REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université El Hadj Lakhdhar – BATNA

Faculté des Sciences

Département d'Informatique

N° d'ordre :……

Série :……

Mémoire

Présenté en vue de l'obtention du diplôme

Magister en Informatique

Option: **Ingéniérie Des Systèmes Informatique**

SUJET DU MÉMOIRE :

Gestion De L'économie D'énergie Dans Les Réseaux Sans Fil 802.11 Ad Hoc

Présenté le: / / .

Par : **Saida HEDNA**

Composition de jury :

Dr. Abdelmadjid ZIDANI	Président	(Maître de conférences à l'université de Batna).
Pr. Azzeddine BILAMI	Rapporteur	(Professeur à l'université de Batna).
Dr. Ammar LAHLOUHI	Examinateur	(Maître de conférences à l'université de Batna).
Dr. Okba KAZZAR	Examinateur	(Maitre de conférences à l'université de Biskra).

A mes Parents,

à la mémoire de mon grand-père,

et à toutes les personnes importantes dans ma vie.

REMERCIEMENTS

En premier lieu je remercie ALLAH le tout puissant pour la santé, la volonté et la patience qu'il ma a donné durant toutes ces années d'étude afin que je puisse arriver là.

Je tiens à remercier en premier lieu *Dr Bouam Souheila* , mon directeur de thèse pour sa sympathie, sa disponibilité, ses idées, ses conseils et ses encouragements qui m'ont permis de mener à bien cette thèse. Je remercie bien évidemment Pr Bilami Azzedine d'avoir accepté de dirigé cette thèse et Melle Keddar Lamia du laboratoire PRiSM de l'université de Versailles pour les informations et les idées qu'elle m'a prodiguées au début de ce travail. Je remercie Dr Abdelmadjid Zidani d'avoir accepté de présider mon jury de soutenance. Merci également au Dr Lahlouhi ainsi qu'au Dr Kezzar qui s'est déplacé pour faire partie de ce jury.

Je voudrais remercier ma famille pour leur support tout au long de mes études : À ma chère mère et à mon père pour m'avoir élevé et donné un certain regard sur ce qui m'entoure; À mes frères (*mon frère et mon fils Halim*); À ma sœur; À ma grand-mère pour leur soutien; À l'ensemble des familles *Hedna* et *Lounis* pour les moments de détente passés ensemble.

Je remercie plus particulièrement mon mari, pour sa confiance, sa patience, son soutien incessant et son encouragement durant la rédaction de ce mémoire et tout au long de mes études en informatique. Tu sais d'où je viens et c'est en grande partie grâce à toi que tu me verras atteindre les objectifs que je me suis fixés.

Je souhaite à tous mes collègues une bonne continuation et tous mes vœux de réussite. Je pense à Mehdaoui Asma, Mehdaoui Rahima, Benbekhta Affaf, Kalkil Naima, Sabeg Samra, Smair Fhadila, Radjai Wahiba, Ibrir Radhia, et Haid Nabila. Pour d'autres, je leurs souhaite bonne chance pour leur future carrière, spécialement pour Sedrat Saida, Mansouri Rahma, Berrou Yasmina.

RÉSUMÉ

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 comme le mécanisme PSM (*Power Saving Mode*) défini par le standard 802.11.

Nous présentons dans ce travail une approche permettant de modifier le protocole de routage OLSR afin que ce dernier soit en mesure de supporter la notion d'économie d'énergie. Cette amélioration est basée sur l'interaction entre le protocole de routage OLSR et un mécanisme d'amélioration du protocole MAC, appelé Power-Aware Alternation(PAA) qui se base sur l'élimination de l'activité réseau d'un ensemble de nœuds durant certaines périodes afin de conserver leur énergie. Les nœuds choisissent des nœuds supporteurs, parmi l'ensemble des MPRs sélectionnés par OLSR, avec qui ils vont alterner des périodes d'activité et d'inactivité.

Cette approche a comme avantage de mieux conserver l'énergie et la connectivité du réseau. Nous détaillons dans ce rapport la conception de notre mécanisme et nous effectuons une évaluation de ses performances par simulation.

Cette étude nous a permis de comparer les performances d'OLSR-PAA à celles d'OLSR en termes de ces incidences sur la performance du réseau MANET particulièrement sur sa consommation d'énergie.

Mots clés : Réseaux sans fil, Réseaux ad hoc, OLSR, PSM, économie d'énergie, Routage ad hoc.

TABLE DES MATIÈRES

LISTE DES FIGURES

LISTE DES TABLES

INTRODUCTION

1. Introduction

1.1 Contexte et motivations

Un MANET[1] [1] est un cas particulier de réseaux sans fil où chaque nœud peut directement joindre ses voisins en utilisant son interface radio où il a la possibilité de contacter n'importe quel autre nœud à l'intérieur du réseau en utilisant les nœuds intermédiaires (situés entre la source et la destination). Ces derniers se chargent de relayer les messages et offrir, ainsi, un réseau autonome, conçu et supporté par l'ensemble des participants.

Une fonctionnalité très importante des MANETs est le routage. La notion de routage regroupe un ensemble de procédures assurant l'ouverture et l'entretien d'une communication entre deux nœuds. Dans les MANETs, il est nécessaire de créer de nouveaux protocoles qui répondent aux nouveaux besoins des applications et qui prennent en compte les nouveaux paramètres du réseau (mobilité, liens asymétriques, nœuds cachés, etc.). Ces protocoles peuvent être classifiés selon plusieurs critères en différentes familles, la plus utilisée est : *la classification Proactifs/Réactifs/Hybride*. Donc, ces derniers essaient de satisfaire plusieurs propriétés, comme: mise en œuvre distribuée, utilisation effective de la bande passante et capacité de la batterie,

Une autre fonctionnalité des MANETs est la consommation d'énergie. L'épuisement de l'énergie d'un nœud n'affecte pas uniquement sa capacité de communication mais peut carrément causer le partitionnement du réseau. L'objectif d'allongement de la durée de vie du réseau ne peut être achevé que si tous les nœuds mobiles sont traités équitablement.

Viser une exploitation efficace de l'énergie dans les MANET fait recours à toutes les couches de la pile des protocoles de communication. Les solutions proposées dans

[1] Mobile Ad hoc Network

cette optique, sont classées en trois familles à savoir : le contrôle de la puissance de transmission, le mode d'énergie basse et le routage orienté énergie. Toutes ces approches proposées dans les MANET visent une consommation efficace d'énergie.

Dans le cadre de notre travail, nous nous intéresserons seulement aux approches visant les deux niveaux : mode d'énergie basse (basé sur le mécanisme PSM du protocole MAC) et le routage orienté énergie. Etant donné que ces deux protocoles, en plus de leurs fonctionnalités de bases, peuvent supporter des mécanismes de sauvegarde de l'énergie il est évident que l'échange d'informations entre eux sur l'état des nœuds est primordial. L'absence de ces informations conduira, d'une part, le protocole de routage à solliciter souvent des nœuds à faible énergie qui sont sensés d'être mis en veille par le protocole MAC et d'autre part, le protocole MAC à mettre en veille des nœuds non actifs à grande énergie sélectionnés éventuellement par le protocole de routage pour acheminer des données. Ces deux derniers problèmes nécessitent de considérer les interactions entre les protocoles en question et de bien les étudier afin de dégager des solutions qui les optimisent. Notre étude rentre dans cette optique et vise l'amélioration des performances du protocole de routage OLSR pour une meilleure économie d'énergie dans les MANET.

1.2 Organisation du rapport

L'ensemble de ce document est partagé en cinq chapitres.

Le premier est une introduction qui présentera notre travail.

Le second est dédié à donner une vue générale sur les réseaux sans fil et 802.11. Dans ce chapitre, les caractéristiques fondamentales sont énumérées telles que le modèle en couches, les modes, les topologies et les protocoles d'accès de la norme. Les différentes dérivées de la norme de base sont aussi spécifiées.

Le troisième chapitre s'intéresse particulièrement aux réseaux Ad hoc et aux protocoles de routage dans ce type réseaux. Parmi ces protocoles, on va prêter une attention particulière au protocole de routage proactif OLSR.

Le quatrième chapitre propose un état de l'art sur les principales approches proposées pour résoudre le problème d'économie d'énergie dans les réseaux mobile ad hoc.

Le chapitre final présente l'implémentation ainsi que la simulation du mécanisme proposé. Une analyse et une comparaison des résultats obtenus est faite dans ce chapitre.

LES RÉSEAUX SANS FIL

2 Les réseaux sans fil

2.1 Introduction

Les télécommunications jouent un rôle très important dans la vie des hommes. Ces derniers ont de plus en plus besoin de communiquer, d'échanger des informations, de n'importe quel lieu, à n'importe quel moment, avec des exigences accrues sur la rapidité et la qualité de transmission. Avec le développement très rapide des multimédias et l'avènement de l'Internet, le besoin de transmettre des flux de voix, de vidéo, d'images fixes ou autres types d'informations, en plus des données, augmente sans cesse. De plus, pour pouvoir communiquer librement sans le besoin d'infrastructures coûteuses, ou l'encombrement du câblage, ou dans des zones d'accès difficile, la solution est **le sans-fil**.

Les réseaux sans fil (***Wireless Networks***) constituent de plus en plus une technologie émergente permettant à ses utilisateurs un accès à l'information et aux services électroniques indépendamment de leurs positions géographiques. Le succès de ce type de réseaux ces dernières années est suscité par un grand intérêt de la part des particuliers, des entreprises et du milieu industriel. En effet, ce type de réseaux est perçu comme une nouvelle alternative complémentaire aux réseaux filaires traditionnels, car ils sont autant utilisés dans le cadre des réseaux locaux d'entreprise, pour une utilisation purement professionnelle, que dans le cadre des réseaux locaux personnels à domicile. Dans les réseaux à moyenne et large couverture aussi, la technologie sans fil devient dominante.

2.2 Définition d'un réseau sans fil

Un réseau sans fil est un réseau dans lequel au moins deux terminaux sont capables de communiquer entre eux grâce à des signaux radioélectriques. Grâce aux réseaux sans fil, un utilisateur a la possibilité de rester connecté tout en se déplaçant dans un

périmètre géographique plus ou moins étendu, c'est la raison pour laquelle on entend parfois parler de "**mobilité**".

Il existe plusieurs technologies se distinguant d'une part par la fréquence d'émission utilisée, ainsi que par le débit et la portée des transmissions.

2.3 Les catégories de réseaux sans fil

On distingue habituellement plusieurs catégories de réseaux sans fil, caractérisés par la taille de leur zone de couverture :

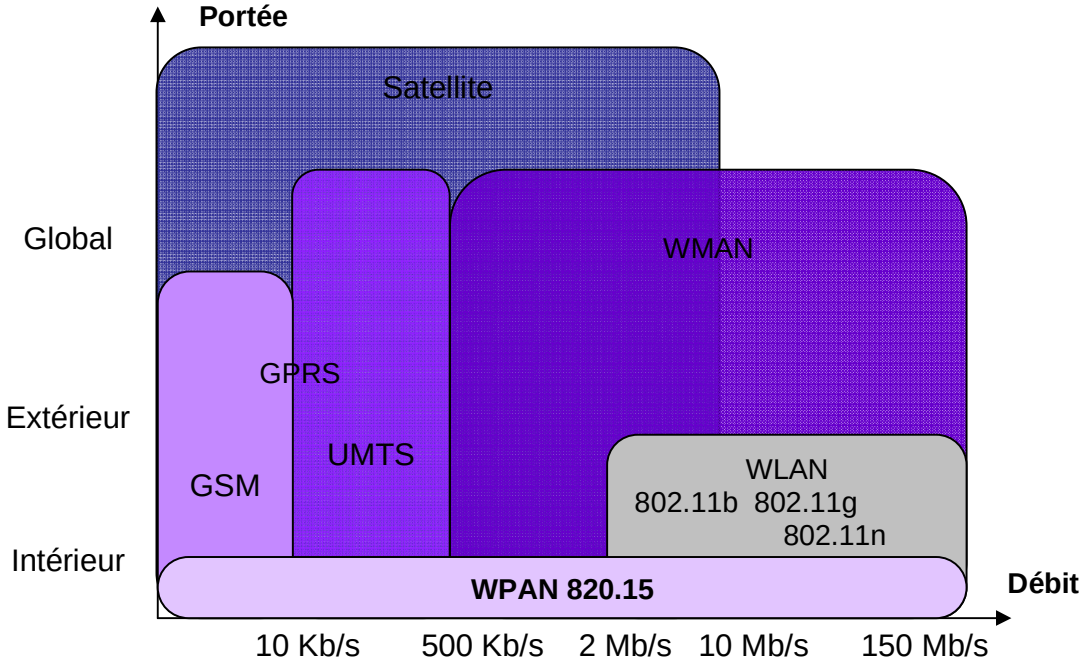


Figure 2.1 : les catégories de réseaux sans fil.

2.3.1 Réseaux personnels sans fil (WPAN)

Le réseau personnel sans fil (**WPAN**[2]) concerne les réseaux sans fil d'une faible portée: de l'ordre de quelques dizaines mètres. Ce type de réseau sert, généralement, à relier des périphériques ou un assistant personnel (PDA) à un ordinateur sans liaison filaire ou bien à permettre la liaison sans fil entre deux machines très peu distantes. Le groupe de travail qui se charge de la normalisation pour les réseaux WPAN est l'*IEEE*[3] *802.15*. Dans ce groupe, trois sous-groupes normalisent des gammes de produits en parallèle :

[2] Wireless Person Area Network
[3] Institute of Electrical and Electronics Engineers

- IEEE 802.15.1, le plus connu, en charge de la norme **Bluetooth**, lancé par Ericsson en 1994, proposant un débit théorique de 1 Mbps pour une portée maximale d'une trentaine de mètres. La technologie **Bluetooth** possède l'avantage d'être très peu gourmande en énergie, ce qui la rend particulièrement adaptée à une utilisation au sein de petits périphériques. Bluetooth opère dans la bande de fréquence des 2.45 GHz.
- IEEE 802.15.3, en charge de la norme **UWB**[4], qui met en œuvre une technologie très spéciale : l'émission à une puissance extrêmement faible, sous le bruit ambiant, mais sur pratiquement l'ensemble du spectre radio (entre 3,1 et 10,6 GHz). Les débits atteints sont de l'ordre du Gbit/s sur une distance de 10 mètres.
- IEEE 802.15.4, en charge de la norme **ZigBee**, qui a pour objectif de promouvoir une puce offrant un débit relativement faible mais à un coût très bas. **ZigBee** est avant tout normalisé pour le passage des commandes plutôt que des données. Cependant, une version sortie en 2007 propose d'utiliser l'UWB et offre donc malgré tout un débit important. Le domaine d'application: les différents types de senseurs, de télémétrie, Jouets Interactifs.

La technologie **infrarouge** ou **IrDA** est également utilisée dans ce type de réseaux. Cette technologie est cependant beaucoup plus sensible que Bluetooth aux perturbations lumineuses et nécessite une vision directe entre les éléments souhaitant communiquer ce qui la limite bien souvent à un usage de type télécommande.

2.3.2 Réseaux locaux sans fil (WLAN)

Le réseau local sans fil (**WLAN**[5]) est un réseau permettant de couvrir l'équivalent d'un réseau local d'entreprise, soit une portée d'environ une centaine de mètres. Il permet de relier entre-eux les terminaux présents dans la zone de couverture. Il existe plusieurs technologies concurrentes :

- L'**IEEE 802.11**, soutenu par l'alliance WECA[6] offre des débits allant jusqu'à 54 Mbps sur une distance de plusieurs centaines de mètres. Dans la suite du rapport nous nous intéresserons principalement à ce type de réseaux sans fil locaux. Une description plus détaillée des différentes normes sera présentée dans la section 2.4.6.

[4] Ultra-Wide Band
[5] Wireless Local Area Network
[6] Wireless Ethernet Compatibility Alliance

- **HiperLAN2**[7], norme Européenne élaborée par l'ETSI[8]. HiperLAN2 permet d'obtenir un débit théorique de 54 Mbps sur une zone d'une centaine de mètres dans la gamme de fréquence comprise entre 5 150 et 5 300 MHz. mais il semble difficile de prévoir un avenir à la normalisation de l'ETSI dans ce domaine car celle-ci n'est pas soutenue par les industriels.

- **DECT**[9], norme des téléphones sans fils domestiques. Alcatel et Ascom développent pour les environnements industriels, telles les centrales nucléaires, une solution basée sur cette norme qui limite les interférences. Les points d'accès résistent à la poussière et à l'eau. Ils peuvent surveiller les systèmes de sécurité 24/24h et se connecter directement au réseau téléphonique pour avertir le responsable en cas de problèmes.

2.3.3 Réseaux métropolitains sans fil (WMAN)

Les réseaux métropolitains sans fil (**WMAN**[10]) également appelés ***Boucle Locale Radio*** (*BLR*) étaient à l'origine prévus pour interconnecter des zones géographiques difficiles d'accès à l'aide d'un réseau sans fil. Actuellement ces réseaux sont utilisés dans certaines villes américaines (San Francisco) pour fournir un accès internet aux habitants. Les réseaux basés sur la technologie **IEEE 802.16** ont une portée de l'ordre de quelques dizaines de kilomètres (50km de portée théorique annoncée) et un taux de transmission radio théorique pouvant atteindre 74 Mbit/s pour IEEE 802.16-2004 [2] plus connue sous le nom commercial de **WiMAX**.

C'est également dans cette catégorie que peuvent être classés les réseaux téléphoniques de troisième génération utilisant la norme UMTS[11] pour transmettre de la voix et des données. Cette norme UMTS propose des taux de transmission radio théoriques pouvant aller jusqu'à 2 Mbit/s sur des distances de plusieurs kilomètres.

2.3.4 Réseaux étendus sans fil (WWAN)

Le réseau étendu sans fil (**WWAN**[12]) est également connu sous le nom de *réseau cellulaire mobile*. Il s'agit des réseaux sans fil les plus répandus puisque tous les téléphones mobiles sont connectés à un réseau étendu sans fil. Les principales technologies sont les suivantes:

[7] HIgh Performance Radio LAN 2.0
[8] European Telecommunications Standards Institute
[9] Digital Enhanced Cordless Telecommunication
[10] Wireless Metropolitan Area Network
[11] Universal Mobile Telecommunication System
[12] Wireless Wide Area Network

- **GSM** (*Global System for Mobile Communication* ou en français *Groupe Spécial Mobile*)
- **GPRS** (*General Packet Radio Service*)
- **UMTS** (*Universal Mobile Telecommunication System*)

En ce qui concerne les **WWAN**, c'est plutôt l'interconnexion des réseaux précédents qui les supporte. Pour cela, il fallait définir une norme d'interconnexion, qui a été apportée par les spécifications du groupe **IEEE 802.21**. On peut aussi classer dans cette catégorie la norme **IEEE 802.20**, qui correspond à des cellules cohérentes et permet les accès large bande.

2.4 Réseaux IEEE 802.11

En 1997 l'élaboration du standard IEEE 802.11 pour les réseaux sans fil et son développement rapide fut un pas important dans le développement de tels réseaux. Il a ainsi permis de mettre à la portée de tous un vrai système de communication sans fil pour la mise en place des réseaux informatiques hertziens. Ce standard a été développé pour favoriser l'interopérabilité du matériel entre les différents fabricants ainsi que pour permettre des évolutions futures compatibles, un peu à la manière de l'Ethernet. Ceci signifie que les consommateurs peuvent mélanger des équipements de différents fabricants afin de satisfaire leurs besoins. De plus cette standardisation permet d'obtenir des composants à bas coût, ce qui se traduit par des prix plus faibles pour le consommateur.

Pour définir la norme WirelessLAN, les concepteurs ont pris en considération les points suivants :

- Robustesse et simplicité de la technologie contre les défauts de communication, ces caractéristiques ont été vérifiées par l'utilisation d'une approche distribuée du protocole de la couche MAC.
- Utilisation du WirelessLAN mondialement. C'est-à-dire le respect des différentes règles en usage dans les différents pays du monde.
- Totale compatibilité avec les anciens produits et aussi avec les produits actuels qui composent les réseaux LAN. C'est-à-dire que le passage du WirelessLAN au LAN et vice-versa devra être transparent à l'utilisateur.
- Une sécurité acceptable pour le passage de l'information dans l'air. (ex : l'utilisation du protocole WEP[13]).

[13] Wired Equivalent Privacy

- Gestion intelligente de la puissance afin de garantir une durée accrue des batteries composant les différents systèmes.

2.4.1 Topologies des réseaux IEEE 802.11

2.4.1.1 **Le mode Infrastructure**

Ce mode de fonctionnement est très semblable au protocole Ethernet des réseaux filaires. Dans ce mode, un réseau 802.11 est un ensemble de cellules de base appelé ***Basic Service Set*** BSS. Chaque cellule BSS comporte un point d'accès (AP[14]) matérialisé par un dispositif d'émission/réception. L'AP donne l'accès au réseau aux machines qui le désirent, on peut le comparer aux concentrateurs (hub) des réseaux fixes. Les APs sont en général câblés entre eux afin de créer un réseau de bornes d'accès. Donc les cellules sont reliées par une infrastructure de communication fixe et interconnectées par un système de distribution afin de former un ***Extended Service Station*** ESS. Les BSS d'un ESS sont différenciés via leur ***BSS Identifier*** (**BSSID**) de 6 octets correspondant à l'adresse MAC de l'AP. Cette infrastructure incorpore un portail permettant d'assurer l'interface avec un réseau local.

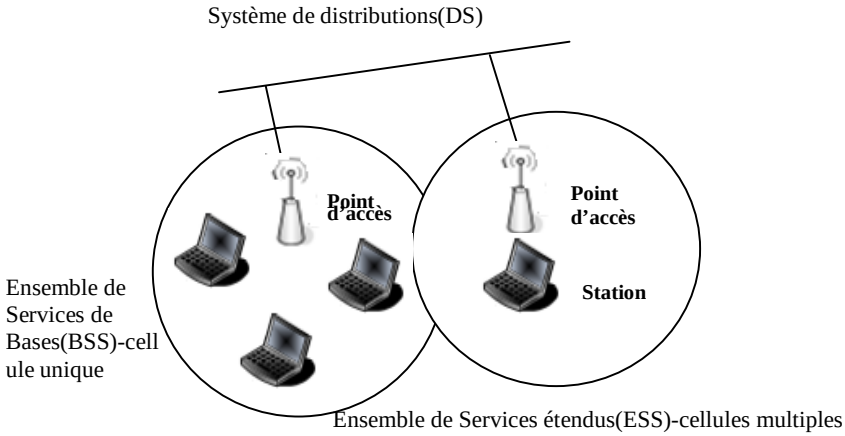


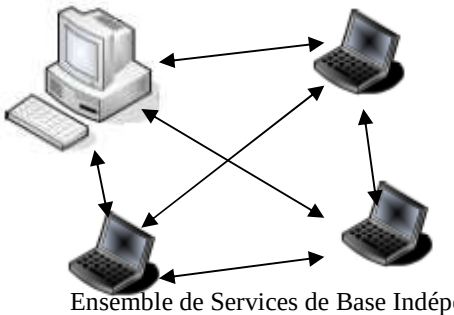
Figure2.2 : Exemple de réseau en mode infrastructure

2.4.1.2 **Le mode Ad hoc**

Un réseau Ad Hoc ou encore **IBSS**[15] est un ensemble de stations possédant une carte Wireless LAN sans la présence d'un **AP**. Contrairement au réseau à infrastructure, les stations dans un réseau Ad Hoc communiquent directement entre elles [1].

[14] Access Point
[15] Independent Basic Service Set

L'avantage de ces réseaux réside dans la facilité de mise en place et d'ajouter de nouvelles stations sur le réseau. L'absence de structures fixes diminue aussi le coût de leur mise en œuvre.



Ensemble de Services de Base Indépendant
(IBSS)

Figure2.3 : Exemple de réseau en mode ad hoc

2.4.2 Services des réseaux 802.11

Les services offerts par 802.11 sont séparés en deux catégories : *Station Service* (SS) et *Distribution System Service* (DSS).

• **Station Service** comprend les services suivants :

Authentification, désauthentification, sécurité (*privacy*), livraison des MSDU[16]

• **Distribution System Service** comprend les services suivants :

Association, désassociation, distribution, intégration, réassociation.

2.4.2.1 **Station Service (SS)**

- Authentification, désauthentification

L'authentification permet aux stations d'un BSS d'échanger leurs identités. 802.11 ne propose qu'un seul type d'authentification au niveau liaison, les fonctions plus avancées ne sont pas traitées dans le cadre de la norme. La désauthentification consiste simplement à effacer de la mémoire une station authentifiée.

- Sécurité

802.11 spécifie un mécanisme pour protéger les informations véhiculées sur le réseau. Ce mécanisme, appelé **WEP**, est optionnel.

[16] MAC Service Data Unit

2.4.2.2 Distribution System Service (DSS)

Les DSS servent à transmettre des messages dans le DS[17], ce qui permet entre autre d'assurer la mobilité (*roaming*). Le 802.11 définit trois types de mobilité :

- **No-transition**, lorsque les stations sont immobiles ou ne se déplacent qu'à l'intérieur d'un BSS.
- **BSS-transition**, lorsque les stations changent de **BSS** mais restent à l'intérieur du même ESS.
- **ESS-transition**, Lorsqu'une station passe d'un **BSS** d'un ESS à un autre **BSS** d'un autre ESS. 802.11 ne spécifie pas le changement d'**ESS**, cette opération entraînera donc une interruption de la communication.

Pour assurer la mobilité des stations, 802.11 a besoin des services appelés les ***services d'association***. Il est important de garder en mémoire qu'une association n'est possible que si le BSS dispose d'un AP. Un réseau ad hoc ne génère aucune association.

Association

Ce service permet à un AP de connaître les stations contenues dans son BSS. Une station arrivant dans le BSS d'un AP doit s'identifier auprès de cette AP. Il est important de relever qu'une station ne peut être associée qu'à un seul AP à la fois.

Cette particularité facilite le routage des MSDU dans le DS. Bien qu'une station ne soit associée qu'à un seul AP, elle peut, dans la mesure où le nombre d'AP visible est supérieur à un, choisir entre plusieurs AP.

Désassociation

Lorsqu'une station quitte un BSS, l'association entre AP et la station est supprimée. Cette opération est appelée désassociation.

Réassociation

Lorsqu'une station change de BSS, l'association est transmise d'un AP à l'autre par le DS. La réassociation permet le roaming entre BSS. Pour améliorer la rapidité du changement de BSS, une pré-authentification est possible.

2.4.3 Description des couches IEEE 802.11

La norme générique IEEE 802.11 correspond au niveau 1 et à une partie du niveau 2 dans le modèle OSI[18], soit les niveaux : Physique et MAC[19].

[17] Distribution System
[18] Open System Interconnection

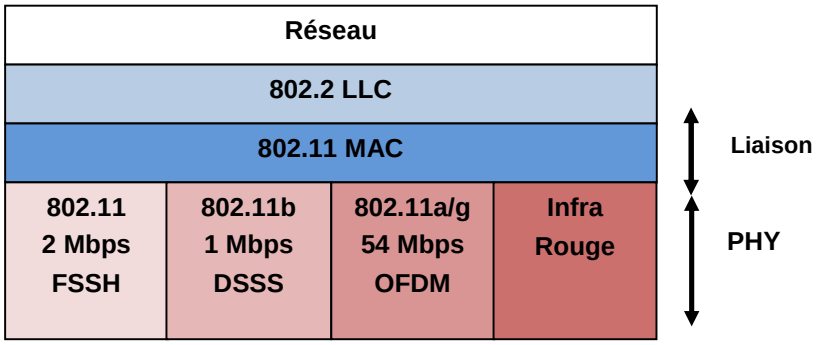


Figure 2-4 : Description des couches IEEE 802.11

2.4.4 La couche Physique

La couche Physique est divisée en deux sous couches :

- **PLCP**[20] : s'occupe de l'écoute du support et de la signalisation en fournissant un CCA[21] à la couche MAC.
- **PMD**[22] : traite l'encodage des données et la modulation.

