

République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

UNIVERSITE ABOU BEKR BELKAID TLEMEN

FACULTE DE TECHNOLOGIE

DEPARTEMENT DE TELECOMMUNICATION



# MEMOIRE

Pour l'obtention du diplôme de

MASTER en

Réseaux Mobiles et Services de télécommunications

Réalisé par

*M<sup>lle</sup>. BOUABDALLAH Imane Karima*

*M<sup>lle</sup>. BOUDERBANE Yasmina*

THEME

Étude de la norme 802.11v dans les réseaux WLAN mobile  
sous l'environnement de simulation NS-3

Soutenu le 16/06/2015 devant le Jury :

Mr. Merzougui Rachid

Docteur, Université de Tlemcen

Président

Mr. Slimani Hicham

Docteur, Université de Tlemcen

Examineur

Mr. FEHAM Mohamed

Professeur, Université de Tlemcen

Encadreur

Mr. Benmoussat Chems Eddine

Docteur, Université de Tlemcen

Co-Encadreur

## *Remerciements*

*Nous exprimons notre reconnaissance et nos amples remerciements à notre encadreur Mr Benmoussat Chems Eddine ainsi qu'à Mr Faham Mohamed qui nous ont encouragées, guidées et soutenues tout au long de la préparation de notre mémoire, nous remercions également l'honorable jury qui a consenti à juger notre travail.*

*Nous souhaitons également exprimer notre profonde gratitude à nos familles et nos amis pour leur soutien indéfectible.*

*Enfin, nous remercions tous ceux qui de près ou de loin ont bien voulu nous encourager à accomplir ce travail.*

*Les modestes contributions apportées tout au long de ce travail en firent une expérience très intéressante et formidablement enrichissante.*

# Dédicace

Par la grâce d'Allah je dédie ce travail ...✍

## MAMAN

*Autant de phrases et d'expression aussi éloquentes soient-elles ne sauraient montrer le degré d'amour et de reconnaissance que j'éprouve pour toi Ma maman chérie. Ma conseillère, et amie fidèle, qui m'a assistée dans les moments difficiles, Tu représentes pour moi le symbole de la bonté par excellence, tu m'as comblée avec ta tendresse et affection tout au long de ma vie. Tu n'as cessé de me soutenir, de m'encourager et de prier pour moi durant toutes les années de mes études, tu as toujours été présente à mes côtés pour me consoler quand il le fallait.*

## PAPA

*Toutes les lettres ne sauraient trouver les mots qu'il faut, Tous les mots ne sauraient exprimer la gratitude, L'amour, le respect et la reconnaissance pour ton affection, pour tous les sacrifices consentis, pour l'éducation que tu m'as donnée et pour tous les efforts que tu ne cesses de fournir pour ma réussite.*

## MON ADORABLE SŒUR

*Ma très chère sœur NAZIHA, les mots ne me suffisent pas pour exprimer l'attachement, l'amour l'affection et la profonde tendresse que je te porte. Tes encouragements et ton soutien étaient la lumière dans l'obscur des moments difficiles. Que dieu le tout puissant te garde et te protège.*

## A MA TENTE TATI, ET SES FILS ROMAYSSA, ISLAM ET TOUTE LA FAMILLE DEBBAL

*Vous étiez toujours présents pour les bons conseils. Je souhaite que vous trouviez dans ce modeste travail ma reconnaissance pour tous vos efforts.*

*A ma grands mère MATIDJA qui ma tend soutenu avec ses prières.*

*A la mémoire de ma grand-mère hadja Yamna qui a été toujours dans mon esprit et dans mon cœur, je te dédie aujourd'hui ma réussite. Que Dieu, le miséricordieux, t'accueille dans son éternel paradis.*

## A MON TRES CHER BINOME IMANE

*Plus qu'un binôme, ma sœur, ma très chère amie, ma confidente, que j'adore et avec laquelle j'ai partagé les moments les plus difficiles, beaucoup d'émotion, de complicité dans notre travail scientifique et dans la vie quotidienne, mes sentiments restent éternels.*

**À MES AMIS DE TOUJOURS :** Ikram, Houda, Lyna, Malika, Fadia, Manine, Ilyes, Ismail.

Yasmina...

# *Dédicace*

*Je dédie ce modeste travail ;*

*A mon très cher Père qui a toujours répondu présent dans les moments les plus difficiles, son soutien et son courage, m'ont toujours donné la force de poursuivre mes études.*

*A ma douce Maman, qui a su me prêter l'attention, l'affection et l'amour qui m'ont permis d'écrire ce mémoire dans de bonnes conditions;*

*A la deuxième maman de la maison ma très chère sœur Lamia, ses conseils ont pu me guidé dans ma vie professionnelle tout comme ma vie personnelle, sa bonne humeur et son enthousiasme, me donne la joie de vivre;*

*A mon binôme Yasmina qui m'a supporté et avec qui j'ai passé des moments mémorables durant tout le temps d'accomplissement*

*Ainsi qu'à mes amis (es), auprès de qui, j'ai souvent trouvé réconfort et soutien;*

*A toute la famille ;*

*Merci à Vous Tous.*

*Melle Bouabdallah Imane Karima*

# **Table des matières**

## Table des matières

<i>Remerciements</i> .....	2
<i>Dédicace</i> .....	3
Table des matières .....	6
Acronymes .....	10
Liste des figures .....	15
Liste des tableaux .....	16
Liste des graphes .....	17
Introduction générale .....	19
Chapitre I : Introduction au standard 802.11v.....	22
I.1.    Introduction.....	22
I.2.    Le standard 802.11.....	24
I.2.1.  IEEE (Institute of Electrical and Electronics Engineers).....	24
I.2.2.  Standard 802.11 .....	25
I.3.    L'évolution du standard 802.11 .....	25
I.4.    Architecture 802.11 .....	30
I.5.    Principe de fonctionnement 802.11 .....	32
I.6.    Le standard 802.11/v wireless network management.....	37
I.7.    Principe de fonctionnement du 802.11v .....	38
I.8.    Application du standard 802.11v .....	39
I.9.    Conclusion .....	40
Chapitre II : Les caractéristiques du standard IEEE 802.11/v .....	42
II.1.   Introduction.....	42
II.2.   Augmentation du débit.....	42

II.2.1.	La technique MIMO.....	42
II.2.2.	Amélioration de la méthode d'accès CSMA/CA .....	42
II.3.	Localisation.....	43
II.3.1.	Les réseaux VANET .....	43
II.3.2.	Le GPS .....	45
II.4.	Consommation d'énergie.....	48
II.4.1.	Introduction.....	48
II.4.2.	Réseaux de capteur.....	48
II.5.	Conclusion .....	54
Chapitre III : État de l'art sur l'économie d'énergie .....		56
III.1.	Introduction.....	56
III.2.	Consommation d'énergie d'un nœud-capteur .....	56
III.2.1.	Formes de dissipation d'énergie .....	56
III.2.2.	Sources de surconsommation d'énergie .....	58
III.3.	Mécanismes de conservation de l'énergie .....	59
III.3.1.	Mode d'économie d'énergie .....	59
III.3.2.	Traitement local .....	60
III.3.3.	Organisation des échanges.....	60
III.3.4.	Limitation des accusés de réception .....	60
III.3.5.	Répartition de la consommation d'énergie .....	60
III.4.	Durée de vie d'un réseau .....	62
III.5.	Conservation d'énergie .....	62
III.6.	Techniques du Duty-cycling.....	63
III.6.1.	Protocoles Sleep/Wakeup .....	63

III.7.	Protocoles du niveau MAC.....	64
III.7.1.	Protocoles MAC reposant sur TDMA .....	65
III.7.2.	Protocoles MAC avec contention .....	66
III.7.3.	Protocoles MAC hybrides.....	68
III.7.4.	Techniques orientées données .....	69
III.7.5.	Acquisition de données efficace en énergie .....	70
III.7.6.	Techniques de mobilité.....	72
III.8.	Techniques de routage .....	73
III.8.1.	Définition du routage :.....	74
III.8.2.	Les protocoles de routage proactifs .....	74
III.8.3.	Les protocoles de routage réactifs .....	76
III.8.4.	Le routage hybride .....	79
III.9.	Principe de clustering.....	81
III.9.1.	Rayon des clusters .....	81
III.9.2.	Métrique de sélection des cluster-Heads .....	81
III.9.3.	Structure de l'ensemble des cluster-Heads.....	82
III.9.4.	Avantage de clustering .....	83
III.10.	Conclusion .....	83
	Chapitre IV : Analyse et résultats de simulation.....	85
IV.1.	Introduction.....	85
IV.2.	Présentation du simulateur ns-3.....	85
IV.2.1.	Outil de NS-3.....	86
IV.2.2.	Quelques possibilités de simulation en NS-3 .....	87
IV.2.3.	Modules présent en NS-3 .....	87



IV.2.4. Comparaison entre ns-2 et ns-3 .....	88
IV.3. Notre modèle.....	88
IV.4. Simulation et interprétation des résultats.....	89
IV.4.1. Économie de l'énergie .....	89
IV.4.2. Résultat obtenu après la simulation.....	89
IV.4.3. Augmentation du débit .....	93
IV.4.4. Résultat obtenu après la simulation du protocole OLSR .....	94
IV.4.5. Résultat obtenu après la simulation du protocole CBRP .....	95
IV.5. Conclusion .....	96
Conclusion générale .....	99
Références bibliographiques .....	101
Annexe.....	110

## **Acronymes**

**ACK** acquittement

**ADSL** Asymmetric Digital Subscriber Line

**AES** Advanced Encryption Standard

**AODV** Ad hoc On Demand Distance Vector

**AP** Access Point

**B-MAC** MAC Berkeley

**CBRP** Cluster Based Routing Protocol

**CDMA** Code division multiple access

**CDS** Connected Dominating Set

**CEDAR** Core Extraction Distributed for Adhoc Routing algorithm

**CMOS** Complementary Metal Oxide Semiconductor

**CPU** Central Processing Unit

**CRC** Chain Reaction Cycles

**CSMA/CA** Carrier Sense Multiple Access with Collision Avoidance

**CSMA/CD** Carrier Sense Multiple Access / Collision Detection

**CTS** Clear To Send

**DIFS** distributed Inter Frame Space

**DS** Dominating Set

**DSDV** Destination Sequenced Distance Vector

**DSR** Dynamic Source Routing

**DSRC** Dedicated Short Range Communication

**DSSS** Direct Sequence Spread Spectrum

**EARP** Energy Aware Routing Protocol

**ECN** Explicit Contention Notification

**FHSS** Frequency Hopping Spread Spectrum

**FSR** Fisheye State Routing

**GSM** Global system of mobile

**GSR** Global State Routing

**GPRS** General Packet Radio Service

**HAN** Home Area Network

**HCL** High Contention Level

**HEED** Hybrid Energy-Efficient Distributed clustering

**IEEE** Institute of Electrical and Electronics Engineers

**IR** infra-RED

**IS** Independent Set

**LAN** Local Area Network

**LAR** Location Aided Routing protocol

**LBT** Listen Before Talk

**LCL** Low Contention Level

**LEACH** Low-Energy Adaptive Clustering Hierarchy

**LED** Light-Emitting Diode

**LPL** Low Power Listening

**LSR** Link State Routing Protocol

**LWT** Listen While Talk

**MAC** Media Access Control

**MCU** Microcontroller Unit

**MIMO** Multiple Input Multiple Output

**MIS** Maximal Independent Set

**NAV** Network Allocation Vector

**NIC** Network Interface Card

**OBU** On Board Unit

**OFDM** Orthogonal Frequency Division Multiplexing

**OLSR** Optimized Link State Routing

**PAN** Personal Area Network

**PCF** Point Coordination Function

**PEGASIS** Power-Efficient Gathering in Sensor Information Systems

**QoS** Quality of Service

**RADIUS** Remote Authentication Dial-In User Service

**RLAN** Radio Local Area Network

**RSU** Road Side Unit

**RTS** Request To Send

**SIFS** Short Inter Frame Space

**SISO** Single-Input Single-Output

**S-MAC** Sensor MAC

**SSID** Service Set Identifier

**SSR** Signal Stability Routing

**STEM** Sparse Topology and Energy Management

**TC** Topology Control

**TCP** Transmission Control Protocol

**TDMA** Time Division Multiple Access

**TKIP** Temporal Key Integrity Protocol

**T-MAC** Timeout MAC

**TORA** Temporally Ordered Routing Algorithm

**TRAMA** Traffic Adaptive Medium Access

**UMTS** Universal Mobile Telecommunications System

**VANET** Vehicular Ad hoc Network

**WAN** Wide Area Network

**WCDS** Weakly Connected Dominating Set

**WEP** Wired Equivalent Privacy

**WIMAX** Worldwide Interoperability for Microwave Access

**WLAN** Wireless Local Area Network

**WPA** Wi-Fi Protected Access

**WPS** Wireless Position System

**WSN** Wireless Sensor Networks

**ZHLS** Zone-based Hierarchical Link State

**Z-MAC** Zebra MAC

# **Liste des illustrations**

## Liste des figures

Figure I.1: Couverture des réseaux sans fils. ....	23
Figure I.2 : Topologie ad-hoc. [Patrick,2011] .....	31
Figure I.3 : Topologie infrastructure. [Patrick,2011].....	31
Figure I.4 : Composant des couches du 802.11. [Anry, al ,2007].....	33
Figure I.5 : Déroulement de communications entre les stations émettrices et réceptrices. [Anry, al ,2007] .....	34
Figure I.6 : Echanges d'informations entre les stations. [Anry, al ,2007] .....	35
Figure I.7 : Algorithme du fonctionnement de CSMA/CA. [Anry, al ,2007].....	36
Figure II.1 : Composition du système GPS [Albert, 1998].....	45
Figure II.2 : Capteur sans fils. [Fares, al,2008].....	49
Figure II.3 : Architecture d'un capteur sans fils. [Fares, al,2008] .....	50
Figure II.4 : Exemple de représentation d'un réseau de capteurs. [Vijay, al, 2002]. .....	53
Figure III.1 : (a) - Transmissions directes. (b) - Transmission saut par saut. (c) - Hiérarchisation en clusters.....	61
Figure IV.1 : Les modules présents dans NS-3. [Oxygen, 2011]. .....	87
Figure VI.1 : Table des membres .....	111
Figure VI.2 : Table des chefs de groupe (cluster Head) .....	111
Figure VI.3 : Table de la passerelle (gateway) .....	111

## **Liste des tableaux**

Tableau I-1 : Caractéristiques du standard 802.11 .....	40
Tableau IV-1 : Comparaison entre ns2 et ns3 .....	88



## Liste des graphes

Graphe IV-1 : Résultat du modèle d'énergie Basic energy model .....	90
Graphe IV-2 : Résultat du modèle d'énergie Rv battery model .....	91
Graphe IV-3 : Résultat du modèle d'énergie Energy source container .....	92
Graphe IV-4 : Résultat du modèle d'énergie Wifi radio energy model.....	93
Graphe IV-5 : Résultat du protocole OLSR appliqué sur une variété de nœuds .	94
Graphe IV-6 : Résultat du protocole CBRP appliqué pour une variété de nœuds .....	95
Graphe IV-7 : Résultat du protocole CBRP et le modèle d'énergie appliqué dans la couche MAC pour 40 nœuds .....	96

# **Introduction générale**

## **Introduction générale**

Au cours des dernières années, la technologie de l'information et de la communication (TIC) a connu une grande évolution et une large utilisation de notre vie quotidienne.

La révolution informationnelle est due principalement au développement fulgurant des technologies de l'information qui permettent actuellement le traitement, le stockage et la transmission d'énormes quantités de données quasiment en temps réel. En plus, la numérisation des données et l'élaboration de nouveaux standards et de nouveaux composants électroniques de plus en plus petits et de plus en plus performants, ont permis aux réseaux de devenir numériques, sans fil et mobiles.

Les WLAN offrent aux utilisateurs la possibilité de se déplacer tout en restant connecté dans la zone de couverture du point d'accès. Ces réseaux sont faciles et rapides à déployer et permettent la transmission de données et d'autres applications.

Nous commençons d'ailleurs à les trouver partout : dans les aéroports, les hôtels, les bureaux et ainsi que dans les environnements domestiques. Les entreprises et les gouvernements déploient les réseaux sans fils qui, grâce à leurs simplicités et souplesse d'une part, ainsi que leur coût et leur débit d'autre part, rendent l'accès au réseau plus confortable aux utilisateurs. En effet, les équipements sans fil sont moins chers comparés au filaire et permettent d'économiser le coût de câblage dans les bâtiments. Cependant, l'utilisation de ces réseaux est très efficace pour les services de données et elle doit être optimisée pour les services de la voix ou de la vidéo.

Cependant, comme les utilisateurs sont de plus en plus exigeants en termes de mobilité, et d'énergie, une idée est récemment adressée par les chercheurs. Cette idée a donné naissance à un nouveau standard dans la norme de wifi qui est l'IEEE 802.11v.

En effet, le standard IEEE802.11v est une amélioration de la gestion de la norme IEEE 802.11 b. Ils ont le même principe de fonctionnement, pour mieux s'adapter aux besoins des utilisateurs le IEEE802.11v apporte de nouvelles caractéristiques qui sont : la localisation, l'augmentation du débit et l'économie d'énergie.

Une telle amélioration est assistée par un réseau d'économies d'énergie qui aide les clients à améliorer la vie de la batterie en leur permettant de dormir plus longtemps. À titre d'exemple, les appareils mobiles utilisent généralement une certaine quantité de temps de repos pour assurer qu'ils restent connectés aux points d'accès et consomment donc plus de puissance lors de l'exécution des tâches suivantes que dans un réseau sans fil.

Une autre amélioration est assistée par un réseau d'itinérance qui permet au Wifi d'envoyer des demandes de clients qui sont associés au point d'accès et de les conseiller. Ceci est utilisé à la fois pour l'équilibrage de charge et de diriger les clients mal connectés.

Objectifs de notre recherche est de définir et de combiner un meilleur protocole de routage et un modèle d'énergie sous l'environnement de simulation NS-3( Network Simulator 3) , pour satisfaire les exigences des clients en matière de débit et d'économie d'énergie.

# **Chapitre I**

**Introduction au standard 802.11v**

# Chapitre I : Introduction au standard 802.11v

## I.1.Introduction

Le domaine de la télécommunication a connu ces 20 dernières années des évolutions considérables dans le monde en générale et dans les pays en voie de développement en particulier. Il est indéniable que cette évolution, passe par les systèmes de communication sans fils (*basés essentiellement sur la transmission radio*) qui, se démarquent de plus en plus des autres systèmes de communication à travers les diverses recherches et investissements menés par les différents laboratoires et organismes spécialisés dans le domaine, qui poussent de plus en plus leurs recherches afin de développer des technologies encore plus innovantes dans ce secteur depuis la fin des années 1980. Notre soif de largeur de bande sans fil et la déréglementation ont joué un rôle important à la naissance d'un ensemble de stations fixes ou mobiles, interconnectées par un réseau local de communication radio c'est ce qu'on appelle un réseau sans fil.

Le réseau sans fil couvre plusieurs zones

- ***PAN (Personal Area Network)***

Réseau individuel sans fil

Faible portée (quelques dizaines de m)

Permet la connexion de périphériques (PDA, imprimante d'ordinateurs...)

**Ex :** Bluetooth, ZIGBEE

- ***HAN ( Home Area Network) Ex :***

Home RF

- ***LAN (Local Area Network) Réseau local d'entreprise***

Couvre l'équivalent d'un réseau local d'entreprise (100 m)

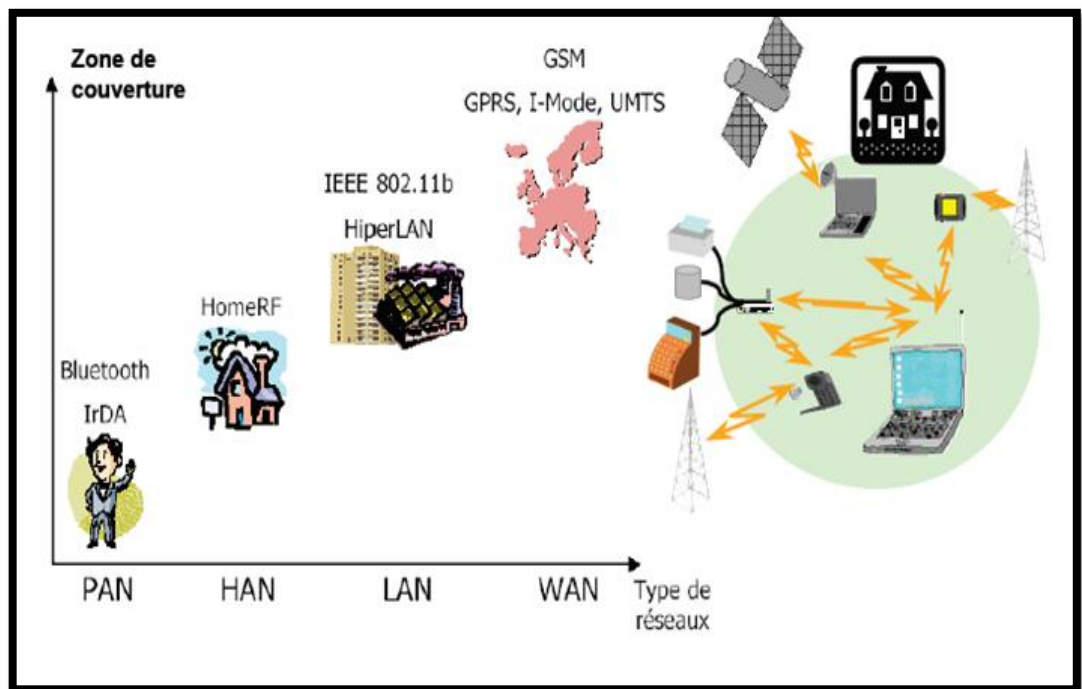
Relie entre eux les équipements présents dans la zone de couverture **Ex:** DECT, IEEE 802.11

- **WAN (Wide Area Network) Réseau étendu sans-fil**

Plus connu sous le nom de « réseaux cellulaire mobile »

Utilisé par les téléphones mobiles **Ex :** GSM, GPRS, UMTS, CDMA, Satellites.

[Cristian, 2006]



**Figure I.1: Couverture des réseaux sans fils.**

Le réseau sans fil utilise deux modes de transmissions :

- **Une transmission unidirectionnelle (point à point)**

Elle a une portée importante et une vitesse assez élevée les avantages qu'elle apporte c'est la rareté des interférences et la confidentialité, elle est utilisée pour interconnecter entre deux bâtiments sans passer par un opérateur privé. [Anry, al ,2007]

➤ **Une transmission omnidirectionnelle (point à multipoint)**

Sa portée et sa vitesse et assez faible par rapport à la transmission unidirectionnelle, les interférences sont assez fréquentes et la confidentialité n'est pas très satisfaisante, elle est utilisée afin de gérer un parc de portables. [Anry, *al*, 2007]

Les technologies de réseaux-locaux sans-fil se démocratisent notamment grâce aux offres Internet grand public.

- Facilité d'utilisation
- Sécurité
- Mobilité
- Topologie dynamique
- Facilité d'installation
- Coût

Malheureusement, il existe un nombre d'inconvénients liés au déploiement d'un réseau sans fil. Le choix des fréquences pose un problème de compatibilité entre les différents pays. Ces fréquences peuvent être réservées pour des utilisations militaires ou des services de secours.

La totalité de la bande n'est donc pas disponible pour les équipements RLAN (Radio Local Area Network). [Bruno, 2006]

## **I.2. Le standard 802.11**

### **I.2.1. IEEE (Institute of Electrical and Electronics Engineers)**

Les normes IEEE sont élaborées par les comités techniques des sociétés IEEE et par les comités de coordination des normes de l'IEEE Standards Board. Toute norme élaborée à l'IEEE représente un consensus des vastes compétences sur le sujet réunies au sein de l'Institut, ainsi que des activités extérieures à l'IEEE qui ont souhaité participer à l'élaboration de la norme.

En 1990 l'IEEE a lancé le projet de création d'un réseau local sans fil dans le but d'offrir une connectivité sans fils a des stations fixe ou mobile qui demande un



déploiement rapide au sein d'une zone local on utilisant différentes bandes de fréquences.

