

République Algérienne Démocratique et Populaire
Ministère de l'enseignement supérieur et de la recherche scientifique

Université Kasdi Merbah - Ouargla
Faculté des Nouvelles Technologies de l'Information et de la Communication
Département d'Informatique et de la Technologie de l'Information



Mémoire

Présenté en vue de l'obtention du diplôme de **Master**

Domaine : Mathématiques et informatique.

Filière : Informatique.

Spécialité : Administration et Sécurité des Réseaux.

Thème

Etude et évaluation de performances des protocoles de routage géographiques GeRaF et SIF pour les réseaux de capteurs sans fils

Présenté par : - KHEZZANE Hind.
- MAYOU Saliha.

Encadré par : M. KAHLESSENANE Fares.

Devant le jury composé de :

Président
Examineur

Promotion : 2018/2019

Remerciement

**Un grand remerciement à notre bon Dieu, le tout puissant
qui nous a fourni la volonté et la patience pour la
réalisation de ce travail**

**Nous remercions notre encadreur M. Fares kahlessenane
qui n'a pas manqué à nous fournir son aide, ses conseils et
ses efforts**

**Nous tenons à remercier les membres de notre jury pour
avoir bien voulu consacrer une partie de leurs temps à
examiner et à évaluer ce travail.**

Nous remercions tous nos professeurs et en particulier :

Fouad Bakkari, Messaoud Mezati et Nour Elhadi Ben Amar

**Un merci tout spécial au collègue d'étude Hamza Ouali, qui
nous a aidé beaucoup durant notre travail**

**ainsi que nos camarades qui ont veillé sur nous pendant
ces cinq (05) années d'études supérieures**

Résumé

A cause de leur limitation en ressources, les réseaux de capteurs sans fil (RCSFs) nécessitent des protocoles de routage appropriés. Le routage géographique constitue l'une des solutions de routage les plus efficaces pour les RCSFs. Dans les dernières années, un ensemble de recherches a été conduit pour l'amélioration de ces derniers à des protocoles BLR. L'objectif de ces recherches est de proposer des protocoles qui résolvent les problèmes d'utilisation des beacons, dont le but est de gérer les fonctionnalités du réseau tout en optimisant les ressources disponibles. Dans ce travail, nous allons essayer de concevoir les protocoles BLR économe en énergie pour les RCSFs.

Mots clés : Réseaux de capteurs sans fil, routage géographique BLR, économie d'énergie.

Abstract

Because of their limited resources, wireless sensor networks (RCSFs) require appropriate routing protocols. Geographical routing is one of the most efficient routing solutions for RCSFs. In recent years, a set of research has been conducted for the improvement of these to BLR protocols. The objective of this research is to propose protocols that solve the problems of use of beacons, whose goal is to manage the functionalities of the network while optimizing the available resources. In this work, we will try to design protocols BLR thrifty energetic for WSN.

Key words: Wireless sensor networks, BLR geographical routing, energy saving.

المخلص

بسبب محدودية مواردها، فإن شبكات اللواقط اللاسلكية RCSFs تحتاج إلى بروتوكولات توجيه ملائمة. التوجيه الجغرافي يمثل أحد الحلول الأكثر نجاعة لـ RCSF في السنوات الأخيرة مجموعة من الأبحاث أدت إلى تحسينها إلى بروتوكولات BLR وتهدف هاته الأبحاث إلى اقتراح بروتوكولات تحل مشاكل استعمال beacon التي تهدف إلى تسيير وظائف الشبكات وذلك بتحسين الموارد المتاحة. في هذا العمل سنحاول تصميم بروتوكولات BLR اقتصادية للطاقة للـ RCSFs

الكلمات المفتاحية : شبكات اللواقط اللاسلكية . التوجيه الجغرافي، اقتصاد الطاقة

Table des matières

Résumé	II
Table des figures	VI
Liste des tableaux	VIII
Introduction générale	2
<i>Chapitre I : Généralités sur les réseaux de capteurs sans fil</i>	
1. Introduction	3
2. Le capteur	3
2.1. Définition d'un capteur	3
2.2. Architecture d'un capteur	4
2.2.1. Unité d'énergie	4
2.2.2. Unité de captage	5
2.2.3. Unité de traitements (processeur	5
2.2.4. Unité de communication	5
2.2.5. Unité de stockage(Mémoire)	6
3. Réseaux de capteurs sans fil (RCSF)	6
3.1. Description des réseaux de capteurs	6
3.2. Pile protocolaire d'un réseau de capteurs	8
3.3. Facteurs et contraintes de conception d'un RCSF	9
3.4. Applications des RCSF	12
4. Conclusion	14
<i>Chapitre II : Consommation d'énergie dans les RCSF</i>	
1. Introduction	16
2. Consommation d'énergie dans les RCSF	16
2.1. Energie de capture	17

2.2. Energie de traitement	17
2.3. Energie de communication	17
3. Facteurs intervenants dans la consommation d'énergie	18
3.1. Etat du module radio	18
3.2. Accès au medium de transmission	18
3.2.1. La retransmission	19
3.2.2. L'écoute active	19
3.2.3. La sur écoute	19
3.2.4. La surcharge (L'overhead des paquets de contrôle)	19
3.2.5. La surémission	20
3.2.6. La taille des paquets	20
3.2.7. Problème de la station cachée	20
3.2.8. Problème de la station exposée	21
3.3. Modèle de propagation radio	22
3.4. Routage des données	22
4. Techniques de minimisation de la consommation d'énergie	23
5. Conclusion	25
<i>Chapitre III : Etude des protocoles de routage BLR</i>	
1. Introduction	27
2. La norme IEEE 802.11	27
2.1 la couche physique	27
2.2 la couche Mac	28
2.2.1 le mécanisme RTS/CTS	28
3. Routage géographique avec beacons	30
4. routage géographique sans beacons	33
5. Présentation de certains protocoles de routage BLR	32

4.1 Protocole XLP	32
4.2 Protocole IGF	34
4.3 Protocole SIF	36
4.4 Protocole CBF	38
4.5 Protocole GeRaF	42
4.6 Protocole BLR	44
5. Conclusion	45
<i>Chapitre IV : Evaluation de performance de certains protocoles BLR.</i>	
1. Introduction	47
2. Généralité sur la simulation	47
2.1 Types de simulation	47
2.1.1 Système de simulation discret	47
2.1.2 Système de simulation continue	47
3. Le simulateur OMNeT++	48
3.1 concepts de modélisation OMNeT++	48
3.2 les principaux fichiers d OMNeT++	49
4. Le plateforme d OMNeT++ Castalia	50
4.1 le module de nœud	51
5. Paramètres de simulation	52
6. Scenarios de simulation ,résultats et discussion	54
6.1 1^{er} scenario: Field length	54
6.2 2^{ième} scenario: Scalability	55
6.3 3^{ième} scenario: Node speed	56
7. conclusion	57
Conclusion générale	59

Table des figures

Figure I.1	Quelques capteurs existants sur le marché	4
Figure I.2	Anatomie d'un capteur	6
Figure I.3	Exemple d'un réseau de capteurs sans fil	7
Figure I.4	Architecture de communication d'un RCSF	8
Figure I.5	La pile protocolaire utilisée dans les réseaux de capteurs	9
Figure I.6	Applications des RCSFs	13
Figure II.1	l'énergie consommée par un nœud capteur	16
Figure II.2	La sur écoute dans une transmission	19
Figure II.3	Problème de la station cachée	20
Figure II.4	solution de problème de la station cachée	21
Figure II.5	Problème de la station exposée	22
Figure II.6	Les techniques de conservation d'énergie	23
Figure III.1	les différentes couches de la norme IEEE 802.11	27
Figure III.2	L'échange RTS/CTS	29
Figure III.3	handshake pour IEEE 802.11	29
Figure III.4	Routage basé sur l'angle	34
Figure III.5	Secteur de symétrie : Zone de relayage dans IGF	35

Figure III.6	Handshake IGF	35
Figure III.7	Zone de relayage dans SIF	36
Figure III.8	handshake SIF	37
Figure III.9	Zone de relayage du protocole CBF	39
Figure III.10	Progression du paquet (plage de transmission 250 m	40
Figure III.11	Zone de duplication	41
Figure III.12	duplication des paquets dans le schéma de base	42
Figure III.13	Zones d'acheminement	42
Figure IV.1	module simple et composés	49
Figure IV.2	les modules et leurs connexions a castalia	51
Figure IV.3	le module composite de nœud	52
Figure IV.4	énergie consommé vs field length	54
Figure IV.5	énergie consommé vs nombre des nœuds	55
Figure IV.6	la latence vs nombre des nœuds	56
Figure IV.7	énergie consommé vs mobility speed	57

Liste des tableaux

Tableau IV.1 **Paramètres de simulation**

53

Introduction générale

Introduction générale

Les récents progrès dans les domaines de la micro-électronique et des technologies de communication sans fils permettent aujourd'hui de produire à coût bas des micros - composants embarqués communément appelés capteurs. Le déploiement de plusieurs capteurs sans fils dans une zone d'intérêt forme un réseau de capteurs sans fils (RCSFs).

L'activité de recherche autour des réseaux de capteurs sans fils a été initialement motivée par des applications militaires puis elle s'étend pour des applications environnementales, médicales, domotique et industrielles. Les RCSFs sont constitués d'une station de base (SB) qui récolte et traite les informations de captage d'un phénomène physiques (humidité, température, ...), et de nœuds capteurs qui jouent le rôle d'intermédiaires pour l'acheminement de paquet.

L'économie d'énergie est le premier facteur qu'il devrait être pris en considération pour le bon fonctionnement des réseaux de capteurs. En effet, les nœuds capteurs sont généralement alimentés au moyen d'une petite batterie limitée en puissance, généralement non rechargeable et non remplaçable. Par conséquent, l'épuisement des réserves énergétique des nœuds capteurs implique la mise hors service du réseau tout entier.

Les protocoles de routages géographiques sont des solutions prometteuses en termes d'économie d'énergie. Ils sont basés sur la position géographique, chaque nœud diffuse périodiquement un petit message appelé « beacon » pour connaître la position de ses voisins, ce type de routage géographique est appelé routage avec beacons. Cependant, l'utilisation des beacons surcharge le réseau ce qui influe sur la bande passante. Pour remédier, une autre catégorie de protocoles de routage a été proposée ; c'est les protocoles de routage sans beacon ou routage beacon-less.

L'objectif principal de notre étude consiste à présenter certains protocoles BLR et d'évaluer la performance de certains d'entre eux. Parmi ces derniers on a choisi XLP, IGF, SIF, CBF, Geraf, BLR.

Notre travail est divisé en quatre chapitres :

Premièrement, on introduira quelques généralités sur les réseaux de capteurs sans fil, en présentant description d'un capteur et d'un RCSF en global en on a conclu ce chapitre avec les différentes applications du RCSFs.

Deuxièmement, on présentera la problématique de la consommation d'énergie dans les RCSFs et après on a présenté les facteurs intervenants dans la consommation d'énergie (état du module radio, accès au medium de transmission, Modèle de propagation radio, routage des données) et on a terminé ce chapitre avec les solutions proposées dans le terrain pour la gérer soit au niveau de capture, de traitement ou de communication.

Ensuite on détaillera le fonctionnement des protocoles ci-dessus. Dans ce chapitre, nous définissons en premier temps le principe de routage géographique avec beacons et sans beacons (beaconless), ensuite on a passée en revue certains des protocoles de routage BLR et le fonctionnement de base de chacun de ses derniers.

Enfin, On terminera avec une description, simulation et comparaison entre deux protocoles BLR.

Chapitre I : Généralités sur les réseaux de capteurs sans fil

1. Introduction

Le progrès dans le domaine des communications sans fil ont donné naissance à des composants capables de prélever des mesures physiques et des données environnementales. Ces composants sont appelés des nœuds capteurs et ils ont la capacité de s'auto-organiser pour former un réseau de capteurs sans fils¹ (RCSF). Les RCSFs permettent de faciliter le suivi et le contrôle à distance avec une meilleure précision.

Ils peuvent aussi être déployés pour exploiter diverses applications (environnementales, militaires, médicales, etc.). Un réseau de capteurs est constitué généralement d'un grand nombre de nœuds capteurs car ces derniers sont des sujets de panne diverse.

Chaque nœud est composé principalement d'un ou plusieurs capteurs, d'une unité de traitement et d'un module de communication. Ces nœuds communiquent entre eux selon une certaine topologie du réseau afin d'acheminer les informations a un centre de contrôle distant de la zone de leurs d'éploiement appelée une station de base.

La mise en place d'un RCSF pose de nombreux problèmes, par exemple le routage des informations vers la station de base via les différents nœuds du réseau.

Pour résoudre les contraintes des RCSFs, plusieurs contributions ont été proposées dans la littérature. Ces contributions visent à minimiser la consommation d'énergie afin d'optimiser l'autonomie des nœuds qui constituent le réseau, dans le but de garantir une longue durée de vie pour le réseau entier. Dans ce chapitre, nous allons donner un aperçu sur les réseaux de capteurs sans fil. Pour cela, nous allons commencer par la définition, leurs architectures, leurs caractéristiques, ensuite nous allons présenter la topologie, les différents facteurs de conception, ainsi que les domaines d'application des réseaux de capteurs sans fil et nous allons conclure ce chapitre par une conclusion.

2. Le capteur

Un capteur est un petit appareil autonome capable d'effectuer de simples mesures sur son environnement immédiat, telles que la température, les vibrations et la pression. Cet appareil est augmenté de capacités de calcul et de communication ainsi que de batteries lui conférant une autonomie [1].