Comme montré dans Table 2.1. Trois couches PHY différentes sont disponibles pour l'IEEE 802.11 WLAN. Par exemple IEEE 802.11b utilise l'Étalement de Spectre à Séquence Directe (**DSSS**), l'infrarouge (**IR**), et l'étalement de Spectre avec Saut de Fréquence (**FHSS**); alors qu'IEEE 802.11a utilisent le Multiplexage par Répartition Orthogonale de la Fréquence (**OFDM**).

Caractéristique	802.11a	802.11b	802.11g
Fréquence	5GHz	2.4 GHz	2.4 GHz
Débit(Mbps)	6, 9, 12, 18, 24, 36, 48, 54	1, 2, 5.5, 11	1, 2, 5.5, 6, 9, 11, 12, 18, 22, 24, 33, 36, 48, 54
Modulation	BPSK, QPSK, 16QAM, 64QAM (OFDM)	DBPSK, DQPSK, CCK (DSSS, IR, and FSSH)	BPSK, DBPSK, QPSK, DQPSK, CCK 16 QAM, 64 QAM (OFDM and DSSS)

Table2.1: Caractéristiques des différentes couches physiques dans le standard IEEE 802.11

[19] Medium Access Control
[20] Physical Layer Convergence Protocol
[21] Clear Channel Assessment
[22] Physical Medium Dependent

2.4.4.1 DSSS : Étalement de Spectre à Séquence Directe

Le DSSS [23] est une couche physique utilisant une technique radio. C'est une technologie de transmission par spectre étalé, où la porteuse est successivement modulée par l'information et par un code pseudo aléatoire de débit beaucoup plus important. Le signal résultant occupe donc une bande très importante.

Dans cette technique, la bande des 2.4 GHz est divisée (comme le montre la figure 2.5) en 14 sous-canaux de 22MHz. Pour minimiser le bruit de fond et les interférences locales, une technique dite "***chipping***" est utilisée. Elle consiste à convertir les bits de données en une série de bits redondants. Le bit **1** sera remplacé par une succession de **11** bits 0 ou 1 (appelée **code PN**) pendant le temps de transmission. Le bit 0 sera remplacé par le complément de la succession de bits utilisée pour le bit 1.

On étale ainsi le signal sur une bande de fréquence plus large en sur-modulant chaque bit du paquet à transmettre par ce code PN répétitif. Au niveau du récepteur, le signal original est retrouvé après la réception de tout le canal étalé et en le démodulant avec le même code.

Le DSSS du protocole 802.11 spécifie donc un chipping de 11 bits appelé ***Barker sequence*.** Chaque séquence de 11 bits représente un bit (0 ou 1) de données. Elle est ensuite convertie en onde appelée *symbol* transmis à 1 MS/s (1 millions de Symboles par seconde). C'est la modulation utilisée qui permet d'avoir des débits différents. La **BPSK** [24] pour un débit de 1 Mbit/s et la **QPSK**[25] pour un débit de 2 Mbit/s.

Dans le protocole 802.11b, pour pouvoir supporter les 2 nouveaux débits 5.5 Mbit/s et 11 Mbit/s, seul le DSSS est utilisé. En effet, le FHSS ne pourrait pas supporter ces nouveaux débits sans violer les règles actuelles du **FCC**[26] .

Cette augmentation des débits est réalisée grâce aux techniques de modulation et de codage comme le CCK[27]. Mais quelle que soit le débit employé, et c'est d'ailleurs pourquoi ces techniques ont été autorisées, le signal est toujours étalé sur 22 MHz *(=2*taille codage*vitesse de symbole).*

Comme nous avons dit, dans cette technique la bande passante est divisée en 14 canaux de 22MHz, ceci implique que seuls 3 canaux (sur les 14 prévus par la norme) peuvent être utilisés de manière adjacente si on veut éviter totalement le recouvrement de spectre.

---

[23] *Direct Spread Spectrum Sequence*
[24] *Binary Phase Shift Keying*
[25] *Quadature Phase Shift Keying*
[26] *Federal Communication Commission*
[27] *Complementary Code Keying*

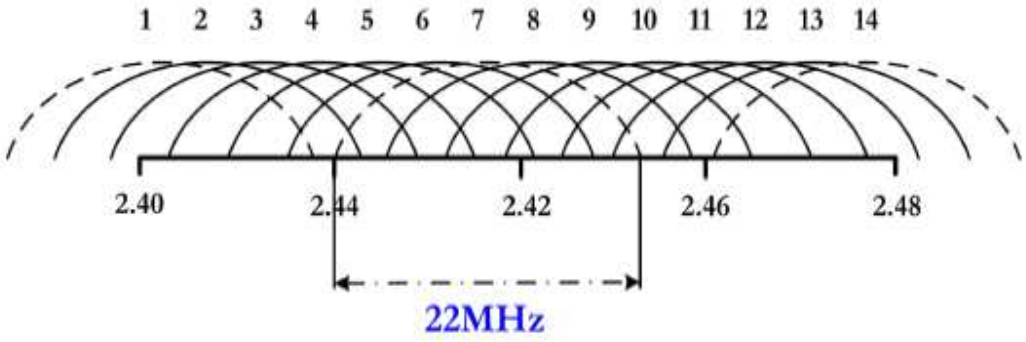


Figure 2-5 : Étalement de Spectre à Séquence Directe

Cette technique offre des débits de transmission allant de 5.5 à 11 Mbps. Avec comme avantages :

- Une densité spectrale faible du signal transmis, car ce dernier est large bande,
- Une sécurité assurée, tant que le code d'étalement reste secret,
- Une tolérance obtenue vis à vis du multi-trajet en choisissant des codes avec des facteurs d'auto-corrélation faibles.

2.4.4.2 FHSS : Étalement de Spectre avec Saut de Fréquence

La technologie FHSS[28] utilisée dans les réseaux 802.11b et d'autres technologies sans fil, a été créée et brevetée en 1942. En utilisant la transmission sur des canaux changeant en permanence de fréquence de manière pseudo-aléatoire, cette technologie utilise la technique de **saut de fréquence**. Son principe est de diviser la bande passante en 79 sous-canaux [3], de 1 MHz de largeur de bande offrant chacun, un débit allant de 1 à 2 Mbps avec un codage binaire.

L'émetteur et le récepteur s'accordent sur une séquence de sauts de fréquence porteuse et les données sont envoyées successivement sur les différents sous canaux en évitant (de manière temporaire) d'utiliser les sous-canaux fortement perturbés. Chaque communication sur le réseau s'effectue suivant un schéma de saut différent et cela de façon à minimiser le risque que deux émissions utilisent le même sous-canal.

La technologie FHSS est plus simple à mettre en œuvre, car l'utilisation d'un simple microcontrôleur suffit à la gestion des fonctions de sauts de fréquences pour la conception des systèmes en FHSS. En effet, cette technique coûte moins chère que des systèmes utilisant la technologie DSSS qui nécessite l'utilisation de circuits LSI[29]

[28] Frequency Hoping Spread Spectrum
[29] Large-Scale Integration

pour la conception des algorithmes de codages [3]. De plus elle offre une meilleure portée due à une plus grande sensibilité de l'étage de réception, ainsi qu'une bonne réjection des interférences. Les modules développés en FHSS peuvent être considérés comme des récepteurs à bande étroite changeant continuellement de fréquences et disposant d'un très bon niveau de réjection vis-à-vis des signaux d'interférences.

Par contre, cette méthode est limitée par son débit maximum de 2 Mbits/s. Elle introduit aussi une certaine complication au niveau MAC, qui se traduit par une de multiplication d'en-têtes et donc de réduction de débit [4].

2.4.4.3 Infrarouge

Le mode de communication par infrarouge est simple, peu réglementé et peu coûteux. En utilisant un faisceau de lumière, ce mode est basé sur l'utilisation des mêmes fréquences que celles utilisées sur les fibres optiques. Malgré que la lumière infrarouge possède une large bande passante, offrant par conséquent des débits relativement importants, la portée de ce type de communications reste faible. En revanche, les infrarouges peuvent pénétrer à travers le verre, mais pas à travers des obstacles opaques, ce qui représente un avantage en termes de sécurité. Mais, comme les réseaux infrarouges sont sensibles aux interférences lumineuses, la coupure du faisceau lumineux implique l'interruption de la transmission.

Il existe dans la pratique quatre types de réseaux infrarouges :

- Les réseaux à visibilité directe.
- Les réseaux infrarouges à diffusion.
- Les réseaux réflecteurs.
- Les réseaux à liaison optique à large bande.

2.4.4.4 OFDM : Multiplexage par Répartition Orthogonale de la Fréquence

L'OFDM [30] est une technique née dans les années 50-60. Cependant, dans les années 80, a été commencé à prendre conscience de l'intérêt que représente l'OFDM et ses applications [4]. Cette technologie représente une technique de modulation numérique des signaux, utilisée entre autres pour les systèmes de transmissions mobiles à haut débit. Elle consiste à répartir le signal sur un grand nombre de sous-porteuses orthogonales modulées individuellement à bas débit.

L'OFDM est particulièrement bien adapté aux réseaux locaux ou métropolitains, mais perd de son intérêt sur des réseaux à grandes échelles. Ceci est dû au fait que cette technique élimine les phénomènes de bruits ponctuels ou d'évanouissements

[30] Orthogonal Frequency Distributed Multiplexing

temporaires du signal sans recourir à des techniques complexes. En revanche, cette technologie paraît moins efficace lorsque les perturbations s'amplifient, car il faut mettre en place des méthodes de filtrages ou de codages qui réduisent de manière significative les débits. Actuellement l'OFDM est utilisé dans plusieurs applications telles que les satellites, l'ADSL ou le câble pour la diffusion des données, du son ou de l'image.

Mais, cette technologie s'oriente de plus en plus vers les systèmes de communications sans fil. Ainsi, des normes telles que 802.11a et 802.11g peuvent offrir des débits théoriques jusqu'à 54 Mbps, là où la norme 802.11b qui n'utilise pas OFDM, se limite à 11 Mbps.

2.4.5 La couche MAC

La norme 802.11 spécifie trois techniques pour l'accès au canal. Ces trois techniques se nomment *CSMA/CA*[31], *RTS/CTS* et *Polling*, parmi lesquelles, on distingue deux types de méthodes : **DCF**[32] et **PCF**[33]. CSMA/CA et RTS/CTS sont des méthodes dites DCF car la gestion de l'accès au canal est laissée aux stations. Par contre, Polling est une méthode PCF car l'accès au canal est géré par un AP.

Avant d'expliquer les trois techniques. Il faut noter que 802.11 utilise un intervalle de temps appelé IFS[34] qui a été défini pour permettre la gestion de l'accès au canal

- **IFS :** Cet intervalle de temps représente le temps écoulé entre deux trames. La norme propose quatre intervalles de temps différents :
  - **PIFS** (PCF IFS)
  - **DIFS** (DCF IFS)
  - **EIFS** (Extended IFS)
  - **SIFS** (Short ou Small IFS)

Tel que : **SIFS < PIFS < DIFS < EIFS**

2.4.5.1 CSMA/CA

Dans les réseaux filaires, lorsqu'un émetteur souhaite envoyer un signal sur le canal, il est capable de détecter la présence d'une communication coexistente sur le médium de transmission. En effet, s'il émet un signal sur le canal filaire et qu'il ne retrouve pas son propre message sur le câble, il peut en déduire qu'il y a eu une collision avec un signal également présent sur le médium. Cette détection de collision est la base de la

---

31 Carrier Sense Multiple Access/collision Avoidance
32 Distributed Coordination Function
33 Point Coordination Function
34 Interframe Space

technique d'accès CSMA/CD (*collision detection*). En CSMA/CD, s'il y a détection de collision, l'émetteur cherche à émettre à nouveau ses données après un temps d'attente aléatoire. La détection de collision est possible car la distance de transmission dans un câble est limitée de sorte que les niveaux de puissance de tous les signaux émis sur le support sont du même ordre de grandeur.

La transmission dans l'environnement radio ne permet pas d'utiliser la même technique d'accès car dans un environnement ouvert, l'atténuation des ondes est bien plus importante que dans un câble de transmission. Donc avant de commencer à émettre, une station doit sonder le canal pour savoir s'il est libre. Si la station désirant émettre ne détecte aucune activité pendant un temps DIFS alors elle émet sa trame. Si une activité est détectée sur le canal pendant la période DIFS, la station diffère l'envoi de la trame et lance le processus de ***Backoff***. Le processus de **Backoff** (*Backoff process*) consiste, dans un premier temps, à calculer un nombre aléatoire compris entre zéro et **CW** (*Contention Window* : fenêtre de contention). Ce nombre est ensuite multiplié par une durée appelée ***slot time***.

Backoff time = Random (0, CW) x Slot Time.

- **CW** peut prendre des valeurs différentes en fonction de la modulation utilisée. Ainsi en FHSS, CW peut valoir entre 15 et 1023, alors qu'en DSSS, CW est compris entre 31 et 1023.

- Un **slot time** est un intervalle de temps défini par la norme 802.11. La durée d'un slot est de 50 µs lorsque la couche PMD se base sur FHSS et 20 µs pour une modulation DSSS.

Le résultat de la multiplication permet à la station d'initialiser un timer. Le timer est ensuite décrémenté jusqu'à zéro. Si aucune activité n'est détectée à la fin de timer, la station est autorisée à émettre. Si, au contraire, la station détecte une activité elle stoppe son timer. Lorsque le canal redevient libre, la station attend DIFS et reprend la décrémentation du timer.

La figure 2-6 [50] montre l'envoi et l'acquittement d'une trame, l'utilisation des **IFS** est bien mise en évidence dans cet exemple.

Bien que cette méthode permette de limiter les collisions, il est cependant possible que deux stations viennent à émettre en même temps. Dans ce cas, il y a une collision et la trame est perdue. Contrairement aux réseaux câblés utilisant CSMA/CD, une station 802.11 n'a pas les moyens de détecter une collision.

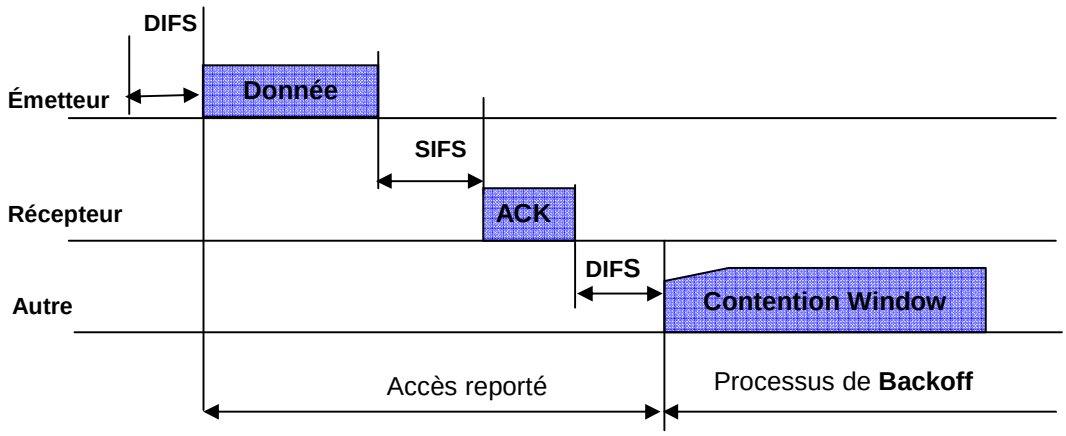


Figure 2-6 : Envoi de données avec acquittement

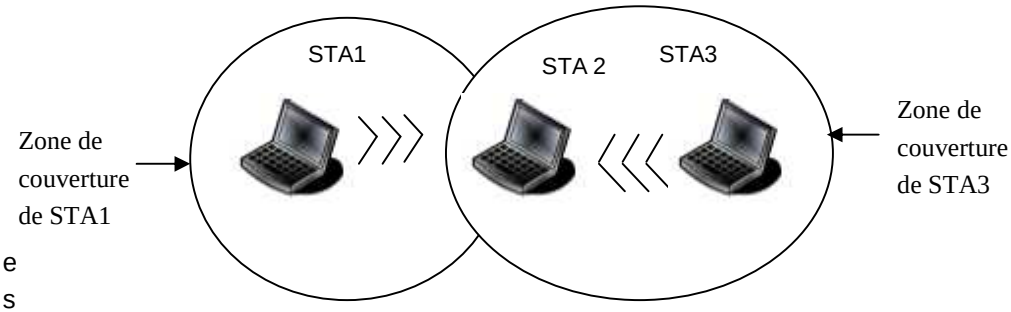
Chaque trame doit donc être acquittée par la station de destination. Lorsqu'une trame n'est pas acquittée, la station retransmet la trame après avoir attendu DIFS et après un processus de Backoff.

La probabilité d'avoir des collisions sur le canal dépend de la dimension de la fenêtre de contention CW. Plus la fenêtre est grande, plus la probabilité que les temps d'attente de deux stations soit identique est faible. Cependant une fenêtre de contention trop importante nuit aux performances car les temps d'attente sont plus longs. Une solution consiste à contrôler dynamiquement la dimension de la fenêtre de contention. CW est donc recalculer en fonction du nombre de collisions détectées sur le canal. A chaque collision détectée, la formule est la suivante :

$$CW_i = 2CW_{i-1}+1$$

2.4.5.2 RTS/CTS

Les WLANs sont victimes d'un phénomène appelé « *station cachée* » (*hidden station*). La figure ci-dessous [50] permet de mieux comprendre le problème.



e

s

Figure 2-7 : Station cachée

S

Les stations STA1 et STA3 sont trop éloignées l'une de l'autre pour être en mesure de détecter si l'autre est en train de transmettre. Donc si STA1 transmet des informations à STA2 et que STA3 désire faire de même, il y aura une collision car STA3 n'a pas détecté la transmission entre STA1 et STA2.

RTS/CTS résout le problème des stations cachées. Lorsqu'une station désire transmettre une trame, elle commence par envoyer une trame **RTS**[35] après avoir attendu un temps DIFS. La trame RTS permet de réservé le canal pendant la durée de la transmission.

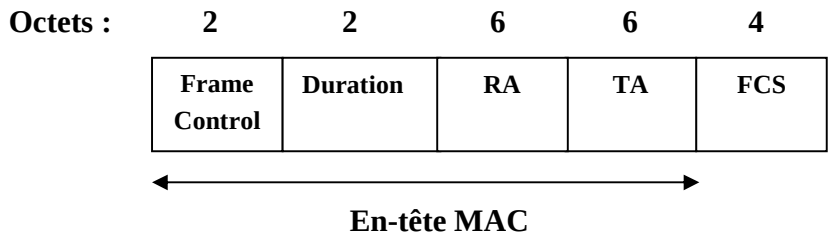


Figure 2-8 : Trame RTS

La trame RTS contient la durée de la transmission (champ *Duration*). Chaque station, hormis la station destinatrice, sait alors que le canal est réservé et pour combien de temps. Afin de savoir quand elles pourront recommencer à émettre, les stations utilise un NAV[36]. Le NAV est initialisé à partir de la durée transmise par la trame RTS. Lorsqu'une station reçoit un RTS qui lui est destiné, elle attend SIFS et envoie une trame CTS. Une station n'ayant pas reçu de RTS, car est trop éloignée de la station émettrice, peut recevoir le CTS et configurer son NAV.

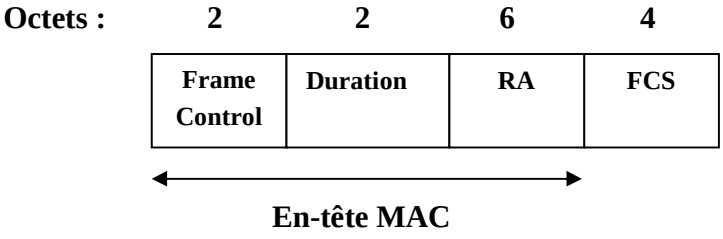


Figure 2-9 : Trame CTS

[35] Request To Send
[36] Network Allocation Vector

Le mécanisme utilisé par RTS/CTS peut laisser penser qu'il est moins performant que CSMA/CA car il nécessite l'envoi de deux trames avant de pouvoir émettre de l'information. Cela est vrai mais seulement dans le cas où la longueur des données est petite. Le fait qu'avec RTS/CTS les collisions ne peuvent survenir que pendant l'envoi de la trame RTS garantit que de longues trames ne seront pas à répéter suite à une collision. Pour optimiser les transmissions un seuil appelé *RTS threshold* a été introduit.

Lorsque les trames à envoyer sont petites, c'est CSMA/CA qui est utilisé. Dans le cas où les trames sont plus grandes qu'un certain seuil (*RTS Threshold*), c'est alors RTS/CTS qui est utilisé.

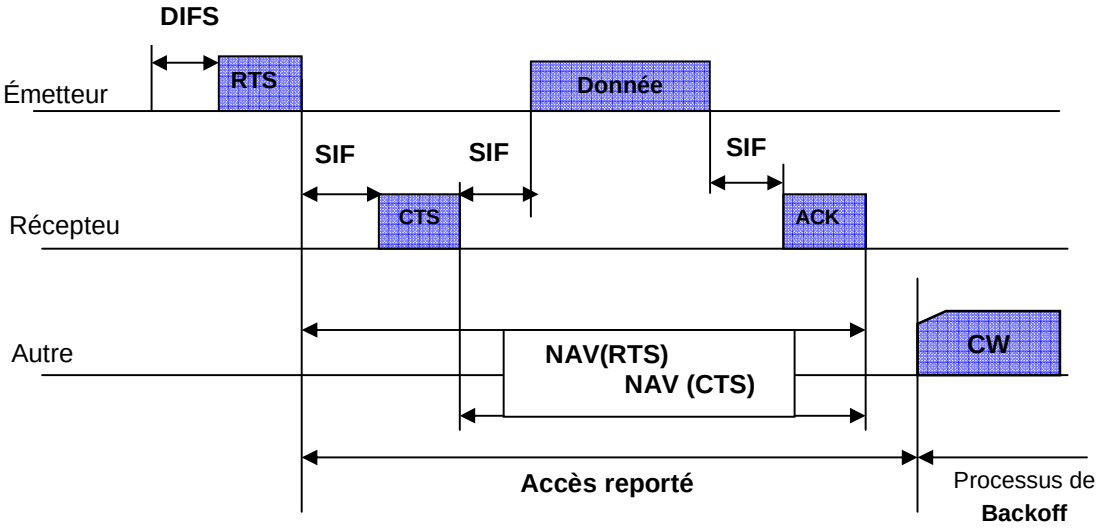


Figure 2-10 : Fonctionnement de RTS/CTS

2.4.5.3 Polling

La méthode du Polling est une méthode PCF[37], elle nécessite un point de coordination (PC[38]). Le point de coordination est un AP, le Polling ne fonctionne donc pas dans un réseau ad hoc.

Le PC contrôle périodiquement l'envoi des trames pendant des périodes sans contention (CFP[39]). Les CFP sont alternées avec des périodes de contention DCF durant lesquelles les stations sont habilitées à envoyer des trames. La fréquence des répétitions des CFP est déterminée par le CFPRate (taux de périodes sans-contention). Une CFP commence par la transmission d'un paquet de balise *« beacon» (*dans le reste de ce rapport on utilisera le terme 'Beacon' au lieu de paquet de balise*)*. La balise

[37] Point Coordination Function
[38] Point Coordination
[39] Contention-Free Period

contient la durée de la CFP (*CFP Max Duration*), ce qui permet aux stations du BSS d'initialiser leur NAV, garantissant ainsi qu'aucune d'entre elles n'émettra pendant la CFP.

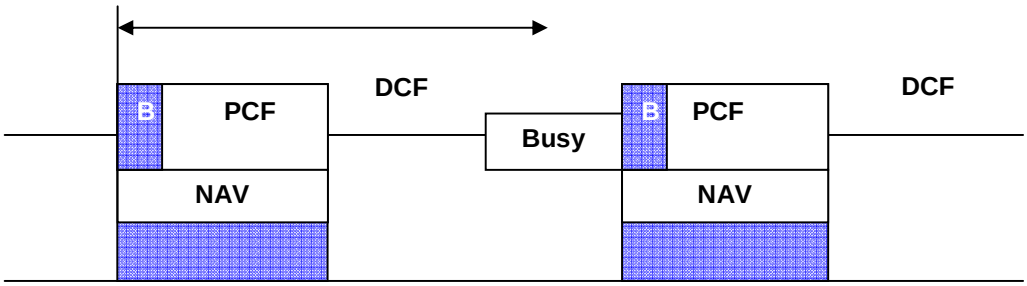


Figure 2.11 : PCF et DCF

Lorsque le PC désire commencer une CFP, il attend PIFS avant de transmettre la balise. Comme les stations en mode DCF ne peuvent émettre qu'après un temps DIFS, le PC est certain de prendre le contrôle car DIFS est plus grand que PIFS. Afin de déterminer l'ordre des stations avec lesquelles il doit dialoguer, le PC tient à jours une liste appelée Polling List. Cette liste contient les adresses (AID[40]) des stations désirant communiquer avec le PC. Les stations sont ensuite consultées à tour de rôle par le PC en fonction de la liste. Les stations attendent SIFS avant de répondre au PC et le PC attend à nouveau SIFS avant de passer à la station suivante. Le PC termine une CFP par une trame CF-End. Lorsque les stations reçoivent un CF-End, elles effacent leur NAV et sont à nouveau habilitées à travailler en DCF. Le CF-End marque le passage d'une période sans contention (CFP) à une période avec contention.

En plus du CF-end et de la balise, deux autres trames ont été spécifiées pour le polling ; CF-Poll et CF-Ack. CF-Poll permet au PC de désigner la station avec laquelle il désire communiquer. CF-Ack est utilisé aussi bien par le PC que par les stations pour acquitter les trames reçues.

Le Polling, contrairement à CSMA/CA et RTS/CTS, permet de garantir la qualité de service.

2.4.5.4 **Fragmentation**

Afin d'optimiser les performances, la couche MAC offre un service de fragmentation. En effet, dans le cas où la probabilité d'erreur par bit est importante, le fait d'envoyer des trames trop longues rend la probabilité qu'elles soient erronées trop importante. Pour diminuer le risque de devoir renvoyer une trame suite à une erreur, il s'agit de diminuer la dimension des trames en les fractionnant en trames plus petites.

[40] Association Identifier

La fragmentation est différente pour CSMA/CA et RTS/CTS. Avec CSMA/CA, lorsqu'une station a accès au canal, elle le conserve jusqu'à ce que tous les fragments soient transmis. Chaque segment doit, bien sûr, être acquitté séparément.

Avec RTS/CTS, le principe est un peu différent. Lorsqu'une station a pris le contrôle du canal, les autres stations ont déjà initialisé leur NAV. Pour cela, les nouvelles durées de réservation pour la réinitialisation des NAV sont incluses dans les fragments et dans les acquittements échangés par les stations. À la fin de la transmission, le dernier fragment et le dernier acquittement ne contiennent aucune réservation (durée de la réservation égale à 0).