L'apparition du premier standard internationale (IEEE802.11) pour les réseaux locaux sans fils était en 2001. *[Le comité, 1993]*

### **I.2.2.Standard 802.11**

À l'origine fut un premier standard 802.11 tout court, ratifié en 1997, pour émettre dans la bande 2,4 GHz. Il prévoyait trois types de partage du média : FHSS, DSSS et IR (infrarouge). Le protocole d'accès CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), technique issue d'Ethernet sera conservé sur toutes les évolutions du standard. Ce standard annonçait un débit théorique de 1 ou 2 Mbits/s selon le type de modulation. L'infrarouge, peu performant, fut rapidement classé sans suite.

Le FHSS (Frequency Hopping Spread Spectrum) et le DSSS (Direct Sequence Spread Spectrum) sont tous deux basés sur une large utilisation du spectre par le signal à émettre, d'où la notion d'étalement. En FHSS, chaque communication utilise un canal de 1 MHz et l'étalement se fait en faisant varier périodiquement la position de ce canal sur la largeur du spectre alloué. Bien que présentant pas mal d'avantages, notamment au niveau de l'immunité au bruit, le FHSS ne permet pas d'évoluer vers de très hauts débits et fut rapidement abandonné.

Le DSSS prévoit un étalement du signal sur un canal de 30 MHz en le multipliant par un code donné (chipping code). Le DSSS permet d'évoluer vers de plus hauts débits. *[Anry, al ,2007]*

### **I.3. L'évolution du standard 802.11**

802.11 est un ensemble de standards qui régissent les transactions sur les WLAN. Chaque standard ou sous standard est désigné par une lettre de l'alphabet. Ceci ne correspond pas à une appellation empirique, mais désigne le groupe de travail chargé l'IEEE de l'étude et de la publication d'un standard ou sous standard de la famille 802.11. *[Michèle, 2012]*

➤ **802.11/a HIGHER SPEED PHY EXTENSION IN THE 5GHZ BAND (1999)**

Moins connu que son frère 802.11b, 802.11a fut ratifié en 1999, mais les premiers produits n'apparurent qu'en 2002. Contrairement au standard d'origine, il émet dans la bande 5 GHz, bien moins encombrée que la bande 2,4 GHz. Autre variante avec le standard d'origine, l'accès au média se fait en OFDM (Orthogonal Frequency Division Multiplexing). L'OFDM répartit le signal à émettre sur différents canaux radio. Le signal occupe ainsi toute la largeur du spectre, mais par petits morceaux. Chaque canal est modulé sur des porteuses orthogonales. Cette technique permet d'utiliser des porteuses qui se chevauchent sans interférer et ainsi de faire passer plus de canaux dans une largeur de bande donnée. Sur de telles bases, 802.11a annonce des débits théoriques de 54 Mbits/s. [Michèle, 2012]

➤ **802.11/b HIGHER SPEED PHY EXTENSION IN THE 2.4 GHZ BAND (1999)**

Frère jumeau de 802.11a, puisqu'il fut également ratifié en 1999, 802.11b se développa plus rapidement et les premiers produits apparurent en 2000.

Beaucoup plus proche du standard 802.11 d'origine, il reprend la bande de fréquences 2,4 GHz et le DSSS. Une amélioration des techniques de modulation lui permet d'atteindre des débits théoriques de 11 Mbits/s. Lorsque les conditions de transmission se dégradent, la modulation courante se replie automatiquement vers une autre de performances inférieures, le processus pouvant se répéter jusqu'au repli vers la modulation et les performances du 802.11 DSSS original. Bien sûr, il se produit la même chose en sens inverse, la modulation devenant plus performante au fur et à mesure que les conditions de transmission s'améliorent.

L'édition b de 802.11 connut très rapidement un vif succès et pour mettre fin à l'anarchie des implémentations du standard, la Wi-Fi Alliance (initialement WECA)

édita des règles propres à garantir l'interopérabilité des équipements. C'est alors qu'on commence à parler de Wi-Fi. [Michèle, 2012]

➤ **802.11/g FURTHER HIGHER DATA RATE EXTENSION IN THE 2.4 GHZ BAND (2003)**

Nous avons vu que 802.11b était limité à des débits théoriques de 11 Mbits/s et qu'une amélioration sensible du débit était obtenue par 802.11a. Ce dernier n'a pas eu un développement foudroyant, en partie à cause des limitations d'émission dans la bande 5 GHz, mais surtout à cause de son incompatibilité totale avec 802.11b, rendant impossible la migration des réseaux existants.

Une alternative fut trouvée avec 802.11g, ratifié en 2003. Cette nouvelle version du standard fonctionne dans la bande 2,4 GHz, comme 802.11b, mais utilise l'OFDM comme 802.11a, ce qui lui permet d'atteindre le même débit théorique de 54 Mbits/s (toutefois les débits utiles restent inférieurs à ceux de 802.11a). Un Access Point 802.11g sait gérer bien sûr des terminaux 802.11g mais sait se replier en mode 802.11b pour supporter des terminaux de génération antérieure. Cette particularité permet donc une migration « en douceur » des réseaux, sans avoir à intervenir immédiatement sur le parc de terminaux.

Depuis sa ratification, 802.11g s'est imposé sur le marché pour améliorer les performances des réseaux sans fil. Sa prise de position massive a évidemment été facilitée par sa compatibilité avec les équipements 802.11b. [Michèle, 2012]

➤ **802.11/i MAC SECURITY ENHANCEMENTS (2004)**

Très attendu fut aussi 802.11i qui introduit des mécanismes avancés de sécurité dans les réseaux 802.11.

Le standard 802.11 ne prévoyait qu'un mécanisme de sécurité plutôt faible, le WEP, qu'un hacker bien entraîné pouvait « casser » en un quart d'heure. Cette fâcheuse caractéristique fut bientôt contournée par des solutions propriétaires, bien sûr

incompatibles, et l'IEEE revit sa copie sur la sécurité. Dans une première phase, apparut un protocole WPA-1 (Wi-Fi Protected Access), basé sur une authentification forte RADIUS et le protocole de gestion de clés TKIP, permettant d'améliorer l'ancien WEP. Les équipements WEP ne nécessitent qu'une mise à jour logicielle pour passer en WPA-1.

La seconde version WPA-2 est le résultat du processus de standardisation 802.11i qui est l'aboutissement du processus de sécurisation du Wi-Fi. Il reprend les grandes lignes de WPA-1 mais avec un mode de chiffrement AES, beaucoup plus puissant. L'envers de la médaille est que les anciens équipements WEP doivent subir une mise à niveau matérielle pour supporter WPA-2, par contre les équipements natifs WPA-1 sont prêts pour la migration. *[Michèle, 2012]*

➤ **802.11/e MAC ENHANCEMENTS (QOS) (2005)**

Le développement de 802.11e fut long et laborieux et sa ratification repoussée d'année en année.

Il introduit la QoS (Qualité de Service) sur les réseaux 802.11 et répond à l'attente des utilisateurs de communications de phonie (Vo Wifi) et d'applications de streaming multimédia. Il est basé sur la priorisation des flux et la fragmentation des trames longues.

En attendant sa ratification, des solutions ont été développées sur des drafts du standard qui n'assurent pas l'interopérabilité des produits. *[Michèle, 2012]*

➤ **802.11/n HIGH THROUGHPUT (2009)**

Après sept ans de réflexion, ce standard a été ratifié en juillet 2009, et après l'apparition de produits 802.11n sur le marché. Ceux-ci ont en effet été développés sur la base d'un draft dit « draft N » dont l'IEEE avait garanti la compatibilité avec le standard définitif. Il n'y a donc aucun souci quant à l'interopérabilité de ces produits avec ceux produits sur la base du 802.11n officiel.

Le but de 802.11n est d'augmenter la portée et le débit des réseaux Wi-Fi et promet 300 Mbit/s (théorique), et n'exclut pas la possibilité de faire mieux.

Pour arriver à ce résultat, 802.11n mise sur la technique MIMO (Multiple Input Multiple Output). Un signal radio transmis entre deux points est censé aller en ligne droite. En fait il n'en est rien car les ondes se réfléchissent un peu partout sur les murs, meubles plafonds... et le récepteur ne reçoit pas un signal unique mais plusieurs signaux décalés en fonction de la longueur de chaque trajet. Ces trajets multiples, plutôt considérés comme calamiteux dans les réseaux radio, MIMO va en tirer parti pour optimiser la transmission entre deux points. Le principe est d'utiliser plusieurs antennes en émission et plusieurs antennes en réception. Il n'est pas nécessaire qu'il y en ait le même nombre de chaque côté. Les antennes émettrices émettent les mêmes signaux, déphasés de façon à ce que la puissance émise à chaque fois soit maximale. L'optimisation de la transmission sur antennes multiples, en réduisant les pertes dues aux interférences, a pour autre conséquence l'amélioration de la portée de réseau en termes de couverture radio.

Le standard 802.11n reprend l'OFDM des versions a et g et est compatible avec les deux bandes de fréquences 2,4 et 5GHz. Il est possible de doubler la largeur canal dans la bande 5 GHz, moins encombrée, afin de quasiment doubler le débit. *[Michéle, 2012]*

➤ **802.11/s MESH NETWORKING (2009)**

Jusqu'ici nous connaissons le réseau Wi-Fi constitué de plusieurs Access Points reliés par une infrastructure filaire. Le principe du mesh networking est de supprimer cette infrastructure en laissant les Access Points communiquer directement entre eux. Ils se comportent alors comme des routeurs et transmettent les paquets de proche en proche jusqu'à leurs destinataires.

Les Access Points communiquent directement et définissent dynamiquement un routage entre eux. Le réseau étant maillé, il existe potentiellement plusieurs routes entre deux Access Points. De ce fait, le mesh networking améliore la fiabilité d'un

réseau car il est capable de redéfinir un routage lorsqu'un Access Point est en panne ou en surcharge. Il améliore également les performances en équilibrant le trafic de transit sur les Access Points, toujours en redéfinissant des routages alternatifs.

Les atouts majeurs du mesh networking sont sa rapidité de déploiement et son auto évolutivité par simple adjonction d'Access Points. Par ailleurs il offre une solution aux zones difficiles à câbler (sites classés, accès malaisé...) en éliminant trous et fils inesthétiques.

Le rôle de 802.11s est de définir un protocole d'auto configuration des routes entre les stations sur des technologies multi-hops auto configurables pour supporter des flux de trafic broadcaste/multicast et unicast. *[Michèle, 2012]*

➤ **802.11/v WIRELESS NETWORK MANAGEMENT(2011)**

802.11/b et 802.11/v ont la même architecture. On va le développer dans les points suivants.

#### **I.4.Architecture 802.11**

➤ **Topologie ad-hoc**

Il n'y a pas dans le réseau de point émetteur/récepteur ayant un rôle particulier. C'est le mode que l'on choisira si l'on souhaite juste faire communiquer entre elles deux ou trois machines disposant chacune d'une interface Wi-Fi. C'est un mode de fonctionnement rudimentaire, qui peut rapidement devenir compliqué si le nombre de machines en réseau augmente. Chaque station ne peut communiquer qu'avec les stations qui sont à portée. *[Michèle,2011]*

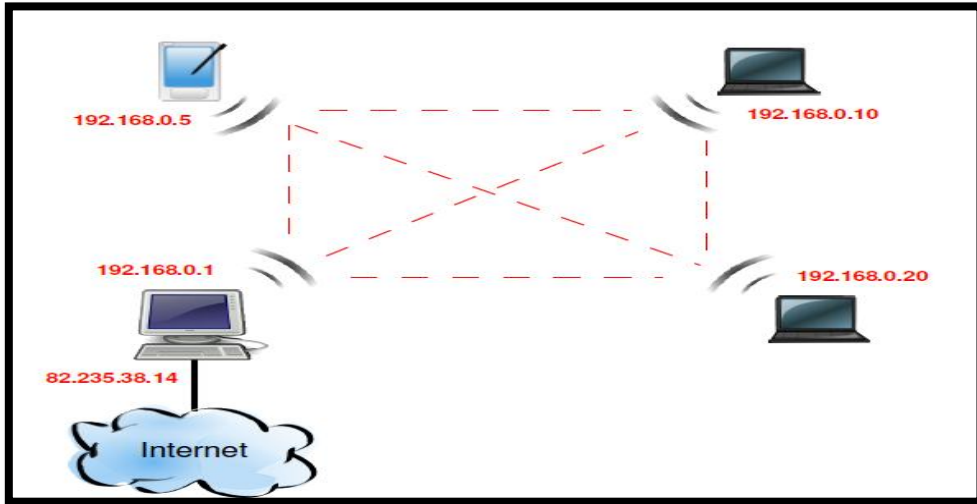


Figure I.2 : Topologie ad-hoc. [Patrick,2011]

➤ Topologie infrastructure

Dans ce mode, il y a au moins un émetteur/récepteur Wi-Fi qui joue un rôle particulier, celui de point d'accès (Access Point). C'est typiquement le mode utilisé lorsque l'on souhaite étendre un réseau câblé, genre Ethernet, avec une couverture Wi-Fi pour les portables, ou pour les machines que l'on ne souhaite pas câbler.

Les "modems Wi-Fi", entendez par là les modems ADSL ou câble, qui proposent une connectivité Wi-Fi fonctionnent généralement dans ce mode. [Michèle,2011]

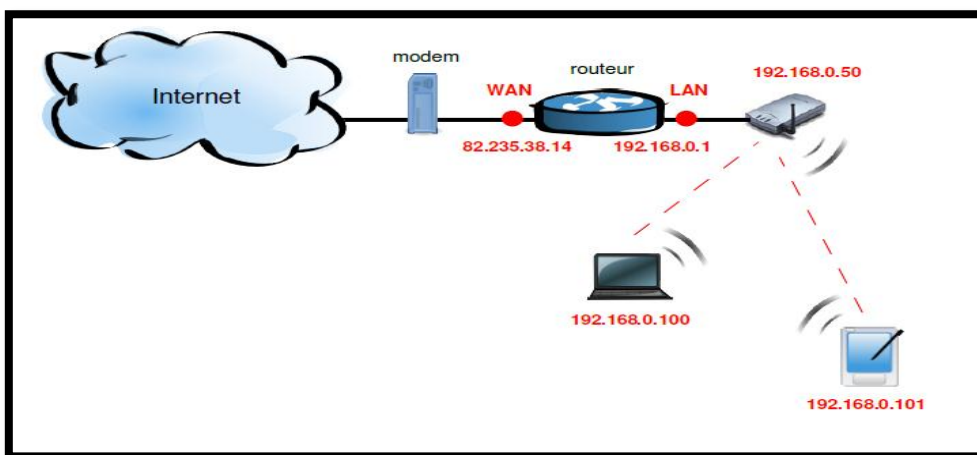


Figure I.3 : Topologie infrastructure. [Patrick,2011]

Le protocole 802.11 correspond aux couches MAC et physique des réseaux locaux. La couche MAC est unique mais la couche physique se décline en trois catégories.

## **I.5.Principe de fonctionnement 802.11**

### ➤ **Couche physique**

Initialement, le standard IEEE 802.11 permettait l'utilisation de trois couches physique différentes (FHSS, DSSS, Infra Red).

- **FHSS**

La plupart des interférences nuisibles aux transmissions radio n'agissent en fait que sur des bandes de fréquences assez étroites. Si par malchance de telles interférences ont lieu au moment où sont transmis les paquets, alors le signal sera fortement dégradé. Une technique pour protéger ce signal consiste à régulièrement changer de fréquences. Bien sûr, les paquets envoyés sur la bande perturbée seront affectés, mais ils ne représenteront plus qu'une minorité des transmissions et leurs retransmissions seront moins coûteuses. L'émetteur et récepteur doivent connaître à l'avance le séquençement des sauts de fréquences, mais les informations portées par les paquets permettent à un mobile connecté au réseau de savoir à partir d'un paquet qu'il reçoit ou en est le déroulement de la séquence. [Anry, al, 2007]

- **DSSS**

Dans le but de lutter contre les interférences importantes mais n'affectant que des plages de fréquences assez étroites, il existe la technique de l'étalement de spectre. Des manipulations sur le signal vont le faire occuper un spectre plus large (généralement il est multiplié par une séquence pseudo-aléatoire ayant certaines propriétés d'auto corrélation). A la réception, une manipulation inverse est effectuée. Cette technique est moins sensible aux interférences dues aux fréquences à faible largeur spectrale. [Anry, al, 2007]



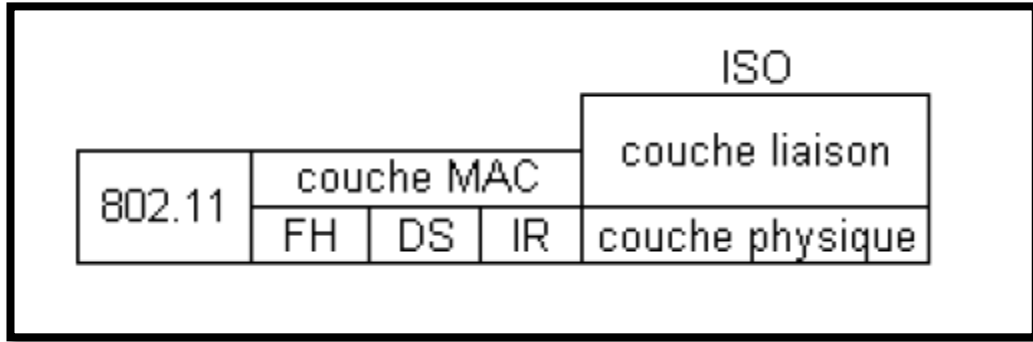


Figure I.4 : Composant des couches du 802.11. [Anry, al ,2007]

➤ La couche MAC :

La couche MAC 802.11 définit la méthode d'accès qui est ici CSMA/CA qui est une dérivée de CSMA/CD (Carrier Sense Multiple Access / Collision Detection) utilisée par Ethernet et qui consiste en deux principes :

• LBT

Listen Before Talk (écouter avant de parler) ; la station qui veut émettre « écouter » pour détecter si le support (bus) est libre. Si oui elle émet, sinon elle attend et reprendra plus tard.

• LWT

Listen While Talk (écouter en parlant) ; deux stations qui constatent que le support est libre peuvent émettre en même temps et provoquer une collision de signaux ; cette collision est un signal particulier qui peut être détecté par les stations émettrices. Dans le cas elle arrête d'émettre et reprendront plus tard après un délai aléatoire.

La norme 802.11 met en œuvre le principe LBT (qui correspond à CSMA) : La station émettrice écoute si le canal est libre. S'il l'est pendant un temps DIFS (d'Istributed Inter Frame Space), la station peut émettre une trame. La trame comporte un CRC ce qui permet à la station réceptrice de vérifier l'intégrité de la

trame. Si tout va bien, la station réceptrice envoie après un temps SIFS (Short Inter Frame Space) un accusé de réception ACK. [Anry, al ,2007]

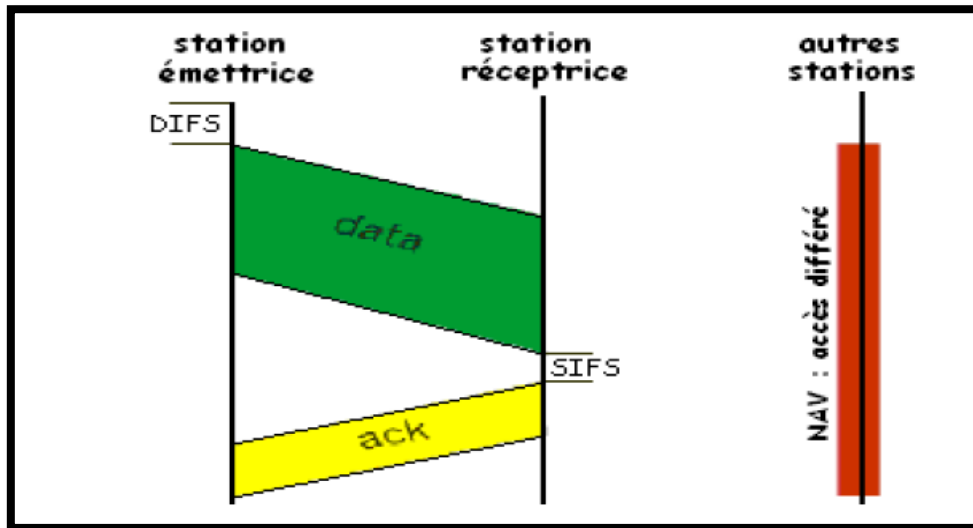


Figure I.5 : Déroulement de communications entre les stations émettrices et réceptrices. [Anry, al ,2007]

La durée de la transaction (data+SIFS+ack) figure dans un champ spécial de la trame et les autres stations qui « voient passer » la trame peuvent le noter sous forme d'un NAV (Network Allocation Vector) : c'est le temps qu'elles doivent attendre avant d'envoyer la suite de messages. Le NAV est décrémenté au rythme de l'horloge.

Cette méthode ne permet toutefois pas d'éviter les collisions ni de les détecter. En effet, pour les réseaux sans fil, l'RTS n'est pas possible car il faudrait, d'une part, qu'une station puisse émettre et recevoir simultanément (ce qui n'est pas impossible mais complexe et coûteux), et d'autre part, il est quasi impossible de supposer qu'une station entende toutes les autres (notamment celles qui ne sont pas dans la même cellule). La méthode employée est alors CSMA/CA (collision avoidance) basée sur l'envoi de la suite de messages : RTS, CTS, DATA, ACK.

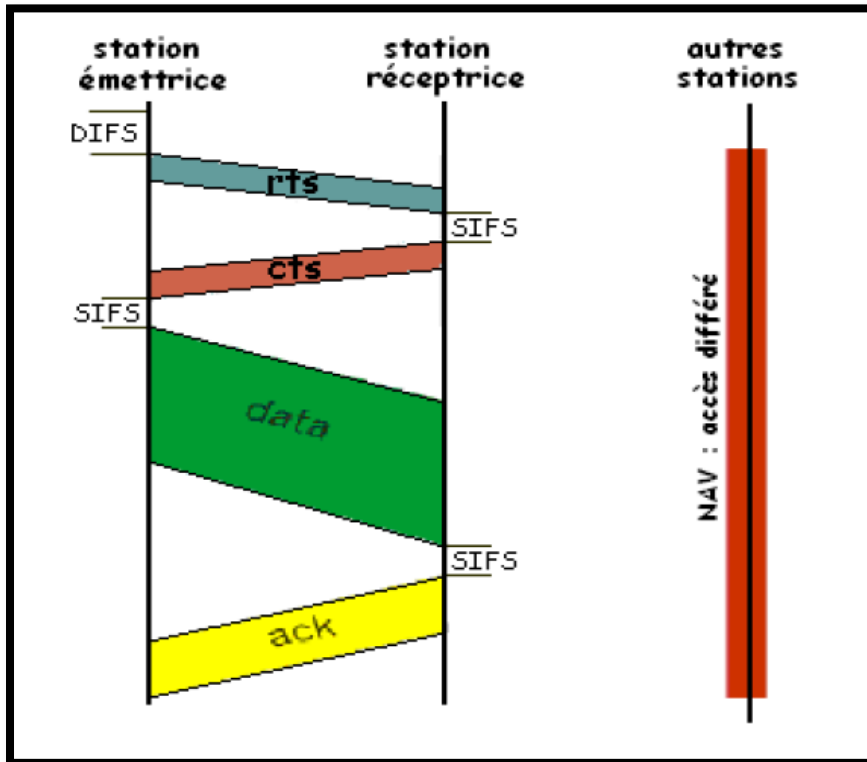


Figure I.6 : Echanges d'informations entre les stations. [Anry, al ,2007]

Une station qui veut émettre envoie un message RTS (Request To Send) à la station destinataire. RTS contient les adresses sources et destination ainsi que la durée de la transaction totale. Les autres stations notent la durée et positionnent l'indicateur NAV.

La station destinataire, si tout va bien, après avoir reçu le RTS, envoie à son tour c'est un CTS (Clear To Send) avec les mêmes informations que celles du RTS.

La station émettrice, si tout va bien, après avoir reçu CTS, enverra une trame d'information.