2.1 Définition

Les capteurs sont des dispositifs de taille extrêmement réduite avec des ressources très

limitées, autonomes, capable de traiter des informations et de les transmettre, via les sondes radio, à une autre entité (capteurs, unité de traitements...) sur une distance limitée à quelques mètres [1].

Les réseaux de capteurs utilisent un très grand nombre de ces capteurs, pour former un réseau sans infrastructure établie. Un capteur analyse son environnement, et propage les données récoltées aux capteurs appartenant à sa zone de couverture. Chaque capteur relayant l'information sur sa propre zone de couverture, le réseau se trouve entièrement couvert [1].

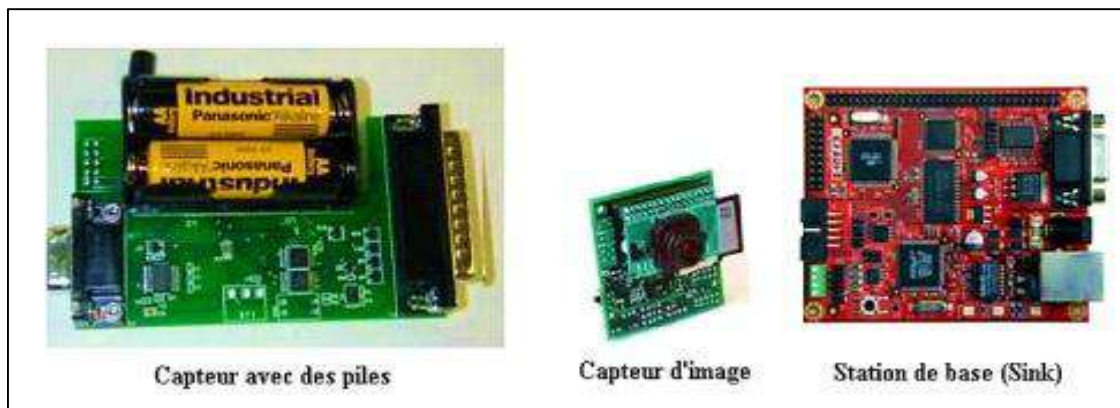


Figure I.1 : Quelques capteurs existants sur le marché [1]

2.2 Architecteur d'un capteur

On peut voir sur la figure 2 les différents composants qui constituent un capteur. Pour être plus précis chaque groupe de composants possède son propre rôle [1] :

2.2.1 Unité d'énergie

C'est la batterie qui n'est généralement ni rechargeable ni remplaçable. La capacité d'énergie limitée au niveau des capteurs représente la contrainte principale lors de conception de protocoles pour les RCSF. Les unités d'énergie peuvent être alimentées par des photopiles qui permettent de convertir l'énergie lumineuse en courant électrique [2].

2.2.2 Unité de captage

LED, interface, capteur : On retrouve donc des équipements de différents types de détecteur et d'autre entrée. Le capteur est généralement composé de deux sous-unités : le récepteur (reconnaissant l'analyste) et le transducteur (convertissant le signal du récepteur en signal électrique). Le capteur est responsable de fournir des signaux analogiques, basés sur le phénomène observé, au convertisseur Analogique/Numérique. Ce dernier transforme ces signaux en un signal numérique compréhensible par l'unité de traitement [3].

2.2.3 Unité de traitements (processeur)

Motte, processeur, RAM et Flash : On appelle généralement Motte la carte physique utilisant le système d'exploitation pour fonctionner. Celle-ci a pour cœur le bloc constitué du processeur et des mémoires RAM et Flash. Cet ensemble est à la base du calcul binaire et du stockage, temporaire pour les données et définitif pour le système d'exploitation. Cette unité est chargée d'exécuter les protocoles de communications qui permettent de faire collaborer le nœud avec les autres nœuds du réseau. Elle peut aussi analyser les données captées pour alléger la tâche du nœud puits [3].

2.2.4 Unité de communication

Radio et antenne : les équipements étudiés sont donc généralement équipés d'une radio ainsi que d'une antenne. Cette unité est responsable d'effectuer toutes les émissions et réceptions des données sur un medium sans fil. Elle peut être de type optique (comme dans les nœuds Smart Dust), ou de type radiofréquence. Les communications de type optique sont robustes vis-à-vis des interférences électriques. Néanmoins, elles présentent l'inconvénient d'exiger une ligne de vue permanente entre les entités communicantes. Par conséquent, elles ne peuvent pas établir de liaisons à travers des obstacles [3].

2.2.5 Unité de stockage(Mémoire)

L'unité de stockage inclut la mémoire de programme (dont les instructions sont exécutées par le processeur) et la mémoire de données (pour conserver des données fournies par l'unité de captage et d'autres données locales). La taille de cette mémoire est souvent limitée essentiellement par les considérations économiques et s'améliorera aussi probablement au fil des années [6].

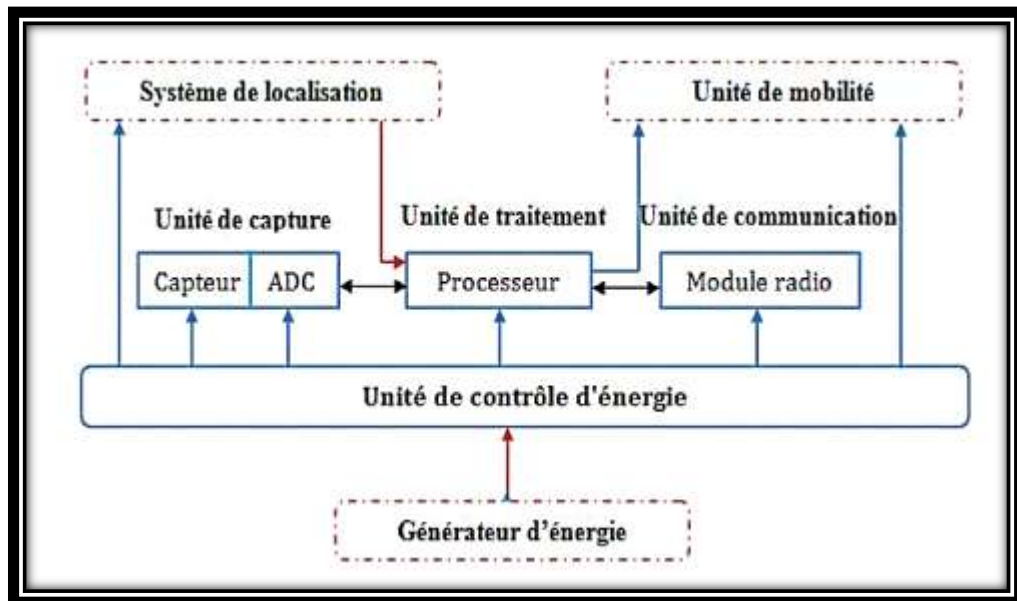


Figure I.2: Anatomie d'un capteur [1]

3. Réseaux de capteurs sans fil (RCSF)

Les réseaux de capteurs sans fil sont considérés comme un type spécial des réseaux Ad hoc où l'infrastructure fixe de communication et l'administration centralisée sont absentes et les nœuds jouent, à la fois, le rôle des hôtes et des routeurs. [1]

3.1 Description des réseaux de capteurs

Ce type de réseaux consiste en un ensemble de micro-capteurs éparpillés aléatoirement à travers une zone géographique qui définit le terrain d'intérêt pour le phénomène capté. Les micro-capteurs déployés sont capables de surveiller, d'une manière continue, une grande variété de conditions ambiantes telles que la température, l'humidité, et de détecter également l'occurrence des événements tel que

les séismes. Malgré leur capacité limitées de captage et de traitement de donnée, qui n'est qu'une conséquence de leur taille miniaturisé (de l'ordre de 1cm³), les composants de communication sans fil intégrés à ces capteurs leur permettent de collaborer et de coordonner entre eux afin d'accomplir des tâches de captage complexes [1].

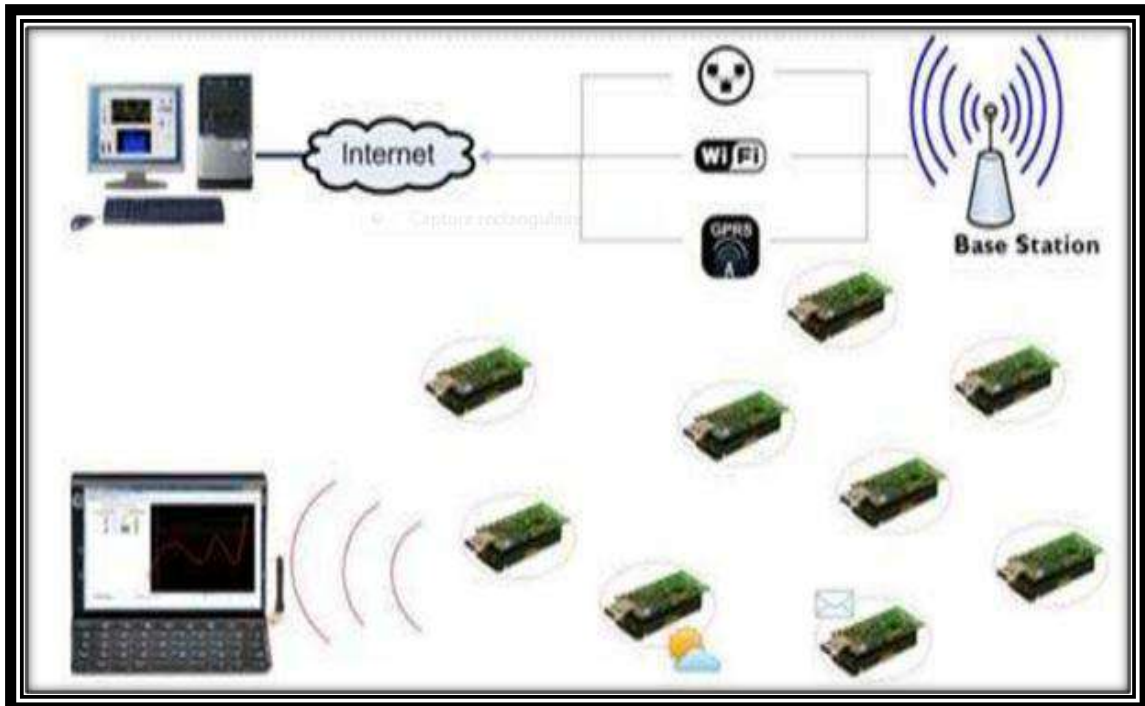


Figure I.3: Exemple d'un réseau de capteurs sans fil

3.2 Pile protocolaire d'un réseau de capteurs

En général, un réseau de capteur est relié avec d'autres types de réseaux. Pour que ce réseau puisse communiquer avec eux, il a besoin d'une interface de communication standard. Comme il n'y a aucune pile protocolaire standard pour les réseaux de capteurs, en comparant la pile protocolaire dans l'architecture de réseau de capteurs pour être semblable aux sept couches d'OSI (Open Système InterConnect) d'architecture de réseau conventionnelle. La pile protocolaire utilisée par le nœud puits ainsi que tous les autres capteurs du réseau est illustrée par la figure en bas (Figure 4). Cette pile prend en charge le problème de consommation d'énergie, intègre le traitement des données transmises dans les protocoles de routage, et facilite le travail coopératif entre les capteurs. Elle est composée de cinq couches : la couche physique,

la couche de liaison de données, la couche réseau, la couche transport et la couche application [1].

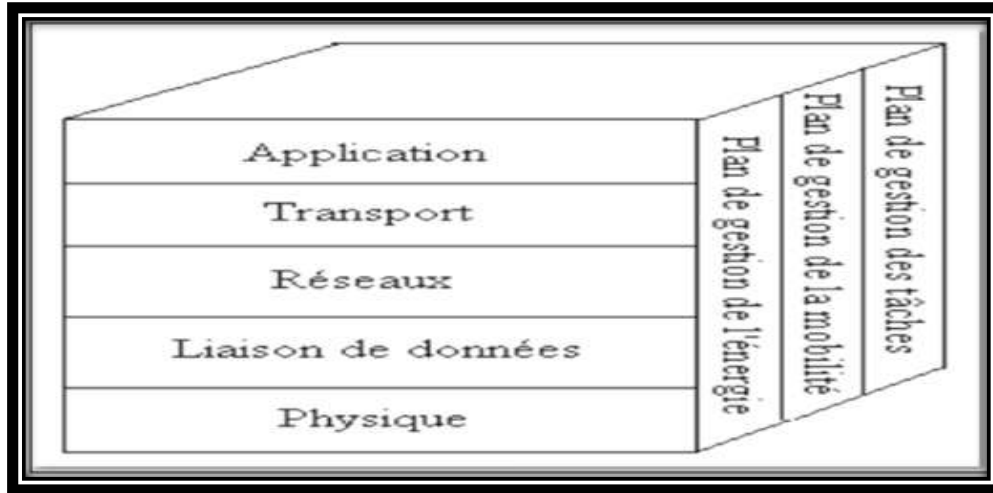


Figure I.4: La pile protocolaire utilisée dans les réseaux de capteurs [1]

1. **La couche physique** : doit assurée des techniques d'émission, de réception et modulation de données d'une manière robuste.
2. **La couche de liaison de données** : comme l'environnement des réseaux de capteurs est Tapage et les nœuds peuvent être mobiles, la couche de liaison de données doit garantir une faible consommation d'énergie et un taux de collision minimum entre les données diffusées par les nœuds voisins.
3. **La couche réseau** : s'occupe du routage des données fournies par la couche transport.
4. **La couche transport** : quant à elle, sert à maintenir le flux de données en cas de nécessité dans les applications utilisées, particulièrement lors d'une connexion avec Internet.
5. **La couche application** : suivant la fonctionnalité des capteurs, différentes applications peuvent être utilisées et bâties sur cette couche.