2.4.5.5 **Synchronisation**

Toutes les stations appartenant à un même BSS sont synchronisées par la même horloge. En effet, chaque station dispose d'une horloge interne mais se synchronise à l'horloge commune au BSS. La procédure de synchronisation (TSF[41]) est réalisée par la diffusion périodique d'un *beacon* contenant un *timer*. La gestion de la synchronisation est différente pour un réseau ad hoc comparé à un réseau basé infrastructure.

2.4.5.5.1 Synchronisation dans réseau basé infrastructure

L'AP est chargé d'envoyer périodiquement le *beacon*. Dans le cas où le canal est occupé au moment de la synchronisation, l'émission du *beacon* est retardée. Le temps indiqué dans le *beacon* est donc incorrecte. L'inexactitude sera conservée jusqu'à la procédure de synchronisation suivante, où interviendra le TBTT[42].

2.4.5.5.2 Synchronisation dans un réseau ad hoc

Un réseau ad hoc ne dispose pas d'AP, c'est donc aux stations de se synchroniser entre elles. Comme pour n'importe quelle trame, toutes les stations essaient d'envoyer leur *beacon*. Les méthodes d'accès au canal décrites dans les paragraphes précédents permettront de déterminer quelle est la station dont le *beacon* sera utilisé pour synchroniser l'ensemble des stations.

2.4.5.6 **Mode De Getion D'énergie**

La norme 802.11 définit un moyen d'économiser l'énergie. Cela permet à 802.11 d'être mieux adapté aux équipements fonctionnant avec des batteries et pour qui l'énergie est une ressource précieuse. Pour réduire sa consommation en énergie, une station

[41] Timing Synchronization Function
[42] Target Beacon Transmission Time

peut, lorsqu'elle n'a pas besoin de communiquer, se mettre à l'état ***Doze***[43]. A l'opposé, lorsqu'une station désirant communiquer, elle doit se trouver dans l'état ***Awake***[44]. Comme pour la synchronisation, les méthodes de sauvegarde d'énergie sont différentes pour un BSS basé infrastructure et un BSS ad hoc.

2.4.5.6.1 Sauvegarde d'énergie dans un réseau basé sur infrastructure

L'AP insère dans une liste les stations qui sont dans le mode *doze*. Lorsque l'AP reçoit une trame destinée à une station dans le mode *doze*, il la conserve en mémoire.

Périodiquement l'AP diffuse un *beacon* contenant la liste des adresses des stations pour lesquelles il a un message en mémoire, cette liste est appelée **TIM**[45]. Les stations sont programmées pour se réveiller (mode *awake*) à chaque *beacon* et ainsi, être en mesure de recevoir la liste TIM. Les stations n'appartenant pas à la liste retournent dans le mode *Doze*. Si une station se reconnaît dans la liste fournie par l'AP, elle envoie, alors, une trame PS-Poll indiquant à l'AP de lui faire parvenir les trames qui lui sont destinées. L'AP transmet les trames et la station concernée les acquitte. Les stations peuvent alors se remettre en mode *Doze*.

Lorsque l'AP doit transmettre une trame multicast ou broadcast, il utilise alors une balise contenant le champ **DTIM**[46] à la place du champ TIM. Dans ce cas, toutes les stations doivent rester éveillées et recevoir la trame multicast ou broadcast.

2.4.5.6.2 Sauvegarde d'énergie dans un réseau ad hoc

Comme un réseau ad hoc ne dispose pas d'AP, chaque station doit conserver en mémoire les trames qu'elle désire transmettre à des stations endormies (mode *Doze*).

Périodiquement les stations endormies se réveillent pour recevoir le *beacon*, elles restent alors éveillées pendant une durée appelée fenêtre **ATIM**[47] (*ATIM window*).

Pendant la fenêtre ATIM, les stations ayant des trames à échanger à des stations qui étaient endormies envoie leur liste de stations.

Au bout de la fenêtre ATIM, les stations qui n'ont aucune trame à recevoir retourne en mode *Doze*, les autres acquittent la liste reçue, reçoivent les données qui leur sont destinées et les acquittent.

---

[43] *La station est incapable de transmettre ou de recevoir, elle utilise le minimum de son énergie. Si elle a des messages à envoyer, elle les sauvegarde localement.*
[44] *La station utilise toute sa puissance pour envoyer et recevoir des paquets à tout moment*
[45] Traffic Indication Map
[46] Delivery Traffic Indication Message
[47] Ad hoc Traffic Indication Map

2.4.6 Les variantes de la norme IEEE 802.11

La norme IEEE 802.11 est en réalité la norme initiale offrant des débits de 1 ou 2 Mbps.

Des révisions ont été apportées à la norme originale afin d'optimiser le débit (c'est le cas des normes 802.11a, 802.11b et 802.11g, appelées normes 802.11 physiques) ou bien préciser des éléments afin d'assurer une meilleure sécurité ou une meilleure interopérabilité. Dans la section suivante on va citer un ensemble des variantes de la norme IEEE 802.11 :

2.4.6.1 **802.11b (Wi-Fi)**

Le comité IEEE a défini en 1999 une nouvelle couche physique, 802.11b ou 802.11HR (High Rate), permettant d'atteindre des débits de 5,5 à 11 Mbit/s. Cette nouvelle couche physique, dénommée Wi-Fi par le WECA[48], s'implémente sur le standard 802.11. Cette norme utilise toujours une bande ISM (2.4 GHz) et une modulation DSSS, ce qui la rend entièrement compatible avec 802.11 DSSS. Par contre le codage n'est plus à base de séquence *Barker*, mais de codage **CCK[49]** . Il utilise aussi un mécanisme de modulation de phase **QPSK** à une vitesse de 1,375 MS/s, ce qui lui permet d'atteindre un débit de 11 Mbits/s. De plus un mécanisme d'adaptation environnemental permet de régler automatiquement le débit (*Variable Rate Shifting*) en fonction des conditions de réception (interférences, portée du matériel …).

Débit	**Longueur de code**	**Modulation**	**Débit (symboles)**	**Nombre de bits/symbole**
1 Mbit/s	11bits (séquence *Barker*)	PSK 1	1 MS/s	1
2 Mbit/s	11bits (séquence *Barker*)	QPSK	1 MS/s	2
5.5 Mbit/s	8 bits (CCK)	QPSK	1.375 MS/s	4
11 Mbit s	8 bits (CCK)	QPSK	1.375 MS/s	8

Table2.2 : Type de codage et modulation de phase

[48] Wireless Ethernet Compatibility Alliance
[49] Complementary Code Keying

2.4.6.2 **802.11a**

En parallèle à la norme précédente, en 1999 l'IEEE a finalisé une nouvelle couche physique: 802.11a. Dénommée Wi-Fi5 par le WECA, cette couche physique utilise la bande radio U-NII des 5GHz, qui offre une largeur de bande plus importante (300MHz) et qui est beaucoup moins encombrée que la bande ISM. Par contre, elle est totalement incompatible avec les autres normes physiques. De plus la modulation de fréquence utilisée, OFDM[50] est différente des autres normes physiques. On a constaté que plus les trames sont longues plus le chevauchement, dû aux interférences, inter trame est moindre. Cela démontre que plusieurs canaux à faible débit sont plus efficaces qu'un seul à haut débit.

De même que pour Wi-Fi, Wi-Fi5 utilise le " ***Variable Rate Shifting*** " lorsque l'environnement se dégrade, le débit passant de 54Mbit/s à 48 puis 36, 24, 12 et 6 Mbit/s pour finir. Il est à noter que la portée est inférieure aux normes utilisant la bande ISM, car plus la fréquence est élevée, plus la portée diminue.

2.4.6.3 **802.11c (pontage 802.11 vers 802.1d)**

La norme 802.11c n'a pas d'intérêt pour le grand public. Il s'agit uniquement d'une modification de la norme 802.1d afin de pouvoir établir un pont avec les trames 802.11 (niveau liaison de données).

2.4.6.4 **802.11d (internationalisation)**

La norme 802.11d est un supplément à la norme 802.11 dont le but est de permettre une utilisation internationale des réseaux locaux 802.11. Elle consiste à permettre aux différents équipements d'échanger des informations sur les plages de fréquences et les puissances autorisées dans le pays d'origine du matériel.

2.4.6.5 **802.11e (amélioration de la qualité de service)**

La norme 802.11e vise à donner des possibilités en matière de qualité de service au niveau de la couche liaison de données. Ainsi, cette norme a pour but de définir les besoins des différents paquets en termes de bande passante et de délai de transmission de manière à permettre, notamment, une meilleure transmission de la voix et de la vidéo.

2.4.6.6 **802.11f (roaming)**

La norme 802.11f est une recommandation à l'intention des vendeurs de points d'accès pour une meilleure interopérabilité des produits. Elle propose le protocole *Inter-Access point roaming protocol* permettant à un utilisateur itinérant de changer de point d'accès de façon transparente lors d'un déplacement, quelles que soient les

[50] Orthogonal Frequency Division Multiplexing

marques des points d'accès présents dans l'infrastructure réseau. Ceci concerne le roaming.

2.4.6.7 **802.11g**

Dernière couche physique apportée au standard 802.11 avant le 802.11n (elle a été validée en juin 2003), cette norme utilise la bande ISM comme Wi-Fi ainsi que la technique de codage CCK, ce qui la rend compatible avec Wi-Fi. Par contre elle utilise l'OFDM, ce qui lui permet d'atteindre un débit max de 54Mbit/s mais avec une consommation d'énergie plus importante.

2.4.6.8 **802.11h**

La norme 802.11h vise à rapprocher la norme 802.11 du standard Européen (HiperLAN 2, d'où le h de 802.11h) et être en conformité avec la réglementation européenne en matière de fréquences et d'économie d'énergie.

2.4.6.9 **802.11i (sécurité)**

La norme 802.11i a pour but d'améliorer la sécurité des transmissions (gestion et distribution des clés, chiffrement et authentification). Cette norme s'appuie sur l'AES[51] et propose un chiffrement des communications pour les transmissions utilisant les technologies 802.11a, 802.11b et 802.11g.

Pour remédier à ces défauts, le groupe IEEE 802.11i travaille dans les quatre directions suivantes :

- intégration du standard IEEE 802.1*x*, permettant de gérer l'authentification et l'échange de clés dans un réseau IEEE 802.11 ;
- gestion et création de clés dynamiques à partir d'une clé initiale ;
- complémentation du WEP[52] pour améliorer le contrôle d'intégrité de chaque paquet et lutter contre les clés faibles de RC4 ;
- utilisation dans la norme IEEE 802.11 du nouveau standard de cryptage AES pour un chiffrement sûr.

2.4.6.10 **802.11Ir**

La norme 802.11IR a été élaborée de manière à utiliser des signaux infrarouges. Cette norme est désormais dépassée techniquement.

[51] Advanced Encryption Standard
[52] Wired Equivalent Privacy

2.4.6.11 **802.11j**

La norme 802.11j est à la réglementation japonaise ce que le 802.11h est à la réglementation européenne.

2.4.6.12 **802.11n (**WWiSE[53]**)**

Le débit théorique atteint les 540 Mbit/s (débit réel de 100 Mbit/s dans un rayon de 90 mètres) grâce aux technologies MIMO[54] et OFDM. En avril 2006, des périphériques à la norme 802.11n commencent à apparaître mais il s'agit d'un 802.11 N draft (brouillon) ou plutôt provisoire en attendant la norme définitive qui est sortie cette année [5].

2.4.6.13 **802.11s (**Réseau Mesh**)**

La norme 802.11s est actuellement en cours d'élaboration. Le débit théorique atteint aujourd'hui 1 à 2 Mbit/s. Elle vise à implémenter la mobilité sur les réseaux de type ad hoc. Tout point qui reçoit le signal est capable de le retransmettre. Elle constitue ainsi une toile au dessus du réseau existant.

2.4.7 Les équipements **802.11**

Il existe différents types d'équipement pour la mise en place d'un réseau sans fil 802.11 :

2.4.7.1 **Les adaptateurs sans fil ou cartes d'accès**

En anglais *Wireless Adapters* ou *Network Interface Controller*, noté NIC. Il s'agit d'une carte réseau à la norme 802.11 permettant à une machine de se connecter à un réseau sans fil. Les adaptateurs 802.11 sont disponibles dans de nombreux formats (carte PCI, carte PCMCIA, adaptateur USB, carte compact flash, ...). On appelle station tout équipement possédant une telle carte. A noter que les composants 802.11 deviennent des standards sur les portables (label Centrino d'Intel).

2.4.7.1.1Cartes PCMCIA

Il existe plusieurs sortes de cartes PCMCIA se distinguant par leur puissance ou la présence d'un connecteur antenne.

a. Le connecteur antenne

Généralement de type Lucent (Orinoco, avaya), MCX, MMCX ils permettent de rajouter une antenne à gain, ce qui peut être intéressant si vous êtes situé assez loin d'un point d'accès par exemple.

[53] World-Wide Spectrum Efficiency ou TGn Sync
[54] Multiple-input multiple-output

b. La puissance

La puissance des cartes Wireless va de 30mW à plus de 200mW, habituellement les cartes que vous rencontrerez dans le commerce auront une puissance de 30 mW (env. 15 dBm).

2.4.7.1.2Cartes PCI

L'atout principal des cartes PCI par rapport aux cartes PCMCIA est l'antenne, qui est soit intégrée à la carte, soit amovible (donc possibilité de connecter l'antenne de votre choix).

Il est important de ne pas prendre une carte PCI avec antenne intégrée, le PC étant généralement situé sous un bureau la qualité de réception sera souvent médiocre, optez donc pour une carte avec connecteur antenne.

En ce moment la carte la plus intéressante est la DWL-520+ de chez D-link (SMC vend aussi un modèle similaire), elle fait partie des cartes les moins chères du marché et possède un mode 22 Mbits/s + 4x pouvant atteindre une vitesse de 44 Mbits (théoriquement).

2.4.7.1.3Cartes USB

Les cartes USB se divisent en 2 grandes familles :

a. Les cartes "adaptateur"

Une partie des cartes USB sont en fait des adaptateurs avec à l'intérieur une carte PCMCIA (généralement orinoco) comme certains modèles HP par exemple.

Ces cartes sont assez intéressantes car elles possèdent généralement un connecteur antenne sous leur coque, la modification est donc à la portée de tout le monde.

b. Les cartes "classiques"

Les cartes USB classiques n'ont généralement pas de connecteurs antennes, mais sont intéressantes dans le sens qu'elles peuvent êtres orientées, grâce à, généralement, 2m de câble, donc êtres considérées comme des petites antennes.

A noter que Linksys a sortie une carte USB qui ressemble à un "Pen drive", donc qui peux intéresser les possesseurs de portables sans ports PCMCIA.

Une bonne partie des cartes USB sont modifiables pour y ajouter un connecteur antenne.

2.4.7.1.4Cartes COMPACT FLASH

Il y a peu de différences entre les cartes Compact Flash et les cartes PCMCIA, si ce n'est leur format et leurs pilotes, certaines cartes sont fournies avec des pilotes Windows (pour PC de bureau et portable) en plus des pilotes pocket PC et d'autres non.

Les cartes Compact Flash sont le plus souvent dépourvues d'un connecteur pour antenne externe.

2.4.7.2 **Les points d'accès**

Notés AP pour *Access Point*, parfois appelés bornes sans fil, permettant de donner un accès au réseau filaire (auquel il est raccordé) aux différentes stations avoisinantes équipées de cartes 802.11. Cette sorte de hub est l'élément nécessaire pour déployer un réseau centralisé en mode infrastructure. Certains modèles proposent des fonctions de modem ADSL et comprennent plus ou moins de fonctions comme un pare-feu.

2.4.7.2.1Le Linksys WAP11

Le WAP11 de Linksys, est un AP très répandu. Il existe deux versions du WAP11 la v1.1 et la v2.2.

Figure 2.12 : *Le Linksys Wap11 est un point d'accès IEEE 802.11b*

La différence primordiale entre les deux versions est que la configuration du v1.1 pouvait se faire grâce à un port USB présent à l'arrière de l'appareil. La configuration par USB s'étant avérée une mauvaise idée, le port USB a donc été supprimé dans la version 2.2.

2.4.7.3 **Les autres types d'équipements**

- **Smart Display**: écrans mobiles, soutenus par Microsoft.

- **Chaînes WiFi 802.11**: offrant la capacité de lire les MP3 directement sur le disque dur d'un ordinateur grâce à l'interface Ethernet sans fil intégrée. Elle préfigure toute une génération de produits, capables de lire, outre les CD audio, les radios qui émettent en MP3 sur Internet.
- **Assistant personnel**: le PDA intégrant le 802.11 est parfois plus avantageux qu'un portable pour lire ses mails, importer des documents voir surfer sur le net.
- **Rétroprojecteurs**: pour des présentations avec portables mobiles.
- **Caméra vidéo**: transmettre des images à distance à l'ordinateur qui les enregistre.

Les composants Wi-Fi 802.11 ne sont pas plus onéreux que ceux des réseaux filaires, bientôt toutes les plates-formes seront vendues avec des modules Wi-Fi intégrés. C'est déjà le cas dans le monde des PC portables, qui, sous l'impulsion d'Intel, fait sa révolution sans fil grâce au Centrino.

2.5 Conclusion

Ce chapitre a donc introduit les connaissances de bases, commençant par la définition des réseaux sans fil et les différentes catégories de réseaux sans fil, et plus précisément les réseaux IEEE 802.11, à démontrer l'importance des couches basses du modèle en couche. On a cité aussi les différentes variantes de cette norme, et enfin on a fait un parcours rapide sur les équipements 802.11.

Dans le chapitre suivant, nous nous intéressons plus spécialement aux réseaux ad hoc et au problème de routage dans ce type de réseaux.

RÉSEAU AD HOC ET ROUTAGE

1. Réseau ad hoc

3.1 Définition

L'IETF[55], qui représente l'organisme responsable de l'élaboration des standards pour Internet, définit les réseaux ad hoc, appelé également **MANET** (*Mobile Ad hoc NETworks*), de la manière suivante :

- *" Un réseau ad hoc est un système autonome de plates-formes mobiles (par exemple un routeur interconnectant différents hôtes et équipements sans fil) appelées nœuds qui sont libres de se déplacer aléatoirement et sans contraintes. Ceci provoque des changements rapides et imprédictibles de la topologie du réseau. Ce système peut fonctionner d'une manière isolée ou s'interfacer à des réseaux fixes au travers de passerelles. Dans ce dernier cas, un réseau ad hoc est un réseau d'extrémité".*

Donc, un réseau mobile ad-hoc consiste en un grand nombre d'unités mobiles se déplaçant dans un environnement quelconque en utilisant, comme moyen de communication, des interfaces sans fil sans infrastructure préexistante.

Les caractéristiques de ces réseaux engendrent des contraintes à leur mise en œuvre:

Sans infrastructure : Les MANETs ne dépendent donc pas d'une infrastructure préétablie, chaque nœud opère comme un routeur indépendant. L'organisation du réseau doit donc être distribuée à tous les nœuds, ce qui rend la détection d'erreur et la gestion du réseau complexes.

Topologie dynamique : Les nœuds se déplaçant arbitrairement, la topologie change fréquemment et de façon aléatoire. Cela implique que les routes entre les nœuds changent et des paquets peuvent ainsi être perdus.

[55] Internet Engineering Task Force

Connexions variables : Les nœuds peuvent avoir plusieurs interfaces radios, présentant des propriétés de débits ou de fréquences différents. Ces variations donnent naissance à des connexions asymétriques.

Contraintes d'énergie : Les batteries utilisées par les nœuds ne sont pas illimitées. Les services supportés par ces nœuds sont donc restreints. C'est un problème d'autant plus important que les nœuds sont responsables du routage des paquets dans le réseau, ce qui consomme beaucoup d'énergie.

Taille : la plupart des algorithmes utilisés pour les réseaux ad hoc sont optimisés pour de petits réseaux. Il y a donc des améliorations à apporter dans certains domaines (sécurité, routage,...) pour pouvoir passer à une échelle supérieure.

Vulnérabilité : Les réseaux sans fil sont par nature plus sensibles aux problèmes de sécurité. Pour les réseaux ad hoc, le problème ne se situe pas, principalement, au niveau du support physique mais dans le fait que tous les nœuds sont équivalents et potentiellement nécessaires au fonctionnement du réseau.

3.2 Historique et projets

Historiquement, les réseaux mobiles ad hoc ont été d'abord introduits pour l'amélioration des communications dans le domaine militaire. Dans ce contexte, il n'existe pas d'infrastructure existante pour relier les communications, vue la nature dynamique des opérations et des champs militaires.

Les premières applications dans les réseaux ad hoc sont apparues avec le projet PRNet[56] [6] en 1972. Ce projet a été inspiré par l'efficacité de la technologie par commutation de paquets, le partage de la bande passante, le routage *store-and-forward*, et ses applications dans l'environnement mobile sans fil.

SURAN[57] [6] a été développé par la DARPA en 1983 pour dresser les principaux problèmes du projet PRNet dans le domaine de la scalabilité, la sécurité, la capacité de traitement et gestion d'énergie. Les objectifs étaient de proposer des algorithmes qui peuvent supporter jusqu'à une dizaine de milliers de nœuds, tout en utilisant des mécanismes radio simples, avec une faible consommation d'énergie, et un faible coût. Ce travail a amené à la conception de la technologie LPR[58] [6] en 1987, dotée d'une couche radio DSSS avec un processeur pour la commutation de paquets intégré (Intel 8086). De plus, une famille de protocoles pour la gestion du réseau a été développée, et une topologie hiérarchique du réseau basée sur un groupe «clustering» dynamique est utilisée pour remédier au problème de la scalabilité. Des améliorations pour

[56] Packet Radio Network
[57] Survivable Radio Networks
[58] Low-cost Packet Radio

l'adaptabilité de la couche radio, la sécurité et l'augmentation de la capacité ont été proposées aussi.

L'évolution des infrastructures du réseau Internet et la révolution de la micro informatique ont permis de rendre faisables et applicables les idées initiales des réseaux radio de paquets. Le programme GloMo [59][6] initié par la DARPA en 1994 avait comme objectif de supporter les communications multimédia n'importe quand et n'importe où à travers des équipements sans fil.

Tactical Internet (IT) [6] est l'une des implémentations des réseaux sans fil ad hoc grandeur nature développée par l'armée américaine en 1997, utilisant des débits de plusieurs dizaines de kilobits par seconde.

Un autre déploiement a été réalisé en 1999, avec ELB ACTD[60] [6] qui permet de démontrer la faisabilité de concepts militaires pour les communications des bateaux en mer aux soldats sur la terre par l'intermédiaire d'un relais aérien. Vingt nœuds dans le réseau ont été considérés.

3.3 Domaines d'application des réseaux ad hoc

Comme nous avons vu dans l'historique, les premières applications des réseaux ad hoc concernaient les communications et les opérations dans le domaine militaire. Cependant, avec l'avancement des recherches dans le domaine des réseaux et l'émergence des technologies sans fil (ex : Bluetooth, IEEE 802.11 et Hiperlan); d'autres applications civiles sont apparues. On distingue :

Les services d'urgence : opération de recherche et de secours des personnes, tremblement de terre, feux, inondation, dans le but de remplacer l'infrastructure filaire,

Le travail collaboratif et les communications dans des entreprises ou bâtiments: dans le cadre d'une réunion ou d'une conférence par exemple, Home network : partage d'applications et communications des équipements domestiques mobiles,

Applications commerciales : pour un paiement électronique distant (taxi) ou pour l'accès mobile à l'Internet, où service de guide en fonction de la position de l'utilisateur,

Réseaux de capteurs : pour des applications environnementales (climat, activité de la terre, suivi des mouvements des animaux,…etc.) ou domestiques (contrôle des équipements à distance…etc),

Réseaux en mouvement : informatique embarquée et véhicules communicants (VANETs),

Réseaux Mesh : c'est une technologie émergente qui permet d'étendre la portée d'un réseau ou de le densifier.

[59] Global Mobile
[60] Extending the Littoral Battle space Advanced Concept Technology Demonstration

En plus, dans un WLAN, un réseau ad hoc fournit une solution pour étendre une couverture sans fil avec un coût minimum. Dans un WWAN (ex : UMTS), il permet d'accroître la capacité globale du réseau sans fil. En fait, plus de bande passante agrégée peut être obtenue en réduisant la taille des cellules et en créant des pico-cellules. Afin de supporter une telle architecture, les opérateurs disposent de deux options : déployer plus de stations de base (une station de base par cellule), ou utiliser un réseau ad hoc pour atteindre la station de base. La deuxième solution est clairement plus flexible et moins coûteuse. La figure suivante montre un exemple d'illustration des réseaux ad hoc.

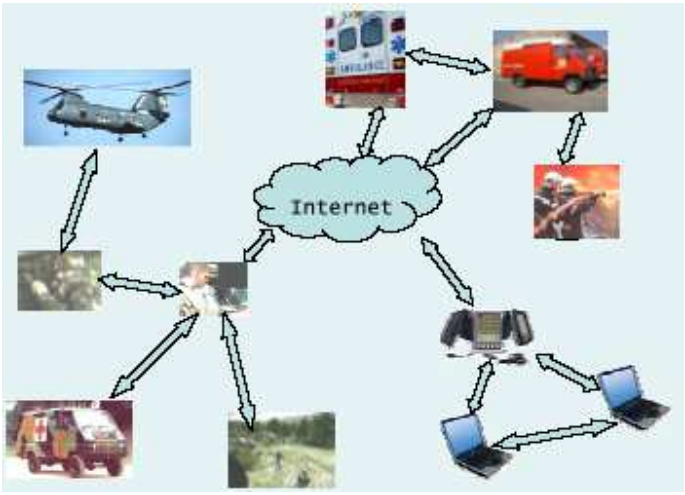


Figure3.1 : Exemple d'illustration des réseaux ad hoc

3.4 Routage dans les réseaux mobiles ad hoc

Les réseaux ad hoc se caractérisent par une absence d'infrastructure et de gestion centralisée. Dans ce type de réseaux, chaque élément peut bien évidemment émettre et recevoir des messages, mais assure également un rôle de relais de l'information afin que les messages circulent dans le réseau de proche en proche. Chaque nœud du réseau doit donc posséder des capacités de routage, c'est le routage dit ad hoc. Grâce à ce routage, la portée radio d'un nœud peut être virtuellement étendue en utilisant ses voisins comme relais de l'information.

La problématique du routage de l'information dans ce type de réseau est complexe. En effet, les réseaux ad hoc sont souvent peu stables :

- Les nœuds peuvent être mobiles;

- Les nœuds peuvent entrer et sortir du réseau à tout moment, soit parce qu'ils s'éteignent, soit parce qu'ils sortent de la portée radio des nœuds du réseau;
- Les ressources des nœuds sont souvent limitées (capacité de calcul, énergie...) car ce sont des équipements embarqués légers et mobiles;
- Le médium radio est peu fiable en termes de perte d'information et de sécurité;
- Les liens radio peuvent être asymétriques, l'information passe dans un sens mais pas dans l'autre (à cause des irrégularités des ondes électromagnétiques).

Il existe différentes méthodes pour résoudre cette problématique et qui correspondent à la proposition de différents protocoles de routage. Ces protocoles s'appuient sur trois modèles de fonctionnement: les protocoles proactifs, les protocoles réactifs et les protocoles hybrides.