La station destinataire, si tout va bien, envoie à la station émettrice un accusé de réception, ACK.

On peut dire que le couple RTS-CTS permet de réserver le canal pour l'envoi d'une trame par une station. [Anry, al ,2007]

- Algorithme CSMA/CA

La figure ci-dessous explique le fonctionnement de l'algorithme CSMA/CA.

[Bruno,2006]

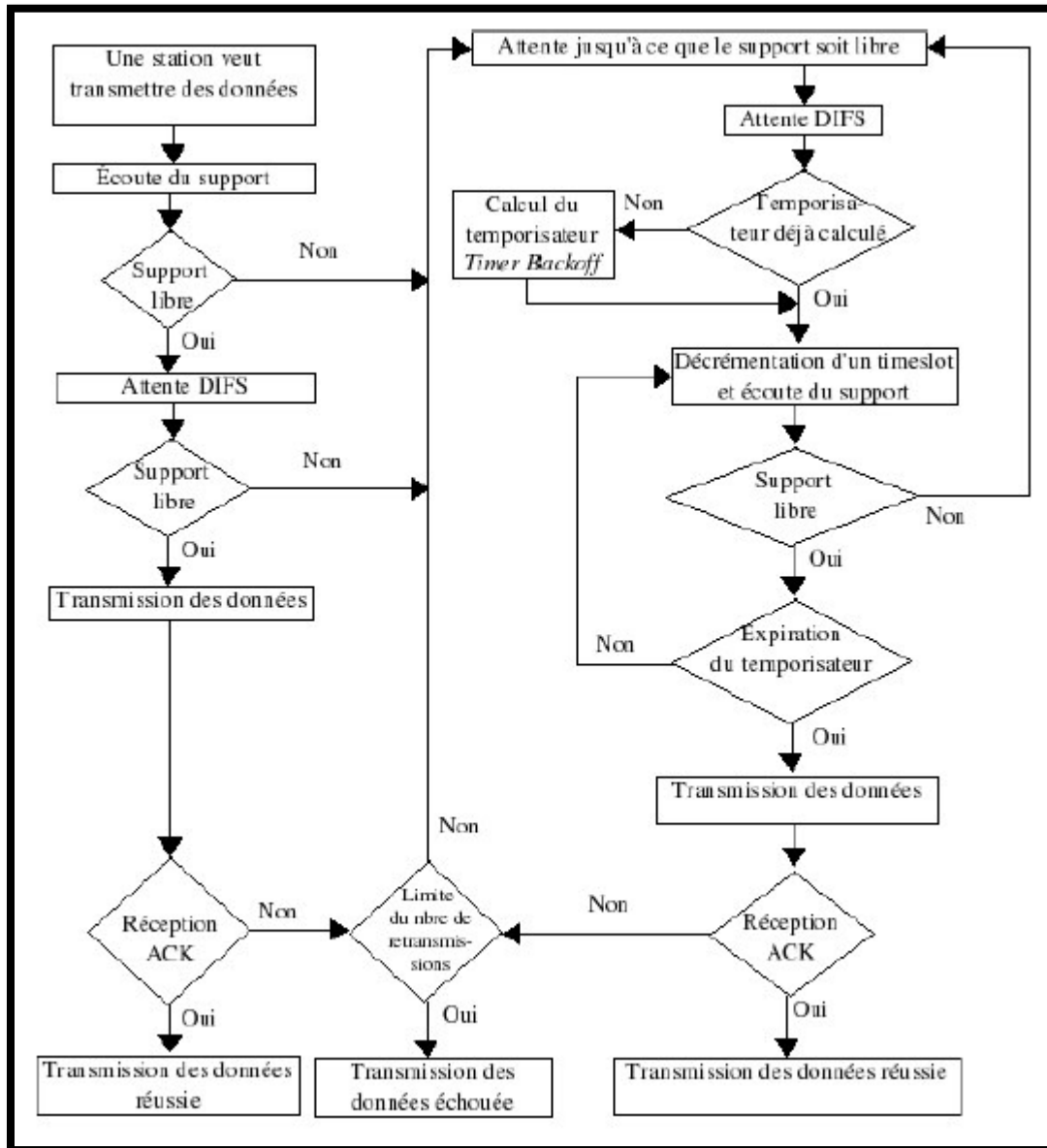


Figure I.7 : Algorithme du fonctionnement de CSMA/CA. [Anry, al ,2007]

## **I.6. Le standard 802.11/v wireless network management**

802.11v est une extension de 802,11 appareils Wi-Fi existant, tout comme les normes a, b, g et n que nous connaissons maintenant. Il a été proposé la première fois en 2004 pour renforcer les capacités réseau de Wi-Fi et d'aborder la gestion de l'alimentation.

802.11v promet de réduire la quantité d'énergie consommée par les puces radios Wi-Fi en passant des modems-routeurs aux ordinateurs portables et les téléphones mobiles. Il va travailler en coupant l'alimentation automatiquement à la puce Wi-Fi lorsqu'il n'est pas utilisé, ce qui devrait contribuer à améliorer la vie de la batterie dans des appareils. A son tour, le 802.11v aide le Wi-Fi à devenir beaucoup plus respectueux de l'environnement qu'il ne l'est maintenant. Les éléments clés de la norme comprennent le Wake (sillage) et le mode en veille de la gestion du réseau sans fil, ce qui devrait réduire la quantité d'énergie que les dispositifs du 802.11v consomment.

802.11v a également d'autres avantages, y compris la synchronisation de calendrier - quelque chose qui vous sera utile lorsque vous transférez les fichiers multimédias en continu d'un endroit à un autre.

802.11v devrait également offrir une gamme de localisation en temps réel (RTLS) services. Ceux-ci devraient vous permettre de garder une trace des appareils, des téléphones portables, des ordinateurs portables et les voitures de société compatible au Wi-Fi, avec un suivi également ouvert aux services de sécurité et d'urgence dispositif. Cela semble similaire à la position Wireless System (WPS) créé par Skyhook, qui vise à combler les lacunes de GPS en offrant une couverture globale de bas niveau sur une zone géographique plutôt que satellites distants qui peuvent avoir leurs signaux bloquée par des obstacles, des bâtiments, et ainsi de suite.

802.11v promet également d'améliorer la fiabilité des réseaux Wi-Fi, d'augmenter les vitesses de transfert de données et de réduire les interférences d'autres appareils.

802.11v son cout est non onéreux, on peut ajouter facilement certaines fonctionnalités a la configuration existante en utilisant le microprogramme (firmware),

par contre les des appareils mobiles, les ordinateurs portables peuvent être couteux.  
[Rob,2010]

### **I.7.Principe de fonctionnement du 802.11v**

Un réseau sans fil 802.11v est composé de bornes ou point d'accès (AP : *Access Points*) et de clients. La borne agit comme un pont entre un réseau filaire et un réseau sans fil, mais peut aussi être vue comme un concentrateur sans fil, et beaucoup de bornes sans fil possèdent aussi des fonctions de routage et de sécurité avec du filtrage IP. Les clients sont les cartes réseau (NIC : *Network Interface Card*), c'est-à-dire l'interface Ethernet sur l'équipement. Le fonctionnement par défaut est lorsque les interfaces Ethernet des clients dialoguent avec les bornes. Ce mode s'appelle "*infrastructure*". Il propose une topologie multipoints. Il est possible d'avoir un dialogue direct entre deux interfaces Ethernet sans fil, c'est le mode "*ad-hoc*", en topologie point à point. Il est également possible pour une machine munie d'une carte Ethernet de se transformer en borne.

Chaque réseau est identifié par un SSID : identificateur du réseau, qui est configuré dans les bornes, et éventuellement dans les clients, et envoyé dans les trames.

Plusieurs réseaux avec des SSID différents peuvent cohabiter au même endroit. La bande de fréquence des 2,4 GHz possède 14 canaux. Un même réseau utilisera plusieurs réseaux pour couvrir correctement un large espace avec plusieurs bornes. À l'inverse, plusieurs réseaux peuvent cohabiter au même endroit, même sur le même canal.

Ces caractéristiques apportent plusieurs considérations vis-à-vis des dénis de service. Dans un même endroit, il faut que les réseaux multipoints (mode *architecture*) et point à points (mode *ad hoc*) utilisent des SSID différents. Si une machine à sa carte en mode *ad-hoc* avec le même SSID que le réseau officiel des bornes, elle va perturber le bon fonctionnement du réseau et provoquer un déni de service pour ses voisins. Une attaque plus violente permettant de s'attirer le trafic est une machine se

transformant en borne. Elle peut s'attirer le trafic par sa puissance ou par une attaque ARP, et, au-delà du déni de service, bâtir des attaques de l'intercepteur en renvoyant le trafic capturé sur la véritable borne.

Au niveau Ethernet, la vision des réseaux sans fil est similaire à celle des réseaux filaires. Elle est identique pour les ordinateurs et pour TCP/IP. Ethernet filaire 802.3 utilise CSMA/CD et détecte les collisions, alors qu'Ethernet sans fil 802.11 utilise CSMA/CA qui prévient les collisions. L'adressage MAC est identique, sauf que dans 802.11 il y a les adresses des bornes en plus, ce qui donne quatre adresses MAC au lieu de deux dans la trame.

802.11v a ajouté une fonction nouvelle WEP (*Wired Equivalent Privacy*), qui permet en théorie d'assimiler un réseau Ethernet sans fil à un réseau Ethernet filaire, en assurant une sécurité équivalente à celle d'un câble. Malheureusement le WEP de première génération n'a pas rempli son objectif. [*Hervé, 2002*]

Les différences entre les standards 802.11/b et 802.11/v sont

- Consommation d'énergie
- Localisation
- Augmentation du débit
- On va les détailler dans le chapitre suivant.

### **I.8.Application du standard 802.11v**

- Usage Professionnel
- Usage privé
- Points d'accès public
- Maison intelligente
- Entreprises
- Réseaux d'urgence

## I.9.Conclusion

Pour conclure ce chapitre, nous avons résumé l'ensemble des caractéristiques du standard 802.11 dans le tableau (I.9.1) avoir une idée plus lisible et détaillé.

<b>Le standard</b>	<b>Débit</b>	<b>Portée</b>	<b>fréquence</b>	<b>année</b>	<b>application</b>
<b>802.11/a</b>	54 Mbps	100 m	5 GHz	1999	LAN-PAN
<b>802.11/b</b>	11 Mbps	100 m	2.4 GHz	1999	LAN-PAN
<b>802.11/e</b>	MAX	150-400 m	-	2005	QoS
<b>802.11/g</b>	54 Mbps	100 m	2.4 GHz	2003	
<b>208.11/i</b>	-	-	-	2004	Sécurité
<b>802.11/n</b>	200 Mbps	MAN	2.4 GHz	2009	Multimédia
<b>802.11/s</b>	100-400 Mbps	WAN	2.4\5 GHz	2009	Multimédia
<b>802.11/v</b>	MAX	150-400 m	2.4 GHz	2011	Divers

**Tableau I-1 : Caractéristiques du standard 802.11**



# **Chapitre II**

**Les caractéristiques du standard**

**IEEE802.11/v**

## **Chapitre II : Les caractéristiques du standard IEEE 802.11/v**

### **II.1.Introduction**

Dans le premier chapitre nous avons fait la différence entre les standards 802.11b et 802.11v et par la suite nous allons aborder l'explication de cette différences entre c'est deux normes.

Les réseaux ad hoc sont des réseaux caractérisés par des ressources limitées en énergie. La conservation d'énergie est donc un facteur primordial pour la durée de vie du réseau. Plusieurs propositions existent pour traiter ce problème. Elles se situent au niveau de différentes couches de la pile des protocoles de communication.

Puisque le 802.11v est basé sur l'augmentation du débit, localisation et l'économie d'énergie, dans le point suivant nous allons citer les différentes techniques et réseaux qui contribuent à satisfaire les trois paramètres de notre réseau.

### **II.2.Augmentation du débit**

#### **II.2.1.La technique MIMO**

MIMO est une technique de multiplexage utilisée dans les réseaux sans fil et les réseaux mobiles permettant des transferts de données à plus longue portée et à plus grande vitesse qu'avec des antennes utilisant la technique SISO (Single-Input Single-Output).

Le MIMO et son algorithme astucieux ont radicalement fait évoluer la technologie Wi Fi. Cette dernière est désormais plus véloce et bénéficie d'une portée bien plus importante. Dans la plupart des cas le MIMO est compatible avec les normes IEEE 802.11. *[Matthieu, 2012]*

#### **II.2.2. Amélioration de la méthode d'accès CSMA/CA**

La norme 802.11 propose un protocole similaire appelé CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), qui utilise un mécanisme d'esquive de collision basé sur un principe d'accusé de réceptions réciproques entre l'émetteur et le récepteur (chapitre I).

La couche MAC du protocole 802.11 vérifie l'intégrité des trames par le mécanisme de contrôle d'erreur, il s'agit là d'une différence fondamentale avec le standard Ethernet. En effet Ethernet ne propose aucun système de détection ou de correction d'erreurs, cette tâche étant laissée aux protocoles de transports de niveau supérieur (TCP). Dans un réseau sans fil le taux d'erreur est plus élevé, c'est la raison pour laquelle un contrôle d'erreur a été intégré au niveau de la couche liaison de données.

D'autre part le taux d'erreur de transmission sur les réseaux sans fils augmente généralement avec des paquets de taille importante, c'est la raison pour laquelle la norme 802.11 offre un mécanisme de fragmentation, permettant de découper une trame en plusieurs morceaux (fragments).

La Point Coordination Function (PCF) appelée mode d'accès contrôlé. Elle est fondée sur l'interrogation à tour de rôle des stations, ou polling, contrôlée par le point d'accès. Une station ne peut émettre que si elle est autorisée et elle ne peut recevoir que si elle est sélectionnée.

Cette méthode est conçue pour les applications temps réel (vidéo, voix) nécessitant une gestion du délai lors des transmissions de données. *[Cecille, 2014]*

### **II.3.Localisation**

#### **II.3.1.Les réseaux VANET**

- ***Définition des réseaux VANET***

Les VANETS sont des réseaux pour lesquelles les nœuds de communications sont des véhicules. Ces réseaux améliorent particulièrement la sécurité du trafic sur la route et globalement, la sécurité du système de transport grâce à des applications dites de sécurité. Ils améliorent aussi l'expérience de conduite grâce à des applications dites de confort. Les communications se déroulent d'une part entre les infrastructures placées le long des rues et les véhicules et d'autres parts entre les véhicules entre eux. En effet lorsqu'un véhicule reçoit une alerte ou un avertissement, il exploite les

informations publiées par l'émetteur telles que sa vitesse, sa position géographique, son accélération, sa direction ou encore son rayon de transmission. Grâce à ces informations et le type d'alerte reçue, le conducteur du véhicule récepteur peut réagir efficacement pour éviter un accident ou une situation dangereuse. *[Richard, 2013]*

- ***Catégories des équipements d'un réseau VANET***

Ils existent deux catégories d'équipements dans un réseau VANET : les équipements internes aux véhicules OBU, les équipements externes aux véhicules RSU

- Les OBU (On Board Unit) : Les "OBUs" sont donc des équipements radio installés dans les véhicules
- Les RSU (Road Side Unit) : Les "RSUs" par contre sont place au bord des route et constitue l'infrastructure réseau, ils sont d'ailleurs utilisé comme des routeurs entre les véhicules.

Les "OBUs" utilisent les signaux DSRC (Dedicated Short Range Communication) pour communiquer avec les « RSU » *[Richard,2013]*

- ***Architecture des réseaux VANET***

L'architecture des VANETs peut être divisé en trois catégories: l'architecture WLAN/Cellulaire, l'architecture ad-hoc, et l'architecture hybride. Si les infrastructures constituant les réseaux sont de type passerelles cellulaires ou WLAN ou encore des points d'accès WIMAX, le réseau est considéré comme cellulaire/WLAN pure. Par contre si aucune infrastructure n'intervient durant les échanges entre les véhicules, il s'agit d'une architecture ad-hoc. Si les véhicules ont le choix d'utiliser une infrastructure disponible ou de communiquer directement de façon ad-hoc, on parle alors d'une architecture hybride. *[Richard,2013]*

- ***Applications des réseaux VANET***

L'application d'avertissement de la violation des feux de signalisation

L'application d'avertissement à l'approche d'un tournant

L'application de lumière d'indication d'un freinage d'urgence

L'application d'avertissement coopératif d'une collision imminente

L'application d'avertissement de changement de voie [Richard,2013]

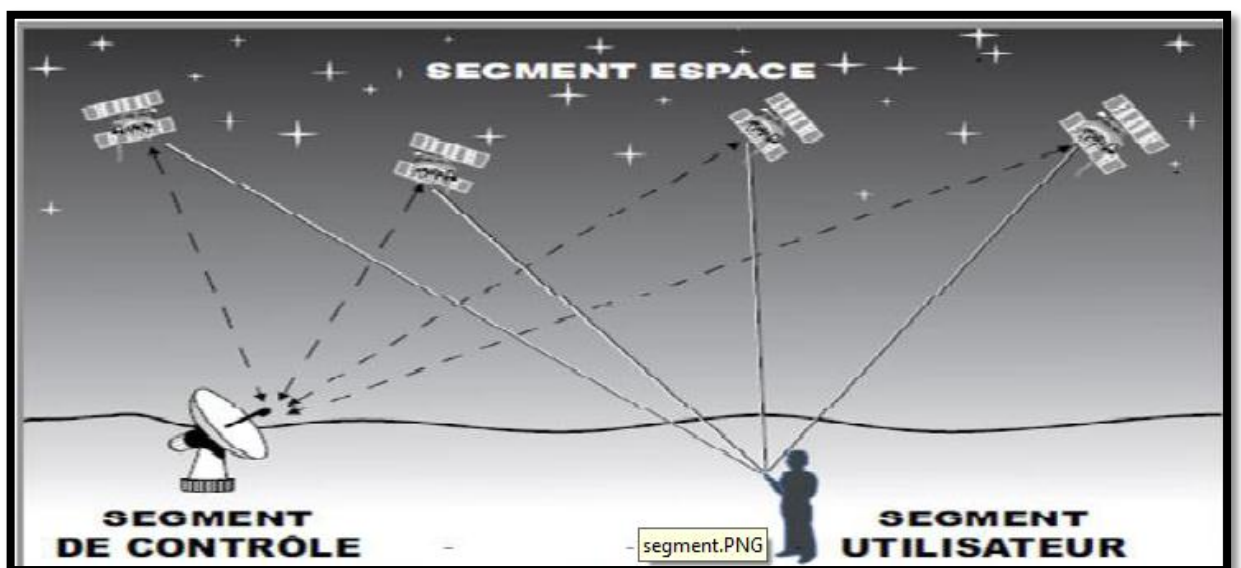
### **II.3.2.Le GPS**

- **Définition du GPS**

Le GPS « Global Positioning System » est un système de localisation par satellite mis en place par le Département Américain de la Défense dans les années 1970. Il permet de déterminer les coordonnées géographiques d'un point situé n'importe où sur le globe terrestre et ce 24 h sur 24 h.

Les coordonnées d'un point sont obtenues en mesurant, à l'aide de signaux radio, sa distance par rapport à un certain nombre de satellites et en appliquant le principe de triangulation. Quatre satellites sont nécessaires pour établir les coordonnées x, y et z du point à définir. [Albert, 1998]

- **Composition du système GPS**



**Figure II.1 : Composition du système GPS [Albert, 1998]**

### **Le segment spatial (les satellites)**

C'est la constellation des satellites du GPS. Le segment spatial, composé d'un minimum de 24 satellites dont 21 actifs et plus de 3 de rechange est le cœur du système.

Ces satellites évoluent en orbite haute soit à plus de 19.000 kilomètres au-dessus de la surface de la terre. Le fait d'être positionné à une telle altitude permet aux signaux de couvrir une très large zone.

Les orbites sont inclinées à 55° par rapport au plan de l'équateur et leur période est d'environ 12 heures. Cette configuration permet à un récepteur à la surface ou au-dessus de la terre de recevoir les signaux de cinq à huit satellites à tout moment de la journée et ce 24 h/ 24 h.

Les satellites transmettent continuellement leurs données de position et d'heure, qui sont reçues et traitées par les récepteurs GPS afin de déterminer la position tridimensionnelle de l'utilisateur (latitude, longitude, altitude).

### **Le segment de contrôle (les stations au sol)**

Ce segment se compose d'une station de contrôle principale, de cinq stations de poursuite et de trois antennes terriennes réparties autour de la terre. C'est la partie qui permet de piloter et de surveiller le système.

Les stations de poursuite surveillent tous les satellites en communication avec les GPS en vue et recueillent les données contenues dans les messages envoyés par les satellites. Ces stations éloignées sont capables de poursuivre et de surveiller la position de chacun des satellites en relation avec le GPS. La station de contrôle principale contrôle les satellites - GPS en les suivant et en leur fournissant les corrections d'orbites et de temps.

Dans le monde, il existe cinq stations de contrôle au sol qui sont situées tout autour de la terre : quatre stations automatiques de surveillance et une seule station principale de contrôle.

Les stations automatiques reçoivent constamment des données provenant des satellites et renvoient ces informations à la station principale de contrôle. La station principale de contrôle corrige et met à jour (éphémérides, paramètres d'horloge..) les données reçues puis renvoie ces informations aux satellites via deux antennes situées sur deux autres sites différents.

### Le segment utilisateur (les récepteurs)

Ce segment comprend les récepteurs, processeurs et antennes qui permettent aux opérateurs se trouvant en mer, sur terre et dans les airs, de recevoir les transmissions des satellites aux GPS et de calculer avec précision leur position ainsi que leurs vitesses et l'heure. [Albert, 1998]

#### • **Principe du Fonctionnement du GPS**

Le GPS fonctionne grâce au calcul de la phase d'onde d'émission et de réception et la distance qui sépare le récepteur du satellite.

La vitesse de transmission des signaux émis par les satellites est égale à celle de la lumière. Chaque signal intègre une éphéméride avec son heure de départ. On mesure donc la distance entre l'utilisateur et un certain nombre de satellites de positions connues grâce au temps qu'a mis chaque signal à parvenir au GPS. Le récepteur GPS est capable d'identifier le satellite qu'il utilise à l'aide du signal pseudo aléatoire émis par chaque satellite. Il reçoit, à l'aide de ce signal, les informations sur l'orbite et la position du satellite. Pour mesurer la distance qui sépare le satellite du GPS, on mesure le temps  $T$  mis par le signal pour aller de l'un vers l'autre. Le système GPS permet également de mesurer la vitesse à laquelle se déplace l'utilisateur.

Avec la réception des signaux de quatre satellites (trois pour obtenir le point d'intersection de trois sphères, un quatrième pour la synchronisation du temps), le récepteur mobile est capable de calculer sa position géographique par triangulation. [Luc, 2003]

- **Les applications du GPS**

La géologie, la topographie, la navigation ...

Le guidage des missiles de croisières ou des munitions tactiques (bombes et roquettes) sur des objectifs précis ainsi que les activités de navigation et de positionnement

Les navigations aériennes, maritimes et terrestres de positionnement. [*Luc, 2003*]

## **II.4.Consommation d'énergie**

### **II.4.1.Introduction**

La norme 802.11v définit un moyen d'économiser l'énergie. Cela lui permet d'être mieux adapté aux équipements fonctionnant avec des batteries et pour qui l'énergie est une ressource précieuse.

L'économie d'énergie est une des problématiques majeures dans les réseaux de capteurs. En effet, la recharge des sources d'énergie est souvent trop coûteuse et parfois impossible. Il faut donc que les capteurs économisent au maximum l'énergie afin de pouvoir fonctionner. Les réseaux de capteurs fonctionnant selon un mode de routage par saut, chaque nœud du réseau joue un rôle important dans la transmission de données. Le mauvais fonctionnement d'un nœud implique un changement dans la topologie et impose une réorganisation du réseau.