En plus de ces cinq couches, la pile protocolaire dans les réseaux de capteurs comporte trois niveaux : le niveau de gestion d'énergie, le niveau de gestion de mobilité et le niveau de gestion de tâches. Ces niveaux sont responsables du contrôle de l'énergie consommée, des mouvements des nœuds et de la distribution des tâches à travers toute la pile protocolaire, ils permettent aux capteurs de coordonner leurs tâches et minimiser la consommation d'énergie [1].

3.3 Facteurs et contraintes de conception d'un RCSF

Les principaux facteurs et contraintes influençant l'architecture des réseaux de capteurs peuvent être résumés comme suit :

- L'environnement :

Les capteurs sont souvent déployés en masse dans des endroits tels que des champs de bataille au-delà des lignes ennemies, à l'intérieur de grandes machines, au fond d'un océan, dans des champs biologiquement ou chimiquement souillés, etc. Par conséquent, ils doivent pouvoir fonctionner sans surveillance dans des régions géographiques éloignées.

- Les ressources limitées :

Généralement les nœuds capteurs ont une taille très petite. La miniature des capteurs limite la quantité de ressources qu'il peut contenir. D'où des capacités de traitement et de mémoire très limitées.

- La scalabilité :

Le nombre de nœuds déployés pour un projet peut atteindre le million. Un nombre aussi important de nœuds engendre beaucoup de transmissions inter nodales et nécessite que la SB soit équipé par beaucoup de mémoires pour stocker les informations reçues

- La tolérance aux erreurs :

Certains nœuds peuvent générer des erreurs ou ne plus fonctionner à cause d'un manque d'énergie, un problème physique ou une interférence. Ces problèmes ne doivent pas affecter le fonctionnement de tout le réseau de capteur, c'est le principe de la tolérance aux erreurs. La tolérance aux erreurs est la capacité de maintenir les fonctionnalités du réseau sans interruptions dues à une erreur intervenue sur un ou plusieurs capteurs.

- Les coûts de production :

Souvent, les réseaux de capteurs sont composés d'un très grand nombre de nœuds. Le prix d'un nœud est critique afin de pouvoir concurrencer un réseau de surveillance traditionnelle.

- Les médias de transmission :

Dans un réseau de capteurs, les nœuds sont reliés par une architecture sans fil, Ces liens peuvent être formés par radio, infrarouge ou des Média optiques. Cependant, il faut s'assurer de la disponibilité du moyen de transmission choisi dans l'environnement de capture et de permettre au réseau d'accomplir la totalité de ses tâches. Le choix des liaisons radio est par rapport à l'utilisation de la bande ISM (Industrial, Scientific and Medical) qui offre une licence gratuite (License-free) dans la plupart des pays.

- Agrégation de données :

Dans les RCSF, les données produites par les nœuds capteurs voisins sont très corrélées spatialement et temporellement. Ceci peut engendrer la réception par la station de base d'informations redondantes. Réduire la quantité d'informations redondantes transmises par les capteurs permet de réduire la consommation d'énergie dans le réseau et ainsi d'améliorer sa durée de vie. L'une des techniques utilisée pour réduire la transmission d'informations redondantes est l'agrégation des données. Avec cette technique, les nœuds intermédiaires agrègent l'information reçue de plusieurs sources. Cette technique est connue aussi sous le nom de fusion de données.

- La bande passante limitée :

Etant donné le fait que la puissance de chaque capteur est limitée, les nœuds ne peuvent supporter des débits élevés.

- La gestion de l'énergie :

Comme les nœuds capteurs sont des composants micro-électroniques, ils ne peuvent être équipés que par des sources limitées d'énergie. De plus, dans certaines applications, ces nœuds ne peuvent pas être dotés de mécanismes de rechargement d'énergie, par conséquent, la durée de vie d'un nœud capteur dépend fortement de la durée de vie de la batterie associée. Sachant que les réseaux de capteurs sont basés sur la communication multi-sauts, chaque nœud joue à la fois un rôle d'initiateur de données et de routeur également. Le dysfonctionnement d'un certain nombre de nœuds entraîne un changement significatif sur la topologie globale du réseau, et peut nécessiter un routage de paquets différent et une réorganisation totale du réseau. C'est pour cela que le facteur de consommation d'énergie est d'une importance primordiale dans les réseaux de capteurs. La majorité des travaux de recherche menés actuellement

se concentrent sur ce problème afin de concevoir des algorithmes et protocoles spécifiques à ce genre de réseau qui doivent consommer le minimum d'énergie [1].

3.4 Applications des RCSF

Les RCSF peuvent avoir beaucoup d'applications Parmi elles, nous citons :

➤ **Découvertes de catastrophes naturelles**

On peut créer un réseau autonome en dispersant les nœuds dans l'espace. Des capteurs peuvent ainsi signaler des évènements tels que feux de forêts, tempêtes ou inondations. Ceci permet une intervention beaucoup plus rapide et efficace des secours [5].

➤ **Détection d'intrusions**

En plaçant, à différents points stratégiques des capteurs, on peut ainsi prévenir des cambriolages ou des passages de gibier sur une voie de chemin de fer (par exemple) sans avoir à recourir de coûteux dispositifs de surveillance vidéo[5].

➤ **Applications métiers**

On pourrait imaginer d'avoir stocké des données nécessitants un certain taux d'humidité et une certaine température (minimale ou maximale). Dans ces applications, le réseau doit pouvoir collecter les différentes informations et alerter en temps réel si les seuils critiques sont dépassés [5].

➤ **Contrôle de la pollution**

On pourrait disperser des capteurs au-dessus d'un emplacement industriel pour détecter et contrôler des fuites de gaz ou de produits chimiques. Ces applications permettraient de donner l'alerte en un temps record et de pouvoir suivre l'évolution de la catastrophe [5].

➤ **Agriculture**

Des nœuds peuvent être incorporés dans la terre. On peut ensuite demander le

réseau de capteurs sur l'état du champ (déterminer par exemple les secteurs les plus secs afin de les arroser en priorité). On peut aussi imaginer équiper des troupeaux de bétail de capteurs pour connaître en tout temps, leurs positions ce qui éviterait aux éleveurs d'avoir recours à des chiens de berger [5].

➤ **Surveillance médicale**

En implantant sur la peau de mini capteurs vidéo, on peut recevoir des images en temps réel d'une partie du corps sans aucune chirurgie pendant environ 24h. On peut ainsi surveiller la progression d'une maladie ou la reconstruction d'un muscle [5].

➤ **Contrôle d'édifices**

On peut inclure sur les parois des barrages des capteurs qui permettent de calculer en temps réel la pression exercée. Il est donc possible de réguler le niveau d'eau si les limites sont atteintes. On peut aussi imaginer inclure des capteurs entre les sacs de sables formant une digue de fortune. La détection rapide d'infiltration d'eau peut servir à renforcer le barrage en conséquence. Cette technique peut aussi être utilisée pour d'autres constructions tels que les ponts, les voies de chemins de fer, les routes de montagnes, les bâtiments et autres ouvrages d'art [5].

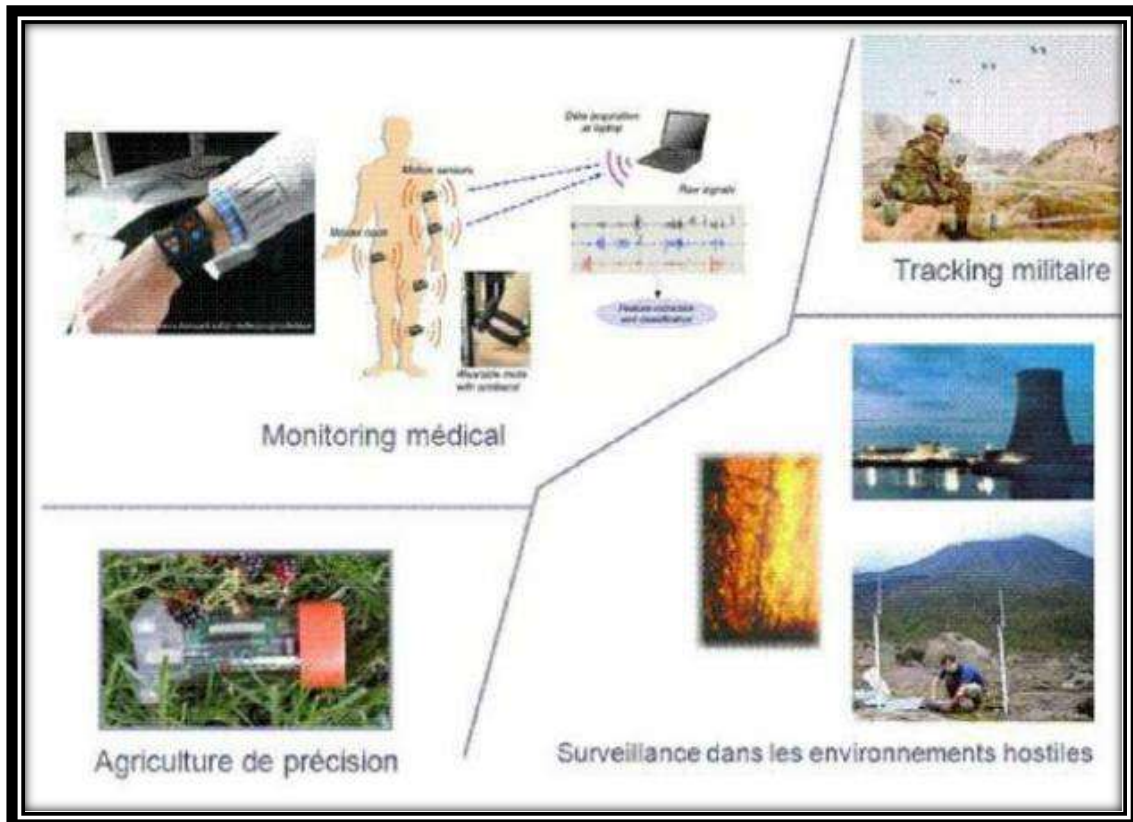


Fig I.6 : Applications des RCSFs. [5]

4. Conclusion

Les réseaux de capteurs sans fil présentent un intérêt considérable et une nouvelle étape dans l'évolution des technologies de l'information et de la communication. Cette nouvelle technologie suscite un intérêt croissant vu la diversité de ces applications : santé, environnement, industrie et même dans le domaine sportif. Nous avons présenté les RCSFs, leurs caractéristiques et les concepts nécessaires à la compréhension des réseaux de capteurs.

Chapitre II : Consommation d'énergie dans les RCSF

1. Introduction

Contrairement aux réseaux traditionnels qui se préoccupent essentiellement à garantir une bonne qualité de service, les réseaux de capteurs prennent en compte la conservation d'énergie afin de maximiser la durée de vie du réseau. Ils doivent intégrer des mécanismes qui permettent aux utilisateurs de prolonger la durée de vie du réseau en entier.

Tous les contraintes des RCSFs (Ressources limitées, Bande passante limitée, Topologie dynamique...) influent d'une façon ou d'une autre la consommation d'énergie.

2. Consommation d'énergie dans les RCSF

La première étape dans la conception de système énergétique de capteurs consiste à analyser les caractéristiques de consommation d'énergie d'un nœud capteur sans fil. Cette analyse systématique de l'énergie d'un nœud capteur est extrêmement importante pour identifier les problèmes dans le système énergétique pour permettre une optimisation efficace. L'énergie consommée par un capteur est principalement due aux opérations suivantes : la capture, le traitement et la communication [7].



Figure II.1 : l'énergie consommée par un nœud capteur

2.1 Energie de capture

La capture est effectuée par les composants d'acquisition qui traduisent les phénomènes physiques en signal électrique. La consommation d'énergie du module de détection dépend de la spécificité du capteur. Dans de nombreux cas, elle est négligeable par rapport à l'énergie consommée par les modules de traitement et communication. L'énergie consommée lors de la capture peut être réduite en utilisant des composants à faible consommation d'énergie. Une autre façon de réduire l'énergie consommée lors de la capture consiste à réduire la durée de capture et supprimer les captures jugées redondantes et inutiles [7].

2.2 Energie de traitement

L'énergie de traitement est composée de deux sortes d'énergie : l'énergie de commutation et l'énergie de fuite. L'énergie de commutation est déterminée par la tension d'alimentation et la capacité totale commutée au niveau logiciel (en exécutant un logiciel). Par contre, l'énergie de fuite correspond à l'énergie consommée lorsque l'unité de calcul n'effectue aucun traitement. En général, l'énergie de traitement est faible par rapport à celle nécessaire pour la communication [7].

2.3 Energie de communication

L'énergie de communication se décline en trois parties : l'énergie de réception, l'énergie de l'émission et l'énergie en état de veille. Cette énergie est déterminée par la quantité des données à communiquer et la distance de transmission, ainsi que par les propriétés physiques du module radio. L'émission d'un signal est caractérisée par sa puissance ; quand la puissance d'émission est élevée, le signal aura une grande portée et l'énergie consommée sera plus élevée. Notons que l'énergie de communication représente la portion la plus grande de l'énergie consommée par un nœud capteur [7].

3. Facteurs intervenants dans la consommation d'énergie

La consommation d'énergie dépend de plusieurs facteurs qui influencent de façon directe cette dernière, ils sont expliqués ci-dessous [8].

