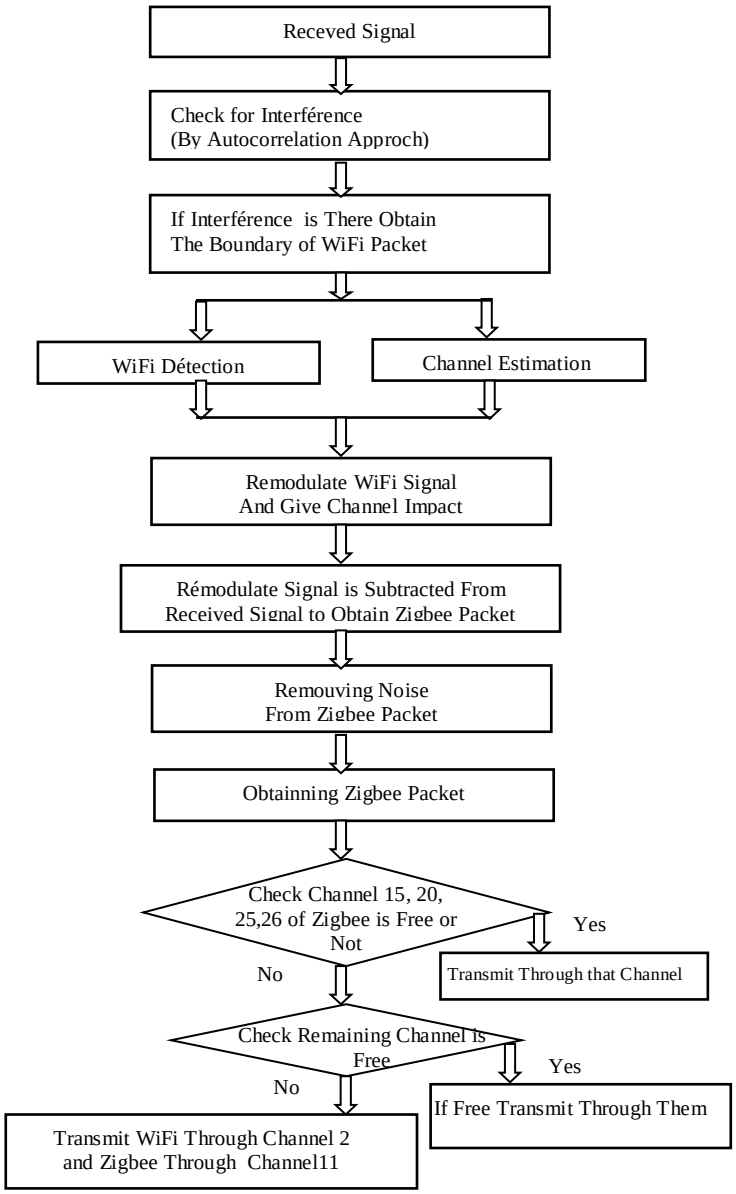


Figure IV.4 : Algorithme WiseBee.

IV.3.3 Sorties du système

Les sorties de notre système représentera une comparaison entre le BER(Bit Error Rate) et le SNR(Signal-to-Noise Ratio) du spectre Zigbee interférant avec wifi et le BER et SNR du spectre géré par l'algorithme WiseBee.

❖ Travaux Connexes

Différents mécanismes ont été adoptés pour améliorer la coexistence de Zigbee et du WiFi.

- les [52] ont mis au point un algorithme DSP appelé Common Multiple Folding (CMF) qui amplifie les signaux périodiques inconnus dans les échantillons d'intensité du signal reçu (RSS). Le principal avantage du CMF est qu'il peut minimiser les coûts de traitement des signaux inconnus dont les périodes possibles se situent dans une large plage. Nous développons ensuite un détecteur de taux de fausse alarme

constant (CFAR) qui peut minimiser le taux de faux négatif (FN) de classification des signaux périodiques en tant que balises 802.11 tout en satisfaisant la limite supérieure spécifiée par l'utilisateur pour le taux de faux positif.

- Le métronome est un autre système qui permet aux réseaux hétérogènes de bien coexister [53]. Metronome fournit un langage de politique flexible et expressif qui permet à l'opérateur de réseau de spécifier des contraintes sur les métriques de performance du récepteur, telles que le débit ou le taux de perte.

- L'algorithme CCS est proposé pour améliorer les performances de Zigbee fonctionnant sous l'influence du WiFi (IEEE 802.11b) fonctionnant sur une fréquence de 2,4 GHz. Le CCS comprend un ordonnanceur pour coordonner la signalisation avec le saut de canal temporaire pour la transformation de données Zigbee opérant à proximité du WiFi. L'annulation d'interférence successive (SIC) permet d'éviter les interférences au niveau de la couche physique et d'améliorer la réception des paquets du côté récepteur de Zigbee. En plus de SIC, le travail propose également le modèle d'optimisation pour l'identification de canaux précis [54] .

Nous déployons divers dispositifs dans Smart Home, dispositifs Zigbee et des dispositifs wifi. La distance entre les appareils wifi et Zigbee doit être supérieure à 2 m.