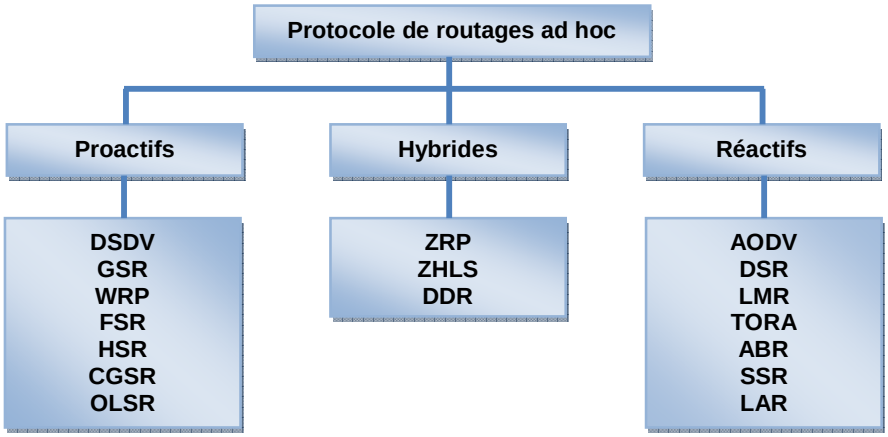


Figure 3.2 : Classification des protocoles de routage ad hoc

Les protocoles proactifs ou "*Table Driven*" se comportent comme les protocoles de routage des réseaux filaires : les routes permettant d'atteindre les nœuds du réseau sont maintenues en permanence et stockées dans des tables de routage au niveau des nœuds. Les protocoles réactifs ou "*On Demand*", quant à eux, ne calculent pas de routes avant qu'il n'y ait une demande par un nœud pour une transmission. Les routes sont donc uniquement cherchées à la demande. Les protocoles hybrides mélangent les deux techniques précédentes.

Avec l'apparition des systèmes de positionnement bas coût, une quatrième catégorie peut être ajoutée aux trois précédentes : elle est basée sur la position des nœuds du réseau, ce sont les protocoles géographiques.

Dans les paragraphes suivants, une présentation non exhaustive des protocoles représentatifs de ces différentes familles est réalisée au travers de leurs principales caractéristiques.

3.4.1 Protocoles de routage proactifs

3.4.1.1 **Fonctionnement**

Les protocoles de routage proactifs pour les réseaux mobiles ad hoc reprennent le principe du routage des réseaux filaires. Ils sont basés sur l'existence de tables de routage au niveau de chacun des nœuds. Lorsqu'un nœud du réseau souhaite envoyer un message, il consulte sa table de routage pour connaître la route à suivre jusqu'au destinataire du message. Les deux principales méthodes utilisées sont :

- La méthode d'état des liens (*link state*)
- La méthode de vecteurs de distance (*distance vector*)

Dans l'approche de routage par vecteur de distance, un nœud échange avec ses voisins une estimation de la distance vers tous les nœuds du réseau. Cet échange d'informations couplé avec un algorithme de recherche du plus court chemin Bellman (1957) et de Ford et Fulkerson (1962) permet à chaque nœud de converger vers une connaissance exacte de la topologie du réseau. C'est-à-dire que chaque routeur communique aux autres routeurs la distance qui les sépare (en nombre de sauts). Ainsi, lorsqu'un routeur reçoit un de ces messages il incrémente cette distance de 1 et communique le message aux routeurs directement accessibles. Les routeurs peuvent donc conserver de cette façon la route optimale d'un message en stockant l'adresse du routeur suivant dans la table de routage de telle façon que le nombre de sauts pour atteindre un réseau soit minimal. Le protocole RIP[61] est le protocole 'vecteur de distance' le plus connu.

Dans le protocole de type 'Link State', les nœuds transmettent en diffusion dans le réseau l'état des liens avec leurs voisins. Ainsi tous les nœuds finissent par détenir le voisinage de chacun des nœuds du réseau. On conçoit alors facilement que l'on puisse connaître la topologie complète du réseau. Pour calculer les routes optimales vers un nœud, il sera facile d'utiliser l'algorithme de Dijkstra. Cet algorithme procède au calcul des distances par une récurrence montante. D'abord on considère ses voisins qui sont donc à distance 1, puis les voisins de ses voisins. Ces nœuds sont à distance 2 et on continuera ainsi.

Les protocoles ad hoc proactifs qui ont été standardisés au sein de l'IETF sont OLSR[62], et TBRPF[63].

[61] Routing Internet Protocol
[62] Optimized Link State Routing
[63] Topology Broadcast Based on Reverse-Path Forwarding

3.4.1.2 **Synthèse**

Le principal avantage de ces protocoles est leur réactivité. En effet, à tout moment chaque élément du réseau connaît un moyen d'atteindre les autres membres du réseau.

En revanche, il faut être capable d'actualiser les tables de routage en permanence pour tenir compte de la mobilité des nœuds, cela entraîne la diffusion de nombreux messages de contrôle qui engendre du trafic sur le réseau réduisant ainsi la bande passante disponible pour envoyer des données. De plus, cette émission permanente de messages entraîne une consommation énergétique plus importante au niveau des nœuds du réseau, ce qui rend l'utilisation de ce type de protocole dans les réseaux de capteurs problématique.

Les différents protocoles réactifs se différencient principalement par le mode de mise à jour des tables de routage.

3.4.2 Protocoles de routage réactifs

3.4.2.1 **Fonctionnement**

Les protocoles de routage réactifs (dits aussi : protocoles de routage à la demande), ne maintiennent pas en permanence des tables de routage de l'ensemble du réseau. En réalité, les protocoles de routage appartenant à cette catégorie, créent et maintiennent les routes selon les besoins. Lorsque le réseau a besoin d'une route, une procédure de découverte globale de routes est lancée, et cela dans le but d'obtenir une information. C'est-à-dire Lorsqu'un nœud a besoin d'envoyer un message vers un autre élément du réseau, il commence par déterminer une route lui permettant d'atteindre le destinataire du message. Cette route sert à envoyer les informations et reste dans une table au niveau du nœud. Les nœuds du réseau n'ont donc qu'une vision partielle du réseau et ne connaissent que les éléments du réseau avec qui ils ont l'habitude de communiquer.

Le protocole ad hoc réactifs qui a été standardisé au sein de l'IETF est AODV[64].

3.4.2.2 **Synthèse**

Le routage à la demande permet de réduire le nombre des messages de contrôle, mais il induit une lenteur à cause de la recherche des chemins, ce qui peut dégrader les performances des applications interactives (par exemple les applications des bases de données distribuées). En outre, il est impossible de connaître au préalable la qualité du chemin (en termes de bande passante, délais,… etc.). Une telle connaissance est importante dans les applications multimédias.

[64] Ad hoc On demand Distance Vector

3.4.3 Protocoles de routage Hybrides

3.4.3.1 **Fonctionnement**

Les protocoles hybrides combinent les deux idées : celle des protocoles proactifs et celle des protocoles réactifs. Ils utilisent un protocole proactif pour avoir des informations sur les voisins les plus proches (au maximum les voisins à deux sauts).

Au-delà de cette zone prédéfinie, le protocole hybride fait appel aux techniques des protocoles réactifs pour chercher des routes.

3.4.3.2 **Synthèse**

Ce type de protocoles s'adapte bien aux grands réseaux, cependant, il cumule aussi les inconvénients des protocoles réactifs et proactifs en même temps (messages de contrôle périodique, le coût d'ouverture d'une nouvelle route, …etc.).

3.4.4 Avantages et limites de ces protocoles

Tous les protocoles présentés ci-dessus ont été implémentés et simulés par leurs auteurs respectifs sur Network Simulator (NS-2). Des comparaisons entre ces différents protocoles ont aussi été effectuées. Nous pouvons déduire de ces résultats les remarques suivantes :

- Les protocoles basés sur le « Source Routing » comme DSR obtiennent de meilleures performances que les autres approches et cela quelles que soient les hypothèses initiales (forte mobilité, overhead, ...). Il faut toutefois remarquer que DSR est légèrement plus lent que les protocoles basés sur une approche proactive.
- Dans l'ensemble, les approches proactives ont de bonnes performances dans la majorité des cas. Cependant, l'inondation du réseau par des messages de contrôle est très pénalisante.
- Les approches hybrides cumulent les avantages des approches réactives et proactives mais aussi de leurs inconvénients. TORA a, par exemple, des performances déplorables lorsque la mobilité des nœuds est élevée : le « flooding » proactif fait effondrer le réseau.
- Aucun de ces protocoles n'a réellement été conçu pour un routage avec QoS, sauf OLSR qui prend en compte la qualité des liens.

3.5 Présentation du protocole OLSR

Un exemple de protocole de routage proactif basé sur la topologie, actuellement largement utilisé dans les réseaux ad-hoc mobiles à sauts multiples est le protocole dénommé **OLSR**[65]. Ce protocole est défini dans le document RFC n°**3626** de l'IETF.

3.5.1 Fonctionnement général

Le concept principal utilisé dans le protocole est celui des relais multipoint, (MPRs[66]). 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[67].

3.5.2 Type de paquets

3.5.2.1 **Message Hello**

Le message HELLO transmet plusieurs informations et a plusieurs utilités. Il sert d'abord à découvrir l'ensemble du réseau. Il transmet ensuite l'état et le type de lien entre le nœud expéditeur et chaque nœud voisin. Enfin, il spécifie le MPR choisi par l'expéditeur.

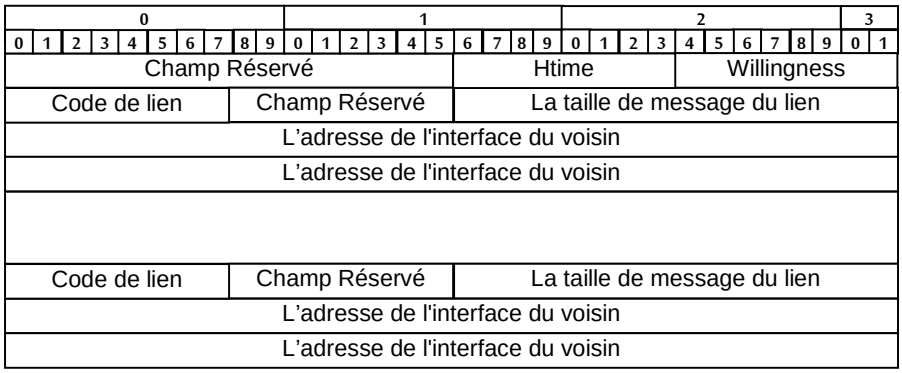


Figure 3.3 : Le datagramme de message Hello

[65] Optimized Link State Routing Protocol
[66] Multi-Point Relays
[67] Topology control

- « champ Réservé » : Ce champ doit contenir « 0000000000000000 »
- « Htime » : Intervalle d'émission des messages HELLO
- « Willingness » : demande à un nœud de devenir un MPR
- « code de lien » : Code identifiant le type de lien (pas d'information, symétrique, asymétrique, etc.) entre l'expéditeur et les interfaces listées dans le champ « les adresses de l'interface des voisins »

En réalité, Les messages HELLO ne sont destinés qu'aux nœuds voisins (à un saut) de l'expéditeur, ils doivent donc ne jamais être routés par un MPR.

3.5.2.2 **Message TC**

Le message TC permet au MPR de transmettre la liste des voisins qui l'ont choisi comme MPR. Il sert à établir les tables de routage. La table de routage est calculée par chaque nœud, à partir des informations contenues dans la table de voisinage et la table topologique, en utilisant par exemple l'algorithme de plus court chemin de Djikstra.

Aussi, pour que le message TC soit diffusé sur tout le réseau, la valeur du TTL dans l'header du message est 255, la valeur maximale. La structure du paquet TC est illustrée à la figure 3.4.

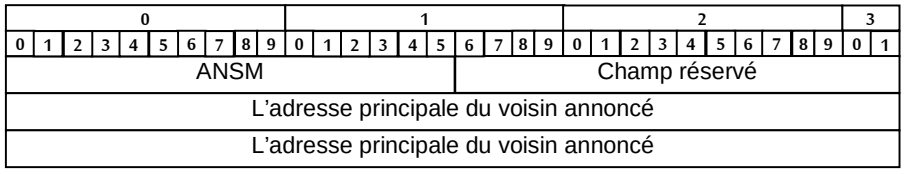


Figure 3.4 : Le datagramme de message TC

- « Champ réservé » : Ce champ doit contenir « 0000000000000000 »
- « ANSN[68] » : Entier incrémenté à chaque changement de topologie. Il permet de ne pas tenir compte des informations obsolètes, pour tenir les tables le plus à jour possible.
- « L'adresse principale du voisin annoncé » : transportent les adresses IP des nœuds à un saut. L'ensemble des nœuds publiés dans les messages TC est un sous-ensemble des voisins à un saut. La version par défaut recommande de publier les "MPR-Selectors", c'est-à-dire les voisins pour lesquels le nœud courant est un relai MPR.

[68] Advertised Neighbor Sequence Number

3.5.3 Découverte de voisinage

Chaque nœud doit détecter ses voisins adjacents, c'est à dire ceux avec qui il a des liens directs. Les liens considérés comme valides sont ceux vérifiés dans les deux directions et sont dits symétriques.

Pour accomplir cette tâche, chaque nœud diffuse périodiquement un massage ***Hello*** contenant des informations sur son voisinage et l'état des liens vers ses nœuds voisins.

Ce type de message est transmis en mode *Broadcast* mais diffusé seulement localement et ne sera pas retransmis. Un message *Hello* envoyé contient :

- La liste des adresses de ses voisins symétriques.
- La liste des adresses de ses voisins asymétriques. Ce sont les voisins que le nœud peut écouter mais que l'inverse n'est pas encore possible. Si par la suite le nœud trouve sa propre adresse sur un *Hello* reçu alors il considère que le lien est désormais valide.

Les échange des paquets Hello permettent à chaque nœud de prendre connaissance de son voisinage à un et à deux sauts.

Dans la table de voisinage, chaque nœud enregistre la liste de ses voisins, l'état des liens et pour chaque voisin la liste des voisins à deux sauts qu'il peut couvrir. Une entrée dans cette table est de la forme : N_time défit la durée pour laquelle l'entrée est valide, si elle expire l'entrée sera supprimée.

N_addr	N_status	N_2hop_list	N_time

3.5.4 Sélection des relais multipoints (MPR)

La sélection des MPRs est réalisée de façon distribuée. Chaque nœud **u** élit, parmi ses voisins, un ensemble de relais multipoints qui permet de couvrir tous ses voisins à deux sauts, l'ensemble des MPR doit être optimal mais suffisamment petit pour atteindre l'objectif attendu de sa construction. Une heuristique a été proposée pour le choix de cet ensemble. Un nœud est un relais multipoint d'un autre, donc c'est une relation binaire.

L'ensemble des MPRs est recalculé s'il ya un changement dans le voisinage à un saut (si un lien bidirectionnel disparaît dans le voisinage) ou le voisinage à deux sauts toujours en terme de liens bidirectionnels.

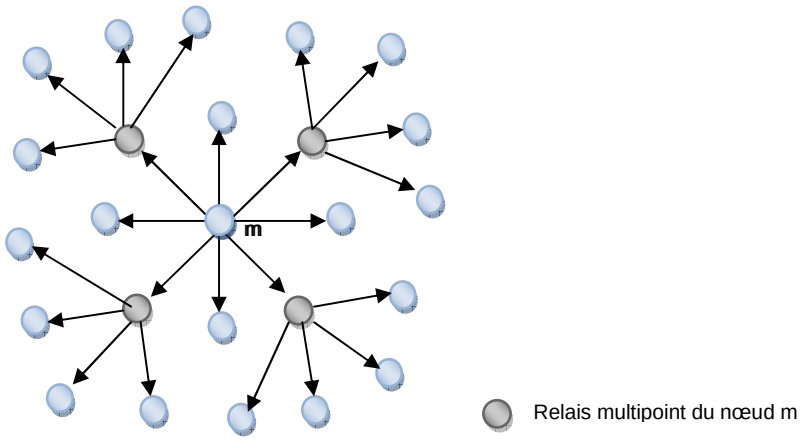


Figure 3.5 : Relais multipoints du nœud m

Grâce aux messages *Hello*, chaque nœud est capable de connaître les voisins qui l'ont choisi comme MPR. Cet ensemble appelé l'ensemble des sélecteurs multipoints[69] et aussi enregistré sur la table des sélecteurs multipoints.

3.5.5 Annonce des MPRs

Dans le but de construire la table de routage qui permet de router les paquets vers n'importe quelle destination, les informations locales doivent être diffusées dans l'ensemble du réseau. Chaque relais diffuse en mode *Broadcast* un message particulier TC. Seuls les voisins MPR rediffusent un paquet TC reçu pour éviter l'inondation. Cette technique prometteuse réduit considérablement l'overhead généré par le trafic de contrôle.

Comme pour tout paradigme proactif, le paquet TC est envoyé par chaque nœud à des intervalles réguliers pour déclarer l'ensemble des sélecteurs MPR. Il s'agit de la liste des voisins du nœud générateur l'ayant choisi comme MPR. Un numéro de séquence(MSSN) est associé à l'ensemble des sélecteurs MPR et est attaché à cette liste. La liste des adresses peut être partielle mais dans ce cas, elle doit être complétée au bout d'une durée de rafraîchissement prédéfinie. Un nœud n'ayant pas été choisi comme MPR ne génère pas de message TC.

L'intervalle entre deux transmissions de message TC est régulier et est positionné à une valeur paramétrable (par défaut 5 secondes). Cependant, si l'ensemble des sélecteurs multipoint change durant cet intervalle alors l'envoi du prochain message TC sera déclenché immédiatement lorsque le temps minimum séparant deux transmissions (il est aussi prédéfini) est écoulé.

[69] MultiPoint Relay Selector

Chaque nœud maintient une table de topologie dans laquelle il enregistre les informations apportées par les messages TC. La table de topologie est ainsi mise à jour après chaque réception d'un message TC. Sur la base de cette table, la table de routage sera à son tour calculée. Une entrée de la table de topologie peut avoir le format suivant : cette entrée se lit comme suit :

T_dest	T_last	T_seq	T_time

T_dest a sélectionné T_last comme un relais multipoint. T_last est à l'origine de l'annonce de cette information via le message TC qu'il a généré (T_dest est donc son sélecteur MPR). De la même manière que pour la table de voisinage, la validité de chaque entrée de la table de topologie est limitée par le champ T_time. Les numéros de séquence servant à reconnaître l'ordre de génération des messages TC. Ainsi, si un message TC arrive plus tard que prévu et si entre temps un autre message généré après lui ait été traité, alors le premier message est jugé obsolète et sera en conséquence supprimé.

3.5.6 Calcul de la table de routage

Chaque nœud maintient une table de routage qui permet d'acheminer les paquets vers n'importe quelle destination dans le réseau. La table de routage sera construire sur la base des informations contenues dans la table de voisinage ainsi que la table de topologie. L'algorithme de Dijkstra, basé sur le plus court chemin en nombre de sauts est appliqué. Une entrée dans la table de routage est de la forme :

R_dest	R_next	R_dist

Ce qui signifie que le nœud identifié par R_dest est estimé être à une distance égale à R_dist du nœud local et le voisin à un saut dont l'adresse est R_next est le prochain saut à emprunter dans le chemin reliant le nœud local à R_dest.

Si l'une des tables de voisinage ou de topologie change alors la table de routage doit être recalculée. La mise à jour de la table nécessite simplement un calcul local et n'implique aucun envoi des paquets supplémentaires.

3.5.7 Hystérésis des liens

Les liens établis par le protocole OLSR devraient être aussi fiables que possible pour éviter la perte de données. Cela implique que le processus de découverte de voisinage devrait faire face aux connexions temporaires entre les nœuds et aux pertes. Pour cela, le mécanisme de découverte de voisinage a été raffiné en introduisant « l'hystérésis des liens » présentée ci-après.

Chaque tuple désignant un lien doit contenir les informations supplémentaires suivantes :

- L_link_pending : est un booléen qui indique si le lien est considéré comme établi ou non. Initialement, tout nouveau lien est considéré comme transitoire en positionnant le booléen L_link_pending à vrai,

- L_link_quality : est un nombre compris entre 0 et 1 qui indique la qualité du lien. La qualité du lien peut être estimée sur la base du rapport signal/bruit si une telle mesure est disponible. Autrement, il est possible de considérer le taux de succès des messages *Hello* (c'est le nombre de message *Hello* qui atteignent le voisin sur le nombre total de messages Hello générés).

- L_lost_link : est le temps nécessaire pour déclarer le lien comme perdu une fois il devient transitoire (L_link_pending passe à vrai).

3.6 Conclusion

Dans ce chapitre, un état de l'art sur les réseaux Ad hoc les protocoles de routage qui lui sont dédiés a été présenté. Parmi ces protocoles, nous avons prêté une attention particulière au protocole de routage proactif OLSR, parce qu'ils définissent le contexte de notre travail.

Dans le prochain chapitre, nous allons exposer les travaux récents sur la gestion de l'économie d'énergie dans les réseaux ad hoc.

ÉTAT DE L'ART

4. Etat de l'art

4.1 Introduction

L'énergie est un facteur majeur pour les réseaux sans fil et dans le contexte de mobilité du fait que les stations du réseau sont en activité permanente (*radio* : écoute du canal, réception, transmission ou *niveau supérieur* : routage, traitement de l'information, …). Cette activité ne pourrait être présente et continue qu'à travers les batteries des stations présentant l'inconvénient d'être de charge limitée. Plusieurs travaux ont démontrée que l'activité d'un réseau sans fil est très coûteuse en énergie.

En réalité, la partie radio d'un dispositif sans fil peut être dans l'un des quatre états suivants [7]: Transmission, Réception, Idle ou Sleep.

- **Transmission:** la station transmet une trame de données avec une puissance de transmission $\boldsymbol{P_{transmit}}$;
- **Réception:** la station reçoit une trame de données avec une puissance de réception $\boldsymbol{P_{recevoir}}$;
- **Veille « *Idle* »** (écouter): la station est prête à recevoir ou à transmettre, donc les nœuds restent Inactif et écoutent le medium avec une puissance $\boldsymbol{P_{idle}}$;
- **Sleep**: c'est quand la station est éteinte et le nœud n'est pas capable de détecter des signaux radio, c'est à dire aucune communication n'est possible. La puissance $\boldsymbol{P_{sleep}}$ est le plus petit en général.

Dans la table 4.1, nous rapportons les valeurs référencés de $P_{transmit}$, $P_{recevoir}$, P_{idle} et P_{sleep} prises pour 802.11. L'exemple concerne une carte PC Lucent WaveLan Silver, et pour 802.15.4 l'exemple concerne la FreeScale MC 13192 SARD [7].

L'état	Valeur d'énergie	
	802.11	**802.15.4**
$P_{transmit}$	1.3W	0.1404W
$P_{transmit}$	0.9W	0.1404W
P_{idle}	0.74W	0.0018W
P_{sleep}	0.047W	0.000018W

Table4.1 : Valeurs de la puissance dans chaque état

Donc on remarque que la proportion la plus élevée d'énergie consommée par les interfaces réseaux sans fil (WNIC[70]) est celle consommée durant l'activité de la communication à travers essentiellement la transmission. Les modèles existants pour évaluer le comportement de la consommation d'énergie d'un réseau ad hoc mobile ont montré [8] que les coûts apparentés de plusieurs composants d'énergie comportent la puissance de la transmission aussi bien que la puissance de réception. Cependant, ces activités liées à la communication ne sont pas les seules qui consomment de l'énergie. Même dans les états *idle* et *sleep*, un mobile doit assurer sa connectivité au réseau à travers l'envoie périodique de messages de contrôle et l'écoute du canal. Plusieurs études et recherches [9] ont montré que l'écoute du canal auquel opère le protocole est la source primaire de la perte de puissance. Même au niveau du routage, la participation des nœuds intermédiaires à l'opération de routage et le traitement du trafic de contrôle, associé au protocole de routage utilisé, multiplient la consommation de l'énergie.

En effet, le niveau routage du modèle en couches des réseaux WLANs est plus complexe en mode Ad Hoc qu'en mode infrastructure. Les nœuds devront être à double fonctionnalités : routeur et nœud de terminaison et donc la consommation d'énergie est encore plus importante. En fait, les informations échangées pour n'importe quel protocole de routage proactif ou réactif augmentent la charge des nœuds et celle du réseau. Ceci induit une perte additionnelle d'énergie entre la fonction de gestion et de maintenance des routes et celle de transmission. Donc la conservation d'énergie pourrait être accomplie à différents niveaux avec différentes techniques. Dans notre cas, nous pouvons classer les techniques d'économie d'énergie en trois classes : contrôle de puissance de transmission « *transmission power control »*, mode de puissance basse « *low-power mode»* et routage orienté puissance « *power-aware routing »*.

[70] Wireless Network Interface Card

Nous présentons dans ce qui suit les principales approches existantes pour la conservation d'énergie.

4.2 Le contrôle de la puissance de transmission

Le problème de contrôle de la puissance dans les réseaux ad hoc est celui du choix de la puissance de transmission de chaque paquet de façon distribuée. Le problème est complexe du moment que le choix du niveau de la puissance affecte beaucoup d'aspects du fonctionnement du réseau:

i) Le niveau de la puissance de transmission détermine la qualité du signal reçue au niveau du récepteur,

ii) Il détermine la portée d'une transmission,

iii) Il détermine la magnitude de l'interférence qu'il crée pour les autres récepteurs.

A cause de ces facteurs:

iv) Le contrôle de la puissance affecte la couche physique (dû à i).

v) Il affecte la couche réseau du moment que la portée de la transmission affecte le routage (dû à ii).

vi) Il affecte la couche transport parce que l'interférence cause la congestion (dû à iii).

Donc le contrôle de la puissance de transmission est important dans les réseaux ad hoc, pour au moins trois raisons [10]:

i. Il a un impact sur la durée de vie de la batterie,

ii. Il a un impact sur la capacité du réseau en terme de trafic du transport,

iii. Il peut réduire les interférences des ondes radio et donc augmenter la réutilisation spatiale de la bande passante.

Voici un exemple qui illustre l'importance du contrôle de la puissance de transmission. Considérons un réseau ad hoc basé sur un seul médium partagé, comme montré dans la figure 4.1[10]. La figure 4.1.a montre le cas d'une communication des hôtes A et B, mais A utilise une puissance de transmission pas adéquate (trop grande). Le cercle centré par A représente sa région d'interférence (ce cercle représente aussi la portée des transmissions de A). Cela cause donc des interférences aux hôtes D et F, et affecte alors leur capacité de réception. Avec un contrôle de puissance convenable, comme montré dans la figure 4.1.b, si nous contrôlons intelligemment les puissances de la transmission de A, C, et E, alors trois paires des communications (AB, CD, et EF)

peuvent coexister simultanément. Cela augmentera grandement l'utilisation de la bande passante sans fil.