### **II.4.2.Réseaux de capteur**

#### **a. Introduction**

Les réseaux de capteurs sont de plus en plus utilisés dans l'environnement et l'industrie grâce notamment aux derniers développements réalisés dans le domaine des technologies sans-fils (wireless). Depuis quelques années, le besoin d'observer, d'analyser et de contrôler des phénomènes physiques sur des zones étendues est essentiel pour de nombreuses applications environnementales et scientifiques. Cette



nouvelle manière d'envisager la métrologie, en détectant un phénomène à différents points disséminés sur un système ou un site, fait émerger de nouvelles problématiques technologiques, par exemple sur l'autonomie énergétique des capteurs, et de nouveaux types d'applications nous permettant de mieux connaître notre environnement et d'anticiper les problèmes de sécurité, de pollution, de risques naturels, de défaillances, de maintenances, ou plus généralement de tous phénomènes non désirés qui pourraient être anticipés.

Cette note de veille dresse un état des lieux des derniers travaux et avancées technologiques autour des réseaux de capteurs appliqués à la métrologie environnementale et les tendances futures en termes de technologies et d'applications.

### **b. Définition du capteur sans fils**

Les capteurs sont des dispositifs de taille extrêmement réduite avec des ressources très limitées, autonomes, capable de traiter des informations et de les transmettre, via les ondes radio, à une autre entité (capteurs, unité de traitements...) sur une distance limitée à quelques mètres. *[Fares, al,2008]*



**Figure II.2 : Capteur sans fils. *[Fares, al,2008]***

Les réseaux de capteurs utilisent un très grand nombre de ces capteurs, pour former un réseau sans infrastructure établie. Un capteur analyse son environnement, et propage les données récoltées aux capteurs appartenant à sa zone de couverture.

Chaque capteur relayant l'information sur sa propre zone de couverture, le réseau se trouve entièrement couvert.

### c. Architecture de capteurs sans fils

Un nœud capteur contient quatre unités de base : l'unité de captage, l'unité de traitement, l'unité de transmission, et l'unité de contrôle d'énergie. Il peut contenir également, suivant son domaine d'application, des modules supplémentaires tels qu'un système de localisation (GPS), ou bien un système générateur d'énergie (cellule solaire). On peut même trouver des micro-capteurs, un peu plus volumineux, dotés d'un système mobilisateur chargé de déplacer le micro-capteur en cas de nécessité.

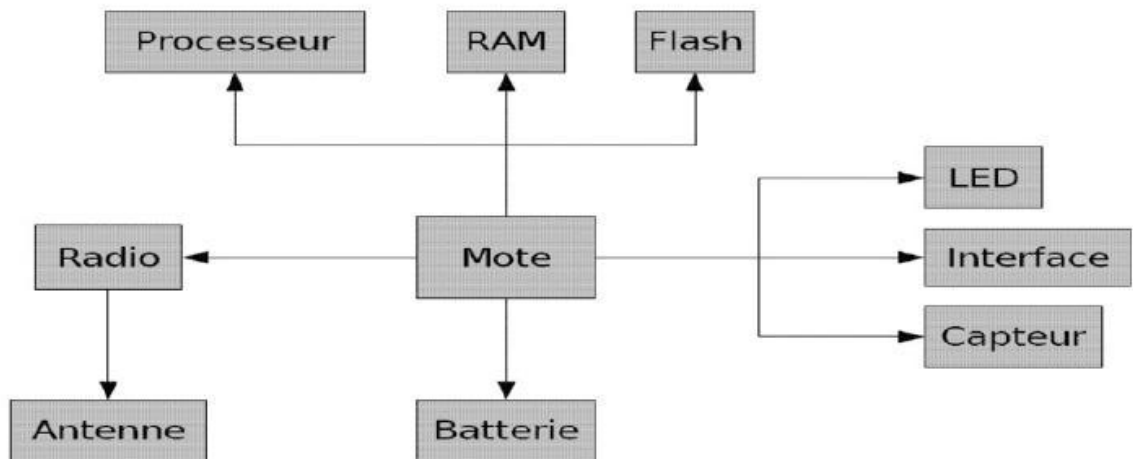


Figure II.3 : Architecture d'un capteur sans fils. [Fares, al,2008]

#### • Unité de traitement

Mote, processeur, RAM et Flash : On appelle généralement Mote la carte physique utilisant le système d'exploitation pour fonctionner. Celle-ci a pour cœur le bloc constitué du processeur et des mémoires RAM et Flash. Cet ensemble est à la base du calcul binaire et du stockage, temporaire pour les données et définitif pour le système d'exploitation. Cette unité est chargée d'exécuter les protocoles de communications qui permettent de faire collaborer le nœud avec les autres nœuds du

réseau. Elle peut aussi analyser les données captées pour alléger la tâche du nœud puits.

- ***Unité de transmission***

Radio et antenne : les équipements étudiés sont donc généralement équipés d'une radio ainsi que d'une antenne. Cette unité est responsable d'effectuer toutes les émissions et réceptions des données sur un medium sans fil. Elle peut être de type optique (comme dans les nœuds Smart Dust), ou de type radiofréquence. Les communications de type optique sont robustes vis-à-vis des interférences électriques. Néanmoins, elles présentent l'inconvénient d'exiger une ligne de vue permanente entre les entités communicantes. Par conséquent, elles ne peuvent pas établir de liaisons à travers des obstacles.

- ***Unités de captage***

LED, interface, capteur : On retrouve donc des équipements de différents types de détecteur et d'autre entrée. Le capteur est généralement composé de deux sous-unités : le récepteur (reconnaissant l'analyste) et le transducteur (convertissant le signal du récepteur en signal électrique). Le capteur est responsable de fournir des signaux analogiques, basés sur le phénomène observé, au convertisseur Analogique/Numérique. Ce dernier transforme ces signaux en un signal numérique compréhensible par l'unité de traitement.

- ***Unités de control d'énergie***

Batterie : Un micro-capteur est muni d'une ressource énergétique (généralement une batterie de type AAA) pour alimenter tous ses composants. Cependant, en conséquence de sa taille réduite, la ressource énergétique dont il dispose est limitée et généralement irremplaçable. Cette unité peut aussi gérer des systèmes de rechargement d'énergie à partir de l'environnement observé telles que les cellules solaires, afin d'étendre la durée de vie totale du réseau. [*Fares, al,2008*]

#### **d. Définition des réseaux de capteurs**

Les réseaux de capteurs sont des systèmes qui regroupent plusieurs capteurs afin de couvrir une zone cible. Cette zone peut être géographique ou délimitée par un système plus ou moins étendu : un ouvrage d'art, un ensemble mécanique, un outillage, un réseau télécoms, ...

Les réseaux de capteurs connaissent de multiples applications telles que la météorologie environnementale, urbaine ou industrielle.

En réseau, ces capteurs peuvent interagir entre eux et avec un système externe (par exemple Internet) par le biais de communication sans fil ou filaire. Les réseaux de capteurs sans-fils concentrent les dernières avancées technologiques et représentent l'opportunité de nouvelles applications. En Anglais, on parle de « WSN » pour « Wireless Sensor Networks ».

Les capteurs sans fil communiquent par le biais des ondes radioélectriques. N'étant pas intégrés à un réseau préexistant; les capteurs communiquent grâce à un réseau dit « ad hoc », capable de s'organiser sans infrastructure définie préalablement. Ceci implique que chaque capteur puisse retransmettre une information indépendamment ou avec l'aide des autres capteurs et ceci afin d'envoyer l'information à une « station de base » capable de transmettre l'information à l'utilisateur final, par le biais d'Internet ou d'un réseau télécom GSM dans la majorité des cas.

Les capteurs sont capables de mesurer des grandeurs physiques, chimiques ou biologiques, de traiter ces informations et de les stocker. Ils sont alimentés électriquement via une batterie individuelle optimisée pour des tâches comme le traitement de l'information et la communication. [Vijay, *al*, 2002].

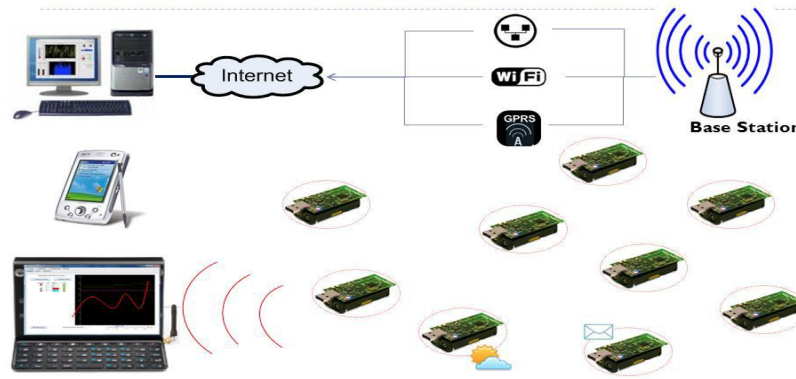


Figure II.4 : Exemple de représentation d'un réseau de capteurs.  
[Vijay, al, 2002].

### e. Application des réseaux de capteurs

- Surveillance
  - Détection d'intrusions
  - Feu de forêt
  - Mesures météorologiques
  - Départ de coups d'artillerie
  - Détection des mouvements ennemis
  - Contrôle de la qualité de l'air
- Couverture
  - Zone/point ponctuel
- Environnement
  - Militaire /Civil
  - Hostile/non-hostile
- Applications
  - Agricole et Environnement
  - Médical

- Structure ou édifice
- Domotique [*Gregory ,al,2000*].

## **II.5.Conclusion**

Dans ce chapitre nous avons cités les différentes techniques que notre réseau peut se basé et aussi les différents réseaux séminaire déjà existant au quel ces paramètres la sont exploiter d'une manier ou une autre. Nous pouvons dire que le 802.11v est un réseau qui englobe beaucoup de similitude et de diverses techniques déjà existantes pour satisfaire le client d'une manier général.

# **Chapitre III**

## **État de l'art sur l'économie d'énergie**

## **Chapitre III : État de l'art sur l'économie d'énergie**

### **III.1.Introduction**

Nous avons vu dans le chapitre précédent la différence entre les deux standards, et dans celui-ci, nous allons nous intéresser à l'étude des protocoles du niveau MAC et celles des routages qui nous permettront de gérer au mieux la consommation d'énergie dans le 802.11v.

La sous-couche MAC définit les modalités avancées telle que la sécurité de communication, l'économie d'énergie, le contrôle d'erreur ou encore la qualité de service, cette sous-couche représente en quelque sorte le cerveau de Wifi.

Un protocole de routage est le choix de route qui se fait selon un ou plusieurs protocoles et permet de distinguer les "bonnes" des "mauvaises" routes, comme il permet de quantifier la qualité d'un lien ou un chemin selon certains critères tels que le taux de perte, l'interférence, la longueur des routes, le délai, ...etc.

### **III.2.Consommation d'énergie d'un nœud-capteur**

#### **III.2.1.Formes de dissipation d'énergie**

Les nœuds-capteurs sont alimentés principalement par des batteries. Ils doivent donc fonctionner avec un bilan énergétique frugal. En outre, ils doivent le plus souvent avoir une durée de vie de l'ordre de plusieurs mois, voire de quelques années, puisque le remplacement des batteries n'est pas une option envisageable pour des réseaux avec des milliers de nœuds. Afin de concevoir des solutions efficaces en énergie, il est extrêmement important de faire d'abord une analyse des différents facteurs provoquant la dissipation de l'énergie d'un nœud-capteur [Vijay, *al*, 2002]. Cette dissipation d'énergie se fait de manière générale selon plusieurs modes :

- **Le MCU**

Généralement les MCUs possèdent divers modes de fonctionnement : actif, "idle", et sommeil, à des fins de gestion d'énergie. Chaque mode est caractérisé par une quantité différente de consommation d'énergie. Toutefois, la transition entre les modes de fonctionnement implique un surplus d'énergie et de latence. Ainsi, les



niveaux de consommation d'énergie des différents modes, les coûts de transition entre les modes mais encore le temps passé par le MCU dans chaque mode ont une incidence importante sur la consommation totale d'énergie d'un nœud-capteur.

- **La radio**

La radio opère dans quatre modes de fonctionnement : émission, réception, "idle", et sommeil. Une observation importante dans le cas de la plupart des radios est que le mode "idle" induit une consommation d'énergie significative, presque égale à la consommation en mode réception [Ya Xu,al,2001]. Ainsi, il est plus judicieux d'éteindre complètement la radio plutôt que de passer en mode "idle" quand l'on a ni à émettre ni à recevoir de données. Un autre facteur déterminant est que, le passage de la radio d'un mode à un autre engendre une dissipation d'énergie importante due à l'activité des circuits électroniques. Par exemple, quand la radio passe du mode sommeil au mode émission pour envoyer un paquet, une importante quantité d'énergie est consommée pour le démarrage de l'émetteur lui-même [Vijay, al, 2002]. Un autre point important est que les données des constructeurs sous-estiment assez régulièrement ces différentes consommations comme ont pu le montrer les auteurs de [Hurni,al,2009], en particulier concernant la consommation dans le mode "idle".

- **Le détecteur ou le capteur**

Il y a plusieurs sources de consommation d'énergie par le module de détection, notamment l'échantillonnage et la conversion des signaux physiques en signaux électriques, le conditionnement des signaux et la conversion analogique-numérique. Etant donné la diversité des capteurs, il n'y a pas de valeurs typiques de l'énergie consommée. En revanche, les capteurs passifs (température, sismiques, ...) consomment le plus souvent peu d'énergie par rapport aux autres composants du nœud-capteur. Notons, les capteurs actifs tels que les sonars, les capteurs d'images, etc. peuvent consommer beaucoup d'énergie. En outre, il existe d'autres formes de dissipation d'énergie telles que les lectures et les écritures mémoire.

Un autre aspect non négligeable est le phénomène d'auto décharge de la batterie. En effet, cette dernière se décharge d'elle-même et perd de sa capacité au fil du temps.

Il est difficile d'apporter ici une étude quantitative et comparative précise de la consommation de chaque composant d'un nœud-capteur en raison du grand nombre de plates-formes commerciales existantes. Cependant, des expérimentations ont montré que c'est la transmission de données qui est la plus consommatrice en énergie [Vijay, al, 2002]. Le coût d'une transmission d'un bit d'information est approximativement le même que le coût nécessaire au calcul d'un millier d'opérations [Gregory ,al,2000]. La consommation du module de détection dépend du type spécifique du nœud-capteur.

### III.2.2.Sources de surconsommation d'énergie

Nous appelons surconsommation d'énergie toute consommation inutile que l'on peut éviter afin de conserver l'énergie d'un nœud-capteur. Les sources de cette surconsommation sont nombreuses, elles peuvent être engendrées lors de la détection lorsque celle-ci est mal gérée (par exemple par une fréquence d'échantillonnage est mal contrôlée) [Cesare, al,2007].La surconsommation concerne également la partie communication. En effet, cette dernière est sujette à plusieurs phénomènes qui surconsomment de l'énergie surtout au niveau MAC ou se déroule le contrôle d'accès au support sans fil. Certains de ces phénomènes sont les causes majeures de la perte d'énergie et ont été recensés dans [Wei, al,2004] [Mahmood, al,2008] [K.Holger, al.2005]

- **Les collisions**

Elles sont la première source de perte d'énergie. Quand deux trames sont émises en même temps et se heurtent, elles deviennent inexploitable et doivent être abandonnées. Les retransmettre par la suite, consomme de l'énergie. Tous les protocoles MAC essayent à leur manière d'éviter les collisions. Les collisions concernent plutôt les protocoles MAC avec contention.

- **L'écoute à vide (idle listening)**

Un nœud dans l'état "idle" est prêt à recevoir un paquet, mais il n'est pas actuellement en train de recevoir quoi que ce soit. Ceci est coûteux et inutile dans le cas des réseaux à faible charge de trafic. Plusieurs types de radios présentent un coût en énergie significatif pour le mode "idle". Eteindre la radio est une solution, mais le

coût de la transition entre les modes consomme également de l'énergie, la fréquence de cette transition doit alors rester ((raisonnable)).

- **L'écoute abusive (overhearing)**

Cette situation se présente quand un nœud reçoit des paquets qui ne lui sont pas destinés. Le coût de l'écoute abusive peut être un facteur dominant de la perte d'énergie quand la charge de trafic est élevée et la densité des nœuds grande, particulièrement dans les réseaux "mostly-on".

- **L'overmitting**

Un nœud envoie des données et le nœud destinataire n'est pas prêt à les recevoir.

- **L'over Head des paquets de contrôle**

L'envoi, la réception, et l'écoute des paquets de contrôle consomment de l'énergie. Comme les paquets de contrôle ne transportent pas directement des données, ils réduisent également le débit utile effectif.

### **III.3.Mécanismes de conservation de l'énergie**

C'est la transmission de données qui se révèle extrêmement consommatrice par rapport aux tâches du nœud-capteur. Cette caractéristique conjuguée à l'objectif de maximisation de la durée de vie du réseau a suscité de nombreux travaux de recherche. Nous allons citer certains mécanismes de base.

#### **III.3.1.Mode d'économie d'énergie**

Ce mode est possible quelle que soit la couche MAC adoptée. Cela consiste à éteindre le module de communication dès que possible. Par exemple, des protocoles MAC fondés sur la méthode TDMA (Time Division Multiple Access) offrent une solution implicite puisqu'un nœud n'échange des messages que dans les intervalles de temps qui lui sont attribués. Il peut alors garder sa radio éteinte durant les autres slots. Comme nous l'avons souligné précédemment, il faut toutefois veiller à ce que le gain d'énergie obtenu en mettant en veille le module radio ne soit pas inférieur au surcoût engendré par le redémarrage de ce module.

### **III.3.2.Traitement local**

L'idée de cette technique est que la source peut se censurer. Ainsi une programmation événementielle semble bien adaptée aux réseaux de capteurs. Seuls les changements significatifs de l'environnement devrait provoquer un envoi de paquets le réseau. Dans le même état d'esprit, une grande collaboration est attendue entre les capteurs d'une même région en raison de leur forte densité et dans la mesure où les observations ne varient presque pas entre des voisins très proches. Ainsi les données pourront être confrontées localement et agrégées au sein d'un seul et unique message. Cette stratégie de traitement local permet de réduire sensiblement le trafic.

### **III.3.3.Organisation des échanges**

Ce procédé revient à limiter les problèmes de retransmission dus aux collisions. La solution extrême consiste à utiliser la technique d'accès au médium TDMA. Les collisions sont ainsi fortement réduites. Cette solution présente l'inconvénient d'être peu flexible et de demander une synchronisation fine des capteurs. Des solutions intermédiaires ont vu le jour, par exemple S-MAC (Sensor MAC) [Wei, *al*,2004] qui est une méthode d'accès au canal de type CSMA-CA avec le mécanisme RTS/CTS (Request to Send, Clear to Send) qui permet d'éviter les collisions et le problème de la station cachée. La principale innovation, apportée par ce protocole, est d'avoir un mécanisme de mise en veille distribué sur chaque nœud du réseau dans le but de réduire la consommation d'énergie. La principale difficulté de S-MAC est également de synchroniser les nœuds entre eux pour que la communication soit toujours possible.

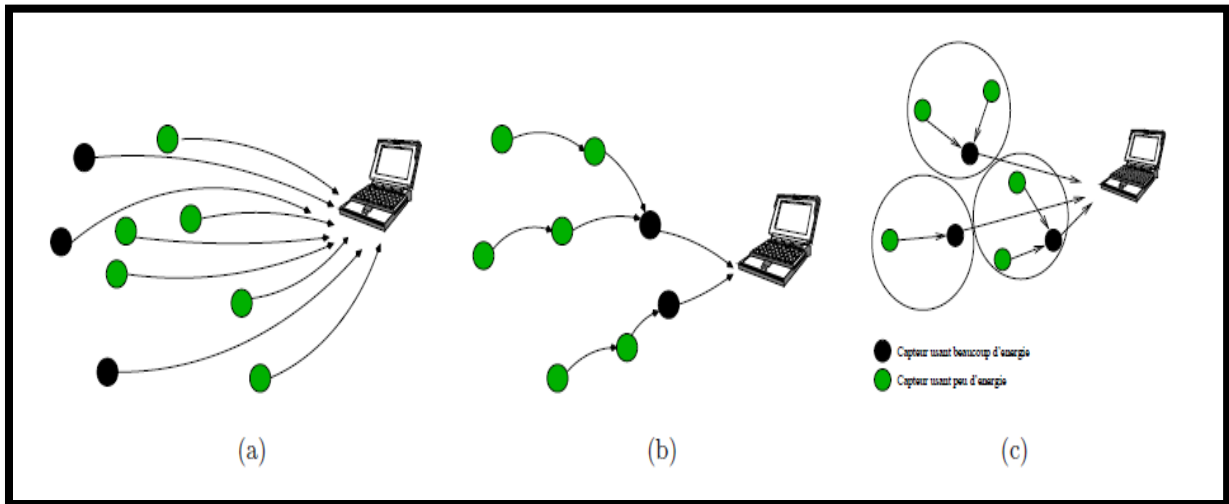
### **III.3.4.Limitation des accusés de réception**

L'acquittement systématique est mal adapté à des réseaux denses : il provoque une surcharge du réseau et donc des collisions et des interférences avec les données utiles échangées dans le réseau. Les acquittements par "piggy-backing" seront à privilégier.

### **III.3.5.Répartition de la consommation d'énergie**

La formation de "clusters" permet d'envisager des réseaux comportant un très grand nombre de capteurs. Elle favorise une meilleure répartition de la consommation

d'énergie. En effet, dans le cas d'une transmission directe vers l'observateur (a), les capteurs éloignés vont plus rapidement manquer d'énergie et les autres nœuds peuvent être sujets au phénomène d'overhearing dans le cas des réseaux "Mostly-On". Au contraire, dans le cas d'une transmission par saut (b).



**Figure III.1 : (a) - Transmissions directes. (b) - Transmission saut par saut. (c) -Hiérarchisation en clusters.**

Les nœuds proches de l'observateur vont être vite en rupture de batterie car ils seront plus sollicités pour relayer les messages des autres. La solution consiste à hiérarchiser les échanges en divisant la zone d'observation en clusters (c). Un "clusterHead" est élu pour chaque cluster. Il s'occupe de récupérer les informations auprès des capteurs de son cluster et de les transmettre directement à l'observateur. En changeant régulièrement de clusterHead, on obtient un réseau dans lequel aucun capteur n'est prédisposé à arriver en rupture de batterie avant les autres. Mettre en place des clusters va également permettre de cloisonner le réseau et ceci dans l'objectif de réduire les interférences. On améliore ainsi la qualité du lien radio et par conséquent, on limite les retransmissions liées aux reprises sur erreur. L'exemple phare d'une solution avec des clusters est le protocole LEACH [Wendi, al, 2000].

Par ailleurs, il existe dans la littérature d'autres mécanismes de conservation d'énergie, telles les techniques de compression, d'agrégation et de fusion de données, d'autres techniques de routage, etc.

### III.4. Durée de vie d'un réseau

Un réseau ne peut accomplir son objectif que tant qu'il est ((en vie)), mais pas au-delà. La durée de vie prévue est critique dans tout déploiement de réseaux de capteurs. Le but des scénarios applicatifs classiques consiste à déployer des nœuds dans un domaine sans surveillance pendant des mois ou des années. La vie d'un réseau de capteurs correspond à la période de temps durant laquelle le réseau peut, selon le cas : maintenir assez de connectivité, couvrir le domaine entier, ou garder le taux de perte d'information en-dessous d'un certain niveau. La vie du système est donc liée à la vie nodale, même si elle peut en différer. La vie nodale correspond à la vie d'un des nœuds du réseau. Elle dépend essentiellement de deux facteurs : l'énergie qu'il consomme en fonction du temps et la quantité d'énergie dont il dispose. Selon la discussion d'Akyildiz et al. Dans [*Ian F,al,2002*], la quantité prédominante d'énergie est consommée par un nœud-capteur durant la détection, la communication puis le traitement des données.

### III.5. Conservation d'énergie

Des mesures expérimentales ont montré que, généralement, c'est la transmission des données qui est la plus consommatrice en énergie, et de façon significative, les calculs eux consomment très peu [*Vijay, al, 2002*]. La consommation d'énergie du module de détection dépend de la spécificité du capteur. Dans de nombreux cas, elle est négligeable par rapport à l'énergie consommée par le module de traitement et, par-dessus tout, le module de communication. Dans d'autres cas, l'énergie dépensée pour la détection peut être comparable, ou supérieure à celle nécessaire à la transmission de données. En général, les techniques d'économie d'énergie se concentrent sur deux parties : la partie réseau (i.e., la gestion d'énergie est prise en compte dans les opérations de chaque nœud, ainsi que dans la conception de protocoles réseau), et la partie détection (i.e., des techniques sont utilisées pour réduire le nombre ou la fréquence de l'échantillonnage coûteux en énergie).