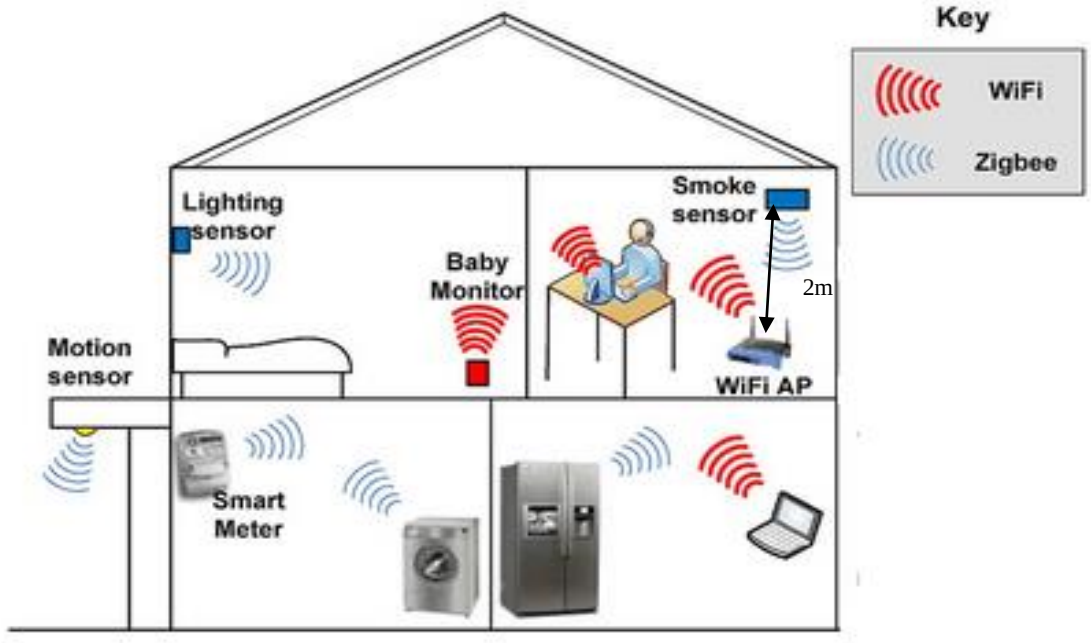


Figure IV.5 : Dispositif IoT dans domotique.

Dans ce travail, et pour résoudre le problème d'interférence entre le wifi et Zigbee nous propose de laisser une distance d'au moins 2 m afin de minimiser les interférences et nous déterminons le meilleur canal adapté à la transmission. On utilise algorithme où après avoir identifié le paquet WiFi présent, l'étape suivante consiste à obtenir la limite du paquet WiFi. La frontière peut être facilement obtenue car la puissance du WiFi et du paquet Zigbee est très variable.

Une fois que la limite du paquet WiFi est obtenue initialement, nous considérons le signal Zigbee comme un bruit de fond et un décodeur WiFi standard est utilisé pour décoder le paquet WiFi. Ensuite, le coefficient de canal est également estimé. Ensuite, le signal WiFi est remodulé et l'impact de canal lui est appliqué. Le signal ainsi obtenu est ensuite soustrait du signal mélangé. À partir du signal restant, nous pouvons extraire les paquets Zigbee.

- **Signal reçu**

Nous supposons d'abord qu'il n'ya pas d'interférence WiFi lors de la communication de Zigbee.

Supposons que X_z (t) soit la valeur échantillonnée du paquet Zigbee et que H_z soit le coefficient de canal correspondant de la transmission Zigbee.

Alors nous avons $y(t) = H_z X_z(t) e^{j2ft} + n(t)$;

Où y est le signal de réception, et *f* le décalage de fréquence centrale entre le WiFi et le signal Zigbee intéressé, et n(t) le bruit de fond.

La conception de découpage / combinaison de spectre comprend trois étapes: conversion de fréquence, filtrage FIR et ré-échantillonneur.

L'objectif de l'étape de translation de fréquence est de supprimer le décalage de fréquence *f*, ce qui peut être obtenu en multipliant le signal entrant par $e^{-j2\pi\delta ft}$. Nous pouvons utiliser $e^{-j2\pi\delta ft}$ y (t) pour extraire le paquet Zigbee. Pour améliorer le SNR du canal de réception Zigbee, nous avons ajouté un filtre FIR afin de filtrer les bruits indésirables hors de la bande.

Nous utilisons ensuite un bloc de ré-échantillonnage abaissant le taux d'échantillonnage pour améliorer la vitesse de décodage tout en conservant les informations de signal nécessaires.

- **Vérifiez les interférences**

Nous appelle le bloc d'annulation d'interférence uniquement s'il confirme que la transmission Wi-Fi commence.

Pour ce faire, nous adoptons l'approche standard d'auto-corrélation qui a été largement adoptée pour détecter les paquets WiFi pour la détection d'interférences WiFi. L'idée principale est d'exploiter des modèles répétés dans un symbole d'apprentissage court (STS) d'un paquet WiFi. L'auto-corrélation consiste à résumer les multiplications entre le signal reçu et sa forme retardée.

Soit rt le tième échantillon et L la longueur de la méta-répétition. La sortie d'auto-corrélation peut être représentée comme :

$$c_n = \sum_{k=0}^{L-1} r_{n+k} r^*_{n+k+L}, \qquad [55].$$

Où r t* est le conjugué du tième échantillon.
Pour obtenir un résultat normalisé, nous avons besoin de calculer

$$p_n = \sum_{k=0}^{L-1} r_{n+k+L} r^*_{n+k+L} = \sum_{k=0}^{L-1} |r_{n+k+L}|^2. \quad [55].$$

Le résultat final de l'auto-corrélation est $Mn=(C)^2/(P)^2$, ce qui signifie essentiellement la corrélation des échantillons actuels avec les échantillons précédents. Ce n'est qu'à l'arrivée d'un paquet realWiFi que la sortie de corrélation automatique Mn est sur le point d'approcher 1, car le paquet WiFi réel comprend dix séquences répétées. Sinon, le bruit randomisé ne donnerait pas une Mn élevée.