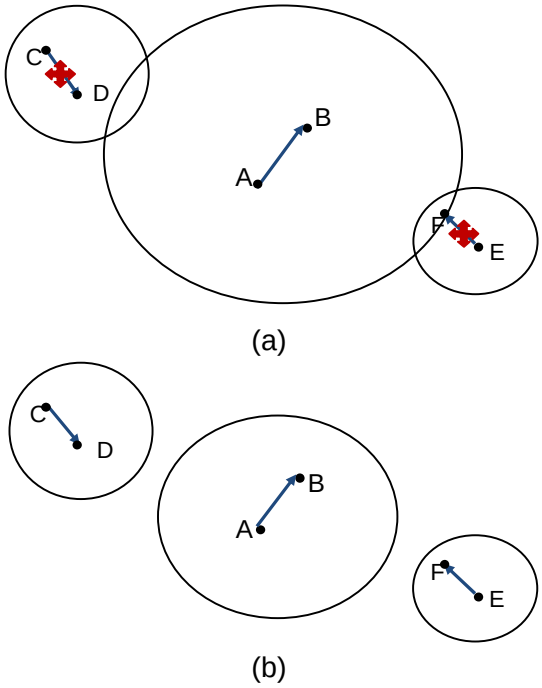


Figure 4.1 : Avantage de contrôle de la puissance- réutilisation spatiale de canal.
(a) sans contrôle de la puissance et (b) avec contrôle de la puissance.

Selon [11], La puissance de transmission détermine la portée sur laquelle le signal peut être reçu d'une manière cohérente, et par conséquent c'est un paramètre critique pour déterminer la performance du réseau (débit, délai, et consommation d'énergie). La sélection de la "meilleure" portée de transmission a été étudiée en détail dans la littérature. En effet, [12] montre que plus la portée des nœuds est grande, plus la puissance nécessaire à la transmission est grande. De plus, la portée d'un nœud influe directement sur la zone d'interférence. Augmenter la portée, implique aussi augmenter la probabilité d'interférence, le taux de collision et le taux de perte et diminue la capacité de transmission des nœuds.

Le contrôle de puissance consiste à adapter les portées et les puissances de transmission des nœuds afin d'assurer une consommation minimale d'énergie tout en sauvegardant la connectivité du réseau. Il s'agit de trouver une portée de transmission optimale pour les nœuds du réseau, pouvant être commune ou pas, permettant d'optimiser l'énergie consommée lors des communications [13][10]. Une autre technique utilisée dans cette classe est le contrôle de topologie, où la topologie d'un réseau sans fil multi sauts est l'ensemble des liens de communication entre paires des nœuds utilisées par un mécanisme de routage (explicitement ou implicitement). La

topologie dépend de facteurs “incontrôlable” tel que mobilité du nœud, interférences, bruit, aussi bien que sur des paramètres “contrôlable” tel que la puissance de transmission et la direction de l'antenne. Alors que des travaux de recherche considérables ont été réalisés sur les mécanismes qui réagissent efficacement aux changements dans la topologie dû aux facteurs incontrôlables, le domaine d'ajustement des paramètres contrôlables a reçu peu d’attention. Donc le contrôle de topologie vise à réduire la portée des nœuds, si possible, d'où la réduction des interférences et les collisions permettant ainsi une meilleure conservation d'énergie [14].

Plusieurs propositions existent pour assurer le contrôle de topologie et/ou de puissance. Nous revoyons au-dessous plusieurs techniques.

Le mécanisme proposé dans [15] permet d'ajuster la puissance d'un nœud jusqu'à ce qu'il ait un nombre de voisins limité. Ceci n'assure pas dans tous les cas la connectivité du réseau. Souvent, les nœuds peuvent se retrouver dans des îlots séparés avec quelques voisins directs. Donc Ramanathan *et al* [15] ont présenté deux algorithmes centralisés « *CONNECT et BICONN-AUGMENT* [71] »pour réduire au minimum la puissance maximum utilisée par un nœud tout en maintenant la connectivité ou la bi-connectivité du réseau. Les auteurs considèrent un réseau bi-connecté si la perte d'un seul nœud ne découpe pas le réseau. L’algorithme *CONNECT* est un algorithme itératif simple qui fusionne différents composants jusqu'à ce qu’il ne reste qu’un seul. Initialement, chaque nœud est son propre composant. Les paires de nœuds sont sélectionnées dans un ordre non-décroissant de leurs distances mutuelles. Si les nœuds sont dans des composants différents, alors la puissance de transmission de chacun est augmentée pour être capable d'atteindre juste l'autre. Cela est fait jusqu'à ce que le réseau soit connecté. Augmenter un réseau connecté à un réseau bi-connecté se fait par l’algorithme *BICONN*-AUGMENT, qui utilise la même idée que *CONNECT* pour la construction itérative du réseau bi-connecté. Sauf qu’en plus, une phase du post-traitement peut être appliquée pour assurer la distribution minimum par-nœud des puissances de transmission par la suppression des connexions redondantes.

Dans un réseau mobile ad hoc, la topologie peut souvent changer comme nous l’avons déjà expliqué. Par conséquent, les puissances de transmission des nœuds doivent être réajustées continuellement afin de maintenir la topologie désirée. En même temps les auteurs proposent deux heuristiques distribuées pour le contrôle de la topologie des réseaux mobiles. Dans *LINT*[72], chaque nœud est configuré avec trois paramètres: Le degré "désiré" du nœud d_d, un seuil élevé d de degré du nœud et un faible seuil d_l. Chaque nœud vérifiera périodiquement le nombre de voisins actifs « le degré » dans sa table des voisins. Si le degré est plus grand que d_h, le nœud réduit sa puissance

[71] Biconnectivity Augmentation
[72] *Local Information No Topology*

opérationnelle. Si le degré est inférieur à d_l, le nœud augmente sa puissance opérationnelle. Si ni l'un ni l'autre est vrai, aucune mesure n'est prise, donc la modification de niveau de la puissance se fait de tel sorte que le degré du nœud soit gardé dans les seuils. *LILT*[73] améliore encore *LINT* en outrepassant le seuil élevé lorsque le changement de la topologie a indiqué par les résultats de la mise à jour de routage dans une connectivité indésirable. Alors LINT utilise les informations du voisin localement disponible collectée par quelque protocole de routage, et tente de garder le degré (nombre des voisins) de chaque nœud borné. Alors que LILT utilise l'information du voisin localement disponible, mais utilise aussi l'information de la topologie globale qui est disponible avec quelques protocoles de routage tel que les protocoles de l'état de lien.

CONNECT et BICONN-AUGMENT sont des algorithmes centralisés qui exigent des informations globales, donc ne peuvent pas être directement déployées dans le cas de la mobilité. D'autre part, les heuristiques proposant LINT et LILT ne peuvent pas garantir la préservation de la connectivité du réseau.

Une autre approche est l'approche de *Relay-region* et *enclosure-based* (R&M) [8]. Cette approche a introduit la notion de région de relais et clôture pour le but de contrôle de la puissance. Soit un nœud transmetteur *i*, le nœud du relais *r* et le nœud récepteur *j,* la région de relais *« Relay-region »* $R_{i\rightarrow r}$ de paire du nœud transmetteur-relais *(i, r)* est définit comme suite :

$$R_{i\rightarrow r} \equiv \{(x, y) \mid P_{i\rightarrow r\rightarrow(x, y)} < P_{i\rightarrow(x, y)}\}$$

Où $P_{i\rightarrow r\rightarrow(x, y)}$ indique la puissance nécessaire pour transmettre du nœud i vers (x, y) à travers le nœud relais *r*, alors que $P_{i\rightarrow(x, y)}$ dénote la puissance nécessaire pour transmettre du nœud *i* à *(x, y)* directement.

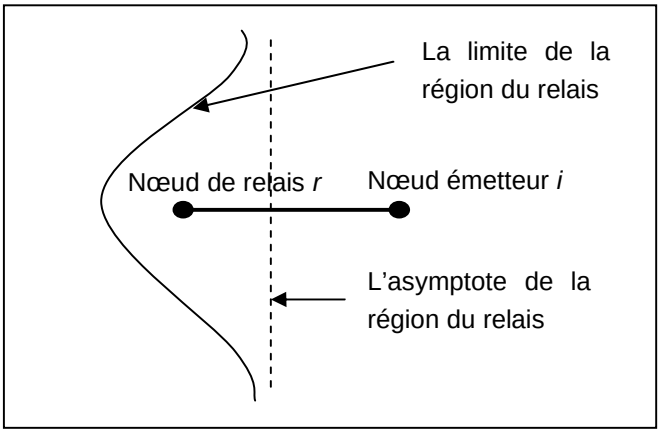


Figure 4.2 : La région de relais de paire du nœud transmetteur-relais (i, r).

[73] *Local Information Link-State Topology*

Pour tout nœud *i* qui a l'intention de transmettre au nœud *j*, où le nœud *j* se trouve dans la région du relais d'un troisième nœud *r*, pour que le nœud *i* consomme moins de puissance, il choisit de relayer par le biais du nœud *r* au lieu de transmettre directement au nœud *j*. La clôture du nœud *i* est alors définit comme l'union du complément de régions du relais de tous les nœuds, que le nœud *i* peut atteindre, en utilisant sa puissance de transmission maximale. Il est montré que le réseau est fortement connecté si chaque nœud maintient des liaisons avec tous les nœuds existant dans sa clôture et la topologie résultante est une topologie avec une puissance minimale. Dans cette approche, l'algorithme donne le graphique de la clôture, supposant qu'il n'y a qu'un seul puit de données (destination) dans le réseau, ce qui est impossible dans la pratique. De plus, un modèle explicite de propagation du canal est nécessaire pour calculer la *région du relais.*

Le protocole COMPOW [10] a pour objectif d'ajuster la puissance des nœuds selon une valeur commune. Ce niveau de puissance est le niveau minimal permettant d'assurer la connectivité du réseau. Ce protocole met en évidence l'importance des liens bidirectionnels puisqu'une destination directe ne peut répondre à une source que si sa puissance de transmission est au moins égale à celle de la source. De ce fait, assurer une puissance commune permet d'assurer des liens bidirectionnels. Ce protocole vise aussi à augmenter la capacité de transmission du réseau avec le plus petit niveau d'énergie ou de portée possible tout en gardant la connectivité du réseau. Ces derniers challenges posent le problème de recherche de la meilleure couverture du réseau et du contrôle de partitionnement. Donc on peut dire que COMPOW marche bien si les nœuds sont distribués de façon homogène dans l'espace, même si un seul nœud éloigné pourrait provoquer que chaque nœud doit utiliser un niveau élevé de puissance.

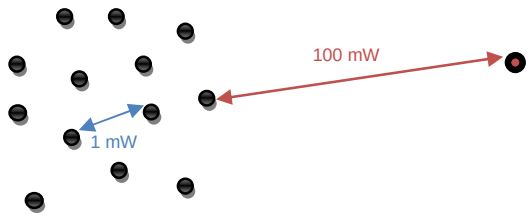


Figure 4.3 : Un niveau de puissance commune n'est pas approprié pour les réseaux non-homogènes.

Dans [16], les auteurs proposent de calculer le digramme de Voronoî [17] sur l'ensemble des nœuds du réseau, dont la topologie et la localisation des nœuds est connue à un instant donné, puis d'en déduire la triangulation de Delaunay qui permet

de relier les nœuds ayant des cellules voisines, aussi on peut extraite l'information du voisinage de la triangulation Delaunay puisque les cellules qui sont proches sont connectées. Dans cette technique l'usage du diagramme de Voronoi, efficacement et sans perte d'optimalité, transforme le problème géométrique continu à un problème du graphique discret. Le diagramme de Delaunay assure une connectivité totale des nœuds du réseau selon des liens courts assurant une portée minimale.

Les auteurs de [18] ont proposé un mécanisme distribué du contrôle de la topologie basé sur le cône, qui garantit la connectivité du réseau global. Ce travail suppose qu'un récepteur est capable de déterminer la direction de l'émetteur à la réception d'un message. Deux phases sont exécutées : Dans la première phase, chaque nœud devrait augmenter sa puissance de transmission jusqu'à ce qu'il existe au moins un voisin dans chaque direction, formant ainsi un cône. La deuxième phase consiste à enlever les liaisons redondantes sans affecter la connectivité globale du réseau. Les résultats de la simulation ont indiqué que cette approche peut avoir de plus longues durées de vie du réseau et réduit les interférences dû aux diminutions des puissances de transmission.

Beaucoup de travaux essaient d'intégrer le contrôle de la puissance dans le protocole MAC d'IEEE 802.11 [7, 18, 19, 20, 21, 22, 23]. L'idée principale est d'utiliser des niveaux de puissance différents pour transmettre les trames RTS, CTS, Données, et ACK.

Parmi ces mécanismes, un mécanisme simple [22] (appelé le mécanisme de base) montre que les stations devraient utiliser la puissance maximale pour transmettre des trames RTS et CTS, et la puissance minimale nécessaire pour transmettre des trames de données et d'ACK. Le dialogue RTS/CTS est utilisé pour décider de la puissance minimale exigée pour les transmissions de Données–ACK subséquentes. La description détaillée est comme suit : soient p_{max} la puissance de transmission maximum. Supposez que la station ***v*** veut envoyer un paquet de données à une station ***u***. La station ***v*** devrait utiliser un niveau de puissance p_{max} pour envoyer sa trame RTS. Lorsque la station ***u*** reçoit cette trame, elle répond aussi par une trame CTS avec un niveau de puissance p_{max}. Quand la station ***v*** reçoit la trame CTS, elle calcule le niveau de puissance minimum exigé,

$$p_{desiré} = (p_{max} / p_r) \times p_{rmin} \times c,$$

où p_r est le niveau de la puissance de réception de la trame CTS et p_{rmin} est la puissance minimum nécessaire pour recevoir le signal et *c* est une constante. Ensuite la station ***v*** utilise le niveau de la puissance $p_{desiré}$ pour transmettre sa trame de

données. De la même façon, la station ***u*** calcule son niveau de puissance $p_{desiré}$ pour transmettre sa trame ACK.

Les auteurs dans [24] indiquent que le protocole précédent peut dégrader le débit du réseau et peut même causer une consommation d'énergie plus grande. Avant d'expliquer les raisons, il y a trois termes qui doivent être définis: *la portée de la transmission* (déjà définie), *la portée de détection de porteuse*, et *la zone de détection de porteuse*. Quand une station ***v*** est dans la portée de la transmission d'une autre station ***u***, la station ***v*** peut recevoir et décoder correctement des trames de la station ***u***, alors que si la station ***v*** est dans la portée de détection de porteuse de la station ***u***, elle peut détecter mais pas nécessairement décoder correctement la transmission de la station ***u***. Habituellement, la portée de détection de porteuse est plus grand que la portée de la transmission (une supposition typique est que le rayon du premier est deux fois plus grand que le deuxième). Noté que la portée de la transmission et la portée de détection de porteuse dépendent aussi du niveau de la puissance de transmission de l'émetteur. La zone de détection de porteuse est définie comme la région du la portée de détection de porteuse à l'exclusion de la portée de la transmission. Donc, quand une station est dans la zone de détection de porteuse d'un émetteur, il peut juste détecter le signal mais pas décoder correctement les données transmises. Ces définitions sont illustrées dans la figure 4.4(a) [24].

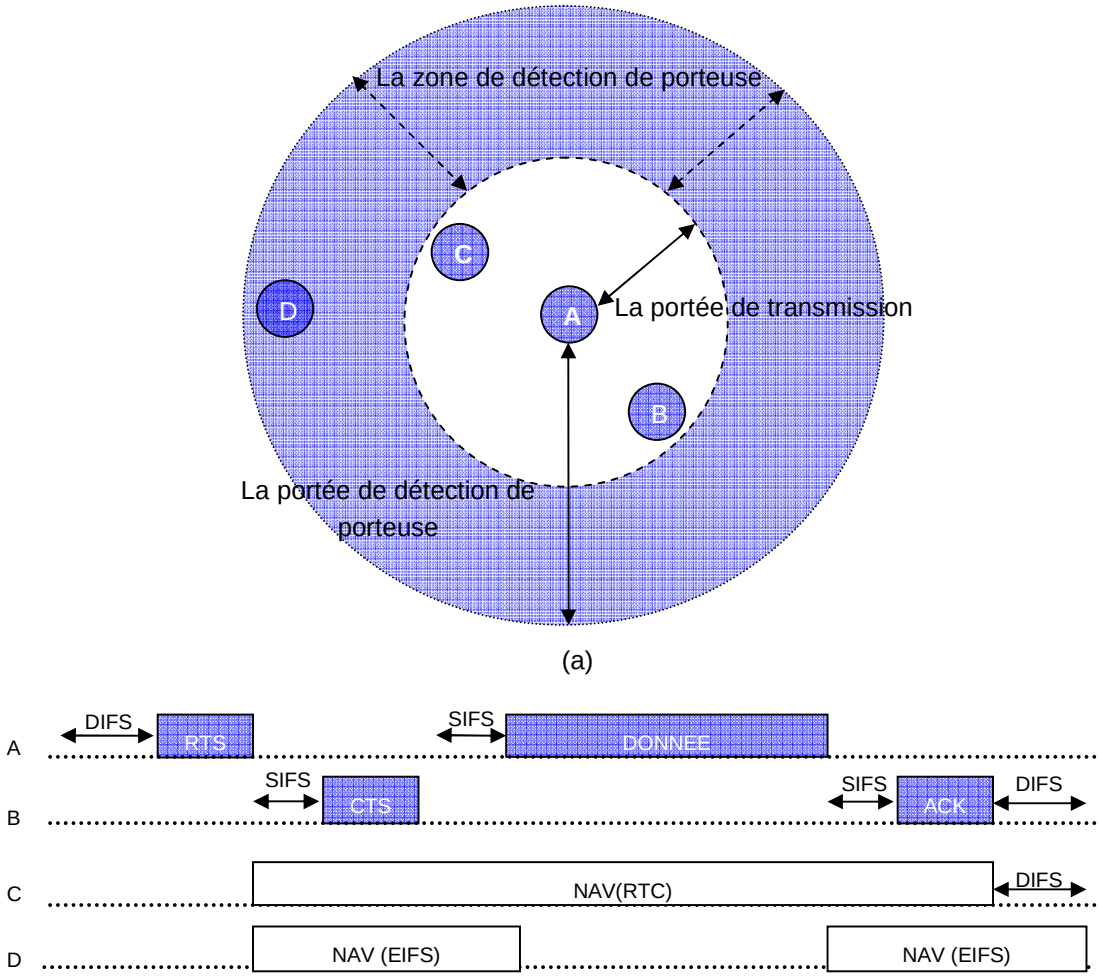


Figure 4.4 : (a) Un exemple de portée de la transmission, la portée de détection de porteuse, et la zone de détection de porteuse. (b) NAVs utilisé par C et D quand A et B échangent leur dialogue RTS–CTS–Données–ACK.

La figure 4.4(b) [24] montre un exemple où A et B échangent des trames RTS–CTS–Données–ACK, C est dans la portée de transmission de A, et D est dans la zone de détection de porteuse de A.

Dans [24], les auteurs ont proposé un nouveau protocole de contrôle de la puissance au niveau MAC pour prévenir le problème de collisions dans le protocole de base. Dans ce protocole, les trames RTS et CTS sont envoyées avec un niveau de puissance $\boldsymbol{p_{max}}$. Les nœuds dans la zone de détection de porteuse ont initialisé leurs NAVs[74] pour une durée EIFS[75] quand ils détectent des signaux qui ne peuvent pas être

[74] *Network Allocation Vector*

décodés correctement. Les trames ACK sont aussi envoyées avec un niveau minimum de la puissance exigé $p_{desiré}$. La différence principale est que le niveau de la puissance pour transmettre des trames de Données est périodiquement augmenté par rapport au niveau de la puissance $p_{desiré}$ et au niveau de la puissance p_{max}. Le niveau de la puissance de transmission des trames de données est alterné entre p_{max} et $p_{desiré}$ avec une période d'un EIFS. La figure 4.5 montre les changements des niveaux de la puissance de transmission pendant l'échange RTS–CTS–Données–ACK. Avec une telle modification, les autres stations qui peuvent causer des collisions observeront périodiquement l'existence des porteurs et remettre leur transmission. Puisque la puissance de transmission des trames de données est augmentée chaque durée EIFS, les NAVs adéquats peuvent être remis à d'autres stations. Aussi, la longueur de la durée de transmission au niveau de la puissance p_{max} devrait être assez importante pour la détection de porteuse.

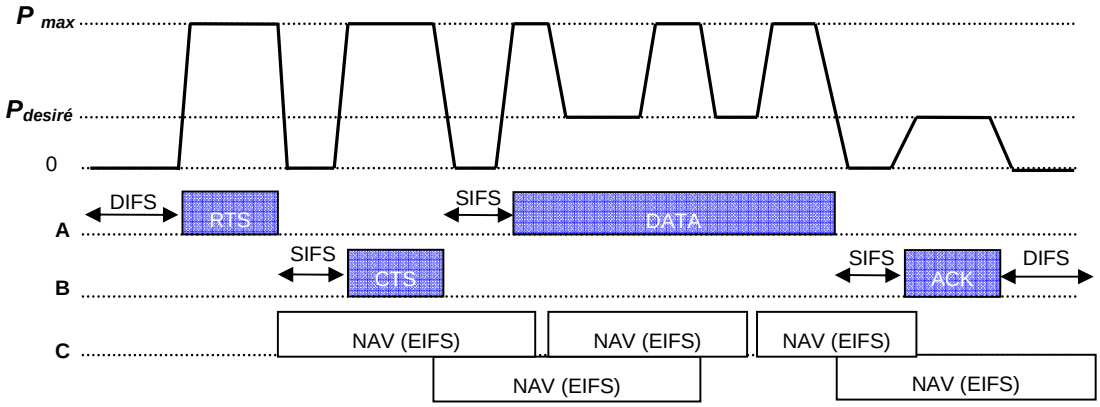


Figure 4.5 : Un exemple d'ajustement de la puissance.

Dans [23], le contrôle de puissance est adopté pour réduire l'interférence et pour améliorer le débit dans la couche MAC. Les auteurs de [23] ont proposé aussi un nouveau protocole MAC qui combine les mécanismes de contrôle de la puissance, le dialogue RTS/CTS et deux tons occupés « *busy tones*». L'idée principale est d'utiliser l'échange des RTS et CTS entre deux stations pour déterminer leurs distances relatives. Cette information est utilisée alors pour contraindre le niveau de puissance à utiliser par le nœud pour transmettre ses paquets de données. L'utilisation des niveaux de puissance inférieurs peut augmenter la réutilisation du canal. Il conserve aussi l'énergie de la batterie et réduit les interférences du Co-canal avec les autres nœuds voisins. Dans ce mécanisme le canal est fendu en deux sous canaux: un canal des données et un canal de contrôle. Le canal de contrôle est utilisé pour transmettre des dialogues RTS/CTS.

[75] *Extended Inter-Frame Space*

Les deux tons occupés sont le ton occupé de transmission '$\mathbf{BT_t}$' et le ton occupé de réception '$\mathbf{BT_r}$'. Ces deux tons occupés sont placés sur le spectre à des fréquences différentes avec assez de séparation. La figure 4.6 montre une allocation du spectre possible. $\mathbf{BT_t}$ indique que certain nœuds transmettent, tandis que $\mathbf{BT_r}$ indique que certain nœuds reçoivent. Un émetteur doit initialiser son $\mathbf{BT_t}$ quand il transmet un paquet de données et un récepteur doit initialiser son $\mathbf{BT_r}$ quand il répond à l'émetteur par un CTS. Quand un hôte désire envoyer un RTS, il doit s'assurer qu'il n'y a aucun $\mathbf{BT_r}$ autour lui. Inversement, un hôte doit s'assurer qu'il n'y a aucun $\mathbf{BT_t}$ autour, pour répondre par un CTS.

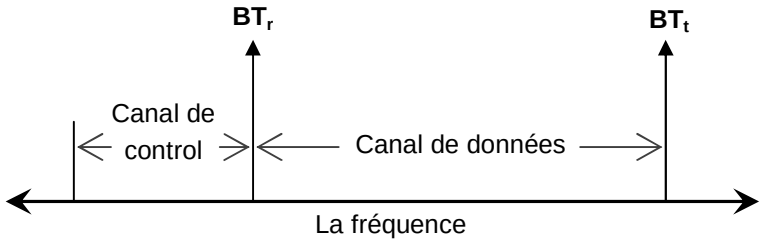


Figure 4.6 : Un diagramme de la fréquence possible pour l'allocation des tons occupés.

A travers les analyses théoriques et les expériences, le protocole est vérifié pour être capable d'augmenter considérablement l'utilisation du canal dû au recouvrement du signal réduit. La Conservation d'énergie et la réduction de l'interférence qui sont accomplies simultanément.

Dans [7], les auteurs étudient le protocole MAC d'IEEE 802.11 et proposent des modifications dans les formats de l'en-tête des paquets CTS et les paquets de données afin de supporter le contrôle de la puissance. En plus, dix niveaux de la puissance de transmission sont définis. Le récepteur informe l'émetteur du niveau de la puissance appropriée à travers un paquet CTS, tandis que l'émetteur informe le récepteur par un paquet de données. Donc, pendant un échange RTS–CTS–Données–ACK, l'émetteur et le récepteur peuvent déterminer des puissances de transmission adéquates à utiliser. Les résultats de l'évaluation des performances montrent une réduction de 10–20% dans la consommation de la puissance et une amélioration de 15% dans le débit.

Le contrôle de la puissance devrait aussi être fait conjointement avec le routage, du moment qu'il a besoin de sauvegarder la connectivité du réseau. Inversement, le routage dépend du contrôle de la puissance puisque le niveau de la puissance impose quels liens sont disponibles pour le routage. Les auteurs de [25] proposent un autre protocole, qui est le *CLUSTERPOW* qui permet aux nœuds d'utiliser un niveau de puissance qui dépend de la destination du paquet. Cela suggère un algorithme simple pour le routage et fait fonctionner le contrôle dans des réseaux rassemblés, qui tentent de maximiser la réutilisation spatiale et aussi la capacité du réseau. Chaque nœud

avance un paquet pour une destination *d* qui utilise le plus petit niveau de puissance *p* tel que la destination *d* soit accessible. On peut le qualifier d'algorithme avide, car chaque nœud utilise le niveau de puissance le plus bas qui garantit l'accessibilité à la destination selon l'information qu'il possède. Cela est exécuté à la source et au niveau de chaque nœud intermédiaire. La conséquence est que si un nœud supplémentaire en aval sait comment atteindre la destination par l'utilisation d'un niveau de la puissance inférieure, alors il utilise le niveau de la puissance inférieure pour avancer le paquet. La figure 4.7 [25] illustre les routes choisies, et le niveau de la puissance utilisée quand l'algorithme précité, est exécuté sur un réseau rassemblé typique.

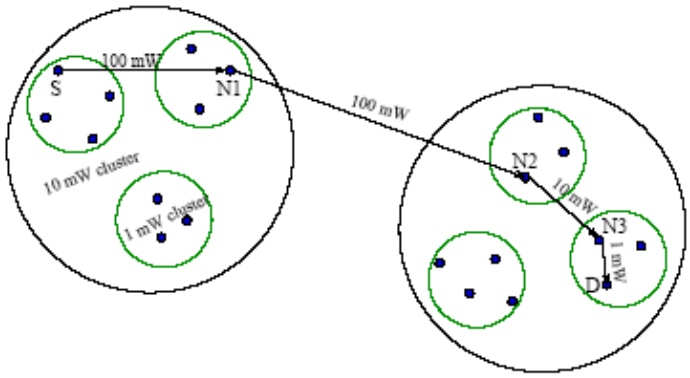


Figure 4.7 : Routage par *CLUSTERPOW* dans un réseau non-homogène typique.