3.1. Etat du module radio

Le module radio est le composant du nœud capteur qui consomme le plus d'énergie, puisque c'est lui qui assure la communication entre les nœuds. On distingue quatre états des composants radio (transmetteur et récepteur) : actif, réception, transmission et sommeil [8].

- Etat actif : la radio est allumée, mais elle n'est pas employée. En d'autres termes, le nœud capteur n'est ni en train de recevoir ni de transmettre. Cet état provoque une perte de l'énergie suite à l'écoute inutile du canal de transmission.
- Etat sommeil : la radio est mise hors tension.
- Etat transmission : la radio transmet un paquet.
- Etat réception : la radio reçoit un paquet.

Il est aussi à noter que le passage fréquent de l'état actif à l'état sommeil peut avoir comme conséquence une consommation d'énergie plus importante que de laisser le module radio en mode actif. Ceci est dû à la puissance nécessaire pour la mise sous tension du module radio. Cette énergie est appelée l'énergie de transition. Il est ainsi souhaitable d'arrêter complètement la radio plutôt que de transiter dans le mode sommeil. Le changement d'état du module radio doit être géré par un protocole de la couche MAC. [8]

3.2. Accès au medium de transmission

La couche MAC joue un rôle important pour la coordination entre les nœuds et la minimisation de la consommation d'énergie. Dans cette section, nous allons analyser les principales causes de consommation d'énergie au niveau de la couche MAC [8].

3.2.1. La retransmission

Les nœuds capteurs possèdent en général une seule antenne radio et partagent le même canal de transmission. Par ailleurs, la transmission simultanée des données provenant de plusieurs capteurs peut produire des collisions et ainsi une perte de l'information transmise.

La retransmission des paquets perdus peut engendrer une perte significative de l'énergie [8].

3.2.2. L'écoute active

L'écoute active (idlelistening) du canal pour une éventuelle réception de paquet qui ne sera pas reçu peut engendrer une perte importante de la capacité des nœuds en énergie. Pour éviter ce problème, il faut basculer les nœuds dans le mode sommeil le plus longtemps possible [8].

3.2.3. La surécoute

Le phénomène de surécoute (overhearing) se produit quand un nœud reçoit des paquets qui ne lui sont pas destinés. La surécoute conduit à une perte d'énergie additionnelle à cause de l'implication des autres capteurs dans la réception des données [8].

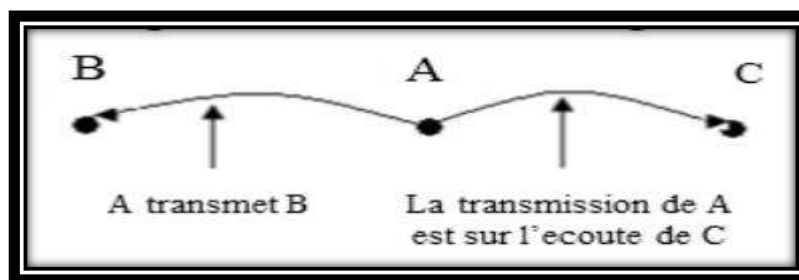


Figure II.2 : La surécoute dans une transmission

3.2.4. La surcharge (L'overhead des paquets de contrôle)

Plusieurs protocoles de la couche MAC fonctionnent par échange de messages de contrôle (overhead) pour assurer différentes fonctionnalités : signalisation,

connectivité, établissement de plan d'accès et évitement de collisions. Tous ces messages nécessitent une énergie additionnelle [8].

3.2.5. La surémission

Le phénomène de surémission (overemitting) se produit quand un nœud capteur envoie les données à un destinataire qui n'est pas prêt à les recevoir. En effet, les messages envoyés sont considérés inutiles et consomment une énergie additionnelle [8].

3.2.6. La taille des paquets

La taille des messages échangés dans le réseau a un effet sur la consommation d'énergie des nœuds émetteurs et récepteurs. Une grande puissance de transmission est nécessaire pour des paquets de grande taille [8].

3.2.7. Problème de la station cachée

Un des problèmes récurrent des réseaux sans fil est le problème de la station cachée. Deux stations peuvent communiquer avec le point d'accès mais ne peuvent se voir à cause de la distance trop grande ou de la présence d'un obstacle entre les deux stations (Figure II.3). C'est pourquoi les réseaux sans fil utilisent le protocole CSMA/CA (Carrier-Sens Multiple Access with Collision Avoidance) pour réserver le Médium[6]

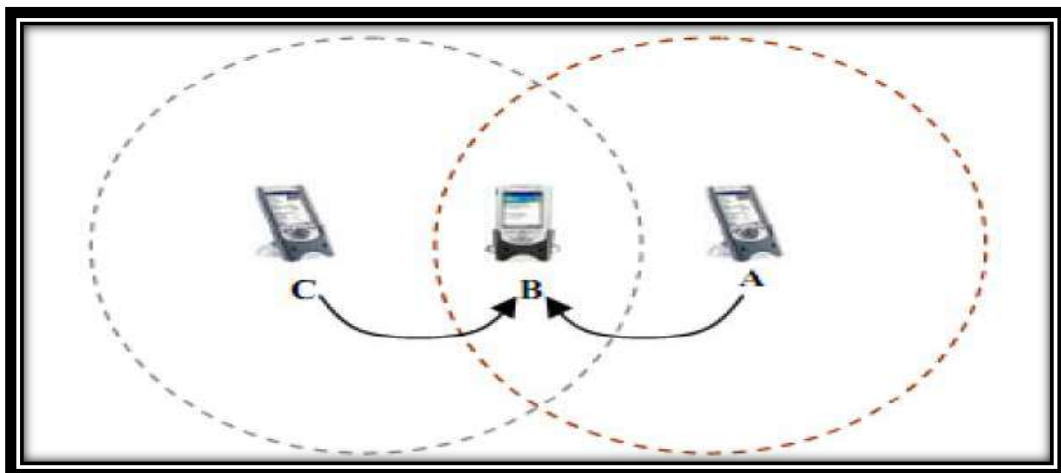


Figure II.3 : Problème de la station cachée [9]

Le protocole CSMA/CA utilise un mécanisme d'esquive de collision basé sur un principe d'accusés de réceptions réciproques entre l'émetteur et le récepteur. Lorsqu'une station souhaite communiquer avec le point d'accès, elle émet un RTS (Request To Send). A réception, le point d'accès émet un CTS (Clear To Send) à toutes les stations environnantes. La station ayant émis le RTS a donc le droit d'émettre ses données et toutes les autres stations sont prévenues qu'elles ne peuvent pas utiliser le médium pendant un certain laps de temps défini dans le RTS. Enfin, un acquittement (ACK) est envoyé par la station destination pour confirmer la bonne réception des données [6].

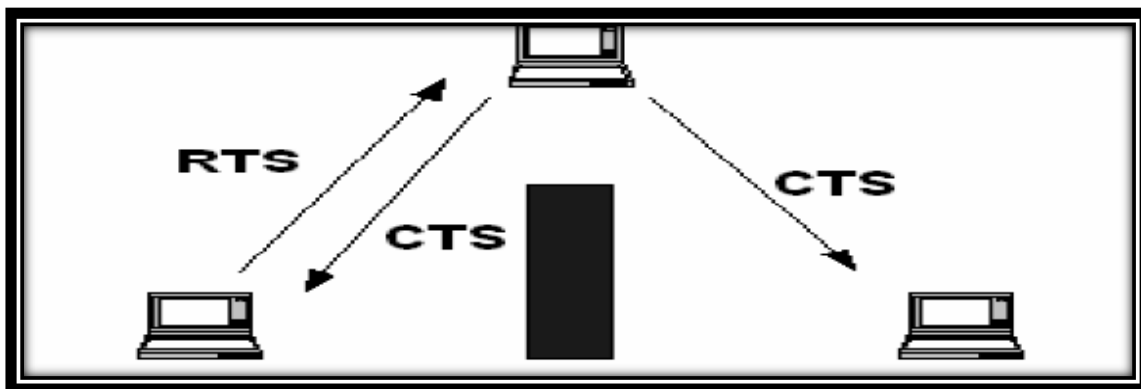


Fig II.4 : solution de problème de la station cachée

Cette solution ne permet pas d'éviter les collisions, mais les collisions de trames RTS/CTS sont moins consommatrices en bande passante que les collisions de données.

3.2.8. Problème de la station exposée

La figure suivante (Figure II.5) présente un scénario typique de ce problème. En effet, supposons que les deux stations A et C peuvent entendre les transmissions de B, mais que la station A n'entend pas C (et vice-versa). Supposons aussi que B est entrain d'envoyer des données vers A et que, au même moment, C veut communiquer avec D. Selon la technique CSMA, la station C va commencer par déterminer si le support est libre. A cause de la communication entre B et A, C trouve le support occupé et il retarde son envoie bien que celui-ci n'aurait pas causé de collision. [9]

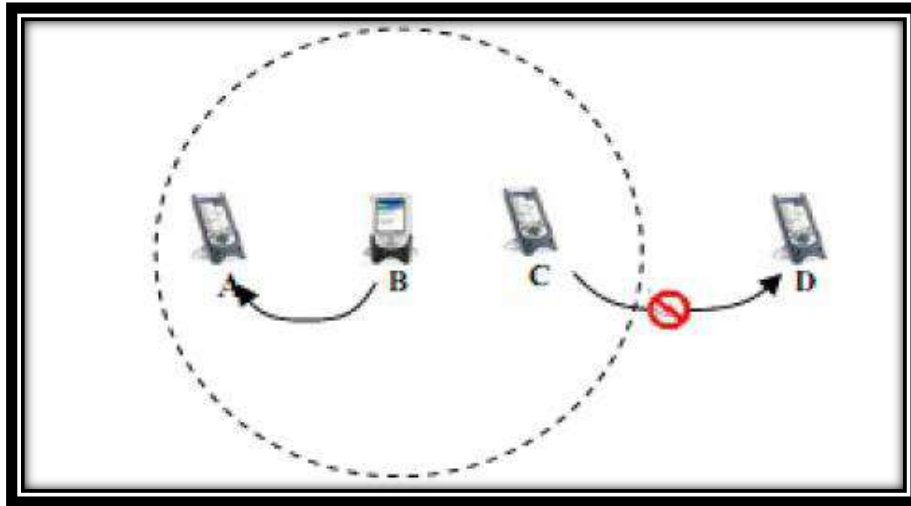


Figure II.5 : Problème de la station exposée [9]

3.3. Modèle de propagation radio

Le modèle de propagation représente une estimation de la puissance moyenne reçue du signal radio à une distance donnée d'un émetteur. La propagation du signal radio est généralement soumise à différents phénomènes : la réflexion, la diffraction et la dispersion par divers objets. Généralement, la puissance du signal reçue est de l'ordre de $1/d^n$, où d est la distance entre l'émetteur et le récepteur, n un exposant de perte d'un chemin [6].

3.4. Routage des données

Le routage dans les réseaux de capteurs est un routage multi-sauts. L'acheminement des paquets d'une source donnée à une destination se fait à travers plusieurs nœuds intermédiaires. Ainsi, un nœud consomme de l'énergie soit pour transmettre ces données ou pour relayer les données des autres nœuds. Dans ce contexte, une mauvaise politique de routage peut avoir des conséquences graves sur la durée de vie du réseau [6].

4. Techniques de minimisation de la consommation d'énergie

Après avoir fait une description des principales causes de consommation d'énergie dans les RCSF, nous allons présenter dans cette section une vue globale de différentes techniques utilisées pour minimiser cette consommation. [8]

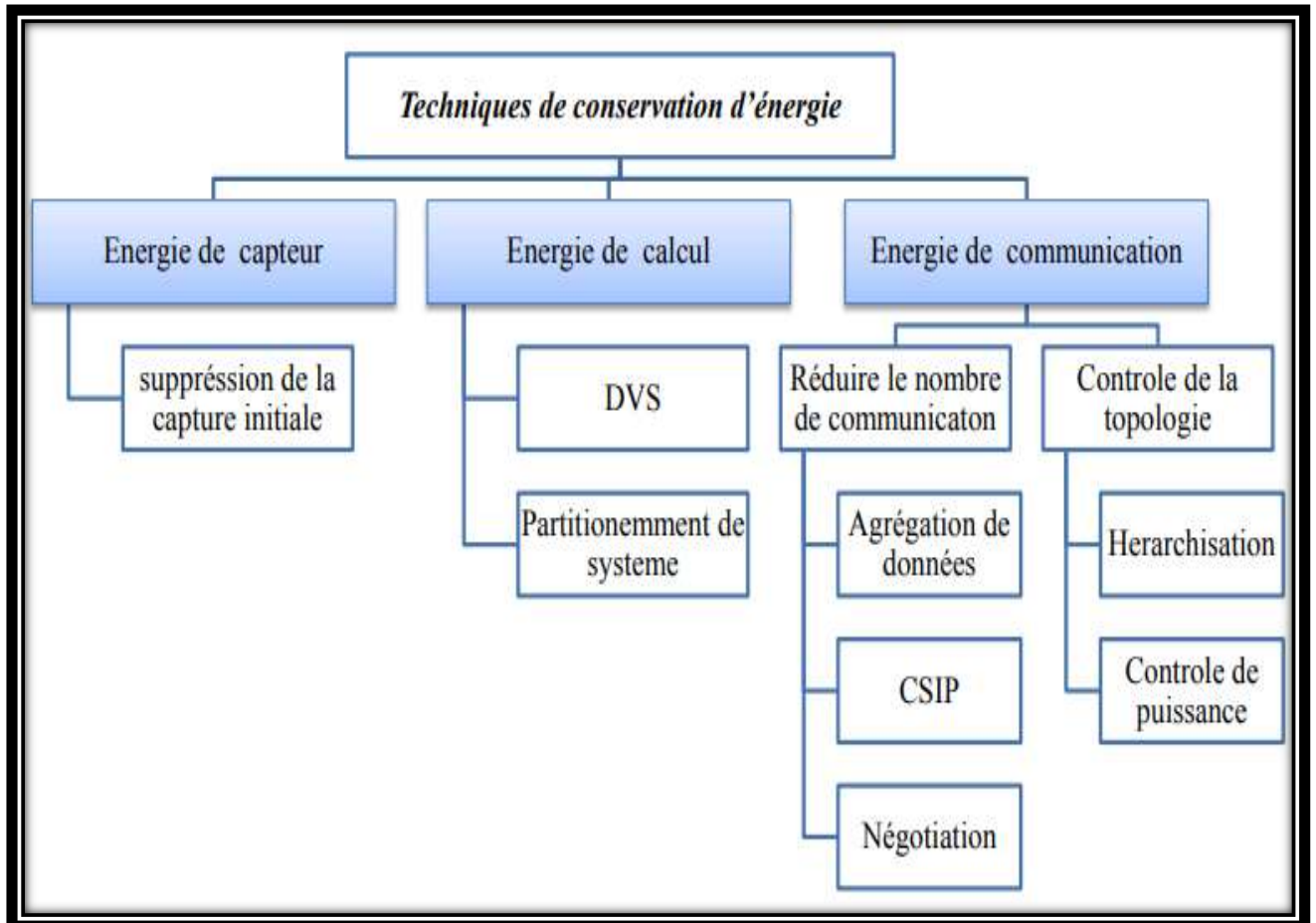


Fig II.6 : Les techniques de conservation d'énergie[8].