Pour la détection des limites de paquets WiFi, nous exploitons les informations de longueur de paquet incorporées dans le symbole SIGNAL au début d'un paquet WiFi. En outre, la diminution spectaculaire de puissance à la fin d'un paquet WiFi pourrait nous aider à vérifier la limite de paquets.

- **L'estimation du canal**

Est effectuée avec une approche de domaine de fréquence. L'estimation du canal peut être calculée comme suit:

$$\hat{H}_k = (R_{1,k} + R_{2,k}) X^*_k$$

Où $R_{1,k}$ et $R_{2,k}$ sont les symboles de formation longs (LTS Long Training Symbols) reçu, X_k est le LTS transmis, X_k est la forme conjuguée de X_k et H_k est la réponse de canal de la sous-porteuse k.

- **La démodulation** comprend le suivi d'erreur de phase, la décision de symbole, le décodage de Viterbi. Nous exploitons la "sous-porteuse pilote" pour le suivi d'erreur de phase. Une fois que le récepteur a effectué la synchronisation susmentionnée, nous utilisons une technique de décision souple pour déterminer quel est le symbole transmis le plus probable pour chaque symbole reçu.

Ensuite, le décodage de Viterbi est effectué pour obtenir les bits les plus probables.

Pour un décodage WiFi robuste, nous utilisons un algorithme de Viterbi. Il utilise des informations supplémentaires pour indiquer la confiance dans les décisions d'entrée et produit une estimation plus précise des codes transmis. Ce bon caractère nous permet de concevoir un décodage WiFi robuste.

Notez que, dans le domaine fréquentiel, le signal Zigbee ne peut interférer qu'une partie des sous-porteuses, et nous pouvons connaître les sous-porteuses exactes grâce au schéma de découpage précédent du spectre.

Profitant de ce mérite, nous attribuons différentes pondérations aux sous-porteuses. Pour les sous-porteuses interférées, le «bruit Zigbee» doit être évalué pour sa valeur SNR.

❖ **Estimation précise du coefficient de canal WiFi**

Pour estimer précisément H_w, nous utilisons les symboles de formation longs (LTS) connus au début d'un paquet WiFi.

L'algorithme d'estimation est appelé algorithme des moindres carrés, qui est largement utilisé en raison de sa faible complexité.

Notez que OFDM module les informations de bits dans le domaine fréquentiel (c'est-à-dire les sous-porteuses). Par conséquent, nous estimons la réponse en fréquence du canal en tant que valeur complexe pour chaque sous-porteuse. Supposons que

$X_m = (X_m [0] ,……, X_m [n - 1])$

Est le même symbole d'apprentissage utilisé dans les n sous-porteuses, et $Y_m[k]$ est la valeur correspondante de la $k^{ième}$ sous-porteuse.

La réponse en fréquence de chaque sous-porteuse k peut être représentée par:

$$\hat{H}_m [k] = \frac{Y_m [k]}{X_m [k]}$$

En pratique, plusieurs symboles sont utilisés pour l'estimation de canal et nous pouvons calculer la moyenne de toutes les estimations $\hat{H}_m [k]$

❖ **Annulation d'interférence**

La conception clé de WiseBee repose sur l'observation selon laquelle il est possible de décoder les paquets WiFi et Zigbee même quand ils accèdent au canal en même temps, car la force du signal du WiFi est supérieure de 5 à 20 dB à celle de Zigbee en raison de la puissance élevée, puissance d'émission.

Par conséquent, nous pouvons d'abord considérer le signal Zigbee comme un bruit de fond et appliquer un décodeur standard pour décoder les paquets WiFi. Avec suffisamment de SNR de signal WiFi, il est possible de décoder d'abord un paquet WiFi. Ensuite, nous remodulons le signal de transmission, ajoutons l'impact réel sur le canal et utilisons la technique de suppression des interférences (IC) pour soustraire le signal WiFi fort connu. Si nous pouvons atténuer le signal WiFi du signal mixte, nous pouvons utiliser le décodeur Zigbee standard pour extraire les paquets Zigbee.

Pour obtenir une précision plus grande de la récupération du signal, nous considérons le signal y (t) mélangé (en collision) et le sous-échantillonnons en utilisant la fréquence centrale avec la bande passante du système WiFi. Soit x_w (t) le signal du WiFi et x_z (t) la valeur du signal de Zigbee. Ensuite nous avons

$$y (t) = H_w x_w (t) + H_z x_z (t)\ e^{j2 f t} + n (t);$$

où H_w et H_z sont respectivement le coefficient de canal du WiFi et de Zigbee, n(t) est le bruit et *f* le décalage de fréquence centrale entre les signaux WiFi et Zigbee.

Lorsque $H_w x_w(t)$ est beaucoup plus grand que $H_z x_z(t)$, nous pouvons considérer $H_z x_z (t)\ e^{j2 f t} + n (t)$ comme un nouveau bruit N (t) et obtenir x_w (t) à l'aide du décodeur standard WiFi. Ensuite, nous re-modulons le signal WiFi sous la forme $S_w = \hat{H}_w x_w (t)$ et configurons une nouvelle formule comme suit:

$$Y(t) = y(t) - S_w = H_z x_z(t) e^{j2 f t} + n(t)$$

❖ **Transmettre le paquet Zigbee**

L'étape suivante consiste à transmettre le paquet Zigbee. La figure IV.3 montre les canaux WiFi et Zigbee dans la bande 2,4 GHz ISM. Les canaux 1, 6 et 11 sont les canaux WiFi les plus communs. Les canaux 15, 20, 25 et 26 de Zigbee sont ceux qui sortent des canaux qui ne se chevauchent pas. Nous vérifions donc initialement si ces chaînes sont libres ou non. Si l'un de ces canaux est libre, nous transmettons à l'aide de ce canal.