La durée de vie d'un réseau de capteurs peut être prolongée par l'application conjointe de différentes techniques [*Giuseppe,al,2009*]. Par exemple, les protocoles

efficaces en énergie visent à réduire au minimum la consommation d'énergie pendant l'activité du réseau. Toutefois, une quantité considérable d'énergie est consommée par les composants d'un nœud (CPU, radio, etc.), même s'ils sont inactifs. Un plan de gestion dédié à l'énergie peut alors être utilisé pour éteindre temporairement les composants du nœud lorsqu'ils ne sont pas sollicités.

### **III.6. Techniques du Duty-cycling**

Cette technique est principalement utilisée dans l'activité réseau. Le moyen le plus efficace pour conserver l'énergie est de mettre la radio de l'émetteur en mode veille (low-power) à chaque fois que la communication n'est pas nécessaire. Idéalement, la radio doit être éteinte dès qu'il n'y a plus de données à envoyer et ou à recevoir, et devrait être prête dès qu'un nouveau paquet de données doit être envoyé ou reçu. Ainsi, les nœuds alternent entre périodes actives et sommeil en fonction de l'activité du réseau. Ce comportement est généralement dénommé Duty-cycling. Un Duty-cycle est défini comme étant la fraction de temps où les nœuds sont actifs. Comme les nœuds-capteurs effectuent des tâches en coopération, ils doivent coordonner leurs dates de sommeil et de réveil. Un algorithme d'ordonnancement Sommeil/Réveil accompagne donc tout plan de Duty-cycling. Il s'agit généralement d'un algorithme distribué reposant sur les dates auxquelles des nœuds décident de passer entre l'état actif et l'état sommeil. Il permet aux nœuds voisins d'être actifs en même temps, ce qui rend possible l'échange de paquets, même si les nœuds ont un faible duty-cycle (i.e., ils dorment la plupart du temps).

#### **III.6.1. Protocoles Sleep/Wakeup**

Comme mentionné précédemment, un régime Sleep/Wakeup peut être défini pour un composant donné (i.e. le module Radio) du nœud-capteur. On peut relever les principaux plans Sleep/Wakeup implantés sous forme de protocoles indépendants au-dessus du protocole MAC (i.e. au niveau de la couche réseau ou de la couche application). Dans le document, les protocoles Sleep/Wakeup sont divisés en trois grandes catégories : à la demande, rendez-vous programmés, régimes asynchrones.

Les protocoles à la demande utilisent l'approche la plus intuitive pour la gestion d'énergie. L'idée de base est qu'un nœud devrait se réveiller seulement quand un autre nœud veut communiquer avec lui. Le problème principal associé aux régimes à la demande est de savoir comment informer un nœud en sommeil qu'un autre nœud est disposé à communiquer avec lui. A cet effet, ces systèmes utilisent généralement plusieurs radios avec différents compromis entre énergie et performances (i.e. une radio à faible débit et à faible consommation pour la signalisation, et une radio à "haut" débit mais à plus forte consommation pour la communication de données). Le protocole STEM (Sparse Topology and Energy Management) [Curt , al, 2002] ,par exemple, utilise deux radios.

Une autre solution consiste à utiliser une approche de rendez-vous programmés. L'idée est que chaque nœud doit se réveiller en même temps que ses voisins. Typiquement, les nœuds se réveillent suivant un ordonnancement de réveil et restent actifs pendant un court intervalle de temps pour communiquer avec leurs voisins. Ensuite, ils se rendorment jusqu'au prochain rendez-vous ;

Enfin, un protocole Sleep/Wakeup asynchrone peut être utilisé. Avec les protocoles asynchrones, un nœud peut se réveiller quand il veut et tant qu'il est capable de communiquer avec ses voisins. Ce but est atteint par des propriétés impliquées dans le régime Sleep/Wakeup, aucun échange d'informations n'est alors nécessaire entre les nœuds. Quelques régimes Sleep/Wakeup asynchrones sont proposés dans [Rong,al,2003].

#### **III.7.Protocoles du niveau MAC**

Plusieurs protocoles MAC pour les réseaux de capteurs sans fil ont été proposés, et de nombreux états de l'art et introductions aux protocoles MAC sont disponibles dans la littérature (par exemple [Ilker,al,2006] [Koen, 2008] [Wei,al,2004]). Nous nous concentrons principalement sur les questions de gestion d'énergie plutôt que sur les méthodes d'accès au canal. La plupart d'entre eux mettent en œuvre un régime avec un faible duty-cycle pour gérer la consommation d'énergie. Nous avons recensés les protocoles MAC les plus communs en les classant en trois



catégories : les protocoles fondés sur TDMA, les protocoles utilisant la contention et les protocoles hybrides.

### III.7.1. Protocoles MAC reposant sur TDMA

Dans les protocoles MAC fondés sur la méthode TDMA [Khaled,al,2002] [Jaap,200] [Wendi,al,2000] [Venkatesh,al,2003] le temps est divisé en trames (périodiques) et chaque trame se compose d'un certain nombre de slots de temps. A chaque nœud est attribué un ou plusieurs slots par trame, selon un certain algorithme d'ordonnement. Il utilise ces slots pour l'émission/réception de paquets de/vers d'autres nœuds.

Dans de nombreux cas, les nœuds sont regroupés pour former des clusters avec un clusterHead qui est chargé d'attribuer les slots de temps pour les nœuds de son cluster (par exemple, Bluetooth [Jaap,200], LEACH [Wendi,al,2000], et Energy-aware TDMA-based MAC [Khaled,al,2002]).

Exemple : un des protocoles TDMA important et efficace en énergie pour les réseaux de capteurs sans fil est TRAMA [Venkatesh,al,2003]. TRAMA divise le temps en deux parties, une période avec un accès aléatoire et une période avec un accès ordonné. La période d'accès aléatoire est consacrée à la réservation des slots et l'accès au canal est fondé sur la contention. A contrario, la période d'accès ordonnée est constituée par un certain nombre de slots de temps attribués à un nœud précis. L'algorithme de réservation des slots est le suivant.

Tout d'abord, les nœuds cherchent des informations sur un voisinage à deux sauts, qui sont nécessaires pour établir un ordonnancement sans collisions. Ensuite, les nœuds commencent une procédure d'élection afin d'associer chaque slot à un seul nœud. Chaque nœud aura une priorité pour être le propriétaire d'un slot. Cette priorité est calculée avec une fonction de hachage de l'identifiant du nœud et du numéro du slot. Le nœud avec la plus grande priorité devient le propriétaire du slot. Enfin, les nœuds envoient un paquet de synchronisation contenant la liste des voisins destinataires pour les transmissions suivantes. Par conséquent, les nœuds peuvent se

mettre d'accord sur les slots où ils doivent être éveillés. Les slots inutilisés peuvent être annoncés par leurs propriétaires pour être réutilisés par d'autres.

Les protocoles TDMA sont par nature efficaces en énergie, puisque les nœuds n'allument leur radio que lors de leurs propres slots et s'endorment le reste du temps. Toutefois, dans la pratique, les protocoles TDMA ont plusieurs inconvénients qui compensent les avantages en termes d'économie d'énergie [Injong,al,2008]. Premièrement, les algorithmes classiques de réservation de slots ont tendance à être complexes, peu flexibles et présentent des problèmes lors du passage à l'échelle. En effet, dans un véritable réseau de capteurs, les changements de topologie sont fréquents (conditions variables du canal, d'échecs de nœuds, . . .) et la répartition des slots peut être problématique dans de nombreux cas ; une approche centralisée peut être adoptée (LEACH [Wendi,al,2000]). Deuxièmement, ils requièrent une synchronisation très fine et ils sont très sensibles aux interférences [Giuseppe,al,2005]. En outre, les protocoles TDMA fonctionnent moins bien que les protocoles avec contention lors d'un trafic faible. C'est pour toutes ces raisons que les protocoles MAC TDMA ne sont pas très fréquemment utilisés dans les réseaux de capteurs.

#### III.7.2. Protocoles MAC avec contention

Les protocoles avec contention sont les plus populaires et représentent la majorité des protocoles MAC proposés pour les réseaux de capteurs sans fil. Ils assurent le duty-cycle par une intégration étroite des fonctionnalités d'accès au canal avec un régime Sleep/Wakeup. La seule différence est que, dans ce cas, l'algorithme Sleep/Wakeup n'est pas un protocole indépendant.

Exemples : un des plus populaires est B-MAC (MAC Berkeley) [Joseph, al,2004], avec une faible complexité et une faible consommation induite par le système d'exploitation TinyOS [tin]. L'objectif de B-MAC est de fournir quelques fonctionnalités de base et un mécanisme efficace en énergie pour l'accès au canal. Il met d'abord en œuvre les caractéristiques de base du contrôle d'accès au canal : un algorithme de back-off, une estimation efficace du canal et des acquittements

optionnels. Deuxièmement, pour atteindre un faible duty-cycle, B-MAC utilise un plan Sleep/Wakeup asynchrone fondé sur l'écoute périodique appelée Low Power Listening (LPL). Les nœuds se réveillent périodiquement pour vérifier l'activité sur le canal. La période entre deux réveils est nommée intervalle de vérification. Après le réveil, les nœuds restent actifs pour un temps de réveil, afin de détecter d'éventuelles transmissions. Contrairement au temps de réveil qui est fixé, l'intervalle de vérification peut être spécifié par l'application. Les paquets B-MAC sont constitués d'un long préambule et d'une charge utile. La durée du préambule est au moins égale à l'intervalle de vérification, afin que chaque nœud puisse toujours détecter une éventuelle transmission au cours de son intervalle de vérification. Cette approche ne nécessite pas que les nœuds soient synchronisés. En fait, quand un nœud détecte l'activité sur le canal, il reste actif et reçoit le préambule en premier puis la charge utile.

Un autre protocole MAC multi-sauts célèbre dans les réseaux de capteurs est S-MAC (Sensor- MAC) [Wei, *al*, 2004]. Il adopte un régime de communication avec planification par rendez-vous. Les nœuds échangent des paquets de synchronisation afin de coordonner leurs périodes Sleep/Wakeup. Chaque nœud peut établir son propre plan ou suivre le plan d'un voisin au moyen d'un algorithme distribué. Les nœuds utilisant le même plan forment un cluster virtuel. Un nœud peut éventuellement suivre deux plans s'ils ne se superposent pas, de sorte qu'il puisse faire un pont de communication entre différents clusters virtuels. Le temps d'accès au canal est divisé en deux parties. Dans la période d'écoute, les nœuds échangent des paquets de synchronisation et des paquets de contrôle pour éviter des collisions. Le transfert de données aura lieu dans le reste de la période. Les nœuds source et destination sont éveillées et communiquent entre eux. Les nœuds qui ne sont pas concernés par cette communication peuvent dormir jusqu'à la prochaine période d'écoute. Pour éviter les latences dans des environnements multi-sauts, S-MAC utilise un plan d'écoute adaptatif. Les paramètres du protocole S-MAC, i.e. les périodes d'écoute et de sommeil, sont constantes et ne peuvent pas être modifiées après le déploiement.

Les auteurs de [Tijs, al, 2003] proposent alors une version améliorée de S-MAC appelée Timeout MAC (T-MAC) et spécialement conçue pour une charge de trafic variable. Bien que les protocoles MAC fondée sur le duty-cycle soient efficaces en énergie, ils souffrent de la latence du sommeil, i.e., un nœud doit attendre que le récepteur se réveille avant qu'il puisse acheminer un paquet. Cette latence augmente avec le nombre de sauts. En outre, la diffusion de données à partir d'un nœud vers le puits peut connaître un problème d'interruption. En fait, la sensibilité de la radio limite la portée de l'overhearing. Les nœuds en dehors de la portée de l'émetteur ne peuvent donc pas entendre la transmission en cours et se rendorment. C'est pourquoi, dans S-MAC et T-MAC la diffusion de données est limitée à quelques sauts.

En outre, ils ont généralement un délai plus faible que ceux reposant sur TDMA et ils peuvent facilement s'adapter aux conditions de trafic. Malheureusement, leur dissipation d'énergie est plus élevée que celle des protocoles TDMA à cause de la contention et des collisions. Des mécanismes Duty-cycle peuvent contribuer à réduire la surconsommation d'énergie, mais ils doivent être conçus avec soin pour être flexibles et à faible latence.

#### **III.7.3. Protocoles MAC hybrides**

L'idée de base des protocoles MAC hybrides (changement du comportement du protocole entre TDMA et CSMA en fonction du niveau de contention) n'est pas nouvelle. Concernant les réseaux de capteurs sans fil, Z-MAC [Injong,al,2008] est l'un des protocoles les plus intéressants.

Afin de définir le schéma principal du contrôle de transmission, Z-MAC commence par une phase préliminaire de configuration. Chaque nœud construit une liste de voisins à deux sauts par le biais du processus de découverte de voisins. Puis, un algorithme distribué d'attribution des slots est appliqué pour faire en sorte que deux nœuds dans un voisinage à deux sauts ne soient pas affectés au même slot. Par conséquent, on est assuré qu'une transmission d'un nœud avec un de ses voisins à un saut n'interfère pas avec la transmission de ses voisins à deux sauts. Z-MAC permet à chaque nœud de maintenir son propre ordonnancement qui dépend du nombre de

voisins et évite tout conflit avec ses voisins de contention. Chaque nœud a des informations sur les slots de tous ses voisins à deux sauts et tout le monde se synchronise sur un slot de référence. Après cette phase d'initialisation, les nœuds sont prêts pour l'accès au canal. Les nœuds peuvent être soit en mode faible niveau de contention (LCL pour Low Contention Level), soit en mode haut niveau de contention (HCL pour High Contention Level). Un nœud persiste dans le mode LCL sauf s'il a reçu une notification (ECN pour Explicit Contention Notification). Dans le mode HCL, seuls les propriétaires du slot et leurs voisins à deux sauts sont autorisés à concourir pour l'accès au canal. En LCL (à la fois les propriétaires et les non-propriétaires) peuvent concourir pour transmettre dans n'importe lequel des slots. En revanche les propriétaires ont une priorité sur les autres. De cette façon, Z-MAC peut atteindre un niveau élevé d'utilisation du canal, même en faible contention, car un nœud peut transmettre dès que le canal est disponible. Les protocoles hybrides tentent de combiner les point forts des protocoles MAC fondés sur TDMA et ceux avec contention tout en compensant leurs faiblesses. Toutefois, ces techniques semblent être complexes pour être réalisables dans un déploiement d'un grand nombre de nœuds.

#### III.7.4. Techniques orientées données

Généralement, les plans Duty-cycling ne tiennent pas compte des données prélevées par les nœuds. Par conséquent, des approches orientées données peuvent être utiles pour améliorer l'efficacité en énergie. En fait, la détection (ou prélèvement de données) affecte la consommation d'énergie de deux manières :

- Des échantillons inutiles : les données échantillonnées ont souvent de fortes corrélations spatiales et/ou temporelle [Mehmet,al,2004], il est donc inutile de communiquer les informations redondantes à la Station de Base. Un échantillonnage inutile implique une consommation d'énergie à son tour inutile. En effet, même si le coût de l'échantillonnage est négligeable, cela induit aussi des communications tout le long du chemin qu'emprunte le message.
- La consommation électrique du module de détection : réduire la communication ne suffit pas lorsque le capteur est lui-même très consommateur. Des techniques orientées données sont conçues pour réduire la quantité d'échantillonnage de données en garantissant un niveau de précision

acceptable dans la détection pour l'application. Réduction des données en termes de volume ou de nombre de paquets, dans le réseau peut avoir un impact majeur sur la consommation d'énergie due à la communication.

Parmi les méthodes de réductions de données, nous trouvons le In-network processing qui consiste à réaliser de l'agrégation de données (par exemple, calculer la moyenne de certaines valeurs) au niveau des nœuds intermédiaires entre la source et le Sink. Ainsi, la quantité de données est réduite tout en parcourant le réseau vers le Sink. Une agrégation de données appropriée est spécifique à l'application. La compression de données peut être appliquée également pour réduire la quantité d'informations transmises par les nœuds sources. Ce régime implique l'encodage d'informations au niveau des nœuds qui engendrent des données, et le décodage au niveau du Sink.

### III.7.5. Acquisition de données efficace en énergie

De nombreuses applications émergentes ont des applications à de réelles contraintes dues à la détection. Ceci va à l'encontre de l'hypothèse générale selon laquelle la détection n'est pas significative d'un point de vue consommation d'énergie. En fait, la consommation d'énergie du module de détection peut, non seulement être significative, mais encore supérieure à la consommation d'énergie de la radio ou même plus grande que la consommation d'énergie du reste du nœud-capteur [Cesare, al,2007]. Cela peut être dû à différents facteurs [Vijay,al,2006].

- Transducteur gourmand en énergie : Certains capteurs ont intrinsèquement besoin d'une forte puissance pour s'acquitter de leur tâche d'échantillonnage. Par exemple, des capteurs d'images CMOS, voire des capteurs multimédias [Ian F, al,2007] ont généralement besoin de beaucoup d'énergie. Les capteurs chimiques ou biologiques peuvent aussi être gourmands en énergie.
- Convertisseurs A/D gourmands : des capteurs tels que les transducteurs acoustiques et sismiques [Geoffrey, al,2006] nécessitent généralement des convertisseurs A/D à haut débit et à grande résolution. La consommation d'électricité des convertisseurs représente la part la plus importante de la consommation d'énergie du sous-système de détection.
- Capteurs actifs : Une autre classe de capteurs peut obtenir des données du phénomène perçu par l'utilisation de transducteurs actifs (par exemple, sonar, radar ou laser). Dans ce cas, les capteurs doivent envoyer un signal de sondage

afin d'obtenir des informations sur la grandeur observée, comme dans [Maarten, al,2006].

- Temps d'acquisition long : Le temps d'acquisition peut être de l'ordre de plusieurs centaines de millisecondes, voire de quelques secondes. Par conséquent, l'énergie consommée par le sous-système de détection peut être élevé, même si la consommation d'énergie du détecteur reste modérée.

Dans ce cas, réduire les communications peut s'avérer insuffisant, mais les stratégies de conservation d'énergie doivent réellement réduire le nombre d'acquisitions (échantillons de données). Il faudrait également préciser que les techniques d'acquisition de données efficaces en énergie ne visent pas exclusivement à réduire la consommation d'énergie du module de détection. En réduisant les données prélevées par des nœuds sources, elles diminuent aussi le nombre de communications. En fait, beaucoup de techniques d'acquisition de données efficaces en énergie ont été conçues pour réduire au minimum l'énergie consommée par la radio, en supposant que la consommation de la radio est négligeable. La classification des approches d'acquisition de données efficaces en énergie présentée dans [Vijay,al,2006] est comme suit :

- Comme les échantillons mesurés peuvent être corrélés, les techniques d'échantillonnage adaptatif exploitent de telles similitudes pour réduire la quantité de données à acquérir par le transducteur. Par exemple, les données intéressantes peuvent changer lentement en fonction du temps. Dans ce cas, des corrélations temporelles peuvent être exploitées pour réduire le nombre d'acquisitions. Une approche semblable peut être appliquée lorsque le phénomène étudié ne change pas brusquement entre les régions couvertes par des nœuds voisins. L'énergie due au prélèvement (et à la communication) peut être alors réduite en profitant des corrélations spatiales entre les données prélevées. Clairement, des corrélations temporelles et spatiales peuvent être conjointement exploitées pour réduire sensiblement la quantité de données à acquérir.

- L'approche d'échantillonnage hiérarchique suppose que les nœuds sont équipés de sondes (ou détecteurs) de différents types. Alors que chaque sonde est caractérisée par une résolution donnée et sa consommation d'énergie associée, cette technique

choisit dynamiquement la classe à activer, afin d'obtenir un compromis entre la précision et l'économie d'énergie.

– Enfin, l'échantillonnage actif fondé sur un modèle adopte une approche semblable à la prévision de données. Un modèle du phénomène mesuré est établi lors des prélèvements de données, de telle sorte que les valeurs futures puissent être prévues avec une certaine précision. Cette approche exploite le modèle obtenu pour réduire le nombre d'échantillons de données, et également la quantité de données à transmettre à la Station de Base bien que ce ne soit pas leur objectif principal.

#### **III.7.6. Techniques de mobilité**

Dans certains cas où les nœuds sont mobiles, la mobilité peut être utilisée comme outil pour réduire la consommation d'énergie (au-delà du Duty-cycling et des techniques orientées données). Dans un réseau de capteurs statiques, les paquets provenant des nœuds suivent des chemins multi-sauts vers la station de base. Ainsi, certains chemins peuvent être chargés (sollicités plus que d'autres), et les nœuds proches de la Station de Base relayent plus de paquets [*Monique, al, 2009*] et sont plus sujets à l'épuisement prématuré de leurs batteries (funneling effet) [*Li Jian, al, 2007*]. Si certains nœuds (éventuellement, la station de base) sont mobiles, le trafic peut être modifié si les nœuds mobiles sont chargés de collecter des données directement à partir de nœuds statiques.

Les nœuds ordinaires attendent le passage d'un dispositif mobile pour lui envoyer leurs messages de telle sorte que la communication ait lieu à proximité (directement ou au plus avec un nombre limité de sauts). Par conséquent, les nœuds ordinaires peuvent économiser de l'énergie parce que la longueur du chemin, la contention et les overheads de diffusion sont ainsi réduits. En outre, le dispositif mobile peut visiter le réseau afin de répartir uniformément la consommation d'énergie due à la communication. Lorsque le coût de la mobilité des nœuds de capteurs est prohibitif, l'approche classique consiste à attacher un capteur à des entités qui seront en itinérance dans le champ de détection, comme des autobus ou des animaux.



Les stratégies reposant sur la mobilité peuvent être classées en deux ensembles : les stratégies avec un Sink mobile et les stratégies avec des relais mobiles, selon le type de l'entité mobile. Il est important de souligner ici que, lorsque nous examinons des systèmes mobiles, un problème important est le type de contrôle de la mobilité des nœuds qu'intègre la conception du réseau, ceci est détaillé dans [Giuseppe,al,2008]. Les nœuds mobiles peuvent être divisés en deux catégories : ils peuvent être spécifiquement conçus comme partie de l'infrastructure du réseau, ou faire partie de l'environnement.

Quand ils font partie de l'infrastructure, leur mobilité peut être entièrement contrôlée dans la mesure où ils sont, généralement, robotisés. Lorsque les nœuds mobiles font partie de l'environnement, ils pourraient ne pas être contrôlables. S'ils suivent un horaire strict, ils ont une mobilité complètement prévisible (par exemple, une navette pour les transports publics [Arnab, al,2003]). Sinon, ils peuvent avoir un comportement aléatoire de sorte qu'aucune hypothèse ne puisse être faite sur leur mobilité.

Enfin, ils peuvent suivre un schéma de mobilité, qui n'est ni prévisible, ni totalement aléatoire. Par exemple, c'est le cas d'un bus se déplaçant dans une ville, dont la vitesse est soumise à d'importantes variations en raison des conditions de circulation. Dans un tel cas, les schémas de mobilité peuvent être tirés en se fondant sur des observations et des estimations d'une certaine précision.

### **III.8. Techniques de routage**

Lors de la transmission d'un paquet d'une source vers une destination, il est nécessaire de faire appel à un protocole de routage pour acheminer correctement le paquet par le chemin le plus optimal. Plusieurs protocoles ont été proposés dans les réseaux ad hoc en général et d'autres réseaux en particulier ayant le même mode de fonctionnement que notre réseau. [E.Cizeron,2009] [Rémi,2011]

Le principal but de toute stratégie de routage est de mettre en œuvre une bonne gestion d'acheminement qui soit robuste et efficace. D'une manière générale, toute stratégie de routage repose sur des méthodes et des mécanismes pouvant être

regroupés en trois grandes classes: les protocoles de routage proactifs, les protocoles de routage réactifs et les protocoles de routage hybrides.