Comme indiqué précédemment l'énergie de capteur peut être économisée soit au niveau de capture, niveau de traitement ou au niveau de communication.

1) au niveau de capture

La seule solution apportée pour la minimisation de la consommation d'énergie au niveau de la capture consiste à réduire les durées de captures. [6]

2) Au niveau de traitement

L'énergie de calcul peut être optimisée en utilisant deux techniques :

- L'approche DVS (*Dynamique Voltage Scaling*), qui consiste à ajuster de manière adaptative la tension d'alimentation et la fréquence de microprocesseur pour économiser la puissance de calcul sans dégradation des performances.
- L'approche de partitionnement de système, qui consiste à transférer un calcul prohibitif en temps de calcul vers une station de base qui n'a pas de contraintes énergétiques et qui possède une grande capacité de calcul

3) Au niveau de communication

La minimisation de la consommation d'énergie pendant la communication est étroitement liée aux protocoles développés pour la couche réseau et la couche MAC. [8]

Ces protocoles se basent sur plusieurs techniques : agrégation de données, Négociation et CSIP (*Collaborative Signal and Information Processing*). Cette dernière technique est une discipline qui combine plusieurs domaines : la communication et le calcul à basse puissance, traitement de signal, algorithmes distribués et tolérance aux fautes, Systèmes adaptatifs et théorie de fusion des capteurs et des décisions. Ces techniques ont pour but de réduire le nombre d'émission/ réception des messages.

Par contre, le contrôle de la topologie permet l'ajustement de la puissance de transmission et le regroupement des nœuds capteurs (hiérarchisation).

- Le contrôle de la puissance de transmission n'a pas seulement un effet sur la durée de vie de la batterie d'un nœud capteur, mais aussi sur la capacité de charge du trafic qui est caractérisée par le nombre de paquets transmis avec succès vers une destination. En outre, il influe sur la connectivité et la gestion de la densité (le nombre de nœuds voisins). Ainsi, il peut conserver l'énergie à deux niveaux : explicitement par l'application de puissances faibles d'émissions et implicitement en réduisant la contention avec d'autres nœuds transmetteurs. Le module de contrôle de la puissance est souvent intégré dans les protocoles soit de la couche réseau soit de la couche MAC
- La hiérarchisation consiste à organiser le réseau en structure à plusieurs niveaux. C'est le cas, par exemple, des algorithmes de groupement (*clustering*), qui organisent le réseau en groupes (*clusters*) avec des chefs de

groupe (*cluster head*) et des nœuds membres.

- Une autre technique a été proposée dans [10]. Cette technique profite de la densité élevée des capteurs déployés pour se permettre d'endormir certains d'entre eux, afin que tous les capteurs ne soient pas actifs en même temps.

5. Conclusion

Dans ce chapitre, nous avons abordé la problématique de la consommation d'énergie dans les réseaux de capteurs sans fil. Par la suite, nous avons discuté également les facteurs de dissipation d'énergie dans ses réseaux. En dernier lieu, nous avons présentées une vue globale des solutions proposées pour la minimisation de la consommation d'énergie. Il est remarquable que cette consommation influe au durée de vie du nœud capteur, qui résulte une influence direct au durée de vie du réseau en global.

Dans le chapitre suivant, on va explorer certains protocoles de routage BLR, en décrivant leurs principes de fonctionnement de chacun d'eux.

Chapitre III : Protocoles de routage géographique BLR dans les RCSFs.

1. Introduction :

Le routage géographique est l'un des algorithmes de routage les plus efficaces et les plus évolutifs pour les réseaux de capteurs sans fil. Dans les protocoles de routage géographiques traditionnels, les nœuds échangent des informations de position périodiques (les beacons). Cela conduit à une utilisation inutile d'énergie et de bande passante. Des recherches récentes ont montré que ces beacons peuvent créer de graves problèmes en raison de la structure extrêmement dynamique des nœuds sans fil.

Dans ce chapitre, nous passons en revue certains des protocoles de routage géographique sans beacons BLR (beaconless) et le fonctionnement de base de chacun de ses derniers.

2. la norme IEEE 802.11

802.11 est une norme établie par l'IEEE. Elle décrit la couche physique et MAC d'interfaces réseau radio et infra-rouge [11].

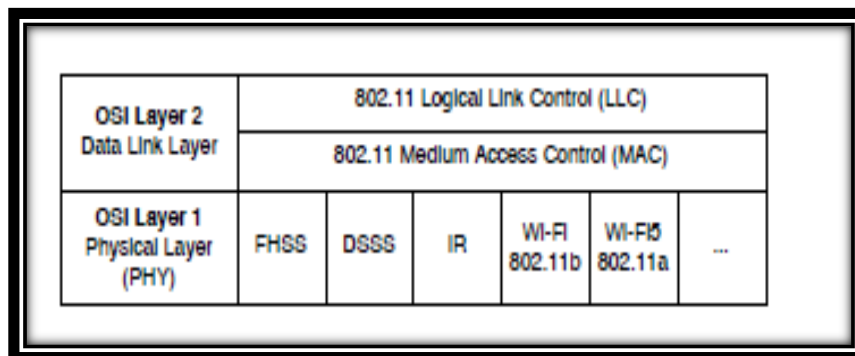


Figure III.1 : les différentes couches de la norme IEEE 802.11 [11]

2.1 La couche physique

Initialement, le standard IEEE 802.11 permet l'utilisation de trois couches physiques différentes (FHSS, DSSS et IR) [11].

2.2 La couche Mac

La couche MAC de 802.11 peut utiliser deux modes de fonctionnement. Distributed Coordination Fonction (DCF) est un mode qui peut être utilisé par tous les mobiles, et qui permet un accès équitable au canal radio sans aucune centralisation de la gestion de l'accès (mode totalement distribué). PCF dans la mesure où les mécanismes qu'il utilise sont fondamentaux dans 802.11 et que leur compréhension apporte à la compréhension globale du comportement de 802.11 [11].

2.2.1 Le mécanisme RTS/CTS

Nous avons vu que le mécanisme CSMA/CA cherche à éviter les collisions en écoutant l'activité sur le canal et en choisissant un délai aléatoire supplémentaire avant l'émission. Mais il existe une famille de configuration où ce mécanisme est insuffisant. Il s'agit du problème des nœuds cachés où deux émetteurs qui ne peuvent pas du tout s'entendre (en général à cause d'un obstacle) veulent atteindre un même récepteur. Comme dans cette configuration un émetteur ne détecte jamais l'activité de l'autre, il croit que le canal est toujours libre et émet dès qu'il a des données disponibles. Les chances de collisions à répétition au niveau du récepteur sont très élevées.[11]

802.11 propose un mécanisme utilisant des paquets de contrôle appelés Request To Send (RTS) et Clear To Send (CTS). Un mobile qui veut émettre ne va plus directement envoyer son gros paquet de données, mais plutôt un petit paquet RTS pour lequel les chances de collision sont plus faibles. A ce paquet RTS, le destinataire va répondre par un petit paquet CTS qu'il diffuse à tout son voisinage. Les paquets RTS et CTS contiennent des informations qui permettent de réserver le canal pour la durée de transmission de données qui vont suivre. Un mobile qui reçoit un CTS alors qu'il n'a pas envoyé (ni même détecté de RTS) sait que quelqu'un d'autre va émettre et doit donc attendre. Le mobile qui a envoyé le RTS sait, quand il reçoit le CTS correspondant, que le canal a été réservé pour lui et qu'il peut émettre. Au niveau des mobiles, la réservation du canal est implémentée grâce au Network Allocation Vector (NAV) [11].

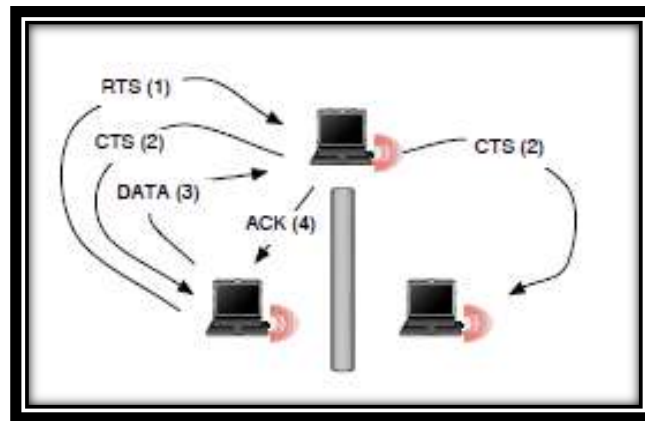


Figure III.2 :L'échange RTS/CTS

Dans chaque nœud, le NAV indique pour combien de temps le canal est utilisé par quelqu'un d'autre, indépendamment de ce qui est physiquement perçu sur le canal (on parle aussi de détection de porteuse logique). Sur la figure III.3 sont présentées les mises à jour du NAV au niveau d'un mobile alors qu'une trame est échangée entre deux autres mobiles. Lorsque le nœud non concerné par l'échange reçoit le RTS, il sait grâce aux informations contenues dans ce dernier pour combien de temps il ne devra pas accéder lui-même au canal. Les CTS et les paquets de données vont donc aussi devoir porter les informations de durée de NAV, afin que leur réception puisse mettre le NAV à jour [11].

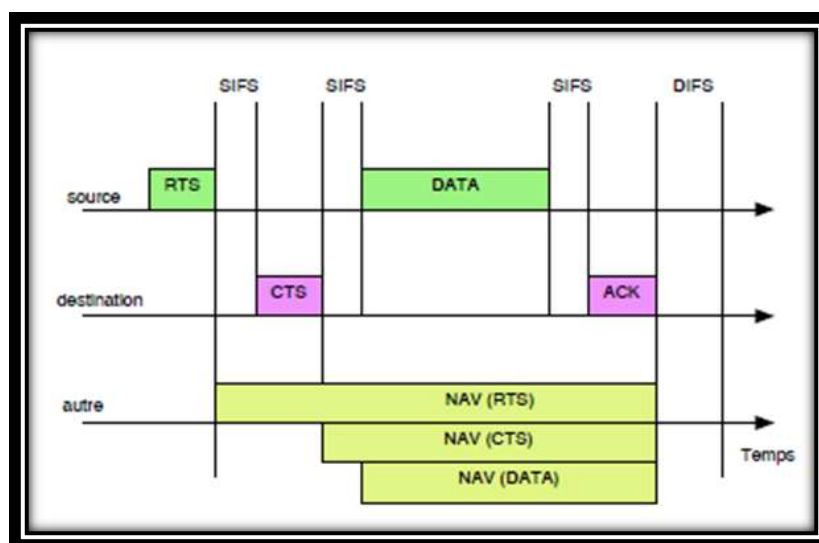


Figure III.3 : handshacke pour IEEE 802.11

Il faut noter que le temps de pause qui sépare un paquet de données de son acquittement est appelé SIFS (Short Inter-Frame Space) et qu'il est plus court que le DIFS. Le mobile en période de defering ne pourra reprendre la décrémentation de son backoff que si le canal est à nouveau libre pendant DIFS. Le fait que SIFS soit plus court empêche que la décrémentation ne reprenne de manière inopportune entre les données et leur acquittement [11].

Lorsque les données d'un mobile ont été acquittées et que DIFS s'est écoulé sans activité sur le canal, l'autre mobile peut reprendre la décrémentation de son backoff. Ici, aucun autre mobile ne vient l'empêcher de terminer et il peut donc finalement envoyer ses données [11].