Si aucun de ces canaux n'est libre, nous vérifions les canaux restants de Zigbee, à savoir les canaux 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24.Si l'un de ces canaux est libre, nous transmettons à travers ces derniers, sinon nous adoptons une autre méthode. En plus du paquet Zigbee, nous avons aussi un paquet WiFi. Nous envoyons donc ce paquet WiFi via le canal 2 du WiFi.

Donc, le canal 1 du WiFi sera libre. Dans le canal 1 du WiFi se trouve le canal 11 de Zigbee. Ainsi, le paquet Zigbee peut être transmis via le canal 11 de Zigbee. Ici, nous avons sélectionné le canal 2 du WiFi car le nombre de canaux Wi-Fi qui se chevauchent est inférieur à celui obtenu si nous nous déplaçons au centre. Le principal avantage est que nous avons un paquet WiFi avec nous. Ainsi, il peut être utilisé pour transmettre le paquet Zigbee. Le paquet Wi-Fi servira de but de brouillage et permettra donc de transmettre le paquet Zigbee sans interférence WiFi.

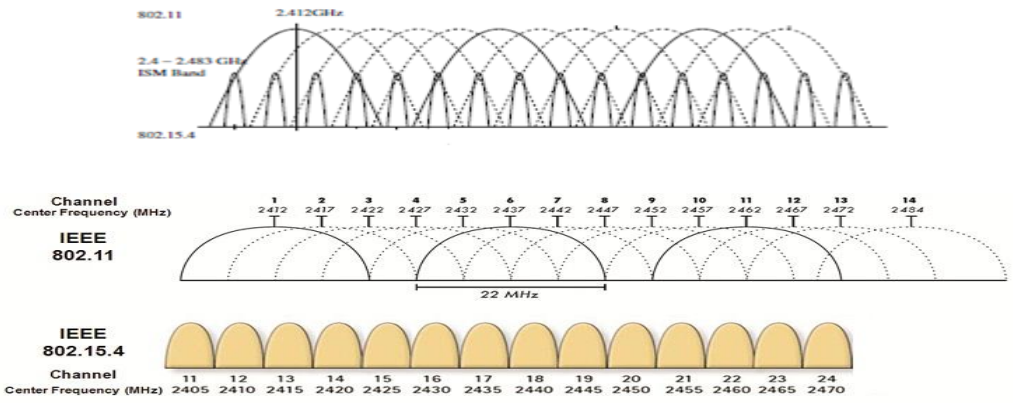


Figure IV.6 : Les canaux WiFi et Zigbee dans la bande 2,4 GHz.

IV.4 Conclusion

Dans ce chapitre nous avons présenté la conception du système qui est basé sur l'algorithme WiseBee qui permet de gérer l'interférence entre WiFi et Zigbee, et qui travaille sur la détermination du meilleur canal *adapté* à la transmission WiFi et Zigbee sans interférence pour une utilisation plus efficace du spectre.