Le protocole PAMAS (*Power Aware Multi-AccesS*) [26] utilise deux canaux séparés pour l'échange de messages de contrôle (c'est-à-dire, les messages RTS et CTS) et des messages de données. L'utilisation de deux canaux séparés limite ainsi le nombre de collisions entre les messages de données et de contrôle. Par conséquent, le nombre de collisions est réduit puisqu'un terminal peut à la fois recevoir ou émettre des données tout en interdisant aux autres terminaux d'utiliser le canal de transmission de données. Concrètement, quand un terminal *A* transmet un paquet à un terminal *B*, *A* envoie en parallèle un message RTS à *B*. Cependant, si un voisin de *A* ou *B* (ou des deux) reçoit ou transmet un paquet, il envoie un *busy tone* avec le message CTS envoyé en réponse.

4.3 Mode de puissance basse

Le principe de L'économie d'énergie dans IEEE 802.11 est d'éteindre le matériel de transmission et de réception (WNIC) « mode PS ». Bien qu'IEEE 802.11 ne définisse pas sous quelles circonstances une station peut entrer dans le mode PS, il est évident d'éteindre un ensemble de circuits de transmission et de réception si aucun trafic ne doit être servi. Malheureusement, plusieurs problèmes surviennent, cela peut avoir un

effet opposé de l'économie d'énergie s'il n'est pas exploité convenablement. Ce mécanisme crée deux problèmes à résoudre:

- Comment fait une station qui envoie des paquets à une autre station dans un mode d'économie d'énergie « PS»?
- Comment fait une station dans un mode d'économie d'énergie durant la réception des paquets?

L'économie d'énergie IEEE 802.11 est basée sur le stockage et la synchronisation. Les paquets destinés à une station dans un mode PS doivent être stockés jusqu'à son "réveil". Les stations doivent être synchronisées de telle manière que les paquets soient transmis seulement si le receveur projeté est prêt (réveillé) pour la réception. Dans le mode infrastructure, le stockage et la synchronisation sont exécutées de façon centrale par un Point d'Accès (AP). Ceci est donc plus compliqué dans un réseau ad hoc, parce que le stockage et la synchronisation doivent être exécutés de manière distribuée.

La synchronisation des nœuds du réseau au niveau du mécanisme PSM fait que tous les nœuds utilisant le mode PS doivent, si leurs activités le permettent, entrer en mode Doze durant la même période puis se réveiller aux mêmes instants. Cette caractéristique fait que durant une communication entre une source et une destination utilisant une route à plusieurs sauts, plusieurs nœuds en mode Doze peuvent se trouver sur la route. Un paquet traversant le réseau peut rencontrer tout un îlot de nœuds en mode Doze empêchant le paquet d'être routé à destination. Ceci représente une faille au niveau de PSM qui peut induire un risque de partitionnement du réseau au moment du routage.

Par ailleurs, un nœud utilisant le mode PS restera actif durant tout le reste de la période Intervalle de balise s'il a reçu des annonces de messages durant la période ATIM ou s'il a des messages à envoyer. Cependant, le nœud ne sera pas réellement en communication durant toute la période puisqu'il n'aura pas accès au canal à tout instant et peut terminer la réception ou la transmission de ses données avant la fin de la période.

4.3.1 Les solutions basées sur des slots déterministes

Une amélioration de PSM consiste à limiter la durée d'activité d'un nœud durant le reste d'un Intervalle de balise afin de limiter la consommation d'énergie inutile et ceci en lui allouant des slots prédéfinis pour l'échange de ses données. En dehors de ses slots, le nœud peut entrer en mode doze.

Slotted PSM [27] consiste donc à diviser la période allant de la fin de la période ATIM jusqu'au reste de la période Intervalle de balise en un certain nombre de slots de temps, chacun sera alloué pour un nœud donné pour effectuer sa communication.

Chaque nœud restera actif uniquement durant les slots qui lui seront alloués et pourra ainsi être en mode doze plus longtemps.

La réservation des slots pour l'échange de données s'effectue dynamiquement durant la période ATIMWindow. La source inclut les informations de réservation de slots dans les messages ATIM. Chaque nœud maintient une table de réservation de slots qui sera actualisée à chaque réception de trames ATIM ou ACK-ATIM. Un nœud source choisit les slots qu'il va inclure dans la trame ATIM en se basant sur ses informations locales à partir de la table des états des slots et la quantité du trafic qui sera échangé.

A la réception du message ATIM, le nœud destination réplique par un paquet ATIMRE (ATIM Réponse) dans lequel il inclut la liste de ses slots libres. La source rectifie alors sa réservation selon le nouvel état des slots et envoie un nouveau paquet ATIM.

Une amélioration récente de PSM, adoptant le même principe que Slotted PSM, est le mécanisme TA-PSM (Traffic Aware Power Saving Mode) [28]. Cette nouvelle approche est partie de la constatation du fait que deux nœuds en mode PS restent en état Awake pour le reste de l'Intervalle de balise afin d'échanger des paquets de données, mais peuvent terminer leur communication avant la fin de cette période. TA-PSM consiste à réduire la consommation d'énergie des nœuds du réseau activant PSM en les rendant plus sensibles à la charge du trafic. Chaque source doit à cet effet, indiquer à sa destination l'éventuelle fin de leur communication et ceci en activant un champ particulier dans le dernier paquet qu'elle lui adresse.

Ce mécanisme permettra ainsi à une source et une destination d'entrer immédiatement en mode Doze dés qu'elles ne sont plus impliquées dans aucun autre trafic, sans attendre la fin d'un Intervalle de balise et ceci jusqu'à la fin de cette période. Ceci est réalisé par l'ajout d'une indication dans le dernier paquet transmis de la source à la destination indiquant ainsi la fin du transfert de données entre eux.

S-MAC [13] est un mécanisme permettant aux nœuds d'entrer en mode veille pour des périodes assez longues. Dans S-MAC, un nœud entre en mode veille quand un voisin est en cours de transmission. S-MAC emploie le modèle d'écoute et de mise en veille périodique pour réduire la consommation d'énergie en évitant l'écoute à vide. Cependant, ceci exige la synchronisation entre les nœuds voisins. La latence est augmentée puisqu'un émetteur doit attendre le récepteur à ce qu'il se réveille avant de commencer la transmission. S-MAC emploie la synchronisation pour former des groupes virtuels des nœuds sur la même liste de sommeil. Cette technique coordonne les nœuds pour réduire au minimum la latence additionnelle. T-MAC [29] étend S-MAC en ajustant la longueur de la période de réveil des nœuds selon les communications environnantes. Ceci permet de réduire l'énergie consommée suite à l'écoute passive du canal.

D'autres propositions [30] se basent sur une architecture à deux canaux radios assurant une conservation de l'énergie à travers la mise en veille d'un premier canal et l'utilisation du second à une puissance minimale pour réveiller un voisin spécifique ou pour écouter périodiquement le canal.

4.3.2 Construction de l'ensemble des nœuds actifs

Dans cette section, nous supposons que les nœuds sont redondants, c.à.d. que le nombre des nœuds déployés est plus grand que le nombre optimal.

L'objectif de ces protocoles est de construire un ensemble de nœuds actifs, de tel sorte que tous les autres nœuds peuvent entrer dans l'état *Sleep* pour garder leur énergie. On assure en même temps la connectivité du réseau et les fonctionnalités d'application.

La GAF[76] [31] est une autre technique qui emploie la connaissance des positions géographiques des nœuds pour choisir les coordonnateurs. Les positions géographiques des nœuds sont employées pour diviser la topologie complète en zones de taille fixes (secteur géographique fixe). Les zones sont créées tels que deux nœuds quelconques dans deux zones adjacentes quelconques peuvent communiquer. La taille de la zone est ainsi dictée par la portée radio des nœuds qui est supposée être fixe. Seulement un nœud dans chaque zone doit être éveillé et peut être le coordonnateur. Ainsi, en exploitant la connaissance des positions géographiques, GAF simplifie la procédure de sélection de coordonnateur.

SPAN [25] est un algorithme distribué et aléatoire pour le choix des coordonnateurs. Chaque nœud prend la décision d'être un coordonnateur ou pas. La transition entre les deux états est faite à base de probabilités. L'équité est assurée en faisant du nœud à la quantité d'énergie la plus importante, le plus probable d'être un coordonnateur. L'autre critère employé dans le choix des coordonnateurs est la valeur qu'un nœud ajoute à la connectivité globale du réseau. Un nœud reliant plus de nœuds aura plus de chances d'être choisit comme coordonnateur. La notion d'aléatoire est employée pour éviter des coordonnateurs multiples simultanés. Pour l'efficacité, ces émissions sont portées (*piggy-backed*) sur les messages de contrôle du protocole de routage.

4.4 Routage orienté économie d'énergie

Le routage est l'un des principaux problèmes dans les MANET en raison de leur nature très dynamique et distribuée. En particulier, *le routage orienté énergie* peut être le critère de conception le plus importante pour les MANETs puisqu'un nœud mobile joue le rôle de nœud et de routeur en même temps. Donc, une panne d'énergie d'un nœud mobile n'affecte pas seulement le nœud lui-même mais également sa capacité de transmettre des paquets à d'autres et donc la durée de vie du réseau totale. Pour cette

[76] Geographic Adaptive Fidelity

raison, beaucoup d'efforts de la recherche ont été consacrés à développer des protocoles de routage orienté énergie.

Les protocoles de routage orientés énergie devraient considérer la consommation d'énergie du point de vue du réseau et des nœuds en même temps. Du point de vue du réseau, la meilleure route est celle qui minimise la puissance de transmission totale. De l'autre côté, du point de vue d'un nœud, la route est celle qui évite les nœuds avec une énergie qui n'est pas importante. En réalité, les protocoles de routage orienté économie d'énergies minimisent l'énergie de la communication active nécessaire pour transmettre et recevoir des paquets de données ou pendant les périodes inactives.

L'efficacité énergétique = nombre total des bits à transmettre / Totale d'énergie consommé

Avant de présenter les protocoles qui appartiennent à cette approche, nous présentons d'abord les métriques qui ont été utilisées pour déterminer le chemin de routage orienté économie d'énergie au lieu du plus court chemin.

4.4.1 Les métriques de routage orienté énergie

Les métriques typique utilisées pour évaluer les protocoles de routage ad hoc sont le saut du chemin le plus court, le délai le plus court, et la stabilité des liens [32]. Cependant, ceux-ci peuvent avoir un effet négatif dans les réseaux sans fil parce qu'ils emploient excessivement les ressources d'énergies d'un petit ensemble de mobiles, se qui décroit la durée de vie du réseau. Les auteurs de [29] ont proposé cinq métriques pour les protocoles orientés économie d'énergie :

- L'énergie consommée par paquet,
- Le temps de partage du réseau,
- La variance du niveau de consommation d'énergie des nœuds,
- Le coût par paquet, et
- Le coût maximum du nœud.

La première métrique est utile pour prévoir le chemin à travers lequel la consommation d'énergie totale pour délivrer un paquet est minimisée. Ici, chaque liaison sans fil est annotée avec le coût de la liaison en termes d'énergie de la transmission sur la liaison et le chemin de la min-puissance est celui qui minimise la somme des coûts de la liaison le long du chemin. C'est-à-dire si on suppose qu'un paquet *j* travers les nœuds $n_1, \ldots, n_k$ où le n_1 est la source et n_k la destination. Soit T(a,b) dénote l'énergie consommée dans la transmission (et la réception) d'un paquet sur un seul saut de ***a*** à ***b***. Alors l'énergie à consommer par le paquet *j* est :

$$\mathbf{e_j} = \sum_{i=1}^{k-1} T(n_i, n_{i+1})$$

Donc, l'objectif de cette métrique est de :

Minimiser $\mathbf{e_j}$, $\forall$ paquet j

Cependant, un algorithme de routage qui utilise cette métrique peut avoir un déséquilibre d'énergie dépensée entre les nœuds mobiles. Quand quelques nœuds mobiles particuliers sont chargés injustement de supporter beaucoup de fonctions et de retransmettre des paquets, ils consomment plus d'énergie et risquent un arrêt de fonctionnement plus tôt qu'autres nœuds qui interrompent leurs activités au sein du réseau ad hoc de temps à autres. Donc, maximiser la durée de vie du réseau (la seconde métrique indiqué au-dessus) est un objectif plus fondamental d'un algorithme de routage orienté énergie: Étant donné plusieurs chemins de routage alternatifs, sélectionner celui qui aura la plus grande durée de vie. Malheureusement, optimiser cette métrique est très difficile si nous avons besoin de conserver un bas délai et un haut débit simultanément.

Cependant, depuis que la durée de vie future du réseau est pratiquement difficile à estimer, les trois métriques suivantes ont été proposées afin d'accomplir l'objectif indirectement. La Variance d'énergies de la batterie résiduelles des nœuds mobiles est une indication simple de balance énergétique et peut être utilisée pour étendre la vie du réseau. La métrique de coût-par-paquet est semblable à la métrique d'énergie-par-paquet mais elle inclue la vie de la batterie résidu de chaque nœud en plus de l'énergie de la transmission. Le protocole de routage orienté énergie correspondant préfère la liaison sans fil qui exige une énergie de la transmission basse, mais en même temps évite le nœud avec faible énergie résiduelle dont le coût du nœud est élevé. Avec la dernière métrique, chaque chemin candidat est annoté avec le coût maximum du nœud parmi les nœuds intermédiaires et le chemin avec le coût minimum, chemin du min-maximum, est sélectionné. Cela est dénommé aussi dans quelques protocoles comme chemin du maximum-min parce qu'il utilise la vie de la batterie résiduelle des nœuds plutôt que leur coût du nœud.

La recherche dans les protocoles de routage avec orienté économie d'énergie a considéré trois types de trafic: *unicast* « point-à-point », *broadcast* «diffusion» et *multicast*. Le trafic Unicast est défini comme trafic dans lequel les paquets sont destinés pour un seul récepteur. Le trafic de diffusion est destiné à tous les nœuds du réseau.

4.4.2 Protocoles de routage point-à-point orienté énergie

Les protocoles de routage, qu'ils soient réactifs, proactifs ou hybrides, utilisent en général le nombre de sauts comme mesure du coût d'une route. Or, cette mesure est inadaptée puisque l'énergie consommée par les nœuds n'augmente pas

proportionnellement avec le nombre de sauts. Donc nous pouvons distinguer trois familles de protocoles de routage orientés économie d'énergie:

- **les protocoles qui sélectionnent le chemin qui consomme l'énergie minimale**

L'avantage est que chaque transmission d'un paquet de sa source à sa destination minimise l'énergie consommée.

Dans [33], Les auteurs proposent de transmettre les messages en leur affectant l'énergie minimale nécessaire pour atteindre la destination. Ensuite, la route choisie est celle qui consomme le moins d'énergie pour arriver à destination. Cette solution est basée sur des protocoles existants tels que DSR ou AODV. La puissance minimale pour accéder au prochain saut de transmission est fournie par la couche MAC. La route sélectionnée est ensuite incluse dans le paquet de demande de route avec l'identification du nœud et est rediffusée sur un saut jusqu'à ce que le message atteigne le destinataire. Le destinataire inverse alors l'ordre de la route incluse dans l'en-tête de la requête de localisation, puis incorpore avec les valeurs les puissances d'émission relatives, dans le message renvoyé à la source. Ainsi, la source obtient la puissance d'émission nécessaire pour chaque saut à partir de la réponse, et calcule le coût énergétique pour ladite route. Un autre protocole de routage est proposé dans [13], ce protocole calcule l'énergie additionnelle dissipée par un flux à acheminer sur un chemin donné, prenant en considération le SINR et l'énergie perdu par les interférences. Ensuite, il utilise l'algorithme de Dijkstra pour trouver le chemin qui minimise cette énergie additionnelle. L'avantage de ce protocole est qu'il prend en considération l'impact de la transmission du flux dans la région d'interférence. Cependant, ce protocole est complexe et exige que tous les nœuds connaissent la topologie globale du réseau. En plus, tels protocoles utilisent toujours les mêmes nœuds (ce qui minimisent l'énergie consommé) sans aucune considération sur leur énergie résiduelle, Par conséquent, ces nœuds épuisent leurs batteries plus rapidement que les autres et donc la vie du réseau est minimisée.

Les auteurs de [34] proposent trois fonctions de coût pour des techniques de routage, ils prennent en considération un modèle d'interférence à deux sauts pour la conception des fonctions de coût, c.à.d. lorsqu'un nœud transmet, tous ses voisins à un saut reçoivent le paquet, le décodent. Ses voisins à deux sauts consomment eux aussi de l'énergie en recevant un signal non intelligible parce qu'ils sont actifs et en état d'écoute. Les fonctions de coût vont utiliser différentes approches pour optimiser la durée de vie du réseau. La première fonction de coût consiste à réduire l'énergie nécessaire pour router un paquet entre une source et une destination. Cette fonction $E_{\theta 1}$ prend en compte l'énergie nécessaire pour la transmission d'un paquet, ils considèrent l'énergie consommée par les voisins à un et deux sauts de l'émetteur pour recevoir ce paquet. Ce qui représente l'énergie totale consommée dans le réseau pour

une transmission. $E_{\theta 1}$est utilisée pour donner un poids aux liens entre un nœud et ses voisins à un saut : le poids du lien (k; i) entre k et n'importe quel voisin à un saut est égal à $E_{\theta 1}$du nœud k. $E_{\theta 1}$ (k; i) a la forme suivante :

$$E_{\theta 1}(k, i) = E_{tx} + \sum_{n1 \in N1(k)} E_{RX} + \sum_{n2 \in K2(k)} E_I$$

Où

- N1(k) est l'ensemble des voisins à 1-saut du nœud k ;
- N2(k) est l'ensemble des voisins à 2-sauts du nœud k ;
- E_{TX}, E_{RX} et E_I désignent respectivement l'énergie consommée pour une transmission, réception et overhearing.

Ensuite, ils ont proposé une heuristique qui calcule le chemin optimal entre une source et une destination. Cette heuristique applique un algorithme du plus court chemin sur le graphe dont le poids des liens est calculé par l'utilisation de $E_{\theta 1}$. Cette technique permet : (1) de minimiser la consommation d'énergie pour le routage d'une information dans le réseau (2) et de trouver un chemin énergétiquement optimal. Par contre, l'énergie restante des nœuds est la seule contrainte non prise en compte dans cette fonction, ce qui augmente le risque qu'un nœud avec une énergie restante faible participe dans un routage.

- **les protocoles qui sélectionnent le chemin qui passe par les nœuds avec la plus haute énergie résiduelle**

Les auteurs de [35] ont proposé un algorithme à la demande. Pour acquérir l'information nécessaire pour le routage orienté économie d'énergie, DEAR[77] n'utilise pas des paquets de contrôle additionnels, mais utilise des paquets RREQ[78] qui sont déjà utilisés dans des protocoles de routage à la demande. DEAR exige seulement le niveau moyen de la batterie résiduel du réseau entier, qui peut être obtenu sans aucuns paquets de contrôle autre que paquets RREQ.

Dans cet algorithme, les nœuds intermédiaires contrôlent le temps de rediffusion du paquet RREQ où le temps de la retransmission est proportionnel au taux de la puissance de la batterie résiduelle moyenne du réseau entier par rapport à sa propre puissance de batterie résiduelle. Autrement dit, les nœuds avec énergie relativement plus grande rediffuseront des paquets RREQ plus tôt. DEAR peut établir la route composée des nœuds avec puissance de batterie relativement importante.

[77] *Distributed energy-efficient ad hoc routing*
[78] *Route-Request*

Le protocole REAR[79] proposé dans [36] garantie que chaque flux puisse avoir assez d'énergie sur le chemin sélectionné: c'est-à-d les nœuds avec une basse énergie résiduelle sont évités. Pour accomplir son objectif, le montant d'énergie demandé par la transmission d'end-to-end du flux doit être réservé dans chaque nœud intermédiaire. En plus, pour améliorer la précision, un deuxième chemin est calculé pour acheminer le flux dans le cas de l'échec du premier chemin. Ce chemin est disjoint par rapport au premier chemin et a assez d'énergie pour router le flux. Mais, il n'y a aucune réservation de ressources d'énergie sur ce deuxième chemin. Ce protocole assure l'énergie nécessaire pour acheminer un flux par les nœuds intermédiaires, mais il ne prend pas en compte l'énergie dissipée par la réception des paquets et les interférences. Cependant, le chemin sélectionné ne minimise pas l'énergie demandé pour transmettre un paquet du flux de sa source à sa destination. Donc, la vie du réseau ne peut être maximisée.

Le protocole de routage LEAR[80] [37] est basé sur DSR [38] mais modifie la procédure de la découverte de la route pour équilibrer la consommation d'énergie. Dans DSR, quand un nœud reçoit un message route-requête, il attache son identité dans l'en-tête du message et l'avance vers la destination. Donc, un nœud intermédiaire relaie toujours des messages si la route correspondante est sélectionnée. Cependant, dans LEAR, un nœud détermine si avancer le message du route-requête ou pas selon sa puissance de batterie résiduelle (Er). Quand Er est plus important que sa valeur du seuil (Thr), le nœud avance le message route-request; autrement, il écarte le message et refuse de participer à relayer des paquets. LEAR est un algorithme distribué où chaque nœud prend en compte seulement l'information locale tel qu'Er et Thr, pour sa décision de routage.

Les auteurs de [13] ont proposé une deuxième fonction de coût qui prend en compte l'énergie résiduelle des nœuds et qui assigne un poids pour un lien entre deux nœuds. Cette fonction prend en compte le minimum de l'énergie résiduelle d'un nœud après une transmission d'un paquet avec le minimum des énergies résiduelles des voisins à un et deux sauts de l'émetteur.

La fonction de coût $E_{\theta 2}$ est la suivante :

$$E_{\theta 2}(k; i) = \min\{(E_r(k) - E_{TX}), \min_{n1 \in N1(k)} (E_r(n1) \_ E_{RX}), \min_{n2 \in N2(k)} (E_r(n2) \_ E_l)\}$$

Où

- $E_r(k)$ est l'énergie résiduelle du nœud k ;
- $E_r(n1)$, $E_r(n2)$ sont les énergies résiduelles des voisins à 1 et 2-sauts affectés par la transmission du nœud k

[79] *Reliable Energy Aware Routing*
[80] *Localized Energy-Aware Routing*

- E_{TX}, E_{RX} et E_I désignent respectivement l'énergie d'une transmission, réception et overhearing.

L'utilisation de cette fonction de coût permet une sélection des nœuds avec une énergie résiduelle importante pour participer dans le routage d'une information.

Pour calculer un chemin, cette fonction de coût utilisent un algorithme qui maximise le minimum des poids des liens constituants la route et qui permet ainsi de choisir les nœuds avec le plus d'énergie pour participer dans le routage.

Gupta *et al.* [39] classifient les nœuds en trois zones: *normal*, *avertissement*, *danger,* qui correspondent respectivement à plus de 20 %, entre 10-20 % et moins de 10 %, de l'énergie maximale. Ce protocole affecte un coût d'utilisation énergétique à chaque zone. Par exemple, le coût correspondant au routage de l'information *via* un nœud se trouvant dans la zone danger ou avertissement est plus important que celui correspondant au routage de l'information *via* un nœud puissant en zone normale. L'idée principale est d'acheminer les informations à travers des n.uds ayant de bonnes capacités énergétiques restantes.

- **les protocoles hybrides**

Ces protocoles sélectionnent le chemin avec le coût minimum, où le coût prend en considération l'énergie résiduel de chaque nœud visité (et peut-être ses voisins) et l'énergie d'un paquet consommé sur ce chemin.

La technique [40] essaie d'utiliser la puissance de la batterie, en utilisant également une fonction du coût qui est inversement proportionnel à la puissance de la batterie résiduelle. Un choix possible pour la fonction du coût d'un nœud ***i*** est donné comme suit : $\boldsymbol{f(b_i) = 1/b_i}$ où le $\boldsymbol{b_i}$ est l'énergie résiduelle de la batterie d'un nœud ***i***. Le coût total pour une route est défini comme la somme des coûts des nœuds qui composent la route, et donc sélectionne une route avec le coût total minimum. Cette méthode paraît étendre la vie du réseau parce qu'il choisit la route composé des nœuds dont la puissance de la batterie restante est haute. Cependant, parce qu'il considère seulement le coût total, le niveau d'énergie restante d'un nœud individuel peut être durement estimé. Donc, la route peut inclure un nœud avec petite énergie si les autres nœuds ont beaucoup d'énergie.

Le protocole CMMBCR [25] utilise le concept d'un seuil pour maximiser la vie de chaque nœud et utiliser la batterie équitablement. Si tous les nœuds dans quelques routes possibles entre une paire source-destination ayant l'énergie de la batterie restante plus grande que le seuil, la route du min-puissance parmi ces routes est sélectionnée. Si toutes les routes possibles ont des nœuds avec capacité de la batterie inférieure au seuil, le chemin maximum-min est sélectionné. Cependant, la valeur du seuil est fixée, cela donne une conception plus simple. Les concepteurs de ce protocole ont proposé une métrique de performance intéressante pour mesurer la

balance d'énergie: **la séquence de l'expiration**, définie comme la séquence de temps quand les nœuds mobiles épuisent leur capacité de la batterie. Les métriques traditionnelles pour estimer l'énergie sont la variation de la puissance de la batterie restante, la capacité moyenne de la batterie restante et la vie du réseau à mesurer par rapport à l'instant où tout nœud épuise sa capacité de la batterie pour la première fois. Depuis que ces métriques fournissent des informations limitées sur la balance de l'énergie, la séquence de l'expiration donne des informations plus exactes sur la manière de consacrer équitablement l'énergie.

Le protocole OMM [81][41] maximise la vie du réseau sans la connaissance du taux de génération des données en avance. Il optimise deux métriques différentes des nœuds dans le réseau: minimiser la consommation de la puissance (min-puissance) et maximiser la puissance résiduelle minimale (max-min). La seconde métrique est utile dans la prévention d'événements des nœuds surchargés.

Le protocole OMM découvre le chemin optimal pour une paire source-destination donné par l'utilisation en premier lieu de l'algorithme de Dijkstra (algorithme du plus court-chemin vers une seule-source). Ce chemin du min-pouvoir consomme une puissance minimale (P_{min}) mais il n'est pas nécessairement le maximum-min chemin. Pour optimiser la seconde métrique, le protocole OMM obtient multiples chemins du min-pouvoir, qui sont proche-optimaux, qui ne s'écartent pas beaucoup de la valeur optimale (c.-à-d., moins de zP_{min} où $z \geq 1$) et sélectionne le meilleur chemin qui optimise le max-min métrique.

La figure 4.8 [41] représente un exemple de l'algorithme pour la source (S) et la destination (D). Dans Figure 4.8(a), S→B→D est le chemin min-puissance qui consomme l'énergie minimale (P_{min} = 18). Si z=2, les chemins alternatifs S→A→D (coût du chemin = 22) et S→C→D (coût du chemin = 31) peut aussi être pris en considération puisque le coût appartient à l'intervalle de la tolérance (zP_{min} =36).

Dans cet exemple, chaque chemin contient seulement un nœud intermédiaire et donc leurs énergies résiduelles (nœuds A, B, et C) sont comparées. Le nœud C a une énergie résiduelle de 30 mais il diminuera à 9 si ce chemin est utilisé pour transférer les paquets de S à D. de même façon, les nœuds A et B aura l'énergie résiduelle de 13 et 2, respectivement, comme montré dans la figure 4.8(b). Donc, le chemin max-min parmi les trois chemins min-pouvoir est S→A→D.