3. Routage géographique avec beacons

Traditionnellement, le protocole de routage géographique utilise les informations du voisinage local contenues dans sa table de routage pour sélectionner le prochain saut du message lors des processus de routage. Cette information est accusée de façon proactive et périodique par chaque nœud à travers l'envoi d'un beacon pour annoncer sa présence dans le réseau ou dans le voisinage du récepteur. Le beacon contient l'identité et la position géographique des nœuds dans le réseau. À la réception d'un beacon, chaque nœud récepteur rajoute ou met à jour dans sa table de voisinage l'identité et la position géographique et déclenche pour la même occasion un temporisateur pour l'entrée du nœud dans la table. Lorsque ce temporisateur arrive à l'expiration, l'entrée du nœud est supprimée de la table de voisinage du nœud [12].

4. routage géographique sans beacons (beaconless)

Après avoir présenté le mécanisme de découverte du voisinage des protocoles de routage géographique avec beacon, dans cette section, nous présentons le principe de fonctionnement des protocoles de routage géographique sans beacons qui découvrent de manière réactive les prochains sauts des messages [12]. Ces approches ont été initialement proposées dans le but de pallier les problèmes liés à l'utilisation des beacons dans un environnement mobile. Ils utilisent les mêmes stratégies de

relayage que les approches avec beacons, à la différence près qu'ils n'utilisent pas les beacons périodiques pour acquérir les informations du 1-voisinage. La découverte du voisinage est faite uniquement à la demande à travers un mécanisme de contention sélective ou globale. Lorsqu'une source a une donnée à envoyer à une destination, la procédure de routage en mode glouton se base sur les étapes suivantes :

- **Diffusion de la donnée**

Il consiste initialement à diffuser dans son voisinage radio un message contenant la donnée comme dans BLR et CBF ou du contrôle à l'image des protocoles IGF, GeRaF et puis à armer un temporisateur d'attente maximale durant qu'il attend une éventuelle réémission du message ou de réponse de la part d'un de ses voisins. À la réception du message chaque nœud détermine en fonction de sa position et des informations contenues dans l'entête du message s'il peut prendre part à l'étape suivante. [12]

- **Armement d'un temporisateur de réémission**

Chaque nœud calcule un délai d'attente additionnel dont la valeur est inférieure ou égale à celle qui est déterminée par la source. Chaque nœud calcule son délai d'attente en fonction du progrès ou la distance à l'image des protocoles BLR, CBF, et GeRaF qu'il peut offrir au message de donnée. Il est aussi possible d'avoir une fonction de délai qui combine le progrès et l'énergie résiduelle à l'image du protocole IGF ou de privilégier des nœuds qui optimisent certains paramètres comme XLP. En effet, si c'est le progrès qui est le critère de choix, plus le progrès est important en termes de distance euclidienne, plus le délai d'attente de ce dernier est court. Pour une majorité de ces protocoles, le critère de choix porte essentiellement sur le progrès [12].

- **Sélection du prochain saut :**

Selon les protocoles, nous distinguons deux façon d'élire le prochain saut : par auto-élection avec transmission de la donnée ou par envoi d'un message de contrôle supplémentaire à la source pour notifier qu'on est candidat. Dans le premier cas de figure, lorsque le temporisateur du nœud ayant le plus court délai d'attente expire, ce nœud s'auto sélectionne comme prochain saut du message et rediffuse à son tour le message de donnée dans son voisinage. Lorsqu'un

nœud reçoit la rediffusion du message s'il a un temporisateur en attente, il arrête son temporisateur, puis repasse à la première étape. Dans le second cas, il s'ensuit une phase d'échanges de messages de contrôles à l'image du mécanisme de type 3-way handshake, le nœud répond par un message de contrôle. À la réception de ce message, la source stoppe son temporisateur de réémission et répond avec le message de donnée à ce dernier. [12]

5. Présentation de certains protocoles de routage BLR :

Dans cette section, nous allons présenter certains protocoles BLR. Tous ces derniers sont des protocoles cross-layer (Mac Routing) c'est à dire ils fonctionnent par le mécanisme de fusion du couches.

5.1 Protocole XLP (Cross-Layer Protocol):

XLP c'est le premier protocole qui intègre les fonctionnalités de toutes les couches (Physique→Transport), il était développé pour l'évaluation de performance de réseau en global, il est basé sur la notion de détermination d'initiative pour participer à la communication comme expliqué ci-dessous [13].

5.1.1 Détermination d'initiative :

Ceci est réalisé en diffusant paquet (RTS). À la réception de ce paquet, chaque voisin du nœud i décide de participer à la communication ou pas si son initiative est 1. Il est déterminé comme suit :

$$I_i = \begin{cases} 1, & \text{si } \left\{ \begin{array}{l} \xi_{RTS} \geq \xi_{Th} ; \lambda_{relay} \leq \lambda_{Th} \text{ relay } \beta \leq \beta_{max} ; E_{rem} \geq E_{min} \end{array} \right. \\ 0, & \text{autrement} \end{cases} \quad (1)$$

- ❖ . La première condition, c'est-à-dire $\xi_{RTS} \geq \xi_{Th}$, assure l'établissement de liens fiables pour la communication en fonction des conditions actuelles du canal.
- ❖ La deuxième condition empêche la congestion en limitant le trafic qu'un nœud peut relayer.

- ❖ La troisième condition garantit que le niveau d'occupation de la mémoire tampon d'un nœud, β , ne dépasse pas un seuil spécifique, β_{max} , de sorte que le nœud ne subit pas au débordement de tampon et la congestion est évitée
- ❖ . La dernière condition, c'est-à-dire $E_{rem} \geq E_{min}$, assure que le reste l'énergie d'un nœud E_{rem} reste au-dessus d'une valeur minimale, E_{min} . Cette contrainte permet de préserver une répartition uniforme de consommation d'énergie sur l'ensemble du réseau [13].

5.1.2 Initiation de la transmission :

Lorsqu'un nœud i a un paquet à transmettre, il écoute d'abord le canal pour une période de temps spécifique. Si le canal est occupé, le nœud effectue un backoff basé sur sa taille de la fenêtre de contention, CW_{RTS} . Lorsque le canal est inactif, le nœud diffuse un paquet RTS contenant les informations de localisation du nœud i et de station de base (SB) [13].

Lorsqu'un voisin du nœud i reçoit un paquet RTS, il vérifie d'abord les emplacements source et de destination. Nous nous référons à la région, où les voisins d'un nœud qui sont plus proches à la SB résident, comme la région de relayage et le reste quartier comme la région infaisable. Un nœud qui reçoit un paquet, vérifie d'abord s'il est dans la région réalisable. Pour économiser de l'énergie, les nœuds de la région infaisable s'endorment pour la durée de la communication. Les nœuds à l'intérieur de la région réalisable effectuent la détermination de l'initiative. Si un nœud décide de participer à la communication, il effectue la contention du récepteur comme expliqué ci-après [13].

5.1.3 Contention du destinataire

La contention du récepteur est basée sur le niveau de routage de chaque nœud, qui est déterminé en fonction de la progression d'un paquet aurait faire si le nœud transmet le paquet. La région réalisable est divisé en régions prioritaires N_p , c'est-à-dire A_i , $i = 1, \dots, N_p$. Nœuds avec des progrès plus longs ont une priorité plus élevée que les autres nœuds [13].

En fonction des informations de localisation, chaque nœud détermine sa région prioritaire et effectue la contention pour l'accès au support comme expliqué ensuite. Chaque région prioritaire, A_i , correspond à une fenêtre de taille, CW_i . En fonction de son emplacement, un nœud recule pour $\sum_{j=1}^{i-1} CW_j + c_{wi}$, où c_{wi} est choisi aléatoirement de telle sorte que $c_{wi} \in [0, CW_i]$ [13].

Le gagnant envoie un paquet CTS au nœud i indiquant qu'il va acheminer le paquet.

Il peut arriver que plusieurs paquets CTS provenant de la même région prioritaire puissent entrer en collision et un nœud d'un niveau inférieur la région prioritaire peut être sélectionné. XLP n'essaie pas

de résoudre ce problème que cette probabilité est très faible car la région faisable est déjà divisée en plusieurs régions et le coût de essayer de résoudre ce problème l'emporte sur les gains.

Dans certains cas ou qu'il n'est pas possible de trouver des nœuds plus proches de l'évier que le nœud lui-même, le nœud passe à mode de routage basé sur l'angle comme expliqué ci-après [13].

5.1.4 Routage basé sur l'angle :

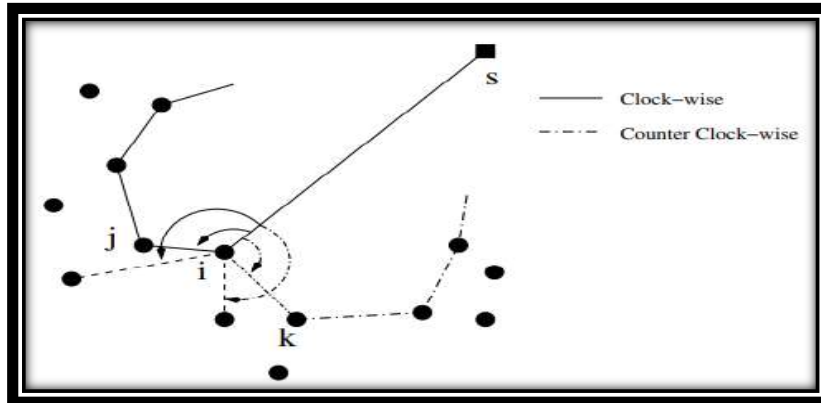


Fig III.4. : Routage basé sur l'angle

Le principe de base du routage basé sur l'angle peut être vu sur la Fig. 2. Quand un paquet atteint le nœud i , qui est en face un vide vers la SB, le paquet doit être acheminé autour du vide soit dans le sens des aiguilles d'une montre (via le nœud j), soit dans le sens antihoraire (à travers le nœud k). Assumer que des lignes sont tracées entre le nœud i et le puits, s , comme ainsi qu'entre le nœud i et ses voisins. Si on compare l'angle entre la ligne i, s et les autres lignes, l'angle S_{ij} (angle sik) a le plus petit angle dans le sens inverse des aiguilles d'une montre (sens des aiguilles d'une montre) direction de routage. [13]

5.2 Protocole IGF(Implicit Geographic Forwarding) :

IGF de Blum & al, est le premier protocole de routage géographique sans beacons. Le routage est utilisé sur une zone restreinte en forme de secteur d'un angle de 30° dans la direction du destinataire. La zone est dimensionnée de telle sorte que toute transmission à l'intérieur de la zone est bien reçue par tous les nœuds de la zone sous les hypothèses d'un canal radio idéal. Cela permet d'éviter la duplication de paquets [12].

ce protocole améliore le processus de prise de décision en intégrant une distance accrue vers la métrique de destination (IDTD) et d'énergie restante (ER) dans le processus de sélection d'itinéraire [14].

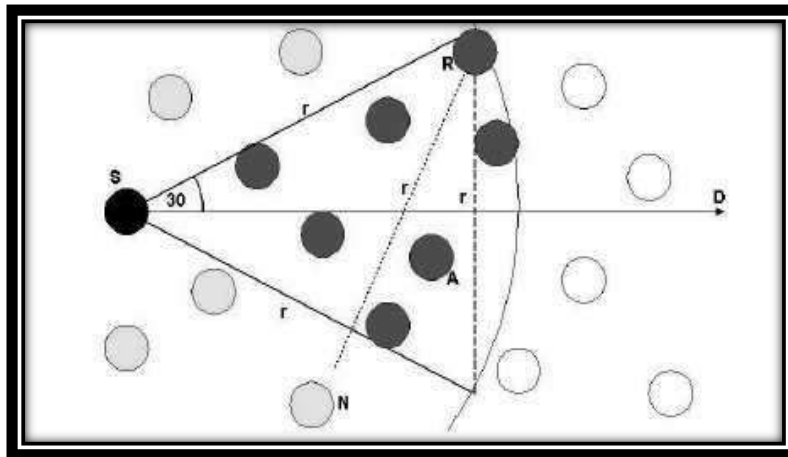


Fig III.5 : Secteur de symétrie : Zone de relayage dans IGF

Handshake IGF :

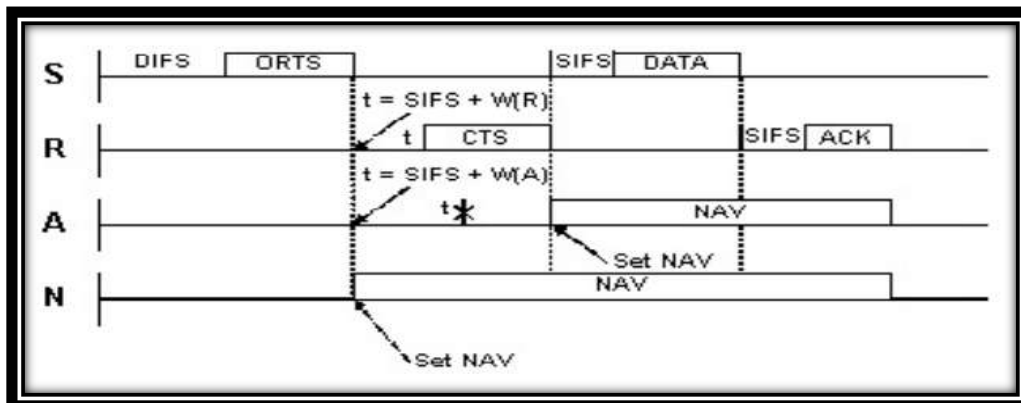


Figure III.6 : Handshake IGF

La prise de contact IGF commence lorsque la minuterie NAV de l'émetteur S est à zéro et que la porteuse détecte un canal inactif pendant le temps DIFS.