Chapitre V

Implémentation

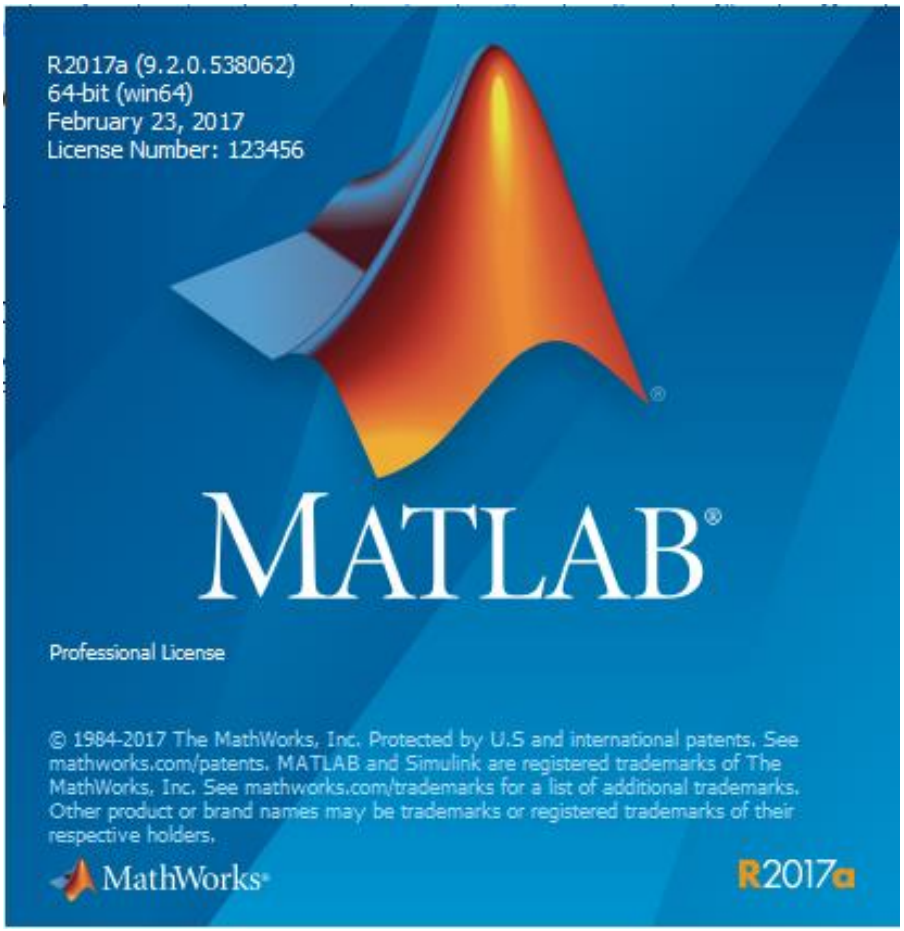
V.1 Introduction

L'implémentation de n'importe quel programme ou application nécessite un ensemble d'étape, qui joue un rôle très important à sa performance. L'une des étapes la plus importante l'environnement de travail, le choix de dernier doit être par conscience, selon les structures nécessaires à l'implémentation. Ainsi que les outils de travail qui facilitent la tâche de programmation et d'utilisation des données.

V.2 Environnement et outils de développement

V.2.1 Environnement de développement

Pour l'implémentation de l'algorithme du système WiseBee, nous avons choisi l'environnement MATLAB.



MATLAB est un logiciel de calcul numérique commercialisé par la société MathWorks1. Il a été initialement développé à la fin des années 70 par Cleve Moler, professeur de mathématique à l'université du Nouveau-Mexique puis à Stanford, pour permettre aux étudiants de travailler à partir d'un outil de programmation de haut niveau et sans apprendre le Fortran ou le C.

MATLAB est une abréviation de *Matrix LABoratory*. C'est un langage pour le calcul scientifique, l'analyse de données, leur visualisation et le développement d'algorithmes.

MATLAB trouve ses applications dans de nombreuses disciplines. Il constitue un outil numérique puissant pour la modélisation de systèmes physiques, la simulation de modèles mathématiques, la conception et la validation (tests en simulation et expérimentation) d'applications. Le logiciel de base peut être complété par de multiples toolboxes, c'est-à-dire des boîtes à outils. Celles-ci sont des bibliothèques de fonctions dédiées à des domaines particuliers. Nous pouvons citer par exemple : l'Automatique, le traitement du signal, l'analyse statistique, l'optimisation…

V.2.2 Outils utilisés

Simulink est une plate-forme de simulation multi-domaine et de modélisation de systèmes dynamiques. Il fournit un environnement graphique et un ensemble de bibliothèques contenant des blocs de modélisation qui permettent le design précis, la simulation, l'implémentation et le contrôle de systèmes de communications et de traitement du signal. Simulink est intégré à MATLAB, fournissant ainsi un accès immédiat aux nombreux outils de développement algorithmique, de visualisation et d'analyse de données de MATLAB.

V.2.3 Les algorithmes

La réalisation de ce travail est faite à l'aide de plusieurs de l'algorithme.

Algorithme1 : Algorithme réception Signal

H_z : coefficient de canal
X_z : valeur échantillonné de paquet Zigbee
f : décalage de fréquence.
Début
Calcule signal
Fin

L'utilisation de cet algorithme permet calculer le signal Zigbee

Algorithme2 : Algorithme détecté interférence

Mn : auto corrélation
Début
Calcule (Mn)
Si Mn ≅ 1 alors
WiFi existe
Finsi

Fin

L'utilisation de cet algorithme permet vérifier l'existence du signal WiFi

Algorithme3 : Algorithme Démodulation le signal WiFi

Début
Fonction Viterbi
Fin

L'utilisation de cet algorithme permet décoder le signal de WiFi, le décodage de Viterbi est effectué pour obtenir les bits les plus probables.

Fonction VITERBI

INPUT

- The observation space $O = \{o_1, o_2, \ldots, o_N\}$
- the state space $S = \{s_1, s_2, \ldots, s_K\}$
- an array of initial probabilities $\Pi = (\pi_1, \pi_2, \ldots, \pi_K)$ such that π_i stores the probability that $x_1 == s_i$
- a sequence of observations $Y = (y_1, y_2, \ldots, y_T)$ such that $y_t == i$ if the observation at time t is o_i
- transition matrix A of size $K \times K$ such that A_{ij} stores the transition probability of transiting from state s_i to state s_j
- emission matrix B of size $K \times N$ such that B_{ij} stores the probability of observing o_j from state s_i

OUTPUT

- The most likely hidden state sequence $X = (x_1, x_2, \ldots, x_T)$

```
function VITERBI(O, S, Π, Y, A, B) : X
    for each state i = 1, 2, ..., K do
        T1[i, 1] ← π_i · B_{i y_1}
        T2[i, 1] ← 0
    end for
    for each observation j = 2, 3, ..., T do
        for each state i = 1, 2, ..., K do
            T1[i, j] ← max_k (T1[k, j − 1] · A_ki · B_{i y_j})
            T2[i, j] ← arg max_k (T1[k, j − 1] · A_ki)
        end for
    end for
    z_T ← arg max_k (T1[k, T])
    x_T ← s_{z_T}
    for j = T, T − 1, ..., 2 do
        z_{j−1} ← T2[z_j, j]
        x_{j−1} ← s_{z_{j−1}}
    end for
    return X
end function
```

Algorithme4 : Algorithme Annulation d'interférence

$X_w(t)$: valeur du signal WiFi

X_z (t): valeur du signal Zigbee

H_w : coefficient de canal WiFi

H_z : coefficient de canal Zigbee

Début

Si $H_w x_w(t)$ >>> $H_z x_z(t)$ alors

ré-modulons le signal WiFi

trouver le signal Zigbee

Finsi

Fin

L'utilisation de cet algorithme permet d'annuler l'interférence et ré-module le signal WiFi et obtenue le signal Zigbee.