### **III.8.1. Définition du routage :**

Le routage est une méthode d'acheminement des informations à la bonne destination à travers un réseau de connexion donné. Le problème du routage ne se résume pas seulement à trouver un chemin entre les deux nœuds du réseau, mais encore à trouver un acheminement optimal des paquets à travers le réseau au sens d'un certain critère de performance. *[Mohammed,2011]*

### **III.8.2. Les protocoles de routage proactifs**

Le principe de cette classe *[E.Cizeron,2009] [Rémi,2011] [Jihene,2010]* repose sur des routes préétablies à l'avance. Les protocoles de routage proactifs utilisent une ou plusieurs tables de routage dans chaque nœud.

Ils essaient de maintenir les meilleurs chemins existants vers toutes les destinations possibles au niveau de chaque nœud du réseau. Pour se faire, ils utilisent l'échange régulier des messages de contrôle pour mettre à jour les tables de routages vers toute destination. Cette approche permet de disposer d'une route vers chaque destination instantanément, au moment où un paquet a besoin d'être routé.

Les tables de routage sont modifiées à chaque changement de la topologie du réseau. Cette approche offre un gain de temps lorsqu'une route est demandée, mais elle est coûteuse en termes de bande passante à cause de l'émission régulière des messages de contrôle surtout dans les réseaux à grande échelle. Les protocoles proactifs les plus utilisés sont DSDV, OLSR, FSR (Fisheye State Routing), LSR (Link State Routing Protocol), GSR (Global State Routing), ZHLS (Zone-based Hierarchical Link State).

- **Protocole OLSR (Optimized Link State Routing)**

OLSR [T .H.Clausen, al,2003] est un protocole de routage proactif à état de liens. Son innovation réside dans sa façon à économiser la consommation de la bande passante lors des diffusions (broadcast).

Ceci est réalisé grâce à l'utilisation du concept des "relais multipoints" (MPRs) dans lequel chaque nœud choisit un sous-ensemble de ses voisins pour retransmettre ses paquets en cas de broadcast.

En se basant sur le broadcast en utilisant les MPRs, tous les nœuds du réseau sont atteints avec un nombre réduit de répétitions. Un ensemble de MPRs d'un nœud  $N$  est l'ensemble minimal de ses premiers sauts voisins qui couvrent (dans le sens de la portée de communication) ses deuxièmes sauts voisins.

Dans OLSR, chaque nœud diffuse périodiquement des messages Hello qui contiennent l'état de ses liens avec ses premiers sauts voisins (unidirectionnel, bidirectionnel ou MPR pour dire que ce voisin est un MPR). Grâce aux messages Hello, un nœud construit sa table des voisins ainsi que la liste des voisins qui l'ont choisi comme MPR dits "MPR-sélecteurs". De plus, un nœud diffuse périodiquement des messages TC (*Topology Control*) contenant la liste de ses MPR-sélecteurs. En exploitant ces messages, chaque nœud remplit les deux champs nommés "destination" (correspond aux MPR-sélecteurs dans le message TC) et "dernier saut" (prend comme valeur l'identificateur du nœud émetteur du message TC) d'une table dite de topologie. Les tables de topologie et des voisins sont exploitées pour construire la table de routage.

Il faut noter que le protocole OLSR est bien adapté à un réseau haute densité. Dans un réseau à faible densité, chaque voisin devient MPR et OLSR se réduit à un protocole à état de liens pur.

- **Protocole DSDV (Destination Sequenced Distance Vector)**

Dans son fonctionnement de base, le protocole DSDV [C.p, al,1994] partage la même philosophie que les algorithmes à vecteur de distances. La contribution principale du protocole DSDV est l'utilisation des numéros de séquence qui permettent d'éviter la formation des boucles de routage.

Quand un nœud reçoit plusieurs paquets de mise à jour au sujet d'un même nœud destination, il choisit celui avec le numéro de séquence le plus haut. Le numéro de séquence est utilisé afin d'éviter le problème des boucles infinies et des transmissions inutiles des messages sur le réseau. Il permet en plus de maintenir la consistance des informations de routage. A cause de la mobilité des nœuds dans le réseau sans fil mobile, les routes changent fréquemment, ce qui fait que les routes maintenues par certains nœuds, deviennent invalides. Les numéros de séquence permettent d'utiliser les routes les plus nouvelles (les plus fraîches (fresh routes)).

Un nœud qui détecte la rupture d'un lien, génère un paquet de mise à jour dont le numéro de séquence possède une valeur infini. En recevant ce paquet, chaque nœud retire l'entrée correspondante de sa table de routage. Pour assurer la consistance des tables de routage, les mises à jour de ces derniers s'effectuent périodiquement et immédiatement après un changement de topologie. Pour réduire la quantité du trafic que génèrent ces mises à jour, deux types de paquets sont utilisés. Le premier, appelé " *full dump* ", contient toutes les informations de routage. Dans le cas d'une mobilité réduite, des paquets plus petits dits "*incremental*" sont utilisés; ils contiennent juste les informations de routage ayant changées depuis la dernière mise à jour complète. Une autre solution pour réduire le trafic dans le réseau est que les nœuds reportent les mises à jour par un laps de temps qui vaut le temps moyen nécessaire à la découverte du chemin le plus court vers une destination donnée.

### III.8.3. Les protocoles de routage réactifs

Le principe de cette classe [E.Cizeron,2009] [Rémi,2011] [Jihene,2010] est que les routes sont établies à la demande. Ces protocoles se basent sur la découverte et le

maintien des routes. Suite à un besoin, une procédure de découverte globale de route est lancée, ce processus s'arrête une fois la route trouvée ou toutes les possibilités sont examinées. Dès que la communication est établie, cette route est maintenue jusqu'à ce que la destination devienne inaccessible ou jusqu'à ce que la route ne soit plus désirée. Ce type de routage minimise l'échange des messages de contrôle, ce qui libère la bande passante, cependant il est lent à cause de la recherche des chemins, ce qui peut dégrader les performances des applications interactives. Parmi les protocoles basés sur ce principe, nous citons DSR, AODV, TORA (Temporally Ordered Routing Algorithm), EARP (Energy Aware Routing Protocol), CEDAR (Core Extraction Distributed for Adhoc Routing algorithm), SSR (Signal Stability Routing), LAR (Location Aided Routing protocol).

- **Protocole AODV (Ad hoc On Demand Distance Vector)**

Le protocole de routage AODV [C.p,2003], tout comme DSR, repose sur le mécanisme de découverte de chemins à la demande mais il n'utilise pas le routage source. Il repose sur le routage saut par saut. Chaque nœud dans AODV, maintient une table de routage et utilise les numéros de séquence comme DSDV pour éviter le problème des boucles de routage.

A la réception d'un paquet RREQ, le nœud destination répond en envoyant un paquet RREP vers le nœud source. Un nœud intermédiaire peut également répondre au paquet RREQ s'il possède un chemin valide vers la destination en question, sinon il incrémente le compteur des sauts du paquet RREQ et garde la trace de ce dernier et il le rediffuse ensuite à ses voisins.

Chaque nœud maintient aussi l'adresse du voisin qui lui a transmis le paquet RREQ, pour pouvoir acheminer ultérieurement le paquet RREP. En recevant un paquet RREP, chaque nœud enregistre l'adresse du nœud qui lui a envoyé le paquet RREP pour qu'il puisse acheminer après les paquets de données, et il le retransmet.

La maintenance des chemins dans AODV est basée sur l'échange périodique de messages «Hello». Un nœud qui ne reçoit pas de messages «Hello» d'un voisin

pendant une période de temps donnée, considère que la liaison avec ce voisin est rompue. Dans ce cas, il envoie un paquet RERR à tous ses voisins actifs pour invalider tous les chemins qui utilisent le lien brisé. Ces nœuds à leur tour renvoient le même paquet à leurs voisins jusqu'à ce que tous les nœuds sources actifs soient prévenus de la rupture. Dès la réception de ce paquet, le nœud source ré-initie une nouvelle découverte de chemins.

- **Protocole DSR (Dynamic Source Routing)**

DSR [D.johnson,2007] est un protocole de routage source. Il est composé de deux mécanismes: la découverte des chemins et la maintenance des chemins. Un nœud qui veut transmettre des données vers une destination, ne maintient aucun chemin vers cette dernière dans sa mémoire. Il initie une découverte de chemins en diffusant un paquet RREQ vers tous ces voisins. Un nœud intermédiaire qui reçoit ce paquet peut répondre de son cache, s'il connaît un chemin vers la destination, sinon il insère son adresse dans le paquet et le rediffuse.

Le nœud qui répond au paquet RREQ, s'il est la destination, génère un paquet RREP et il inclut dans ce dernier la séquence des nœuds enregistrés dans le RREQ. Sinon, il effectue une concaténation de la séquence des nœuds incluse dans le RREQ avec le chemin enregistré dans son cache. Si le nœud générant le RREP maintient un chemin vers la source, il envoie le RREP sur ce chemin. Un nœud qui ne maintient pas un chemin pareil, transmet le RREP en suivant le chemin inverse de celui dans le RREQ si les liens sont bidirectionnels. Sinon une nouvelle découverte de chemins est initiée en incluant la réponse dans un paquet RREQ.

Un nœud qui transmet un paquet en utilisant un chemin source est responsable de confirmer la bonne réception de ce dernier. Le paquet est retransmis jusqu'à la réception d'une confirmation ou jusqu'à ce que le nombre maximal de retransmission soit atteint. Si les tentatives de retransmission échouent ou le nombre maximal de retransmissions est atteint, un paquet RERR sera transmis vers le nœud source identifiant le lien brisé. En recevant ce paquet, le nœud source retire de son cache les

entrées qui contiennent ce lien. Si aucun chemin alternatif n'est disponible, il ré-initialise une nouvelle découverte de chemins.

#### **III.8.4. Le routage hybride**

Les protocoles hybrides combinent les approches réactive et proactive. Le principe est de connaître notre voisinage de manière proactive jusqu'à une certaine distance (par exemple trois ou quatre saut), et si jamais une application cherche à envoyer quelque chose à un nœud qui est dans cette zone, d'effectuer une recherche réactive à l'extérieur. Avec ce système, on dispose immédiatement des routes dans notre voisinage proche, et lorsque la recherche doit être étendue plus loin, elle est optimisée (un nœud qui reçoit un paquet de recherche de route réactive va tout de suite savoir si la destination est dans son propre voisinage. Si c'est le cas, il va pouvoir répondre, et sinon il va propager de manière optimisée la demande hors de sa zone proactive). Selon le type de trafic et les routes demandées, ce type de protocole hybride peut cependant combiner les désavantages des deux méthodes : échange de paquets de contrôle réguliers et inondation de l'ensemble de réseau pour chercher une route vers un nœud éloigné.

- ***LEACH (Low-Energy Adaptive Clustering Hierarchy)***

Il est l'un des protocoles de routage hiérarchique le plus populaire pour les réseaux de capteurs. L'idée est de former des clusters de nœuds de capteurs basés sur les zones où il y a un fort signal reçu, puis utiliser des Clusters-Heads locaux comme passerelle pour atteindre la destination. Cela permet d'économiser de l'énergie car les transmissions ne sont effectuées que par les Cluster-Head plutôt que par tous les nœuds de capteurs. [W.R.heinzelman,2000]

- ***PEGASIS (Power-Efficient Gathering in Sensor Information Systems)***

C'est une version améliorée du protocole LEACH. PEGASIS forme des chaînes plutôt que des clusters de nœuds de capteurs afin que chaque nœud transmette et

reçoive uniquement des données d'un voisin. Un seul nœud est sélectionné à partir de cette chaîne pour transmettre à la station de base. L'idée de PEGASIS est d'utiliser tous les nœuds pour transmettre ou recevoir des données avec ses plus proches voisins. Il déplace les données reçues de nœud à nœud, puis les données seront agrégées jusqu'à ce qu'elles atteignent tous la station de base. Donc, chaque nœud du réseau est tour à tour un chef de file de la chaîne, ainsi que responsable pour transmettre l'ensemble des données recueillies et fusionnées par la chaîne de nœuds au niveau de la station de base. [S.Lindsey,al,2002]

- **HEED (Hybrid Energy-Efficient Distributed clustering)**

C'est un algorithme distribué de clusterisation proposé pour les réseaux de capteurs. HEED construit des Cluster-Heads connectés à plusieurs sauts. Les clusters formés sont disjoints.

Les Cluster-Heads sont élus en se basant sur l'énergie résiduelle de chaque nœud. Les nœuds ayant une haute énergie résiduelle deviennent Cluster-Heads. Cet algorithme invoque aussi une métrique secondaire utilisée pour rompre l'égalité. Le cas d'égalité dans ce contexte inclut le cas quand un nœud se trouve à proximité de deux Cluster-Heads et quand deux

Cluster-Heads se trouvent dans le même rayon. Cette métrique est une métrique de coût de communication qui peut être fonction de la proximité des voisins ou de la densité du cluster. [O.Younis,al,2004]

- **CBRP (Cluster Based Routing Protocol).**

Ce dernier étant très répandu dans les réseaux MANET [Mukesh,2010] [Mohammed,al,2012], notre choix s'est naturellement porté sur lui, vu ses nombreux avantages par rapport aux autres protocoles,



### III.9.Principe de clustering

La technique de clustérisations consiste à organiser les nœuds du réseau en des groupes virtuels appelés “clusters”. Les nœuds, géographiquement voisins, sont regroupés dans un même cluster selon certaines règles. Dans un cluster, on retrouve généralement trois types de nœuds: “cluster-Head”, nœuds “passerelles” et nœuds “ordinaires ” dite aussi membre. Dans chaque cluster, un nœud est élu comme chef de groupe, appelé cluster-Head, qui possède des fonctions supplémentaires (routage, accès au médium, etc.). Une passerelle est un nœud non-cluster-Head qui possède des liens inter-clusters et peut donc accéder à des clusters voisins et acheminer les données entre eux, tandis qu’un nœud ordinaire est un nœud non-cluster-Head qui ne possède pas des liens avec les autres clusters. *[Mario, al, 1995]*

#### III.9.1.Rayon des clusters

Le rayon d’un cluster exprime la valeur maximale de la distance qui sépare le clusterhead à l’ensemble de ses membres. Cette distance est exprimée en nombre de sauts. Nous distinguons alors trois classes d’algorithmes : les algorithmes à 1 saut, les algorithmes à K sauts et les algorithmes à rayon variable. *[Ching-Chuan, al, 1997]*

#### III.9.2.Métrique de sélection des cluster-Heads

Plusieurs métriques ont été proposées dans la littérature pour élire l’ensemble des cluster-heads. Nous proposons de classer les algorithmes de clustérisations dans cinq classes selon le type des métriques employé lors de la sélection des cluster-Heads. Ces cinq classes sont les suivantes :

- **Sans métrique** : regroupe les algorithmes qui déclarent les cluster-heads sans avoir recours à aucune métrique de sélection.
- **Métrique arbitraire** : représente une valeur choisie arbitrairement et généralement non significative. Dans cette classe, nous trouvons les algorithmes qui utilisent des valeurs aléatoires ou l’identifiant des nœuds.
- **Métriques liées à la topologie** : dans cette classe nous groupons tous les algorithmes qui utilisent une métrique issue de la topologie du réseau. Parmi les

métriques qui appartiennent à cette classe nous citons : le degré de connectivité, le k-degré de connectivité et la k-densité.

- **Métriques spécifiques au nœud mobile** : les algorithmes de cette classe utilisent des métriques très spécifiques aux nœuds mobiles. Dans le cas général, ces algorithmes supposent connaître certaines informations sur chaque nœud tel que sa mobilité, la puissance des signaux reçus, le niveau d'énergie ou encore sa position géographique. Dans cette classe nous avons distingué trois sous classes qui sont :

- ⊙ Mobilité requise : regroupe les algorithmes qui supposent que les nœuds ont une connaissance de leur mobilité.

- ⊙ Niveau énergie requis : regroupe tous les algorithmes qui utilisent la valeur de l'énergie restante dans les batteries des nœuds comme métrique de sélection des cluster-heads.

- ⊙ Position géographique requise: cette classe d'algorithmes suppose que chaque nœud a la capacité de déterminer sa position géographique par exemple à travers un système GPS.

- **Métriques combinées** : plusieurs algorithmes combinent plusieurs métriques de différents types pour élire l'ensemble de cluster-Heads. [Mario, al, 1995]

-

### III.9.3. Structure de l'ensemble des cluster-Heads

Les cluster-Heads élus forment des structures particulières parmi lesquelles nous citons :

- DS (Dominating Set) : ensemble dominant ;
- CDS (Connected Dominating Set) : ensemble dominant connecté ;
- WCDS (Weakly Connected Dominating Set) : ensemble dominant faiblement connecté ;
- IS (Independent Set) : ensemble indépendant ;
- MIS (Maximal Independent Set) : ensemble indépendant maximal. [Ching-Chuan, al, 1997]

### III.9.4. Avantage de clustering

- En premier, la structure de clusters permet la réutilisation des ressources du réseau
- Deux clusters peuvent utiliser la même fréquence s'ils ne sont pas voisins
- les nœuds de chaque cluster sont supervisés par leur cluster-Head qui peut coordonner l'accès au canal
- l'ensemble des cluster-Heads et des passerelles peut former une dorsale virtuelle pour le routage inter cluster. [*Mario, al, 1995*]

### III.10. Conclusion

Divers techniques sont appliquées pour satisfaire l'un des paramètres (énergie, débit et localisation) existents déjà, ce chapitre nous a permis de citer la majorité de ces techniques pour avoir une idée très claire afin d'élaborer un modèle propre à nous.

# **Chapitre IV**

## **Analyse et résultats de simulation**

## Chapitre IV : Analyse et résultats de simulation

### IV.1.Introduction

Après l'analyse et l'étude des protocoles de routage, et celle d'économie d'énergie effectuée, dans le quatrième chapitre nous allons expliquer notre proposition et valider nos résultats par simulation, sur ns-3.

Nous avons choisi le logiciel NS3 car c'est un très bon outil dans le domaine de la recherche, et du développement de nouveaux protocoles pour différents types de réseaux.

### IV.2.Présentation du simulateur ns-3

Ns-3 est un simulateur de réseau à événements discrets ciblés principalement pour la recherche et l'utilisation pédagogique. Le projet ns-3, a commencé en 2006, c'est un projet open-source de développement *ns-3*.

Ns-3 a été développé pour fournir une plate-forme extensible de simulation ouverte, pour la recherche de réseaux et de l'éducation. En bref, *ns-3* fournit des modèles de la façon dont les réseaux travail et effectue des données par paquets, et fournit un moteur de simulation pour les utilisateurs pour mener des expériences de simulation. Certaines des raisons à utiliser *ns-3* comprennent de réaliser des études qui sont plus difficile ou impossible de réaliser avec les systèmes réels, pour étudier le comportement du système dans un environnement hautement reproductible contrôlé, et d'apprendre comment fonctionnent les réseaux. Les utilisateurs pourront noter que le modèle disponible mis en *ns-3* se concentre sur la modélisation comment les protocoles de l'Internet et des réseaux travail, mais *ns-3* ne se limite pas aux systèmes d'Internet; plusieurs utilisateurs utilisent *ns-3* pour modéliser des systèmes non basés sur Internet.

- *Ns-3* est open-source, et le projet vise à maintenir un environnement ouvert pour les chercheurs à contribuer et partager leur logiciel.
- *Ns-3* n'est pas une extension vers l'arrière-compatible de ns-2 ; c'est un nouveau simulateur. Les deux simulateurs sont tous les deux écrits en C ++

mais *ns-3* est un nouveau simulateur qui ne supporte pas les *ns-2* API. Certains modèles de *ns-2* ont déjà été portés de *ns-2* à *ns-3*. Le projet continuera à maintenir *ns-2* tandis que *ns-3* est en cours de construction, et étudiera les mécanismes de transition et d'intégration.

- *Ns-3* est conçu comme un ensemble de bibliothèques qui peuvent être combinés ensemble et aussi avec d'autres bibliothèques de logiciels externes. Alors que certaines plates-formes de simulation fournissent aux utilisateurs un environnement unique de l'interface utilisateur, il intègre une interface graphique dans laquelle toutes les tâches sont effectuées, *ns-3* est plus modulaire à cet égard. Plusieurs animateurs externes, des analyses de données et des outils de visualisation peuvent être utilisés avec *ns-3*. Toutefois, les utilisateurs doivent attendre à travailler à la ligne de commande et avec des outils de développement et de logiciels C++ / Python.

- *Ns-3* est principalement utilisé sur les systèmes Linux, mais il existe un soutien pour FreeBSD, Cygwin (pour Windows), et le support de Windows Visual Studio natif est en train d'être développé.

- *Ns-3* n'est pas un produit logiciel officiellement pris en charge de toute entreprise. Le support de *ns-3* se fait sur une base des meilleurs efforts sur le NS-3-liste de diffusion. [*Oxygen, 2011*]

### IV.2.1.Outil de NS-3

- Outils de visualisation du scénario de simulation

PyViz (visualisation en temps réel)

- NetAnim (visualisation basée sur un fichier traçant le scénario)

Outils de traçages d'information

Fichier ASCII

Fichier pcap (wireshark)

Outils de traçage de trafic

Fichier simple

Fichier pour Gnuplots de NS-3

### IV.2.2. Quelques possibilités de simulation en NS-3

- Simulation de protocoles

TCP, UDP, IPv4, IPv6, OLSR, AODV . . .

- Simulation de médias

Ethernet, WIFI, WiMAX . . .

- Définition de la topologie du réseau

Statique ou dynamique (modèles de mobilité)

- Possibilité d'émulation

Exécution d'une implémentation d'un protocole dans ns-3

### IV.2.3. Modules présent en NS-3

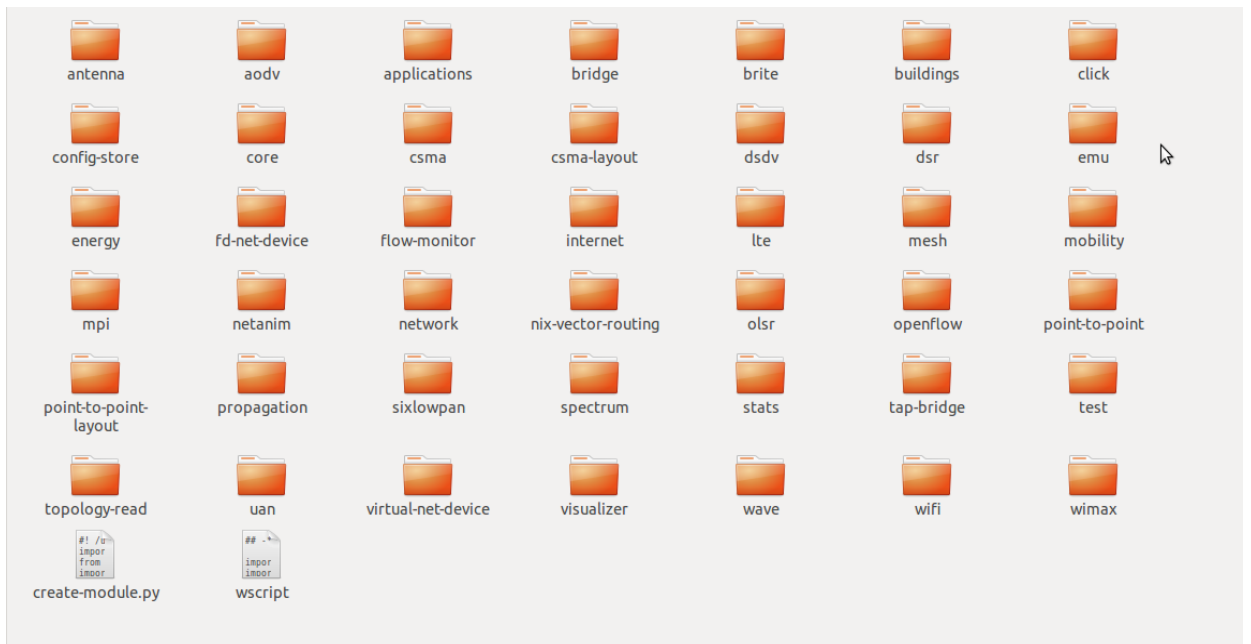


Figure IV.1 : Les modules présents dans NS-3. [Oxygen, 2011].