Après avoir validé que le canal est libre, S envoie, par diffusion, ce que nous appelons Open RTS(ORTS).

Bien que tous les nœuds situés dans le rayon de communication de S reçoivent et traitent cette demande d'envoi, seuls nœuds voisins (R et A), dans la zone de transmission restreinte, définissent un CTS_Response timer (t) qui définit une durée appropriée qui doit être s'écouler avant de répondre au message ORTS reçu. [14]

La valeur de cette minuterie dépend de l'augmentation de la distance vers la destination,

l'énergie restante au récepteur potentiel et une valeur aléatoire supplémentaire.

Tous les nœuds recevant les ORTS qui sont en dehors de cette zone de transfert (N) définissent leur minuterie NAV conformément à la sémantique 802.11. Nous appelons les nœuds dans cette zone de transfert, nœuds candidats. Tous les nœuds candidats définissent leur temporisateur CTS_Response, un seul nœud, spécifiquement le nœud qui attribue la valeur temporelle la plus courte (R) répondra à l'ORTS [14].

Pour prévenir les réponses multiples, les nœuds candidats entendant une réponse CTS annuleront leurs minuterias et régleront leurs minuterias appropriées de NAV. En outre, l'expéditeur S, ayant déjà reçu un CTS valide, ne sera plus accusé des autres messages CTS entendus en réponse à la requête ORTS, désormais obsolète. Ayant isolé un canal de communication avec un récepteur spécifique, l'expéditeur répond au CTS reçu et la communication se poursuit, également conformément à la sémantique 802.11 DCF (CTS-> DATA-> ACK).

Les nœuds voisins qui reçoivent un ORTS, mais ne sont pas dans la plage définie zone de transfert, il suffit de régler leur minuterie NAV pour refléter la durée de la communication. Cela empêche plus tard les collisions résultant d'effets terminaux cachés.[14]

5.3 Protocole SIF (State free Implicit Forwarding):

Le protocole SIF suppose une densité de nœud modérée et une conscience de la distance jusqu'au puits [15].

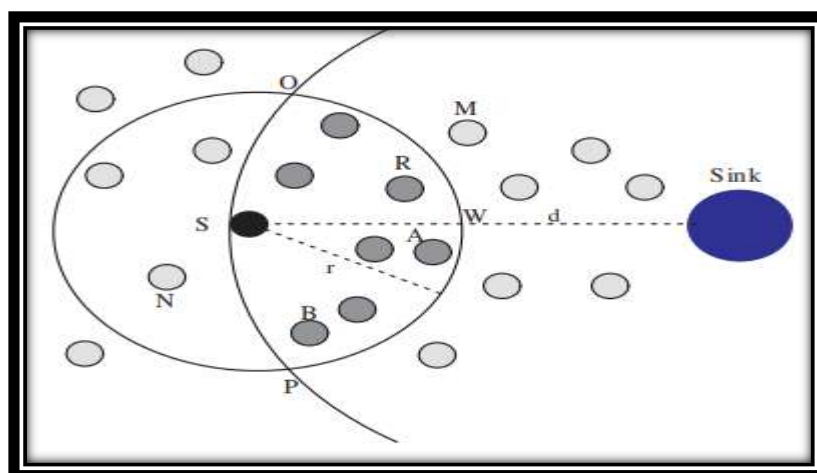


Figure III.7 : Zone de relayage dans SIF [15]

La zone de transfert est définie comme la zone où les nœuds de transmission résident. La figure 1 illustre cette zone en SIF. Le cercle représente le rayon de transmission de l'émetteur S. L'arc est centré sur la SB et avec un rayon de d, la distance entre l'expéditeur et le collecteur de données. Tout capteur dans cette région de chevauchement, OSPW a une distance plus courte que l'expéditeur S et devient un candidat de transfert pour l'expéditeur S [15].

La distribution du capteur dans la région d'intérêt peut être modélisée comme un processus de Poisson à deux dimensions. Ainsi, la probabilité que k capteurs soient situés dans une zone de taille A est donnée par :

$$P(k) = \frac{(\lambda A)^k \times e^{-\lambda A}}{k!} \quad (2)$$

où λ est le nombre attendu de capteurs dans une unité de surface. Soit D une variable aléatoire correspondant à d sur la figure 2, c'est-à-dire que D représente la distance entre l'émetteur S et la SB. [15]

Handshake SIF :

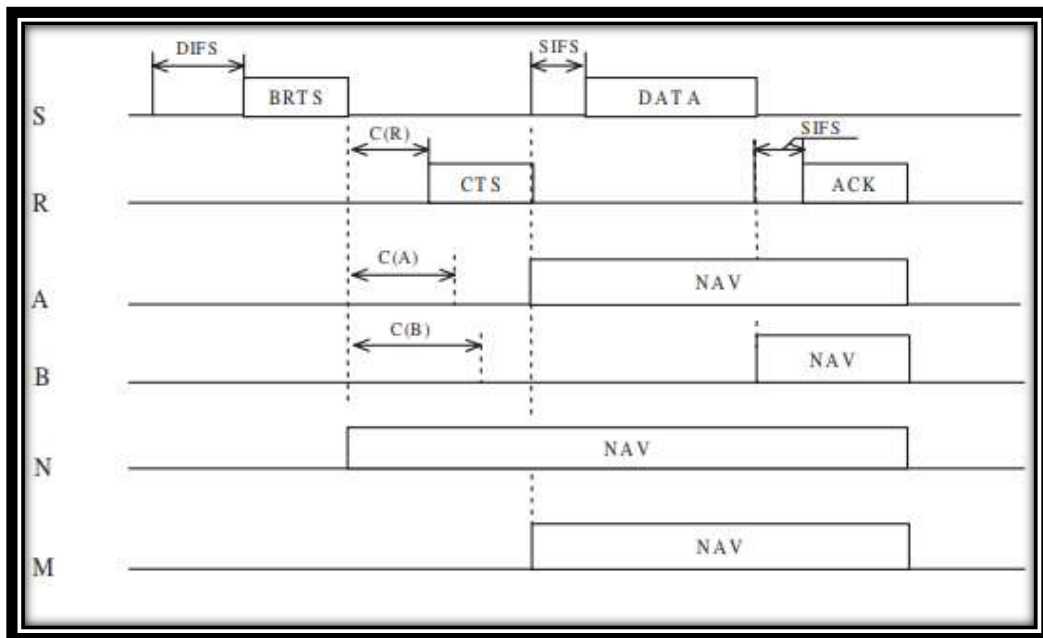


Figure III.8 : handshacke SIF.

La figure III.8 décrit le processus d'échange des messages dans SIF. L'expéditeur S qui veut envoyer un paquet de données écoute le canal physiquement et virtuellement.

Si le support est déterminé à être libre pour un espace DIFS (DCF Interframe Space), l'expéditeur S envoie une diffusion RTS (BRTS) à tous les voisins de son rayon de transmission[15].

Sinon, le protocole obéit à la norme IEEE802.11 et diffère sa transmission. L'information de distance-to-sink de l'expéditeur S est incluse dans le BRTS, les capteurs recevant le paquet BRTS compareront ses distances au puits avec celle de l'expéditeur valeur annoncée. Les capteurs avec une plus petite distance, tels que les capteurs R, A et B, seront automatiquement devenir les candidats d'acheminement [15].

Chaque candidat établit un temporisateur qui définit un laps de temps (appelé temps de réponse en concurrence) correspondant qui doit être expiré avant de répondre au paquet BRTS. L'émetteur S envoie ensuite son paquet de données en unicast au capteur R. Le capteur R récupère le paquet de données et répond avec un ACK pour indiquer la fin de cette étape. Le processus décrit ci-dessus est répété chaque fois qu'un paquet de données doit être transmis au SB [15].

Pour éviter plusieurs réponses CTS, chaque candidat à la transmission écoute le canal pour détecter toute transmission au cours de leur temps d'attente [15].

Un problème potentiel du schéma SIF c'est la duplication des paquets de données. En fait, si le paquet ACK est perdu, le capteur de transfert a déjà reçu le paquet de données alors que la source n'est pas au courant de la réussite de la transmission [15].

Il sera très difficile de détecter et éliminer ces doublons, car les capteurs de transfert ne conservent aucun état /enregistrement pour les paquets transférés et la retransmission peuvent employer un autre capteur d'expédition qui n'est pas au courant de la transmission réussie [15].

5.4 Protocole CBF (Contention Based Forwarding)

L'idée générale de CBF est de baser la décision de transmission sur l'état de voisinage tel qu'il est actuellement comme il existe dans la réalité et non pas comme le perçoit le nœud de relayage, il fonctionne en trois étapes :

Premièrement, Le nœud source transmet le paquet sous forme de diffusion à un seul saut à tous les voisins [16].

Deuxièmement, les voisins en concurrence les uns avec les autres pour le «droit» de relayer le paquet. Pendant cette période de contention, un nœud détermine à quel point il convient comme saut suivant pour ce paquet [16].

Troisièmement, le nœud qui gagne la contention supprime les autres nœuds et établit ainsi lui-même comme le prochain nœud source. Dans la suite, nous décrivons en détail comment la contention peut être réalisée sur la base de biais minuteriers [16].

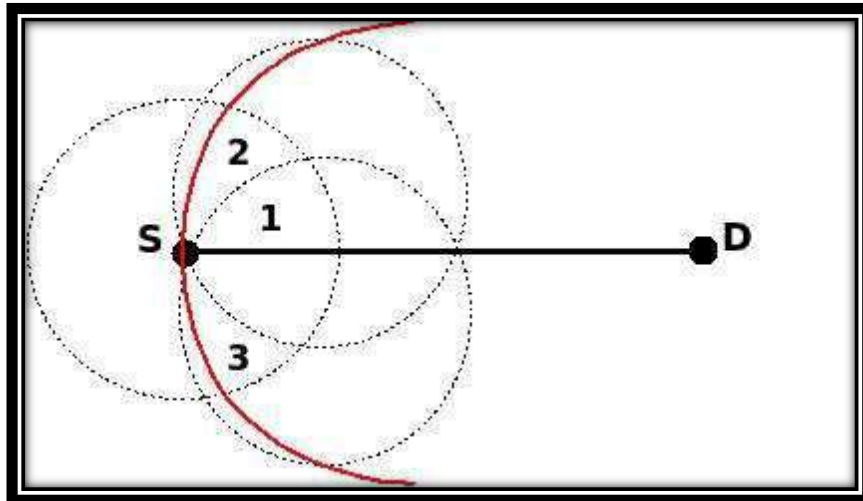


Figure III.9 : Zone de relayage du protocole CBF [12]

5.4.1 Contention basé sur la minuterie

Une approche standard pour la sélection décentralisée d'un nœud est par moyens de temporisateur. Dans sa forme la plus simple, la contention basée sur un temporisateur nécessite que chaque nœud définisse un temporisateur avec une valeur aléatoire. Une fois le premier temporisateur expire, le nœud correspondant répond. Les minuteriers de tous les autres nœuds sont annulés et leurs réponses sont supprimées [16].

Il est important de se rendre compte qu'avec cet algorithme de contention plus d'un nœud peut répondre, même si un bon mécanisme de suppression est utilisé. Le problème de la contention simple basé sur un temporisateur est que tous les nœuds qui sont situés plus près de la destination que le nœud source sont traités équitablement. Ainsi, un nœud fournissant un minimum de progrès aurait la même chance d'être sélectionné comme saut suivant comme un nœud fournissant un grand progrès. Les auteurs de [16] proposent donc de déterminer les valeurs pour les temporisateurs en fonction de combien de progrès un nœud fournit vers la

destination au lieu de déterminer au hasard. Pour minimiser le nombre de sauts, la progression P est définie comme :

$$P(f, z, n) = \max \left\{ 0, \frac{\text{dist}(f,z) - \text{dist}(n,z)}{r_{\text{radio}}} \right\} \quad (3)$$

Étant donné que f est la position de la source, z la position de la destination (la SB) et n la position du nœud voisin candidat. dist est défini comme la distance euclidien entre deux positions et r_{radio} est rayon de transmission [16].