Algorithme5 : Algorithme Transmettre le paquet Zigbee

$canal_w$: canal WwiFi
$canal_z$: canal Zigbee
Début
Si $canal_{zi}$ € {15,20,25,26} est libre alors
Transmettre le paquet Zigbee dans le $canal_{Zi}$
Sinon
Si $canal_{zi}$ € {11,12,13,14,16,17,18,19,21,22,23,24} est libre alors
Transmit le paquet Zigbee dans le $canal_{Zi}$
Sinon
Transmettre le paquet WiF dans le $canal_{w2}$
Transmettre le paquet Zigbee dans le $canal_{Z11}$
Finsinon
Finsi
Finsinon
Finsi
Fin

L'utilisation de cet algorithme permet détermine du meilleur canal *adapté* à la transmission WiFi et Zigbee.

Conclusion générale

L'objectif de ce mémoire, était d'étudier les problèmes liés à la gestion des interférences entre le WiFi et le Zigbee dans l'IoT.

Dans ce projet, nous avons présenté la conception du système qui est basé sur l'algorithme WiseBee qui permet de gérer l'interférence entre le WiFi et le Zigbee. Où WiseBee est un nœud Zigbee dont la puissance d'émission est de 5 à 20 dB plus forts que le signal ZigBee en zone à risque d'interférence entre le WiFi et le Zigbee. Son rôle est d'écouter la communication dans le canal et de détecter une éventuelle interférence (collision) entre le signal Zigbee et le signal WiFi. Lorsque le WiseBee détecte une collision, il récupère l'ensemble des paquets transmis. Il annule ensuite les informations du WiFi et extrait la trame Zigbee et déterminer le meilleur canal adapté à la transmission.

Nous avons tous d'abord présenté dans le premier chapitre le concept et les différentes caractéristiques de l'internet des objets, et leurs défis, ainsi que ces domaines d'applications.

Ensuite, nous avons présenté quelque technique de l'IoT qui gère le spectre, et nous avons choisir deux technologies WiFi et Zigbee, et nous avons présenté la coexistence entre aux.

Après, nous avons présenté notre système qui est basé sur l'algorithme WiseBee qui permet de gérer l'interférence entre WiFi et Zigbee, et qui travaille sur la détermination du meilleur canal adapté à la transmission WiFi et Zigbee sans interférence pour une utilisation plus efficace du spectre.

Bibliographie

[1] Taleb Omar et Mankouri Abdelkrim, **Programmation de la sécurité Internet des Objet, Etude de cas module WIFI Electric imp**, Mémoire Pour l'obtention du diplôme de MASTER Spécialité: Réseaux et Systèmes de Télécommunication, Université Abou BakrBelkaid Tlemcen, pp 7-13, 2016.

[2] Rabeb Saad, **Modèle collaboratif pour l'Internet of Things (IoT)**, Mémoire de Maîtrise, Université du Québec à Chicoutimi, pp 16-19, Mai 2016.

[3] KARA Nadjah**, Conception d'un réseau de communication pour une maison intelligente en utilisant la technique d'internet des objets**, Mémoire de fin de cycle En vue de l'obtention du diplôme Master Professionnel en Informatique, Université A.MIRA - Bejaia, pp 13-29, 2017.

[4] Imad Saleh, **Internet des Objets (IdO): Concepts, Enjeux, Défis et Perspectives**, Article, Laboratoire Paragraphe, Université Paris 8, France, p 3, 2017.

[5] Ala Al-Fuqaha, MohsenGuizani, Mehdi Mohammadi, Mohammed Aledhari, Moussa Ayyash, Internet of Things: **A Survey on Enabling Technologies, Protocols, and Applications**, IEEE COMMUNICATION SURVEYS & TUTORIALS, VOL. 17, NO. 4, FOURTH QUARTER, pp 2347-2354, 2015.

[6] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, Marimuthu Palaniswami, **Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions**, University of Melbourne, Vic -3010, Australia , pp 2-4, 2015.

[7] Pierre-Jean Benghozi, Sylvain Bureau, Françoise Massit-Folea P.-J. Benghozi, S. Bureau, F. Massit-Folléa, C. Waroquiers, and S. Davidson, **L'internet des objets: quels enjeux pour l'Europe**, Éd. de la Maison des sciences de l'homme éd, pp 9-11, 2009.

[8] François Gerin et Jean-Pierre Hauet, **Internet des objets 2018**, Rapport principal, REE >Hors-série, pp 12-22,2017.

[9] Hidjeb Ali, **Implémentation d'un protocole détection d'un serveur d'authentification dans l'internet des objets**, Mémoire de fin de Cycle Master 2 Informatique Professionnel Option: ASR Administration et Sécurité des Réseaux, Université Abderrahmane Mira de Bejaïa, pp 16-17, 2017.

[10] Han Mei et Zhang Hang, **Business intelligence architecture based on internet of things**, Journal of Theoretical & Applied Information Technology, vol. 50, no. 1, pp 90-92, 2013.

[11] Atoumi Yanis et Bensadi Sonia, **Approche évolutionnaire pour la composition de services sensible à la QoS dans l'Internet des Objets à large échelle**, Mémoire de Master Recherche, Université Abderahmane Mira de Béjaia, pp 3-6, 2018.