[81] *Online Max-Min Routing*

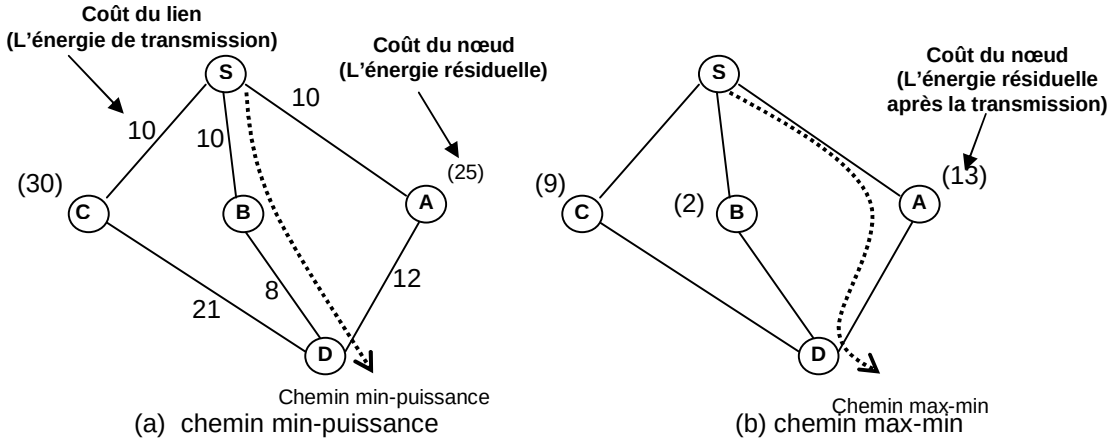


Figure 4.8: Les chemin du Min-puissance et max-min dans le protocole OMM.

4.4.3 Protocoles de routage multi-chemins orienté énergie

Il est intuitif que pour accomplir la vie du maximum de la communication multicast, il serait désirable de consommer autant que possible une petite puissance de la batterie. Cependant, ces deux métriques ne sont pas réciproques [42, 43]. Nous utilisons un exemple simple pour montrer que ces deux métriques ne peuvent pas être optimisées en même temps.

Dans la figure 4.9.a, dans le réseau donné, il y a trois nœuds {a, b, c}, le nœud a est la source. La valeur auprès d'un nœud représente l'énergie résiduelle de la batterie de ce nœud. Nous inscrivons aussi (p_{vu}, t_{vu}) à côté de chaque arc (v, u), où la valeur p_{vu} représente la puissance exigée pour la transmission du données du nœud v au nœud u, et la valeur t_{vu} représente le temps maximum que l'arc (v,u) pourrait écouler avant l'épuisement de la batterie dans le nœud v. Notez que le produit de p_{vu} et t_{vu} sur chaque arc (v,u) est égal à l'énergie résiduelle de la batterie e_v du nœud v. L'objectif est de construire un arbre de diffusion basé sur ces deux métriques. L'arbre de diffusion de la puissance minimale est donné dans Figure 4.9.b avec l'arbre de la puissance total max $\{p_{ab}, p_{ac}\} = p_{ac} = 4$ et de la vie de l'arbre $\min\{t_{ab}, t_{ac}\} = t_{ac} = 3$, et l'arbre de diffusion de la vie maximum est donné dans Figure2.9.c avec l'arbre de puissance totale $t_{ab} + t_{bc} = 2 + 4 = 6$ et de la vie de l'arbre $\min\{t_{ab}, t_{bc}\} = t_{bc} = 4$.

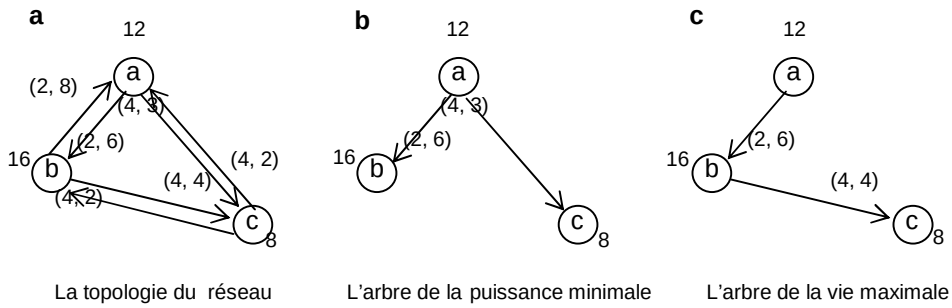


Figure 4.9 : Exemples d'arbre de la puissance minimale et arbre de la vie maximale. (a) Une topologie du réseau; (b) l'arbre de la puissance minimale; (c) l'arbre de la vie maximale.

Nous avons observé qu'il y a un tradeoff entre ces deux métriques de l'optimisation orienté énergie. Quand tous les nœuds ont beaucoup d'énergie, le chemin avec le total d'énergie consommée qui soit considéré comme minimum est le meilleur. De l'autre côté, le chemin avec la vie maximale est meilleur aussi, en incorporant l'énergie de la batterie résiduelle basé sur l'observation des arbres du multicast/broadcast qui devrait éviter des nœuds avec une petite énergie résiduelle.

Dans [44], un acheminement multi-chemins orienté économie d'énergie, est proposé pour maximiser la vie du réseau. C'est un protocole de routage réactif qui investit des données « data sink». Il consiste à trouver tous les chemins entre la source et la destination, d'après une métrique qui prend en considération 1) l'énergie consommée par la transmission et réception du paquet et 2) l'énergie résiduelle des nœuds. Les chemins qui ont un coût plus haut qu'un seuil donné sont abandonnés. A chaque chemin gardé est assignée une probabilité inversement proportionnelle au coût de chemin. Pour acheminer un paquet du flux, un chemin sera choisi aléatoirement d'après sa probabilité. Ce protocole assure le balancement de la charge en utilisant le routage multi-chemins. De plus, la prise en considération de l'énergie résiduelle des nœuds pour calculer des chemins, permet d'éviter des nœuds avec capacité d'énergie basse.

Dans [45], deux variantes de routage multi-chemin avec consommation d'énergie minimale sont considérées pour améliorer la durée de vie d'un réseau et la fiabilité contre les pannes des nœuds et des liens. Ces deux variantes sont: 1) multi-chemin avec des liens disjoints, 2) multi-chemin avec des nœuds disjoints. Les auteurs montrent que l'acheminement avec liens disjoints est plus efficace énergétiquement et l'acheminement avec nœuds disjoints est plus fiable. Cependant, leur modèle ne prend pas les interférences en considération. Les évaluations de performances dans [46], montrent que l'avantage relatif de maintenir un chemin additionnel diminue fortement avec le nombre de chemins a maintenir, alors que la complexité augmente d'une façon remarquable. C'est pourquoi, maintenir que deux chemins, est considéré généralement comme suffisant.

Dans [45], les auteurs proposent MMRE-AOMDV un protocole de routage multi-chemin basé sur AOMDV [82] et exploitant la Maximale Minimale Énergie Résiduelle des nœuds. Ce protocole a été conçu à l'origine pour les nœuds a batterie-limité et les réseaux ad hoc très dynamiques où l'échec du lien et les routes brisées arrivent fréquemment. Dans ce protocole une nouvelle découverte de chemins est nécessaire seulement si tous les chemins vers la destination ne sont plus valables. L'idée principale dans MMRE-AOMDV est d'équilibrer la consommation d'énergie nécessaire, de prévenir les nœuds critiques qui épuisent leurs énergies et de les faire sortir du réseau en cas de besoin. En réalité, si un ou plusieurs nœuds critiques épuisent leurs énergies, le réseau sera découpé finalement, et il peut y avoir la disponibilité de plusieurs nœuds avec énergie importante, qui ne peuvent plus communiquer. Le protocole MMRE-AOMDV utilise les informations de routage disponibles dans le protocole AOMDV. Donc une petite modification additionnelle est exigée pour le calcul de la maximale minimale énergie résiduelle nécessaire sur un chemin. Le protocole MMRE-AOMDV a deux composants principaux :

1. trouver l'énergie résiduelle nécessaire minimale de chaque route dans le processus de la découverte de route.

2. classer les multi-chemins en descendant selon l'énergie résiduelle nécessaire et utiliser le chemin avec l'énergie résiduelle maximale pour envoyer des paquets de données.

4.5 Conclusion

Dans ce chapitre, nous avons dressé un état de l'art sur les principales approches proposées pour résoudre le problème d'économie d'énergie dans les réseaux mobiles ad hoc.

L'objectif de la suite du travail est de proposer une approche permettant d'améliorer le protocole OLSR, afin que ce dernier puisse supporter la notion de consommation d'énergie.

[82] *Ad Hoc On-Demand Multipath Routing Protocol*

OLSR-PAA : AMÉLIORATIONS DES PERFORMANCES D'OLSR AVEC PAA

5. OLSR-PAA

5.1 Introduction

En se basant sur les classes d'économie d'énergie présentées dans la section précédente, on remarque qu'il ya une interaction entre ces différentes classes. D'un coté, le problème majeur d'un protocole de routage est d'assurer un routage unicast. La solution la plus évidente est de router vers la destination en utilisant le minimum de sauts possibles. Cela a été le choix par défaut dans les réseaux filaires et récemment dans les MANET. Cette approche est intéressante dans la mesure où elle est bien étudiée et minimise les délais. Mais, la principale préoccupation des MANET est l'utilisation de l'énergie. Dans ce contexte, la politique de minimiser le nombre de nœuds participants au routage n'est pas toujours la plus adéquate à une meilleure utilisation de l'énergie. Nous avons vu dans la section précédente que beaucoup de propositions ont été faites dans la littérature à savoir la conception des protocoles de routage qui prennent en compte l'aspect "énergie" et qui visent une consommation minimale de cette dernière lors de leur fonctionnement [13][28] [44]. La majorité de ces solutions vise à utiliser, dans le routage, des nœuds avec une quantité assez suffisante d'énergie et éviter au maximum les nœuds à faible énergie. Le principe de cette stratégie est d'éviter une courte vie des nœuds (et donc celle du réseau), ainsi éviter les ruptures de routes et une utilisation non équitable de l'énergie. De l'autre coté, beaucoup des améliorations de protocoles MAC (IEEE 802.11 PSM) proposés dernièrement dans le cadre de l'économie d'énergie optent pour la méthode de mise en veille des nœuds lorsqu'ils ne sont pas actifs (pas de réception et pas d'émission). Un nœud non actif peut être mis en veille même s'il dispose d'une grande quantité d'énergie. Mais du fait de cette grande quantité, le nœud sera plus probable d'être sélectionné par le protocole de routage afin de participer au routage et dire que ce nœud et en phase d'économie d'énergie (mode veille). Ce problème s'accentue si le

nœud passé en mode veille a créé une rupture de connectivité du réseau, alors cela perturbera tout le réseau et conduira à retarder la procédure de découverte de nouvelles routes et regagner la connectivité du réseau (si il y a d'autres nœuds plus adéquats pour participer dans le routage, sinon, attendre le réveil du ou des nœuds qui sont en mode veille). Tous ces processus encombreront le réseau avec le trafic manipulé(les messages de contrôle et les overheads).

Donc, le protocole MAC, dans sa gestion de l'énergie, influence négativement sur le bon fonctionnement du protocole de routage et cela parce que les interactions entre ces deux protocoles ne sont pas prises en compte.

De son coté aussi, le protocole de routage peut influencer négativement sur le mécanisme de sauvegarde de l'énergie du niveau MAC et dégrader ainsi sa performance. Le protocole de routage lorsque il initie une procédure de découverte de route, à partir de la source vers la destination, peut utiliser des nœuds avec une faible énergie, cela encours un très grand risque sur la vie de ces nœuds ainsi que sur celle du réseau.

Les solutions proposées ne mettent pas en œuvre un seuil de faiblesse d'énergie et ne sont pas ainsi efficace en conservant cette dernière et peuvent mener à la disparition de certains nœuds du réseau. Prenons le cas où tous les nœuds ont les même facteurs de connectivité de réseau et les mêmes faibles quantités d'énergie, alors avec cette même quantité d'énergie pour tous les nœuds, un ou plusieurs de ces derniers seront probablement sélectionnés comme routeurs (coordinateurs pour certaines méthodes comme SPAN) et dire que ces derniers peuvent par exemple être évités par une autre route ou un saut plus long. Tous ces compromis devront être étudiés avec soin pour une meilleure interaction entre le protocole MAC et le protocole routage.

Nous proposons, dans la section qui suit, une amélioration pour les interactions entre un des protocoles de conservation d'énergie de la couche MAC et le protocole de routage pour une meilleure prise en compte des problèmes cités précédemment. On doit faire une interaction entre le protocole de routage OLSR et le mécanisme PAA[83][47].

PAA permettra de réduire le nombre de nœuds actifs dans le réseau à un instant donné afin d'augmenter la charge utile du réseau et d'épargner de l'énergie. Cet objectif permettra de :

- Mieux conserver l'énergie des nœuds du réseau puisque même en périodes de veille, un mobile peut provoquer des interférences dans son voisinage à cause des paquets de contrôle qu'il échange. Un mobile est obligé de recevoir, traiter et répondre à des messages qui peuvent être inutiles ou redondants selon le nombre de nœuds voisins (messages en

[83] Power-Aware Alternation

diffusion, routage, maintenance de routes . . .). Rendre inactif un nœud pendant certaines périodes permettra d'allonger sa durée de vie.

- Diminuer les interférences, les collisions et les pertes de paquets résultantes. Le nombre de nœuds actifs dans un réseau est un facteur qui intervient pour la charge utile du réseau. Diminuer le nombre de nœuds du réseau, si la densité des nœuds le permet, permettra de diminuer le taux de perte des paquets [47].

Le point de départ de ce chapitre consiste à décrire l'architecture de notre modèle. Ensuite, nous détaillons chacun de ses modules en exprimant l'interaction et le fonctionnement global. Enfin, les performances du protocole proposé : OLSR-PAA, sont étudiées par simulation.

5.2 Présentation d'OLSR-PAA

Nous présentons dans cette section une approche pour la conservation d'énergie, cette approche est une extension de protocole de routage OLSR, ce dernier est besoin d'une interaction avec l'algorithme PAA afin d'améliorer son comportement d'énergie. Le point commun entre les deus protocoles est le principe d'utiliser un sous ensemble de voisins afin de découvrir d'un coté le bon chemin pour router les paquets (pour OLSR) et de l'autre coté, PAA utilise ce principe pour une meilleure conservation d'énergie. Le but de cette interaction est de garantir un protocole de routage avec un aspect d'économie d'énergie.

Le principe de notre approche consiste que les nœuds choisissent des nœuds parmi leurs MPRs qui seront élus comme *supporteurs* et avec qui ils vont alterner des périodes d'activité et des périodes d'inactivité, si leurs besoins le rendent possible. Durant les périodes d'inactivité d'un nœud, son ou ses supporteurs récupèrent et stockent les messages en sa destination. L'alternance des périodes d'activité et d'inactivité s'effectue d'une manière prédéfinie. Les instants de changements d'états sont fixes, un nœud peut réaliser une alternance complète des états. Nous définissons trois états pour un nœud :

État d'activité : le nœud transmet et reçoit des paquets à n'importe quel instant,

État d'inactivité : le nœud éteint sa carte d'interface ou bien est en mode d'économie d'énergie,

État pré-inactif : lorsqu'un nœud décide d'entrer en état d'inactivité, il arrête d'envoyer ses messages de contrôle périodiques, c.-à-d. messages Hello et TC.

Pour cela nous définissons également une **Inter période** : période séparant deux changements d'états durant laquelle tous les nœuds du réseau doivent être actifs et s'échangent les messages sauvegardés.

5.2.1 Phase d'établissement ou négociation pour l'obtention d'un supporteur

En réalité, un nœud décidera d'entrer en mode inactive si son niveau de batterie devient bas. Dans notre mécanisme, avant que le nœud entré dans l'état inactif, il devient en état pré-inactif et il doit assurer que le changement d'état ne provoquera pas une rupture de connectivité dans le réseau.

Après la définition des MPRs de chaque nœud, le nœud pré-inactif doit définir l'ensemble de supporteurs. Le mécanisme PAA nécessite une phase d'établissement durant laquelle les nœuds du réseau voulant activer PAA s'organisent en un réseau virtuel de supporteurs. Initialement, chaque nœud doit exécuter un algorithme qui lui permettra d'obtenir un supporteur. La relation de support est une relation binaire et réciproque. A un instant donné, un nœud peut avoir plusieurs supporteurs qui l'ont au préalable sollicité à leurs tours. Partons d'un exemple pour expliquer l'algorithme d'obtention d'un supporteur. Considérons un réseau composé de 6 nœuds dont les relations de voisinage sont représentées par des flèches dans la figure 5-1[47].

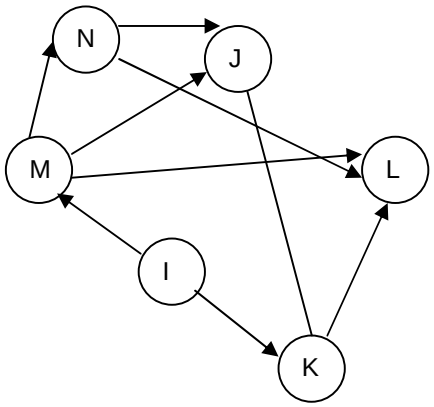


Figure 5-1 : Exemple d'établissement ou négociation pour l'obtention des supporteurs

Supposons que le nœud I cherche un supporteur. Il diffuse une requête d'obtention de supporteur (envoi d'un message " Requête ") à laquelle uniquement ses 2 voisins directs M et K devraient répondre. Il reçoit un message d'" Acceptation " de la part du nœud M. Ce message fait office de candidature et révèle la capacité du nœud M à supporter I. si le nœud M par exemple est le seul candida, le nœud I envoie directement un message de " Confirmation " au nœud M indiquant l'établissement de la relation de support entre les deux nœuds.

5.2.2 Critères de candidature pour être supporteur

Suite à la réception d'une requête d'obtention de supporteur, un nœud peut choisir d'accepter cette requête ou pas selon l'algorithme suivant :

- Si le nœud n'a aucun supporteur et il veut entrer dans cette coopération, alors il accepte directement et devient candidat,
- sinon, il vérifie si son niveau d'énergie lui permet de supporter un nœud supplémentaire ou pas. On peut définir à cet effet, un seuil ***Se***, comme étant le seuil d'énergie au-dessous duquel un nœud est jugé incapable de supporter des nœuds supplémentaires. Si son énergie est suffisante alors :
    - il vérifie s'il a atteint le nombre maximal de supporteurs autorisé. Le nœud étant susceptible d'avoir plusieurs supporteurs, il ne doit pas supporter un nombre important de nœuds en tenant compte de ses capacités de calcul, de mémoire et de la charge réseau.
    - On définit alors N, le nombre maximal de nœuds pouvant être supportés par un nœud. Finalement, une machine peut décider d'être supporteur en vérifiant si elle n'a pas atteint ces 2 seuils à la fois.

Une fois un nœud accepte de devenir supporteur, il doit générer un message d'acceptation vers le nœud ayant émis la requête. Ce message doit comporter le nombre de nœuds qu'il supporte actuellement et son niveau d'énergie.

L'organigramme de la figure 5.2 [47] résume le fonctionnement d'un nœud lançant une requête d'obtention d'un supporteur. Il montre l'utilisation de plusieurs temporisateurs dont les divers rôles.

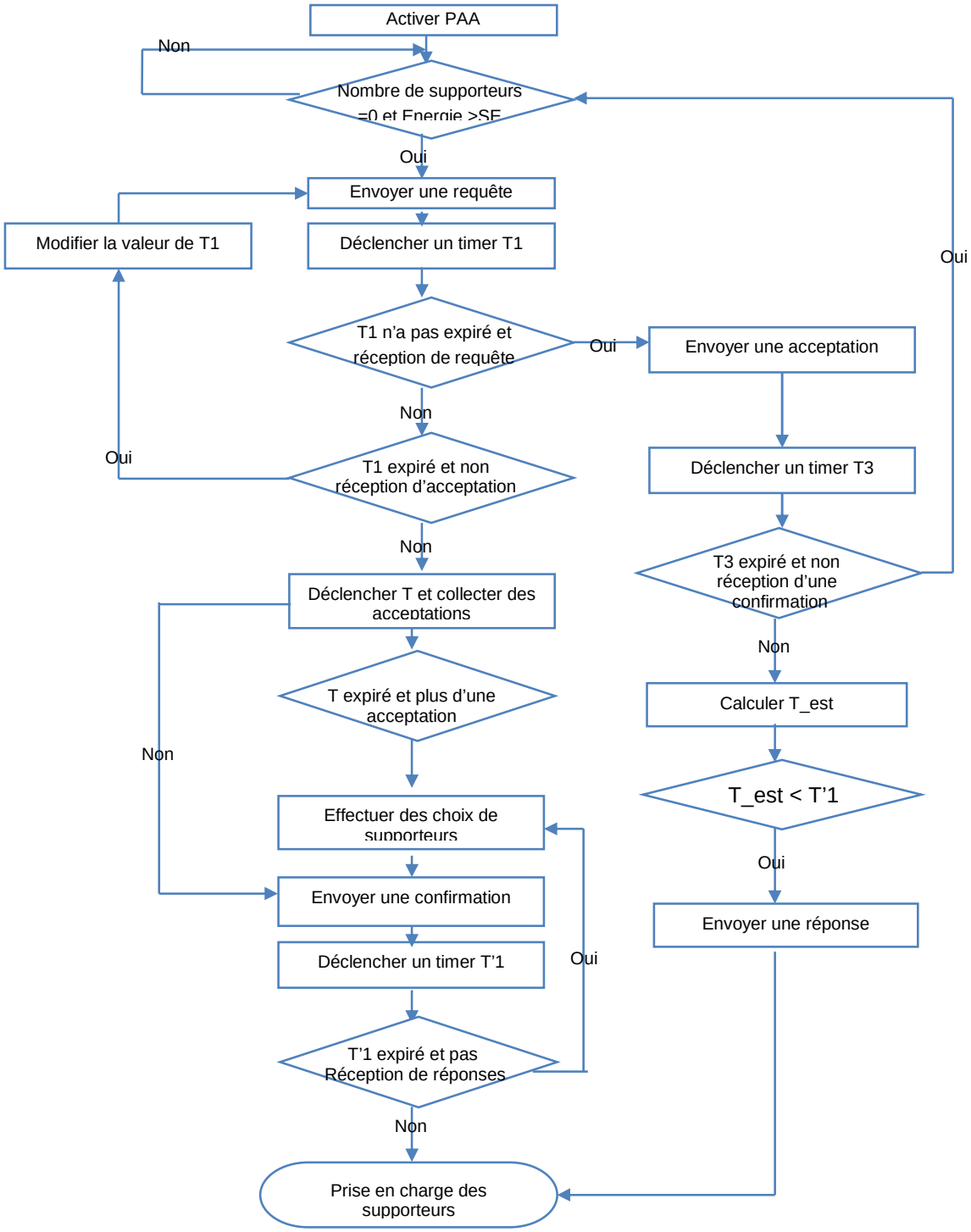


Figure 5-2 : Organigramme résumant le fonctionnement de PAA

5.2.3 Fonctionnement en mode synchrone forcé

Soit le réseau illustré par la figure 5-3. Les relations mutuelles de support sont illustrées par les flèches bidirectionnelles.

A un instant donné, on peut trouver le fonctionnement suivant :

A chaque instant, les nœuds supporteurs ont donc des états opposés (actif/inactif) sauf durant les périodes D.

Aucun message de contrôle n'a besoin d'être transmis pour l'établissement de ce mode ; chaque nœud connaissant au préalable ses instants de changements d'état selon l'axe qu'il adopte dés la phase de négociation.

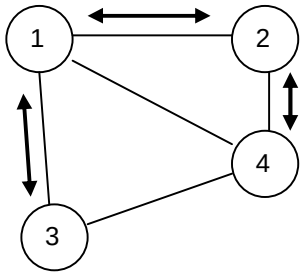


Figure 5-3 : Exemple du réseau utilisé

Ceci présente donc l'avantage de ce mode qui ne requièr pas de trafic de contrôle supplémentaire tout au long du fonctionnement de l'alternance. Durant la période D, tous les nœuds du réseau doivent être actifs. Durant cette période, les nœuds peuvent échanger un trafic normal ainsi que les messages tamponnés. Le délai D est choisi tel qu'il permet aux nœuds qui sortent de la phase d'inactivité de récupérer leurs messages à partir de leurs nœuds supporteurs. Il doit être suffisant pour tenir compte des conditions du réseau et du temps nécessaire pour transmettre les messages stockés.

5.2.4 Amélioration au protocole OLSR

Le protocole OLSR, comme son nom l'indique, est un protocole à état de lien optimisé; il obtient aussi des routes de plus court chemin. Alors que dans un protocole à état de lien, chaque nœud déclare ses liens directs avec ses voisins à tout le réseau, dans le cas d'OLSR, les nœuds ne déclarent qu'une sous-partie de leur voisinage grâce à la technique des relais multipoints. Ils consistent essentiellement, en un nœud donné, à ignorer un ensemble de liens et de voisins directs, qui sont redondants pour le calcul des routes de plus court chemin : plus précisément, dans l'ensemble des voisins d'un nœud, seul un sous-ensemble des ces voisins est considéré comme pertinent. L'algorithme de l'amélioration apportée au protocole OLSR est donné ci-après :

{ ….. }

Si le nœud reçoit un message requête **alors**

Si (le nœud pré-inactif est dans l'ensemble des MPRs) **alors**

MPRs =MPRs – ce nœud ;

Finsi

Consulter la table de routage ;

Si (le nœud pré-inactif est considéré comme le dernier saut au destinataire) **alors**

Recalculer la table de routage ;

Finsi

seuil_énergie = valeur ; *{la valeur est donnée en fonction de plusieurs paramètres tel le type d'application,…}*

Si ((l'énergie de ce nœud > seuil_énergie) et (son adresse est sélectionner dans le message)) **alors**

Envoyer un message d'acceptation

Finsi

Fin si

{……}

5.2.5 Modèle de la consommation d'énergie

Nous supposons que tous les nœuds mobiles sont équipés avec une carte réseau IEEE 802.11, avec un taux des données de 54 Mbps. L'énergie a eu besoin pour transmettre un paquet p de nœud i est : E_{tx} (p, n_i) = i * v * t_p Joules, où i est le courant (en Ampère), v le voltage (en Volt), et t_p le temps pris pour transmettre le paquet p (en secondes). Dans nos simulations, le voltage v est choisi comme 5 V et nous supposons que le temps de la transmission du paquet t_p est calculé par :

$$(p_h/ (6*10^6) + p_d/(54*10^6)) \text{ seconds},$$

Où p_h, est la dimension de l'en-tête du paquet en bits et p_d la dimension de la charge utile. Nous supposons que la consommation d'énergie causée en entendant un paquet est le même comme l'énergie consommée en recevant le paquet. L'énergie E(p, n_a) consommé pour transmettre un paquet de nœud n_a à un nœud n_b est donné par:

$$E(p, n_a) = E_{tx}(p, n_a) + E_{rx}(p, n_b) + (N - 1) * E_o(p, n_i)$$

Où E_{tx}, E_{rx}, et E_o dénotent le montant d'énergie a dépensé pour transmettre le paquet de nœud n_a, pour recevoir le paquet au nœud n_b et pour entendre le paquet, respectivement. N représente le nombre moyen des nœuds voisins affecté par une transmission de nœud n_a. L'équation implique que quand le réseau est plus dense, l'entendre des paquets causent plus de consommation d'énergie.