**IV.2.4. Comparaison entre ns-2 et ns-3**

NS-3	NS-2
<ul style="list-style-type: none"> <li>- <i>Ns-3</i> est activement maintenue avec un rôle actif.</li> <li>- Disponibilité d'un environnement d'exécution de code de mise en œuvre.</li> <li>- Un niveau de base d'abstraction inférieur permettant de mieux aligner avec la façon dont les systèmes réels sont mis ensemble.                             <ul style="list-style-type: none"> <li>- Programmation des scripts en C++ et python.</li> <li>- <i>Ns-3</i> n'est pas rétro compatible avec <i>ns-2</i>.</li> <li>- <i>Ns-3</i> est amélioré continuellement.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>- <i>Ns-2</i> est légèrement maintenus et n'a pas connu un développement significatif dans son arbre principal de code.</li> <li>- Non disponibilité d'un environnement d'exécution de code de mise en œuvre.</li> <li>- Un niveau de base d'abstraction supérieur.</li> <li>- Programmation des scripts en OTcl.</li> <li>- Apports plus nombreux en NS-2.</li> </ul>

**Tableau IV-1 : Comparaison entre ns2 et ns3**

**IV.3. Notre modèle**

Il existe de différentes solutions, et propositions pour améliorer la QoS et maximiser la durée de vie d'un réseau sans fil. Dans notre cas nous allons combiner entre les 3 couches basses du modèle OSI pour satisfaire seulement deux paramètres qui sont l'énergie et le débit.

Au niveau de la couche physique qui consiste à déployer des différentes technique pour améliorer l'économie d'énergie, dans notre cas nous avons exploité l'un des avantages de ns3, nous avons testé tous les protocoles déjà intégré dans une version très ressentie de notre logiciel et exploiter le meilleur.

La couche MAC est une couche très riche en termes d'amélioration de la QoS. Comme le wifi en générale fonctionne avec le CSMA/CA pour éviter les collisions, nous avons supprimé ce protocole, puisque le débit est le seul paramètre de QoS à étudier.

Les protocoles de routage peuvent améliorer la QoS. De nos jours les utilisateurs wifi sont de plus en plus nombreux entourer d'une seule station de base ! et évidemment



plus que le nombre de clients augmente plus que le débit diminue, pour éviter ce problème nous avons choisi une architecture en clustering d'où nous avons intégré un protocole non existant sur ns3 et comparer notre résultats avec le standard

#### **IV.4. Simulation et interprétation des résultats**

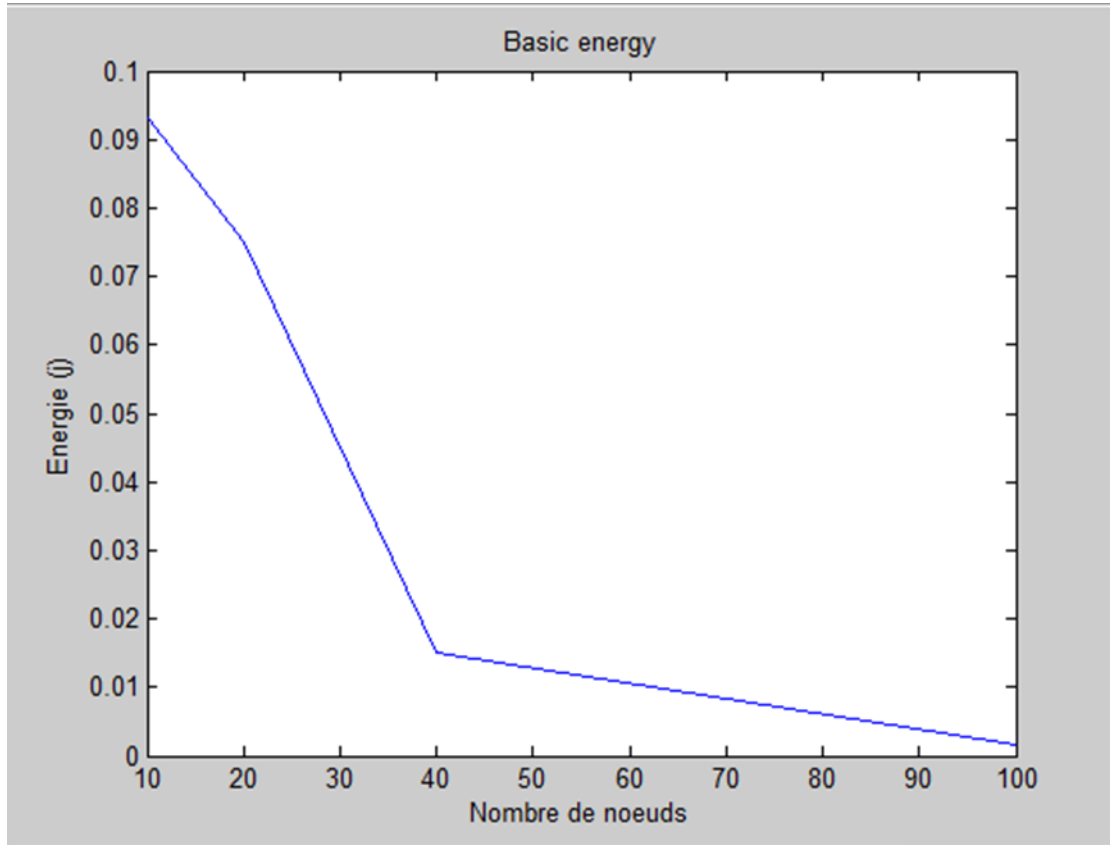
##### **IV.4.1. Économie de l'énergie**

La consommation d'énergie est une question clé pour les appareils sans fil, et les chercheurs du réseau sans fil ont souvent besoin d'enquêter sur la consommation d'énergie à un nœud ou dans l'ensemble du réseau tout en exécutant des simulations de réseau ns-3. Cela nécessite ns-3 pour soutenir la modélisation de la consommation d'énergie. En outre, comme des concepts tels que les piles à combustible et de récupération de l'énergie sont de plus viable pour les appareils sans fil de faible puissance, intégrant l'effet de ces technologies émergentes dans simulations nécessite un soutien pour la modélisation des diverses sources d'énergie en ns-3. Le Cadre de l'énergie ns-3 fournit la base pour la consommation d'énergie, source d'énergie et de la modélisation de la récupération d'énergie.

##### **IV.4.2. Résultat obtenu après la simulation**

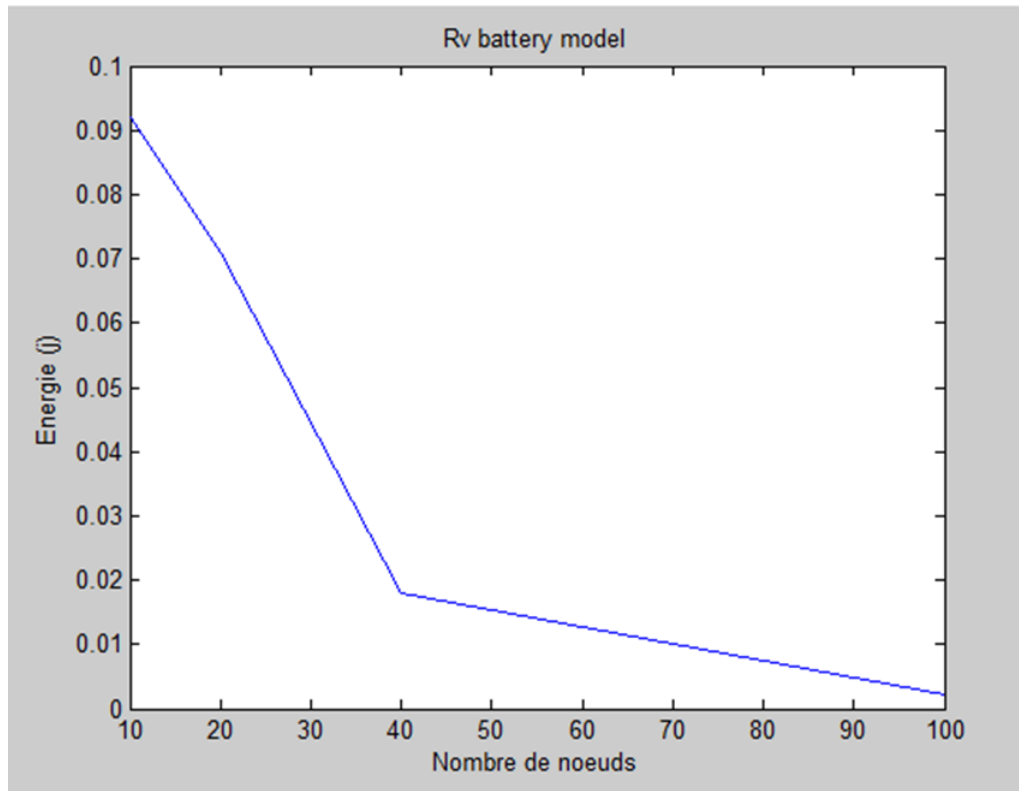
Dans NS-3 il existe quatre modèles d'économies d'énergies, nous avons fait appel à eux un par un, pour voir celui qui consomme moins l'énergie du réseau.

En premier, nous avons utilisé le modèle **Basic Energy** , nous avons remarqué que l'énergie restante au bout de 60 secondes diminue en augmentant le nombre des nœuds est le résultat n'était pas très satisfaisant (énergie restante « 100nœuds » =0.0016j).



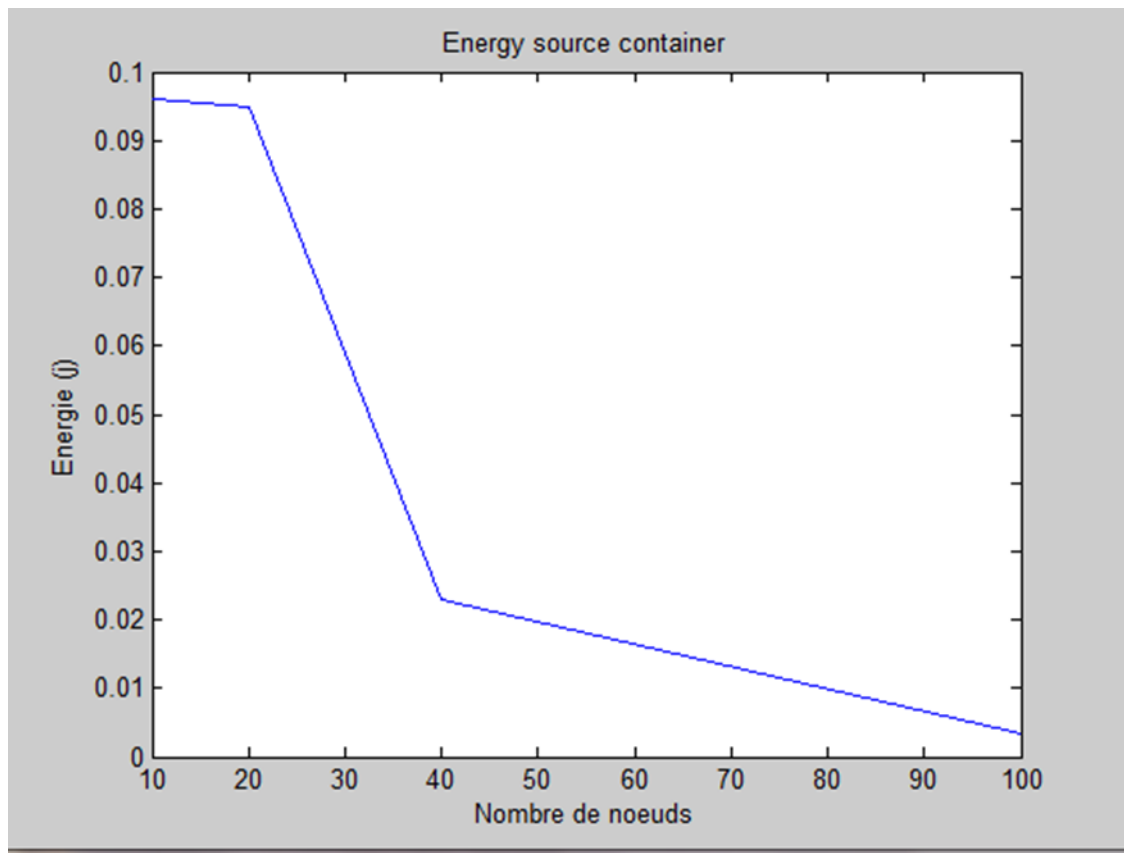
**Graphe IV-1 : Résultat du modèle d'énergie Basic energy model**

Ensuite, nous avons employé le modèle rv battery model, le résultat était plus au moins amélioré que le Protocole précédent (énergie restante « 100noeuds » =0.0023j).



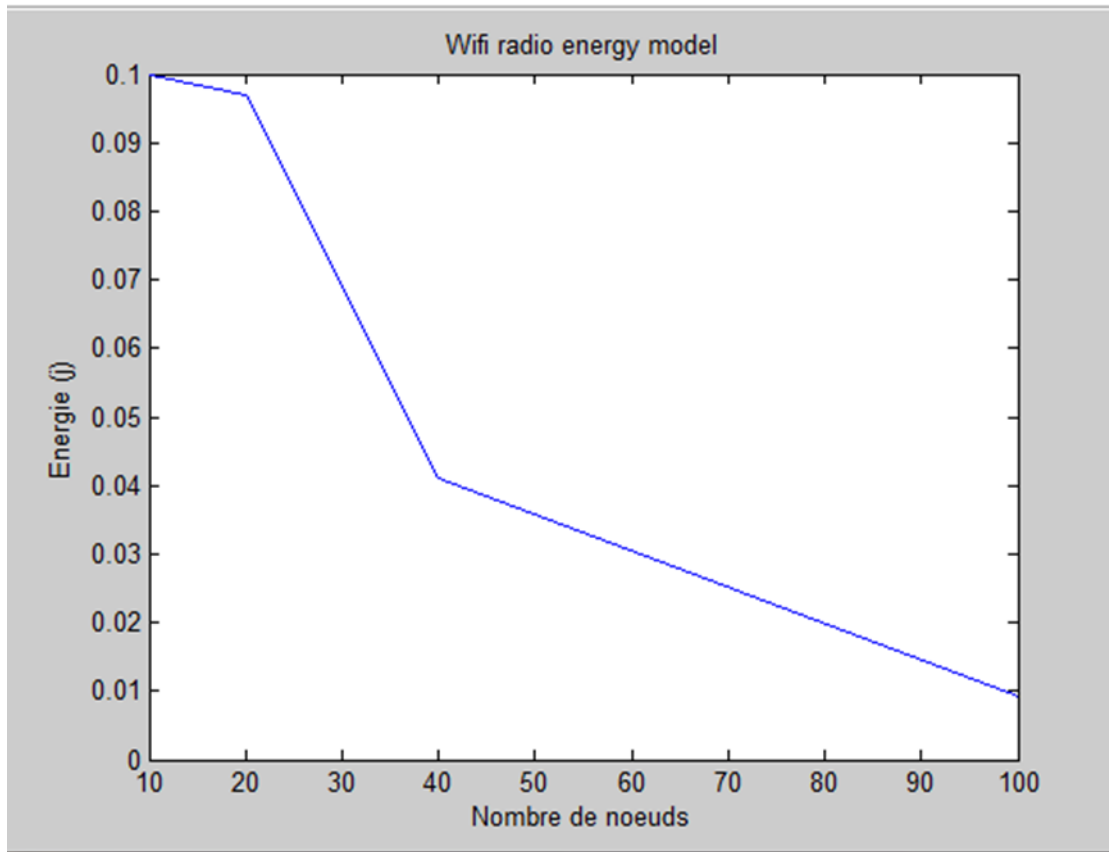
**Graphe IV-2 : Résultat du modèle d'énergie Rv battery model**

Puis, nous avons fait appel au modèle **Energy source container**, nous avons observé que le résultat a augmenté (énergie restante « 100noeuds » =0.0033j).



Graphe IV-3 : Résultat du modèle d'énergie Energy source container

Par contre, lorsque nous avons appliqué le modèle wifi radio Energy model, nous avons constaté une amélioration très importante, cela nous a permis de distinguer que ce Protocol est le plus adaptés avec notre but (énergie restante « 100noeuds » =0.0091j).



**Grphe IV-4 : Résultat du modèle d'énergie Wifi radio energy model**

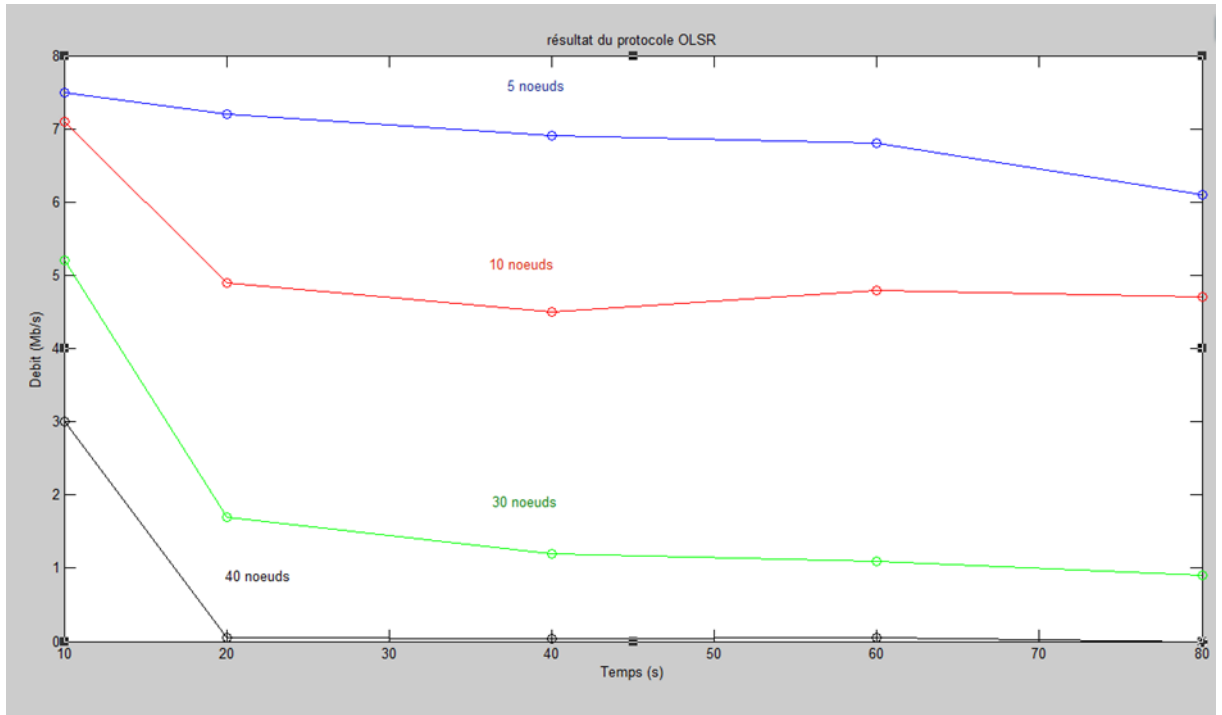
Vue les résultats obtenus, le protocole wifi radio énergie est le meilleur en terme d'augmenté la durée de vie d'un réseau.

#### **IV.4.3. Augmentation du débit**

Pour l'augmentation du débit, nous avons fait une comparaison entre deux protocoles de routages OLSR (Optimized Link State Routing) et le CBRP (Cluster Based Routing Protocol) et nous les avons appliqués avec le modèle d'énergie wifi radio Energy. Cela est effectué par des calculs de débit en fonction du temps dont nous avons varié le nombre des nœuds.

#### IV.4.4. Résultat obtenu après la simulation du protocole OLSR

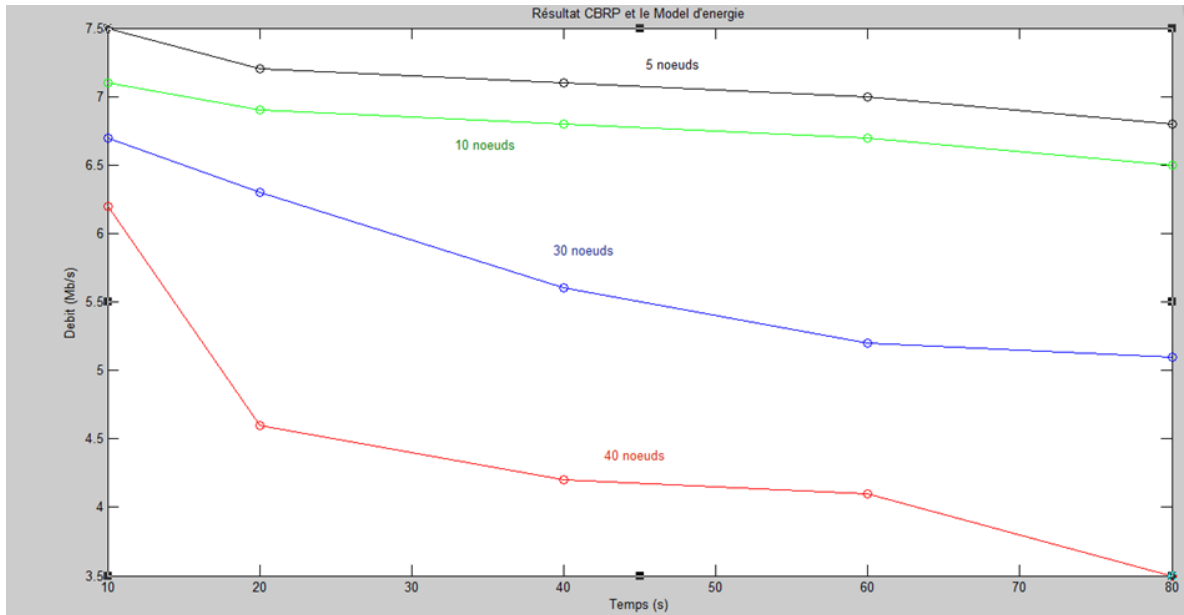
Au début nous avons essayé le protocole OLSR, nous avons aperçus que le débit à diminuer jusqu'à l'annulation lorsque nous avons varié le temps et augmenter le nombre des nœuds.



Graphe IV-5 : Résultat du protocole OLSR appliqué sur une variété de nœuds

#### IV.4.5. Résultat obtenu après la simulation du protocole CBRP

Contrairement à l'OLSR, lorsque nous avons utilisé le CBRP, le débit est resté quasi stable, et pour cela, nous l'avons choisi pour l'obtention de notre objectif.

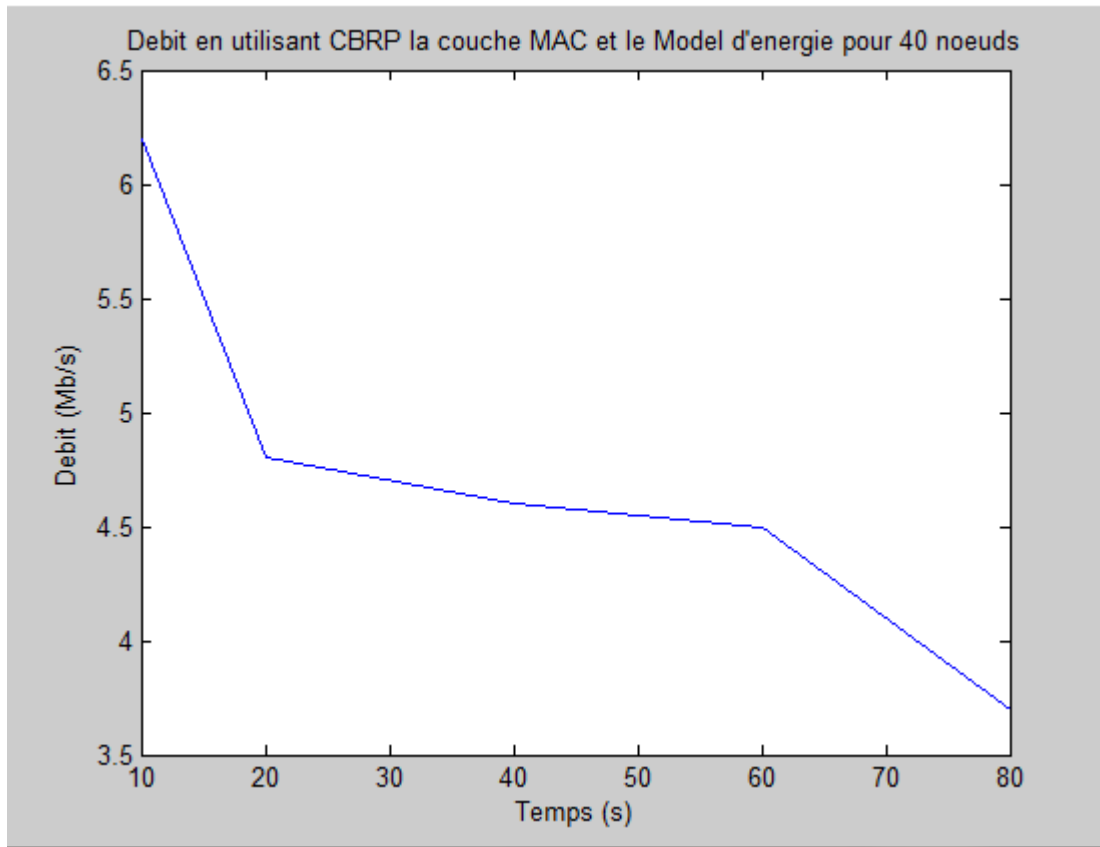


**Graphe IV-6 : Résultat du protocole CBRP appliqué pour une variété de nœuds**

La mobilité des clients pose beaucoup de problèmes dans les réseaux sans fil en général et l'énergie et le débit se dégradent proportionnellement. Dans notre cas, nous avons assimilé les clients aux membres dans l'architecture CBRP.