[12] Rebah Asma, Meghouche Selma, **Méthodologie de la gestion d'un spectre et l'implémentation des points d'accès (AP) dans un réseau -Algérie Telecom Boumerdes**, Projet de fin d'étude En vue de L'Obtention Du Diplôme De Master En Recherche Opérationnelle, Université M'hamed Bougara Boumerdes, pp 27-32, 2016.

[13] Imen BEN CHAABENE, **Gestion du spectre des fréquences outils d'aide à l'assignation des fréquence,** Agence nationale des fréquences, p 4, Séminaire 1-2-3 juin 2009.

[14] EmnaTrigui, MoezEsseghir, Leila MerghemBoulahia, **Gestion dynamique du spectre entre terminaux radio cognitive mobiles**,CFIP 2011 - Colloque Francophone sur l'Ingénierie des Protocoles, Sainte Maxime, France, pp 6-15 , May 2011.

[15] Ibtissam Larbi et Badr Benmammar, **Négociation de spectre dans les réseaux de radio cognitive**, Rapport de recherche, Laboratoire de Télécommunications de Tlemcen (LTT) Université Abou BekrBelkaid Tlemcen Ibtissam Larbi, pp 7-13, Juin 2013.

[16] Rodney Martinez Alonso, David Plets, Ernesto Fontes Pupo, Margot Deruyck, Luc Martens, GlaucoGuillenNieto, and Wout Joseph, **IoT-Based Management Platform for Real-Time Spectrum and Energy Optimization of Broadcasting Networks**, Research Article, Information Technology, Ghent University, Gent 9052, Belgium R&D Telecom, LACETEL, Havana 19200, Cuba, pp2-4, July 2018.

[17] Asma Amraoui, Badr Benmammar, Fethi Tarik Bendimerad, **Utilisation des Enchères dans lesRéseaux Radio Cognitifs pour l'Accès Dynamique au Spectre**, Première Conférence Nationale sur les Télécommunications "CNT'2012", Guelma, Algeria, pp 3-4,Nov 2012.

[18] Bendella Med Saleh, **Gestion de spectre dans les réseaux de radio cognitive par la formation decoalitions**, Mémoire de fin d'études pour l'obtention du diplôme de Master en Informatique, Université Abou Bakr Belkaid– Tlemcen, pp 19-21, 2014.

[19] ORcommaking communications work for every one, **Review of the authorisation regime for spectrum access**, p 4, December 2017.

[20] Gao, Y; Qin, Z; Feng, Z; Zhang, Q; Holland, O; Dohler, M, **Scalable & Reliable IoT Enabled By Dynamic Spectrum Management for M2M in LTE-A**, Research Article, Queen Mary University of London pp 2-7, 2016.

[21] The Hashemite Kingdom of Jordan, **Telecommunications Regulatory Commission, Green Paper of "Internet of Things**", TRC, Jordan, pp 8-11, December 2017.

[22] Lin Zhang, Ying-Chang Liang, and Ming Xiao, **Spectrum Sharing for Internet of Things: A Survey**, the Centre for Intelligent Networking and Communications, University of Electronic Science and Technology of China, Chengdu, China, pp 2-6, October 2018.

[23] Mohieddine El Soussi, Pouria Zand, Frank Pasveer and Guido Dolmans, **Evaluating the Performance of eMTC and NB-IoT for Smart City Applications**, Holst Centre/imec, Eindhoven, The Netherlands, pp 2-4, November 2017.

[24] Christian Schellenberger, Marc Zimmermann, Hans D. Schotten, **Wireless Communication for Modular Production Facilities Draht los kommunikation fürmodulare Produktion sstätten**, Technische Universität Kaiserslautern, Kaiserslautern, Deutschland, pp 3-4, Avril 2018.

[25] Sergio Barrachina-Munoz, Boris Bellalta, Toni Adame, and Albert Bel, **Multi-hop Communication in the Uplink for LPWANs**, Dept. of Information and Communication Technologies Universitat Pompeu Fabra (UPF), Barcelona, pp 2-6, September 2017.

[26] Hamed Rahimi, Ali Zibaeenejad, Ali Akbar Safavi, **A Novel IoT Architecture ased on 5G-IoT and Next Generation Technologies**, Article, Department of Electrical and Computer Engineering, Shiraz University, Shiraz, Iran, 2018.

[27] OFCOM, **Update on 5G spectrum in the UK**, Article, 8 February 2017.

[28] Mmes Corinne Erhel et Laure de La Raudière, **L'internet des objets:le numérique à l'ère de la prédiction**, Rapport, France, p 105, 2016.

[29] Badr Benmammar, **Application des techniques d'enchères dans les réseaux de radio cognitive**, Rapport de recherche Laboratoire de Télécommunications Tlemcen, Université Abou BekrBelkaid, Tlemcen, Algérie, pp 6-12 ,2013.

[30] Jean-Pierre, Loïc Lenoir, **Internet des objets et logistique «Vers des nets avec des objets»**, Rapport, Ministère de l'Economie et des Finances, France, pp 3-4, Mars 2013.

[31] Matej TONIN (Slovénie), **L'Internet des Objets: Promesses et Dangers d'une Technologie de Rupture**, Sous-commission sur les tendances technologiques et la sécurité, pp3-6, 8 octobre 2017.

[32] KHERBACHE Zeynebet LARIBI Amina**, Étude de la Qualité de Service (QoS) dans les réseaux WIFI,** Mémoire de fin d'études Pour l'obtention du Diplôme de Master en Informatique, université Abou Baker BelkaidTelemcen,pp 20-32 **,** 2011.