5.3 Tests et résultats

5.3.1 Le simulateur NS-2

Plusieurs simulateurs de réseaux ont été développés afin de répondre à des besoins divers. NS-2 est, désormais, l'outil de simulation de réseaux le plus puissant et le plus utilisé par la communauté scientifique en raison de sa simplicité et de son implémentation modulaire. C'est les raisons pour lesquelles notre choix s'est porté sur ce simulateur.

NS-2 est un logiciel de simulation de tout type de réseaux informatique développé dans le cadre du projet VINT au Laboratoire National de Lawrence Berkeley [48], sous lequel la version 2.33 est sortie. Les premières versions de ce simulateur ne supportaient que les architectures des réseaux filaires. Cependant avec l'avènement de la technologie sans fil, d'autres versions ont été développées et étendues pour supporter les réseaux sans fil et plus particulièrement les réseaux MANETs.

Le Simulateur NS-2 se compose d'une interface de programmation en Tcl/OTcl et d'un noyau écrit en C++ dans lequel la plupart des couches et protocoles réseaux ont été implémentés :

1- Couche MAC : CSMA, CDMA, 802.X, Token ring, MPLS, liens satellite

2- Couche Réseaux IP : routage dans les réseaux ad-hoc (AODV, DSR, DSDV, TORA, AMODV), routage dans les réseaux filaire (Link state, Distance vector), les réseaux multicast, IntServ, DiffServ.

3- Couche Transport : TCP, UDP

4- Traffic : parreto, ON/OFF, CBR, FTP, telnet

Avant de réaliser nos simulations nous avons testé, à travers des exemples, les différents modules de NS-2. En examinant les résultats obtenus, nous avons pu mettre en évidence quelques bugs au niveau de la couche MAC, et au niveau de la couche physique. Les correctifs nécessaires ont été apportés.

Par défaut le protocole OLSR n'est pas inclus dans NS-2, en tout cas pas dans les versions stables disponibles (jusqu'à la version 2.33 qu'on va adopter). Pour l'installer, il fallait apporter des modifications sur certains fichiers du simulateur, pour pouvoir

intégrer les librairies et classes OLSR. Rappelons qu'on a adopté UM-OLSR [49], l'implémentation de l'université de Muricia, la plus stable, et la mieux commentée.

5.3.2 Paramètres de simulation

Le but principal de nos expérimentations est d'évaluer les performances de notre amélioration. Nous présentons maintenant les paramètres de simulation communs de notre mécanisme. Nous y étudierons la consommation de l'énergie dans le réseau ainsi que la durée de vie du réseau. Le nombre de nœuds mobiles varie entre 0 et 10 nœuds.

Une autre étude de simulation est réalisée, en faisant varier cette fois-ci le nombre de nœuds entre 0 et 50 afin de consulter la charge du réseau en termes de messages de négociation, permettant de sélectionner les supporteurs dans notre Approche.

Nous considérons dans cette section un réseau ad-hoc constitué d'un nombre fixe de nœuds, une topologie peu dense constituée de 10 nœuds dans une région de 870m x 870m. La variation du nombre des nœuds, permet de comparer les performances de notre protocole avec celle d'OLSR classique.

Paramètres du réseau	valeurs
Région	**870*870**
Nombre de nœuds	**10-40**
Durée simulation	**1000**
Energie initiale d'un nœud	**20**
Trafic entre les nœuds	**CBR**
nombre de sources	**3**

Table 5-1 : Paramètres utilisés dans la simulation

5.3.2.1 Etude de la Consommation d'Energie

D'après les résultats de l'étude précédente, nous avons fixé le scénario suivant pour l'étude de la consommation de l'énergie.

Nombre de nœuds = 10 nœuds, nombre de sources CBR = 3 sources, vitesse maximal 2 m/s, temps pause 50 sec, durée simulation 1000 sec, énergie initiale 20 joule.

1 Energie Totale du Réseau

On va s'intéresser à travers cette série de simulations à comparer les performances de notre extension avec les performances d'OLSR classique, en termes de consommation d'énergie.

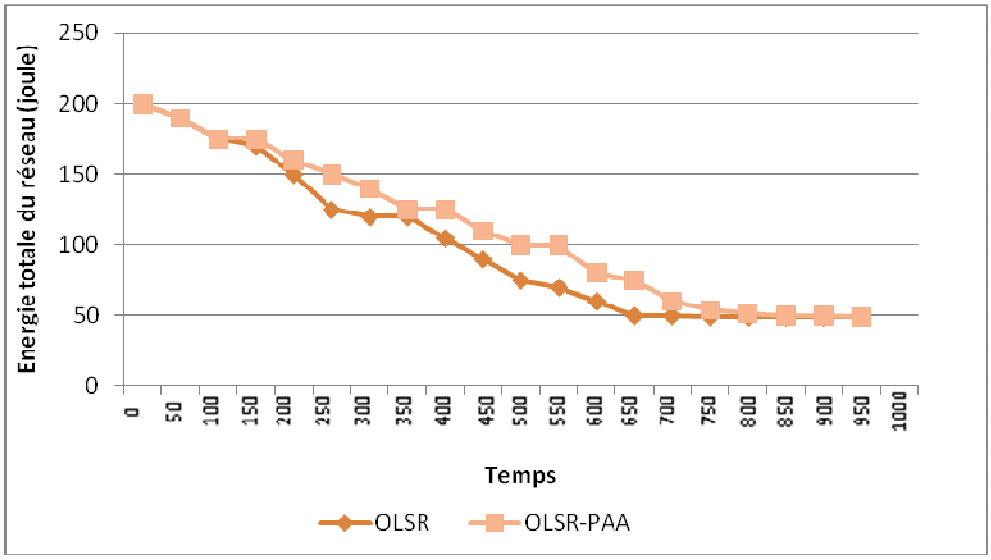


Figure 5-4 : L'évolution de l'énergie totale en fonction du temps

Sur ce graphe l'énergie totale du réseau avant amélioration décroît plus vite que celle du réseau après amélioration sur l'intervalle [0,500] sec. Puis sur l'intervalle [500,1000] sec, nous remarquons une stabilisation du niveau de l'énergie totale du réseau avant amélioration, cela est dû à la perte de connexité du réseau. En effet à t = 500 le nombre de nœud vivant du réseau avant amélioration est de 4, et ces 4 nœuds ne communiquent pas probablement à cause de l'éloignement. Sur le même intervalle, l'énergie du réseau après amélioration continue de décroître, preuve que les nœuds continuent de communiquer. Nous concluons à partir de l'évolution de l'énergie sur l'intervalle 50,600] que notre amélioration a réalisé une économie de 11% sur l'énergie totale du réseau.

2 Durée de Vie du Réseau

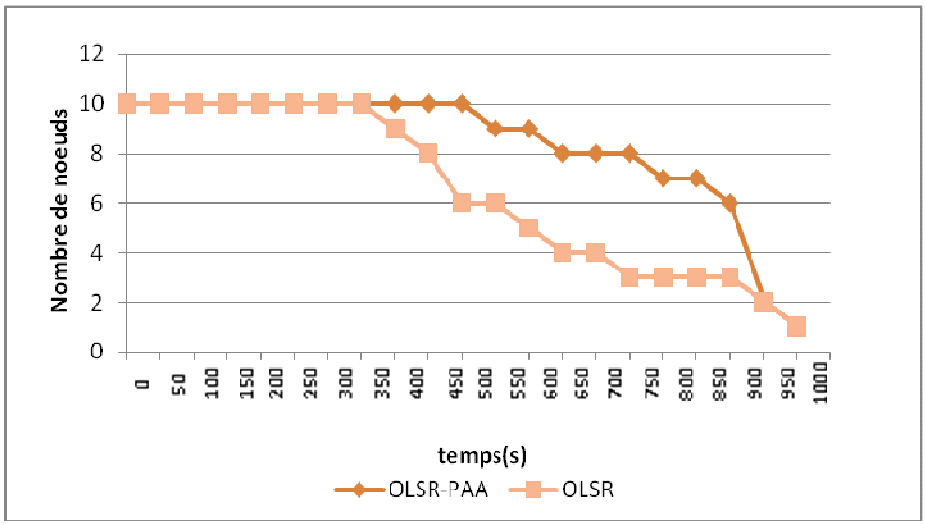


Figure 5-5 : Durée de vie du réseau

Sur ce graphe on remarque que le nombre de nœuds vivants du réseau avant l'amélioration commence à décroître à partir de t = 350 sec, et se stabilise vers t=650sec à cause de la perte de connectivité puis recommence à décroître vers t=900sec.

Par contre pour le réseau après amélioration le nombre de nœuds vivants reste constant jusqu'à t = 750 sec, où il commence à décroître rapidement. Grâce à l'emploi d'un seuil d'énergie par notre solution, le protocole de routage OLSR favorise les nœuds disposant d'une plus grande énergie résiduelle et procède à l'utilisation équitable de cette dernière. A partir de ce graphe, on constate que notre approche a réalisé une augmentation de 20% de la durée de vie moyenne d'un nœud, et par conséquent a augmenté aussi la durée de vie de tout le réseau.

3 Charge du réseau

Dans cet étude, on va modifier le nombre de nœuds entre 0 et 50 afin de consulter la charge du réseau en terme de messages de négociation.

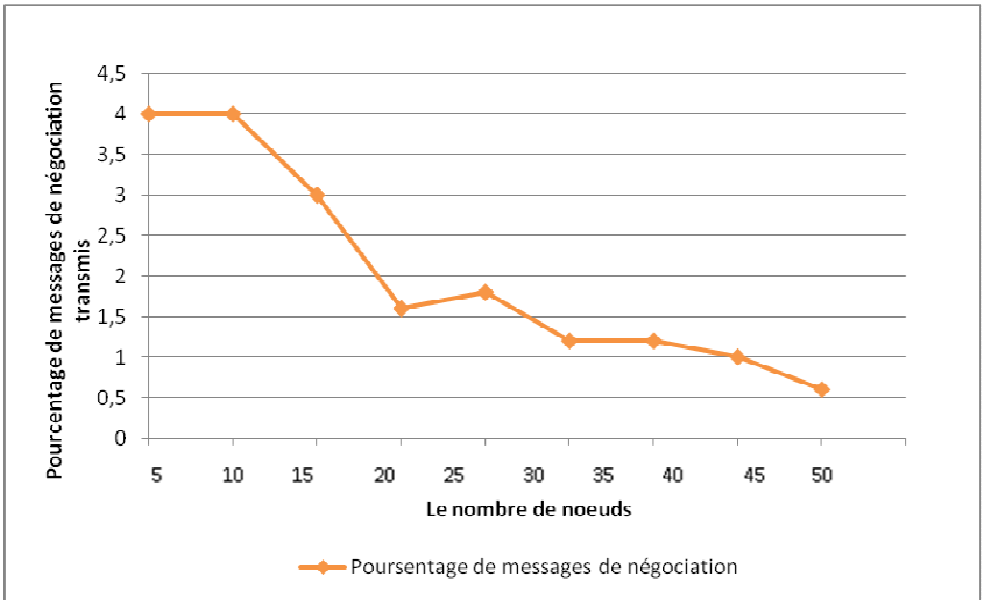


Figure 5-6 : pourcentage de message de négociation générée en fonction du nombre de nœuds

La figure 5-6 représente le pourcentage des messages de négociation hors le nombre totale des messages de contrôle du protocole OLSR.

On remarque que dans notre approche le nombre de messages de négociation est environ 4% du trafic de contrôle totale d'OLSR pour un réseau de 20 nœuds et vers 0.6% pour un réseau de 40 nœuds.

Dans un grand réseau, le total des messages TC grandit de façon considérable à cause des retransmissions sur des sauts multiples pendant qu'ils sont inondés dans le réseau entier. Cependant, les messages de négociation sont des messages de diffusion d'un-saut et augmentent linéairement avec le nombre de nœuds Sleep seulement. C'est pourquoi la proportion de trafic de négociation par rapport au trafic du contrôle total d'OLSR diminuée dans un grand réseau.

5.3.3 Conclusion

Dans ce chapitre, nous avons implémenté, notre solution sous NS-2. Plusieurs simulations ont été lancées, sous des scénarios divers et multiples. L'objectif est de valider les améliorations apportées par notre solution par rapport à OLSR classique.

Les résultats obtenus sont très concluants et satisfaisants, avec des taux de perte de données réduits, une économie de l'énergie importante allant jusqu'à 11% et une augmentation de la durée de vie moyenne d'un nœud mobile allant jusqu'à 20%.

CONCLUSION GÉNÉRALE

6 Conclusion Générale

Dans cette approche de recherche, nous avons présenté, en premier lieu, les solutions existantes pour la conservation d'énergie dans les réseaux ad hoc en mettant l'accent sur les approches au niveau routage et les améliorations touchant le mécanisme PSM de la couche MAC de la norme IEEE 802.11.

Nous avons proposé une amélioration du protocole OLSR dont le but est de satisfaire les besoins des réseaux ad hoc, dans le contexte d'économie d'énergie. L'idée est basée sur une adaptation du protocole OLSR avec l'une des approches d'amélioration du mécanisme PSM. On a alors combiné le mécanisme PAA avec le protocole de routage OLSR.

Le mécanisme PAA se base sur la suppression de toute activité réseau d'un nœud pendant certaines périodes afin de conserver son énergie. Durant son inactivité, les messages en sa destination seront récupérés par un ou plusieurs nœuds appelés supporteurs. Ces supporteurs sont sélectionnés à partir de l'ensemble des MPRs du protocole OLSR, en prenant en considération la contrainte de leurs niveaux d'énergie. Donc, avec cette adaptation, les nœuds ayant une énergie faible sont évités dans le routage afin de maintenir un bon niveau d'énergie pour tous les nœuds mobiles. Nous avons démontré par différents scénarios de simulation que la solution proposée est efficace et apporte une nette amélioration sur les plans que nous venons de citer.

Enfin, comme perspectives nous envisageons de faire une extension du protocole de routage OLSR-PAA dans un réseau sans fil multimédia où il y a plus de contraintes. Une autre perspective est d'étudie l'efficacité énergétique dans les réseaux de capteurs sans fil où l'énergie est le premier point critique, avec un accent particulier sur la conservation d'énergie au niveau routage.

RÉFÉRENCES

7 Références

[1] Rabih MOAWAD « ***QoS dans les WPAN, WLAN et WMAN*** ». Thèse. Université LIBANAISE des réseaux et télécommunications. Décembre 2004.

[2] Emmanuel CONCHON ***« Définition et mise en œuvre d'une solution d'émulation de réseaux sans fil »*** Thèse de doctorat. École doctorale Informatique et Télécommunications de l'Institut National Polytechnique De Toulouse. 27 Octobre 2006.

[3] Mohamed BRAHMA « ***Étude de la QoS dans les Réseaux Ad hoc: Intégration du Concept de l'Ingénierie du Trafic*** ». Thèse de doctorat .Université de haute alsace UFR des sciences et techniques. 13 décembre 2006.

[4] ***« Les réseaux locaux sans fil (RLANs) ».*** Département de Télécommunications. 2006-2007.

[5] Hassan Benchikh, Gabriel Cognard « ***LA NORME 802.11n*** ». Université de Lille1, décembre 2006.

[6] Rabah MERAIHI, « ***Gestion de la qualité de service et contrôle de topologie dans les réseaux ad hoc ».*** Thèse de doctorat, De l'Ecole Nationale Supérieure des Télécommunications 2004.

[7] S. Agarwal, S.V. Krishnamurthy, R.H. Katz, and S.K. Dao, "***Distributed Power Control in Ad Hoc Wireless Networks***", IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), 2001.

[8] L. KADDAR, A. MEHAOU. "***ESTREL: Transmission and Reception Energy Saving Model for Wireless Ad Hoc Networks,*** 32nd IEEE Conference on Local Computer Networks, 2007.

[9] M. Stemm, R. H. Katz, "***Measuring and reducing energy consumption of network interfaces in hand-held devices***", Université de Californie, Berkeley, CA 94720-1776. 1997.

[10] S Narayanaswamy, V Kawadia, R. S. Sreenivas et P. R. Kumar "***Power control in Ad-hoc Networks: Theory, Architecture, Algorithm and Implementation of the COMPOW Protocol"*,** European Wireless Conference, 2002.

[11] Marwan Krunz, Alaa Muqattash, and Sung-Ju Lee. "***Transmission Power Control in Wireless Ad Hoc Networks: Challenges, Solutions, and Open Issues***", Université d'Arizona, mobile and Media Systems Lab Hewlett-Packard Laboratories Palo Alto, CA 94303, 2004.

[12] Gupta P. et Kumar P. R., "***The capacity of wireless networks***", Actes des transactions IEEE sur l'informatique théorique, 2000, p.388-404.

[13] Yumei Liu, Lili Guo,Huizhu Ma,Tao Jiang, *"**Energy Efficient on–demand Multipath Routing Protocol for Multi-hop Ad Hoc Networks**".* IEEE Xplore. Downloaded on October 2008, 978-1-4244-2204.

[14] Burkhart M., von Rickenbach P.,Wattenhofer R. et Zollinger A., "***Does topology control reduce interference****?*", Actes du 5me symposium international ACM sur les réseaux mobiles ad hoc, Tokyo, Japan, 2004, p. 9-19.

[15] Ram Ramanathan et Regina Rosales-Hain, "***Topology control of multihop wireless networks using transmit power adjustment***", Proceedings of INFOCOM, 2000, p, 404-413.

[16] Meguerdichian S., Koushanfar F., Potkonjak M. et Srivastava M. B., "***Coverage problems in wireless ad hoc sensor networks***", Actes de la seconde conférence international ACM sur les réseaux sans fil et de sensors et leurs applications, San Diego, USA, 2003, p. 115-121.

[17] F. Aurenhammer, "***Voronoi Diagrams : A Survey Of A Fundamental Geometric Data Structure***," ACM Computing Surveys 23, 1991, p. 345-405.

[18] R. Wattenhofer, L. Li, P. Bahl, and Y. M. Wang, "***Distributed Topology Control for Power Efficient Operation in Multihop Wireless Ad Hoc Networks***" IEEE INFOCOM, 2001, p. 1388–1397.

[19] A. Gamal et al., "***Energy-Efficient Scheduling of Packet Transmissions over Wireless Networks***" IEEE Infocom 2002.

[20] C. F. Huang, Y. C. Tseng, S. L. Wu, and J. P. Sheu, "***Increasing the Throughput of multihop Packet Radio Networks with Power Adjustment***" International Conference on Computer, Cummunication, and Networks, 2001.

[21] E. Uysal et al, "***Energy-Efficient Packet Transmission Over a Wireless Link***". IEEE/ACM Tran. On Networking. 2002, vol. 10, no. 4, p. 487–499.

[22] Gomez, J., Campbell, A. T., Naghshineh, M., and Bisdikian, C. "***Conserving transmission power in wireless ad hoc networks****"*. In *ICNP'01*. 2001.

[23] S. L.Wu, Y. C. Tseng, and J. P. Sheu, "***Intelligent Medium Access for Mobile Ad Hoc Networks with Busy Tones and Power Control***" IEEE Journal on Selected Areas in Communications, Sep 2000, vol. 18, p. 1647–1657.

[24] E.-S. Jung and N.H. Vaidya. "***A power control MAC protocol for ad hoc networks***". In MOBICOM, 2002, p. 36–47.

[25] Toh C-K. "***Maximum battery life routing to support ubiquitous mobile computing in wireless ad hoc networks***". IEEE Communications 2001; 39(6): 138–147.

[26] K.M. Sivalingam, J.C. Chen, P. Agrawal, et al. "***Design and analysis of low-power access protocols for wireless and mobile ATM networks***". *Wireless Networks*, 6(1), 2000.

[27] Changsu Suh, Young-Bae Ko and Jai-Hoon Kim, "Enhanced ***Power Saving for IEEE 802.11 WLAN with Dynamic Slot Allocation***," LNCS, 2005, Vol. 3794, p. 466-477.

[28] A. Belghith et W. Akkari, "***Traffic Aware Power conservation mechanism for ad hoc networks***", soumis au International Journal of Computing and Information Sciences (IJCIS), Canada, 2006.

[29] S. Singh, M. Woo and C.S. Raghavendra, "***Power-Aware Routing in Mobile Ad hoc Networks***", Proc. of Mobile Computing and Networking (Mobicom), 1998, p. 181-190.

[30] Rabaey J. M., Ammer M. J., da Silva Jr. J. L., Patel D., and Roundy S., " ***PicoRadio Supports for Ad Hoc Ultra-Low Power Wireless Networking*** ", Actes de la conférence IEEE Computer, Juillet 2000.

[31] Van Dam T. et Langendoen K., "***An Adaptive Energy-Efficient MAC Protocol for Wireless Sensor Networks*** ", Actes de la conférence ACM SenSys 2003, Novembre 2003.

[32] V. Kawadia and P. R. Kumar, "***Power control and clustering in ad hoc networks",*** in Proceedings of IEEE INFOCOM, 2003.

[33] S. Doshi, S. Bhandare, et T.X. Brown. "***An on-demand minimum energy routing protocol for a wireless ad hoc network***". In Proc. of ACM SIGMOBILE, 2002.

[34] Rahmé, J., Viana, A., Al Agha, K. "***Avoiding energy-compromised hotspots in resource-limited wireless networks"***. in IFIP International Federation for Information Processing, 2007, Vol 256, Home Networking p. 85–100.

[35] Hong-ryeol Gil, Joon Yoo, and Jong-won Lee. "***An On-demand Energy-efficient Routing Algorithm for Wireless Ad hoc Networks***", 2003.

[36] H. Hassanein, Jing Luo, "***Reliable Energy Aware Routing In Wireless Sensor networks"***, IEEE Workshop DSSNS, April 2006.

[37] V. Rodoplu and T.H.Meng. "***Minimum energy mobile wireless networks***". *IEEE J. Select. Areas Commun*, Aug 1999, vol. 17, no. 8, pp. 1333–1344.

[38] Pei G, Gerla M, Chen T-W. *"**Fisheye state routing: a routing scheme for ad hoc wireless networks**"*. Proceedings of IEEE International Conference on Communications (ICC) 2000; p. 70–74.

[39] N. Gupta, S.R. Das. ***"energy-aware on-demand routing for mobile ad hoc networks"***. In Proc. of IEEE IWDC, 2002.

[40] C. K. Toh. "***Maximum Battery Life Routing to Support Ubiquitous Mobile Computing in Wireless Ad Hoc Networks***". IEEE Communications Magazine, June 2001.

[41] Li Q, Aslam J, Rus D. "***Online Power-aware Routing in Wireless Ad-hoc Networks***". Proceedings of Int'l Conf. on Mobile Computing and Networking (MobiCom'2001), 2001.

[42] J.H. Chang, L. Tassiulas, "***Energy conserving routing in wireless ad hoc networks***", in: IEEE INFOCOM, New York, USA, 2000, p. 22– 31.

[43] Song Guo, Oliver Yang, "***Multicast lifetime maximization for energy constrained wireless ad-hoc networks with directional antennas***", in: IEEE Globecom, Dallas, USA, December 2004, p. 4120–4124.

[44] R.C. Shah, J.M. Rabaey, "***Energy Aware Routing for Low Energy Ad Hoc Sensor Networks***", IEEE WCNC, March 2002, Vol 1, p. 17-21.

[45] A. Srinivas. E. Modiano, "***Minimum Energy Disjoint Path Routing in Wireless Ad-Hoc Networks***", MOBICOM'2003 September 2003.

[46] Woo K, Yu C, Youn HY, Lee B. "***Non-blocking, localized routing algorithm for balanced energy consumption in mobile ad hoc networks***". Proceedings of Int Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems MASCOTS 2001; p. 117–124.

[47] H Idoudi , W Akkar, A Belghith , M Molnar., "***Alternance synchrone pour la conservation d'énergie dans les réseaux ad hoc*** ". Institut De Recherche En Informatique Et Systèmes Aléatoires n°1812, Novembre 2006.

[48] The Network Simulator NS-2, http://www.isi.edu/nsnam/ns/.

[49] F.G Ros, http://masimum.inf.um.es/?Software:UM-OLSR. Université de Muricia, Espagne.

[50] K. Baumgartner et J. Baacloz ***« Coexistence entre WLAN 802.11 et Bluetooth »*** 2002.

ANNEXES

1. Modèle d'énergie dans NS

Le Modèle d'énergie, comme a été implémenté dans ns, est un attribut du nœud. Ce modèle représente le niveau d'énergie dans un hôte mobile. Dans un nœud, Le modèle d'énergie a une valeur initiale qui est leur niveau d'énergie au commencement de la simulation, est connu comme `initialEnergy_`. Il a aussi un usage d'énergie donné pour chaque paquet transmet et reçus, sont appelés `txPower_` et `rxPower_`. Les fichiers où le modèle d'énergie est défini sont ns/energymodel [.cc et .h]. Autres fonctions et méthodes décrits dans cette annexe peuvent être trouvées dans `ns/wireless-phy.cc`, `ns/cmu-trace.cc`, `ns/tcl/lib [ns-lib.tcl, nsnode.tcl, ns-mobilenode.tcl]`.

1.1 La Classe C++ du modèle d'énergie

Le modèle d'énergie de base est très simple et est défini par la classe `EnergyModel` comme montré au-dessous:

```
class EnergyModel : public TclObject
public:
    EnergyModel(double energy) energy_ = energy;
    inline double energy() return energy_;
    inline void setenergy(double e) energy_ = e;
    virtual void DecrTxEnergy(double txtime, double P_tx)
    energy_ -= (P_tx * txtime);
    virtual void DecrRcvEnergy(double rcvtime, double P_rcv)
    energy_ -= (P_rcv * rcvtime);

protected:
    double energy_;
       ;
```

Dans la définition de la classe `EnergyModel` au-dessus, il y a une seule variable classe « `energy_` » qui représente le niveau d'énergie dans le nœud à tout moment donné. Le constructeur `EnergyModel(energy)` exige que l'énergie-initial soit passée le long de comme un paramètre. Les autres méthodes de la classe sont utilisées pour diminuer le niveau d'énergie du nœud pour chaque paquet transmis « `DecrTxEnergy (txtime, P_tx)` » et chaque paquet reçu « `DecrRcvEnergy (rcvtime, P_rcv)` » par ce nœud. `P_tx` et `P_rcv` sont la puissance de la transmission et de la réception (respectivement) exigé par l'interface du nœud ou la couche physique PHY.

Au commencement de la simulation, la variable `energy_` est mis à `initialEnergy_` qui est décrémenté pour chaque transmission et réception des paquets au nœud. Quand le niveau d'énergie du nœud en descend à zéro, aucuns paquets ne peuvent être reçus ou transmis par le nœud. Si le tracement est allumé, la ligne DEBUG: `node <node-id> dropping pkts due to energy = 0`, est imprimée dans le fichier du trace.

1.2 L'interface OTcl

Depuis que le modèle d'énergie est un attribut du nœud, il peut être défini par les APIs de la configuration du nœud suivant:

```
$ns_ node-config -energyModel $energymodel \
                 -rxPower $p_rx \
                 -txPower $p_tx \
                 -initialEnergy $initialenergy
```

D
ans notre scénario de simulation, Les valeurs des paramètres de la configuration précités du modèle d'énergie sont données dans la table suivante:

Attribut	Valeurs facultatives	Valeurs donnés
-energyModel	Modèle d'énergie	aucun
-rxPower	La puissance de réception en watts	1.0 W
-txPower	La puissance de transmission en watts	1.4 W
-initialEnergy	Energie en joules	20 joules