Dans notre étude, nous avons combiné entre deux caractéristiques du standard IEEE802.11v qui sont l'augmentation du débit et la consommation d'énergie. Cela était effectué par un entrepris de comparaison entre les protocoles de routages et les modèles d'économies d'énergies dans la couche MAC, cela en faisant varié le nombre de nœuds en fonction du temps de simulation, nous avons opté pour le meilleur protocole de routage « CBRP : Cluster Based Routing Protocol » et le meilleur modèle d'énergie qui est « Wifi radio model »

Nous avons structuré le résultat dans le graphe suivant :



**Graphe IV-7 : Résultat du protocole CBRP et le modèle d'énergie appliqué dans la couche MAC pour 40 nœuds**

## IV.5.Conclusion

Dans ce chapitre nous avons interprété les résultats des deux protocoles de routage OLSR et CBRP, et ceux des modèles d'économie d'énergie en utilisant le simulateur NS3, dont le but d'avoir à la fin un résultat qui satisfait les clients du standard IEEE802.11v en termes de la consommation d'énergie et l'augmentation de débit. Nous avons touché dans les trois couches basses du modèle OSI pour arriver à notre objectif.

Les résultats de simulation ont été récupérés, traités puis représentés sur des graphes pour distinguer la différence et comprendre le comportement de chaque protocole.



Nous avons proposé aussi l'utilisation du protocole CBRP en lui intégrant un des modèles d'économie d'énergie.

# **Conclusion générale**

## **Conclusion générale**

Les télécommunications occupent une place importante dans le quotidien des hommes qui ont de plus en plus besoin de communiquer, d'échanger des informations, à n'importe quel moment, quelque soit l'endroit où ils se trouvent, avec des exigences plus ou moins accrues sur la qualité des transmissions. Le secteur des télécommunications sans fil a connu une évolution dans le monde avec la naissance de plusieurs solutions comme le GSM, l'UMTS, le Wifi, le Bluetooth et bien d'autres.

Aujourd'hui, il existe une étroite relation entre le monde de la téléphonie mobile et celui de la toile cybernétique fait l'unanimité de tous les acteurs principaux de l'évolution des réseaux sans fil. En effet, Internet est construit sur des standards vivants et évolutifs apportant aux opérateurs la possibilité d'enrichir leurs services et offrant ainsi au grand public une riche expérience et une simplicité d'utilisation.

Les réseaux du futur seront inévitablement un ensemble d'une multitude de technologies opérant conjointement d'une manière transparente à l'utilisateur qui ne sera concerné que par la QoS offerte, le débit et l'autonomie de sa batterie, suite à l'apparition du nouveau standard IEEE802.11v toutes ces craintes seront dépassées. La clé à ce réseau du futur est la maîtrise de la convergence des différentes technologies d'accès réseau.

Notre objectif était l'étude du standard IEEE802.11v et de trouver un protocole pour bien gérer l'économie d'énergie et le débit dans les réseaux WLAN. Nous avons effectué ceci en utilisant l'environnement de simulation NS3.

# **Références bibliographiques**

## Références bibliographiques

[**Albert, 1998**] Albert Head Guide pour le positionnement GPS (Juillet 1993) Troisième impression, avec corrections, pages 68-112, canada, avril 1998.

[**Anry, al ,2007**] Anry H, Stéphanie C, étude sur l'évolution de la sécurité du sans fils dans les réseaux 802.11, pages 12-24, Belgique, mai 2007.

[**Arnab, al, 2003**] Arnab Chakrabarti, Ashutosh Sabharwal, Behnaam Aazhang. Using predictable observer mobility for power efficient design of sensor networks. In Proceedings of the 2<sup>nd</sup> International Workshop on Information Processing in Sensor Networks (IPSN'03), pages 129–145, 2003.

[**Bruno, 2006**] Bruno Kerouanton, étude sur les avantages et les inconvénients du wifi en milieu professionnel, pages 35-61, Lille, France, Fr, septembre 2006.

[**C. p, al, 1994**] C. Perkins and P. Bhagwat, “highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers”, Proc. Of SIGCOMM'94, 1994

[**C. p, 2003**] C. Perkins, “ad hoc on-demand distance vector (AODV) routing, rfc3561, 2003

[**Caimu, al, 2004**] Caimu Tang and Cauligi S. Raghavendra. Compression techniques for wireless sensor networks. Wireless Sensor Networks, pages 207–231, 2004.

[**Cecille, 2014**] Cecille Bovard, La couche liaison Wi-Fi (802.11 ou Wifi), pages 69-73, Montpellier Juin 2014.

[**Cesare, al, 2007**] Cesare Alippi, Giuseppe Anastasi, Cristian Galperti, Francesca Mancini, and Manuel Roveri. Adaptive sampling for energy conservation in wireless sensor networks for snow monitoring applications. In Proceedings of the 4th IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS'07), pages 1–6, October 2007.

**[Ching-Chuan, al, 1997]** Ching-Chuan Chiang, Hsiao-Kuang Wu, Winston Liu, and Mario Gerla. Routing in clustered multihop, mobile wireless networks with fading channel. Proceedings of IEEE Singapore International Conference on Networks (SICON '97), pages 197–211, April 1997.

**[Cristian, 2006]** Cristian Pham universit  de Pau et des pays de l'Adour  tudes sur les r seaux sans fils pages 10-20, France, Fr, avril 2006.

**[Curt, al, 2002]** Curt Schurgers, Vlasios Tsiatsis, and Mani B. Srivastava. Stem: Topology management for energy efficient sensor networks. In Proceedings of the IEEE Aerospace Conference, volume 3, pages 78–89, 2002.

**[D. Johnson, 2007]** D. Johnson, “the dynamic source routing protocol (DSR) for mobile ad hoc networks for ipv4, RFC4728, 2007

**[E. Cizeron, 2009]** E. Cizeron « routage multi chemins et codage   description multiple dans les r seaux ad-hoc » th se de doctorat de l'universit  de Nantes. France 2009.

**[Elena, al, 2007]** Elena Fasolo, Michele Rossi, J'org Widmer, and Michele Zorzi. In-network aggregation techniques for wireless sensor networks: a survey. IEEE Wireless Communications, pages 70–87, April 2007.

**[Fares, al, 2008]** Fares Abdelfattah, Anne Elisabeth Baert, Vincent Boudet, d veloppement d'une biblioth que de capteurs, pages 12-15, Montpellier, France, avril 2008.

**[Geoffrey, al, 2006]** Geoffrey Werner-Allen, Konrad Lorincz, Matt Welsh, Omar Marcillo, Jeff Johnson, Mario Ruiz, and Jonathan Lees. Deploying a wireless sensor network on an active volcano. IEEE Internet Computing, pages: 18–25, 2006.

**[Giuseppe, al, 2005]** Giuseppe Anastasi, Eleonora Borgia, Marco Conti, Enrico Gregori, and Andrea Passarella. Understanding the real behavior of mote and 802.11 ad hoc networks: An experimental approach. Pervasive and Mobile Computing, pages 237–256, 2005.

[**Giuseppe, al, 2009**] Giuseppe Anastasi, Marco Conti, Mario Di Francesco, and Andrea Passarella. Energy conservation in wireless sensor networks: A survey. *Ad Hoc Networks*, pages 537–568, 2009.

[**Giuseppe, al, 2008**] Giuseppe Anastasi, Marco Conti, Andrea Passarella, and Luciana Pelusi. Mobile-relay forwarding in opportunistic networks. In M. Ibnkahla, editor, *Adaptation and Cross Layer Design in Wireless Networks*. CRC Press, New York, USA, 2008.

[**Gregory, al, 2000**] Gregory J.Pottie and W. J. Kaiser. Wireless integrated network sensors. *Communications of the ACM*, pages : 51–58, 2000.

[**Hervé, 2002**] Hervé Schauer, sécurité des réseaux sans fils 802.11B, pages 7-14, Île-de-France, France, juillet 2002.

[**PB09**] [**Hurni, al, 2009**] Hurni Philipp and Torsten Braun. Calibrating wireless sensor network simulation models with real-world experiments. In *Proceedings of the 8th International IFIP-TC6 Networking Conference (NETWORKING'09)*, volume 5550, pages 1–13, Singapore, May 5-6 2009.

[**Ian F, al, 2007**] Ian F. Akyildiz, Tommaso Melodia, and Kaushik R. Chowdhury. A survey on wireless multimedia sensor networks. *Computer Networks*, pages 921–960, 2007.

[**Ian F, al, 2002**] Ian F. Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, and Eredal Cayirci. Wireless sensor networks: a survey. *Computer Networks*, pages 393–422, 2002.

[**Ilker, al, 2006**] Ilker Demirkol, Cem Ersoy, and Fatih Alagoz. MAC protocols for wireless sensor networks: A survey. *IEEE Communications Magazine*, pages 115–121, April 2006.

[**Injong, al, 2008**] Injong Rhee, Ajit Warrier, Mahesh Aia, Jeongki Min, and Mihail L. Sichitiu. Z-MAC: a hybrid MAC for wireless sensor networks. *IEEE/ACM Transactions on Networking*, pages 511–524, 2008.

## REFERENCES BIBLIOGRAPHIQUES

---

[**Jaap, 200**] Jaap C. Haartsen. The bluetooth radio system. IEEE Personal Communications, pages 28–36, February 2000.

[**Jihene, 2010**] jihene rezgui « gestion adaptative des ressources dans les réseaux maillés sans fil à multiples-radios multiples-canaux »Thèse de doctorat en informatique à Université de Montréal, 2010.

[**Joseph, al, 2004**] Joseph Polastre, Jason Hill, and David Culler. Versatile low power media access for wireless sensor networks. In Proceedings of the 2nd international conference on embedded networked Sensor Systems (SenSys'04), pages 95–107, New York, NY, USA, 2004.

[**Khaled, al, 2002**] Khaled A. Arisha, Moustafa A. Youssef, and Mohamed F. Younis. Energy-Aware TDMAbased MAC for Sensor Networks. In Proceedings of the IEEE Workshop on Integrated Management of Power Aware Communications, Computing and Networking (IMPACCT'02), New York City, NY, 2002.

[**K.Holger, al, 2005**] K. Holger and Andreas Willig. Protocols and Architectures for Wireless Sensor Networks. Wiley, 2005.

[**Koen, 2008**] Koen Langendoen. Medium access control in wireless sensor networks. Medium Access Control in Wireless Networks, pages 535–560, May 2008.

[**Le comité, 1993**] le Comité des normes de l'ingénierie de logiciels de la Société d'informatique IEEE, Institute of Electrical and Electronics Engineers, Inc. Pages 4-6, Imprimé aux États-Unis, USA, décembre 1993.

[**Li Jian, al, 2007**] Li Jian and Mohapatra Prasant. Analytical modeling and mitigation techniques for the energy hole problem in sensor networks. Pervasive and Mobile Computing, pages 233–254, 2007.

[**Luc, 2003**] Luc Aebi découvrir l'univers du GPS & Exploiter son potentiel, pages 28-60 Belgique, 2003.

[**Maarten, al, 2006**] Maarten Ditzel and Frans H. Elferink. Low-power radar for wireless sensor networks. In Proceedings of the 3rd European Radar Conference (EuRAD'06), pages 139–141, September 2006.



[**Mario, al, 1995**] Mario Gerla and Jack Tzu-Chieh Tsai. Multicluster, mobile, multimedia radio network. *ACM-Baltzer Journal of Wireless Networks*, pages: 255–265, 1995.

[**Mehmet, al, 2004**] Mehmet C. Vuran, “Ozgür B. Akan, and Ian F. Akyildiz. Spatio-temporal correlation: theory and applications for wireless sensor networks. *Computer Networks*, pages 245–259, 2004.

[**Mahmood, al, 2008**] Mahmood Ali, Annette Böhm, and Magnus Jonsson. Wireless sensor networks for surveillance applications - A comparative survey of MAC protocols. In *Proceedings of the 4<sup>th</sup> International Conference on Wireless and Mobile Communications (ICWMC '08)*, pages 399–403, Washington, DC, USA, 2008. IEEE Computer Society.

[**Matthieu, 2012**] Matthieu GAUTIER, TECHNIQUES MIMO, pages 26-30, PARIS, France, mars 2012.

[**Michèle, 2011**] Michèle Germain, Etudes sur la topologie du 802.11, pages 88-93, PARIS, France, 2011

[**Michèle, 2012**] Michèle Germain, livre : 802.11 DANS TOUS SES ETATS, pages 135-152, PARIS, France, Fr, 3 février 2012.

[**Mohammed, al, 2012**] Mohammed A. Mahdi and Tat-chee wan “performance comparison of manets routing protocols for dense and sparse topology” *International Conference on Information and Computer Networks (ICICN 2012)*.

[**Mohammed, 2011**] Mohammed Mehseur. « Routage dans les réseaux maillés sans fils », Université m’Hamed Bouguara Boumerdés, 2011.

[**Monique, al, 2009**] Monique Becker, André-Luc Beylot, Riadh Dhaou, Ashish Gupta, Rahim Kacimi, and Michel Marot. Experimental study: Link quality and deployment issues in wireless sensor networks. In *Proceedings of the 8th International IFIP-TC6 Networking Conference (NETWORKING'09)*, volume 5550, pages 14–25. Springer, 2009.

## *REFERENCES BIBLIOGRAPHIQUES*

---

**[Mukesh, 2010]** Mukesh Kumar “comparative analyses of cbrp, dsr, aodv routing protocol in Manet” International Journal on Computer Science and Engineering.2010

**[Oxygen, 2011]** ns-3 Doxygen Documentation of the public APIs of the simulator ,Tutorial Manual, and Model Library for the latest release and development tree , 2011

**[O.Younis, al, 2004]** O. Younis, and S. Fahmy, “heed: a hybrid energy-efficient distributed clustering approach for ad hoc sensor networks”, IEEE Transactions on Mobile Computing, pages 366-379, 2004.

**[Patrick, 2011]** Patrick Vincent, Etudes sur le fonctionnement du WIFI, pages 25-30, Marseille, France, janvier 2011.

**[Rémi, 2011]** Rémi Soulage « contribution à l'étude et à l'amélioration de la qualité de services sur un réseau maillé sans fil wifi » Thèse de doctorat en informatique à l'université de Montpellier2. France.2011

**[Richard, 2013]** Richard Engolou, sécurisation des VANETS par la méthode de réputation des nœuds, pages 5-20, MONTRÉAL, CANADA, AVRIL 2013.

**[Rob, 2010]** Rob Mead, New wireless standard 802.11v: cheaper, easier, greener Wi-Fi, pages 18-25, April 2010.

**[Rong, al, 2003]** Rong Zheng, Jennifer C. Hou, and Lui Sha. Asynchronous wakeup for ad hoc networks. In Proceedings of the 4th ACM international symposium on Mobile ad Hoc networking & computing (MobiHoc'03), pages 35–45, New York, NY, USA, 2003. ACM.

**[S. Lindsey, al, 2002]** S. Lindsey, and C. Raghavendra, “pegasis: power efficient gathering in sensor information system”, in proc.ieee aerospace conference, vol.3, pages:1125-1130, 2002.

**[T .H. Clausen, al, 2003]** T. H. Clausen and P. Jacquet, optimized link state routing protocol (olsr), ietf experimental. RFC 362, 2003

[**Tijs, al, 2003**] Tijs Van Dam and Koen Langendoen. An adaptive energy-efficient MAC protocol for wireless sensor networks. In Proceedings of the 1st international conference on embedded networked Sensor Systems (SenSys'03), pages 171–180, New York, NY, USA, 2003.

[**Vijay, al, 2002**] Vijay Raghunathan, Curt Schurgers, Sung Park, and Mani B. Srivastava. Energy-aware wireless microsensor networks. *IEEE Signal Processing Magazine*, pages 40–50, March 2002.

[**Vijay, al, 2006**] Vijay Raghunathan, Saurabh Ganeriwal, and Mani Srivastava. Emerging techniques for long lived wireless sensor networks. *IEEE Communications Magazine*, pages 108–114, April 2006.

[**Venkatesh, al, 2003**] Venkatesh Rajendran, Katia Obraczka, and J. J. Garcia-Luna-Aceves. Energy-efficient collision-free medium access control for wireless sensor networks. In Proceedings of the 1st international conference on embedded networked Sensor Systems (SenSys '03), pages 181–192, New York, NY, USA, 2003.

[**Wendi, al, 2000**] Wendi Rabiner Heinzelman, Anantha Chandrakasan, and Hari Balakrishnan. Energy efficient communication protocol for wireless microsensor networks. In Proceedings of the 33rd Hawaii International Conference on System Sciences (HICSS'00), IEEE Computer Society. Volume 2, pages 3005–3014, Washington, DC, USA, 2000.

[**Wei, al, 2004**] Wei Ye, John Heidemann, and Deborah Estrin. Medium access control with coordinated adaptive sleeping for wireless sensor networks. *IEEE/ACM Transactions on Networking*, pages 493–506, 2004.

[**W. R. Heinzelman, 2000**] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, “energy efficient communication protocol for wireless microsensor networks”, Proceeding of the 33<sup>rd</sup> Hawaii International Conference on System Sciences, IEEE, pp.1-10, 2000.

## *REFERENCES BIBLIOGRAPHIQUES*

---

**[Wei, al, 2004]** Wei Ye and John Heidemann. Medium access control in wireless sensor networks. In Krishna Sivalingam Ty Znati C. S. Raghavendra, editor, *Wireless Sensor Networks*, pages 73–92. Kluwer Academic Publishers, 2004.

**[Ya Xu, al, 2001]** Ya Xu, John Heidemann, and Deborah Estrin. Geography-informed energy conservation for ad hoc routing. In *Proceedings of the 7th annual international conference on Mobile Computing and networking (MobiCom'01)*, pages 70–84, New York, NY, USA, 2001.

# **Annexe**

## **Annexe**

### **Le fonctionnement du protocole de routage OLSR (Optimized Link State Routing Protocol)**

Le concept principal utilisé dans le protocole est celui des relais multipoint, (MPRs). Les MPRs sont des nœuds choisis qui expédient des messages de diffusion pendant le processus d'inondation. Cette technique réduit sensiblement la surcharge due aux messages par rapport à un mécanisme classique d'inondation, où chaque nœud retransmet chaque message quand il reçoit la première copie du message. Dans OLSR, l'information d'état de lien est produite seulement par des nœuds élus comme MPRs, ainsi, une deuxième optimisation est réalisée en réduisant au minimum le nombre des messages de contrôle inondés dans le réseau et comme troisième optimisation, un nœud de MPR doit rapporter seulement des liens entre lui-même et ses sélecteurs. Donc selon le protocole OLSR, chaque nœud du réseau ad-hoc émet principalement deux types de messages de signalisation à intervalles de temps réguliers: messages HELLO et messages TC (Topology control).

### **Le fonctionnement du protocole de routage CBRP (Cluster Based Routing Protocol)**

Dans le Protocole de Routage Basé sur les Clusters CBRP (Cluster Based Routing Protocol), l'ensemble des nœuds du réseau est décomposé en groupes. Le principe de formation des groupes est le suivant. Un nœud  $nI$  qui n'a pas de statut (i.e. qui n'est ni membre ni représentant (chef) de groupe), active un Timer et diffuse un message "Hello". Lorsqu'un représentant de groupe reçoit le message "Hello", il envoie immédiatement une réponse à l'émetteur. Lors de la réception de la réponse, le nœud  $nI$  change son état "indécis" à l'état "membre". Si  $nI$  dépasse un certain timeout en attendant la réponse, et dans le cas où il possède un lien bidirectionnel vers au moins un nœud voisin, il se considère lui-même comme représentant de groupe. Dans le cas contraire,  $nI$  reste dans l'état indécis et il répète la même procédure. À cause des

Changements rapides de la topologie des réseaux ad hoc, l'attente des nœuds indécis est très courte.

Afin de sauvegarder la répartition des nœuds dans les groupes, chaque nœud maintient une table appelé *table des membres*. Chaque entrée de cette table est associée à un voisin. Elle indique l'état du lien (uni ou bidirectionnel) et le statut du voisin (membre, représentant de groupe, passerelle).

<b>ID du Cluster</b>	<b>Statut</b>	<b>Etat du lien</b>
----------------------	---------------	---------------------

**Figure VI.1 : Table des membres**

Un chef de groupe, nommé Cluster Head (CH), maintient dans sa table de routage les informations des membres qui appartiennent à son groupe uniquement, et aussi les identificateurs des passerelles et des clusters Head voisins, pour les utiliser au moment du routage de données

<b>ID des clusters Head voisins</b>	<b>ID des passerelles voisines</b>	<b>ID des membres</b>
---	--	-----------------------

**Figure VI.2 : Table des chefs de groupe (cluster Head)**

Si la distance entre deux Cluster Head voisins reste importante, ses derniers peuvent communiquer via une passerelle (Gateway) jouant le rôle de relais. En gardant la philosophie du routage à base de tables de routage, même la passerelle a sa propre table qui se compose des identificateurs des Clusters Head qui sont en communication directe avec elle, et la liste des membres de chaque CH qu'elle relie

<b>ID des clusters Head voisins</b>	<b>ID des Membres</b>
---	-----------------------

**Figure VI.3 : Table de la passerelle (gateway)**

Le routage dans le protocole CBRP se fait de la manière suivante: quand un nœud source veut envoyer des données à un nœud destination, il diffuse par inondation une requête de demande de chemin, et cela uniquement aux représentants des groupes voisins (CH). Un représentant de groupe qui reçoit la requête, vérifie en utilisant sa table de routage, l'existence du nœud destination dans son groupe. Si la destination existe, le représentant y envoie directement la requête, dans le cas contraire, la requête est diffusée aux représentants des groupes voisins.

L'adresse des représentants des groupes ayant déjà vu la requête, insère leur identité dans la requête de demande de chemin, un représentant de groupe ignore toute requête déjà traitée.

Quand la destination reçoit le paquet contenant la requête, elle répond par l'envoi du chemin qui a été sauvegardé dans le paquet de la requête. Dans le cas où le nœud source ne reçoit pas de réponse après expiration d'une certaine période, il envoie de nouveau une requête de demande de chemin.

Lors de l'acheminement des données, si un nœud détecte qu'un lien est défaillant, il fait retourner un message d'erreur à la source et applique un mécanisme de réparation locale.

Dans ce mécanisme, si un nœud  $n1$  trouve qu'un nœud suivant  $n2$  ne peut pas être atteint, il essaie de vérifier si le nœud  $n2$  ou le nœud qui vient après, peuvent être atteints à travers un autre nœud voisin. Si l'un des deux cas est vérifié, les données sont envoyées en utilisant le chemin réparé.