[33] BELKADI Salim et ABAIDIA Abdelmadjid**, Planification des réseaux Wi-Fi par usage d'une apprche heuristique : Recherche Tabou,** Mémoire de fin d'études Pour l'obtention du Diplôme de Master en Informatique,Université LarbiTebassi – Tebassa, pp 17-29, 2016.

[34] ZHEN Zhao, **Étude des protocoles de communication pour les systèmes de gestion dans le contexte des réseaux intelligents**, mémoire présenté à l'université du QUÉBEC À TROIS-RIVIÈRES, pp 19-28, Mars 2017.

[35] Wahiba BOUHALI**, Optimisation D'une Chaîne de Transmission Vidéo sur Réseau IEEE 802.11g,** Mémoire de Fin d'Etudes pour l'Obtention du Diplôme de Master Recherche, Université Abderahmane MIRA – BEJAIA, 2012.

[36] *Mokri Karima Ikram et Sidhom Zineb,* **Evaluation des performances du réseau wifi en utilisant le simulateur OPNET,** Mémoire de fin d'études pour l'obtention du diplôme de Master en Informatique, Université Abou Bakr Belkaid– Tlemcen, pp 28-32, 2015.

[37] **Bouazzaoui Samira et Dekali Zahira, CONCEPTION DES RESEAUX SANS FILS IEEE 802.11 EN MODES INFRASTRUCTURE ET AD HOC,** Mémoire pour l'obtention du diplôme de Master en Télécommunications, Université Abou Bakr Belkaid– Tlemcen, pp 24-43, 2016.

[38] Shahin Farahani, ***ZigBee Wireless Networks and Transceivers,*** Book, Printed in the United States of America, 2008. http://www.chiaraburatti.org/uploads/teaching/ZigBee-Libro.pdf dernier visite 04/06/2019 à 19 :20.

[39] Najet Boughanmi, **Conception conjointe des systèmes contrôlés en réseau sans fil**, THESE pour l'obtention du Doctorat de l'Institut National Polytechnique de Lorraine, pp 43-60, 2011.

[40] Jackson Francomme, Férial Virolleau, Jiamin Pang, Yan Xin Phang, Thierry Val, **ZigBee, de la théorie à la pratique: création d'un réseau ZigBee avec transmission de données**, La Revue 3 E. I, Société de l'électricité, de l'électronique et des technologies de l'information et de la communication, vol.71, p 2,2013.

[41] Tulin Mangir, Lelass Sarakbi, Harvy Younan**, Analyzing the Impact of Wi-Fi Interference on ZigBee Networks Based on Real Time Experiments**, International Journal of Distributed and Parallel Systems (IJDPS) Vol.2, No.4, p 2, July 2011.

[42] https://blog.xebia.fr/2016/02/26/linternet-des-objets-2-connecter-vos-capteurs-aux-reseaux-iot, dernier visite 02/03/2019 à 21:39.

[43] http://www.smartgrids-cre.fr/index.php?p=objets-connectes-arcep, dernier visite 02/03/2019 à 21:45 .

[44] http://teachnuclear.ca/fr/tout-sur-le-nucleaire/le-rayonnement/spectre-electromagnetique/ dernier visite 27/01/2019 à 18 :06.

[45] 1https://www.itu.int/web/pp-18/fr/backgrounder/5g-fifth-generation-of-mobile-technologies dernier visite 04/02/2019 à 23 : 40.

[46] http://telecomreviewafrica.com/index.php/articles/divers/544-5g-optimisation-de-la-gestion-du-spectre dernier visite 04/02/2019 à 23 : 50.

[47] https://www.commentcamarche.net/contents/1285-transmission-de-donnees-dans-les-reseaux-sans-fils dernier visite 04/06/2019 à 18:20.

[48] https://moodle.utc.fr/file.php/498/SupportWeb/co/Module_RCSF_43.html dernier visite 04/06/2019 à 18:57.

[49] https://www.elprocus.com/what-is-zigbee-technology-architecture-and-its-applications dernier visite 10/04/2019 à 22:52.

[50] https://www.domotique-info.fr/technologies-domotique/zigbee dernier visite 12/04/2019 à 23:00.

[51] https://blog.xebia.fr/2018/08/29/iot-les-protocoles-de-communication-pour-les-reseaux-sans-fil-et-filaires-comment-choisir dernier visite 12/04/2019 à 23:30.

[52] Ruogu Zhou, Yongping Xiong, Guoliang Xing, Limin Sun, Jian Ma, **ZiFi: Wireless LAN Discovery via ZigBee Interference Signatures**, Aricle de recherche,Department of Computer Science and Engineering, Michigan State University, USA, 2010.

[53] R Gummandi, H. Balakrishnan, and S. Sehan,"**Metronome: coordinating spectrum sharing in heterogeneous wireless networks**", in Pro, pp 157-166, 2009.

[54] Vikram. K. and Sarat Kumar Sahoo, **A Collaborative Framework for Avoiding Interference Between Zigbee and WiFi for Effective Smart Metering Applications,** Article de recherche, Electrical Engineering, VIT University, Vellore VOL. 22, NO. 1, p 49, JUNE 2018.

[55] Sunil Jacob, Priyanka Ravi, **Enabling Coexistence of ZigBee and WiFi**, Communications on Applied Electronics (CAE) – ISSN: 2394-4714 Foundation of Computer Science FCS, New York, USA Volume 2 – No.6, August 2015.