La Fig. 1 illustre l'adéquation d'un nœud à être le saut suivant en fonction de son emplacement. Une valeur de progrès (P) = 0 indique qu'un nœud n'est pas approprié alors qu'une valeur 1 est optimale et elle est atteinte si le nœud est situé à l'intersection du cercle délimitant le rayon de transmission du nœud source et la ligne reliant la source et la destination. Ainsi, P augmente linéairement de 0 à 1 avec le progrès qu'un nœud puisse fournir pour le paquet.[16]

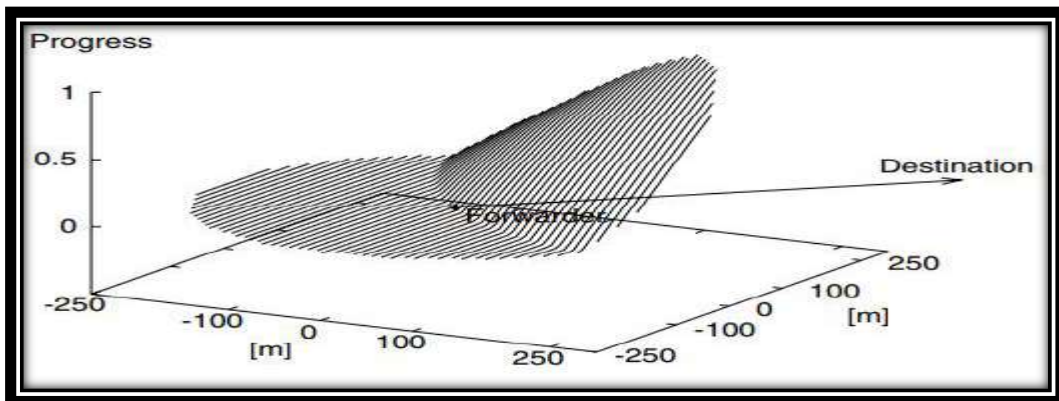


Figure III.10 : Progression du paquet (plage de transmission 250 m [16])

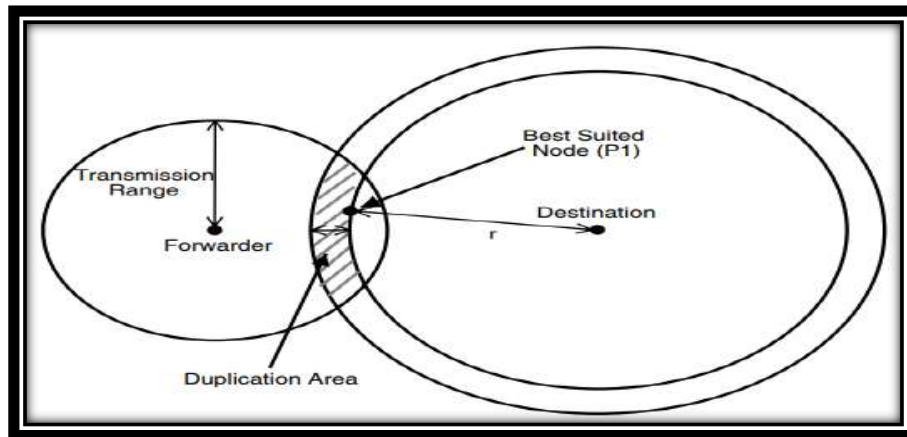


Figure III.11 : Zone de duplication. [16]

Une propriété intéressante de la zone de duplication est qu'elle devient plus petite en se rapprochant vers la destination.

5.4.2 Suppression :

Supposons maintenant que tous les voisins du nœud source défini leur temporisateur de contention en fonction de leurs distances respectives à la destination. Après l'expiration du premier de ces temporisateurs, un algorithme de suppression vise à annuler les temporisateurs tous les autres nœuds pour éviter la duplication de paquets [16].

5.4.2.1 Schéma de suppression de base :

Le mécanisme de suppression le plus fondamental concevable fonctionne comme suit : si le temporisateur d'un nœud expire, le nœud suppose qu'il est le prochain saut et diffuse le paquet. Quand un autre nœud reçoit cette émission et a toujours son temporisateur en marche pour le paquet, le temporisateur est annulé et le nœud ne transmettra pas le paquet [16].

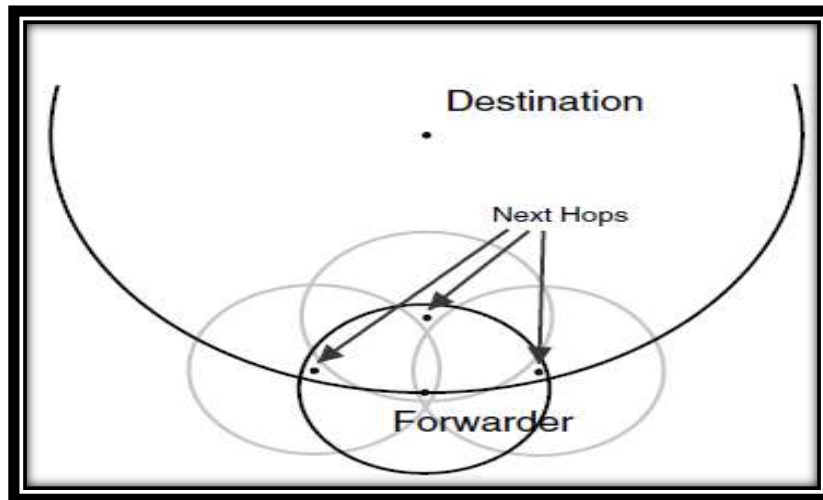


Figure III.12 : duplication des paquets dans le schéma de base [16]

5.4.2.2 Suppression par zone :

Afin d'éviter les duplications de paquets supplémentaires du schéma de suppression de base, nous proposons de réduire artificiellement la zone à partir de laquelle le prochain saut est sélectionné. Nous appelons cette zone réduite la zone de suppression et l'algorithme de suppression basée sur la zone. L'idée clé est de choisir la zone de suppression telle que tous les nœuds de cette zone sont dans le rayon de transmission les uns des autres, en évitant les duplications de paquets supplémentaires ils peuvent apparaître dans le schéma de suppression de base [16].

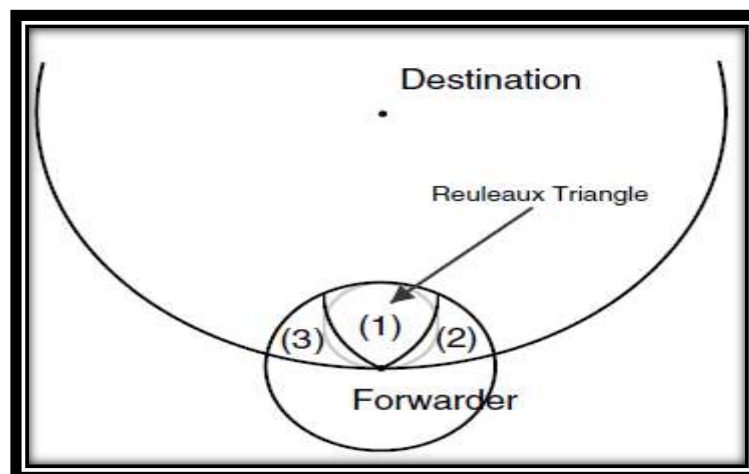


Figure III.13 : Zones d'acheminement [16]

Il y en a d'autre algorithme de suppression, cependant nous n'avons présenté que ces deux stratégies juste pour mieux comprendre ces algorithmes [16].

5.5 Protocole GeRaF (Geographic Random Forwarding)

Considérons un schéma qui utilise l'écoute du canal avant transmission, ce qui évite en partie les collisions mais ne donne aucune garantie contre le problème de terminal caché. Remarquez que le fait que les nœuds ne soient pas toujours allumés rend les mécanismes traditionnels d'évitement de collision basés sur RTS / CTS inefficaces puisque un nœud peut se réveiller après l'émission de la CTS [17].

La solution que les auteurs de [17] ont adoptée est l'utilisation de busy tones (tonalités d'occupation) car ils existent des nœuds de capteurs équipés de deux radios [22].

Plus précisément, dans la première fréquence (fréquence «données»), tous les échanges de messages ont lieu, alors que la deuxième fréquence (fréquence «tonalité d'occupation») est utilisée uniquement pour les busy tones [17].

Lorsqu'un nœud doit envoyer un paquet, il écoute les deux fréquences. Si l'un ou l'autre est actif, le nœud se désactive. Si les deux sont inactifs, le nœud transmet.

La fonction de prévention des collisions de ce schéma est basée sur l'échange de messages RTS / CTS. Cependant, contrairement au message RTS traditionnel qui est adressé à un nœud spécifique, dans ce cas, tout nœud au sein du rayon de transmission peut y répondre, en privilégiant les nœuds les plus proches de la SB. Par conséquent, le message CTS est également sujet à conflit puisque plusieurs nœuds peuvent décider de répondre au même RTS en même temps. La délivrance des messages CTS en réponse à un RTS est faite dans une telle manière à donner la priorité aux nœuds qui fournissent un plus grand avancement vers la destination finale, comme détaillé au-dessous [17].

5.5.1 Emetteur :

Lorsqu'un nœud en veille a un paquet à envoyer, il entre dans l'état actif et surveille les deux fréquences pendant τ secondes [17].

Si l'une des fréquences soit occupée, le nœud annule et ressayera plus tard.

Dans le cas où les deux fréquences sont perçues inactifs pendant cet intervalle, le nœud diffuse un message RTS qui contient en plus des informations de son emplacement, la localisation de la destination finale du paquet [17].

Pendant le processus de contention le nœud source réagit comme suivant :

1. Si un seul message CTS est reçu, il commence la transmission du paquet de données dont la partie initiale agit comme une confirmation CTS pour le nœud qui a émis la CTS.

2. S'il ne reçoit aucun CTS, il envoie un message CONTINUER et écoute à nouveau pour les CTS
3. S'il entend un signal mais il est incapable de détecter un message significatif, il supposera qu'une collision CTS a eu lieu et envoie un message COLLISION qui déclenchera le début d'un algorithme de résolution de la collision.

Après la transmission du paquet, si un ACK est reçu la transaction est terminée. Sinon, il déclare que la transaction a échoué et planifier le paquet pour la retransmission.

Pendant la réception du CTS et de l'ACK, le nœud transmet la tonalité d'occupation pour éviter les interférences de terminaux cachés [17].

5.5.2 Récepteur :

Chaque nœud sera (plus ou moins) périodiquement réveillé et mis lui-même en mode d'écoute. Si rien ne se passe tout au long du temps d'écoute, dont la durée peut être fixe ou aléatoire, le nœud se rendort. Par contre, si le nœud détecte le début d'une transmission, il passe dans l'état de réception [17].

Lors de la détection du début d'un message, un nœud en état d'écoute commence à recevoir. En même temps, il active la tonalité d'occupation sur la fréquence de tonalité d'occupation pendant une durée TRTS.

Si aucune RTS n'est reçu, le nœud revient à l'état d'écoute, où il reste pour la durée initialement prévue.

Sur l'autre part, si un RTS valide est reçu, le nœud lit les informations qu'il contient et détermine sa propre priorité en tant que relais. Cette priorité est basée sur l'emplacement relatif du nœud lui-même par rapport à la distance entre l'émetteur et la destination finale prévue [17].

5.6 Protocole BLR (Beacon-Less Routing Protocol)

Le protocole BLR fonctionne comme suit : Si un nœud source doit envoyer un paquet de données, il détermine la position de la destination et stocke les coordonnées géographiques avec sa propre position dans l'en-tête du paquet. Tous les nœuds intermédiaires remplacent simplement la position du nœud précédent par leur position actuelle dans l'en-tête avant de transmettre le paquet [18].

Puisqu'un nœud ne possède pas la connaissance des voisins, il diffuse le paquet à tous les nœuds voisins. À la réception d'un paquet, la seule information disponible qu'un nœud intermédiaire possède sa propre position et la position du nœud précédent et du nœud de destination, issues

de l'en-tête du paquet. Ainsi, un nœud peut facilement déterminer si il est situé dans une zone spécifique par rapport au nœud précédent [18].

Les nœuds situés dans la zone de transfert appliquent DFD avant de relayer le paquet, alors que les nœuds en dehors de cette zone suppriment le paquet reçu.

La valeur du DFD $[0, \text{Max_Delay}]$ dépend des positions géographiques du nœud courant, nœud précédent et de la destination finale. Finalement, le nœud qui a calculé le plus court DFD transmet le paquet en premier. Chaque nœud de la zone de transfert peut détecter le relayage du paquet et annule sa planification de transmission du même paquet [18].

Le nœud précédent détecte également le relayage ultérieur du paquet et conclut donc qu'il a été reçu avec succès par un autre nœud. L'algorithme continue jusqu'à ce que la destination soit atteinte.

Le seul nœud qui doit envoyer un accusé de réception est le nœud de destination car il ne transmet pas le paquet plus loin. Pour faire face aux imprécisions de position de la position de destination, un protocole réactif adapté et restreint basé sur l'AODV s'applique au voisinage de la destination [18].

6. Conclusion :

Dans ce chapitre, nous avons présenté certains protocoles de routage géographiques sans beacons.

Après avoir introduit le fonctionnement de certains protocoles BLR, nous remarquons que ces derniers réaliser une mieux performance en fonction d'énergie.

Dans le chapitre prochain, nous allons évaluer la performance de certains protocoles BLR.

*Chapitre IV : Evaluation de
performance de certains protocoles
BLR.*

1. Introduction :

Dans le chapitre précédent, nous avons présentée quelque protocoles de routage géographique BLR c'est que notre sujet d'étude dans ce projet.

Dans ce chapitre, nous allons évaluer les performances de certains de ces protocoles.

Pour ce faire, nous avons choisi d'utiliser OMNet ++ [20] avec le simulateur Castalia [21]. Nous avons pu obtenir plusieurs résultats dans différentes conditions d'environnement de simulation.

2. Généralité sur la simulation

La simulation consiste à la modélisation informatique d'un système quelconque, en offrant une représentation de toutes les entités de ce système, leurs comportements propres, ainsi que leurs interactions. Elle met à la disposition de l'utilisateur un environnement d'expérimentation dont on peut faire varier les paramètres [19].

2.1 Types de simulation

En fonction du type d'évènements dans la simulation, nous distinguons deux types de systèmes de simulation : les systèmes discrets et les systèmes continus [19].

2.1.1 Systèmes de simulation discrète

Sont des systèmes pour lesquels les variables concernées par la simulation ne changent d'état qu'en un nombre fini de points sur l'axe du temps. On appelle également ces systèmes : systèmes de simulation à évènements discrets [19].

2.1.2 Systèmes de simulation continue

Ce sont des systèmes pour lesquels les variables peuvent changer d'état à n'importe quel instant pendant la simulation [19].

3. Le simulateur OMNeT ++

OMNeT ++ est un framework de simulation de réseau à événements discrets modulaire et orienté objet. Il a une architecture générique, il peut donc être (et a été) utilisé dans divers domaines problématiques:

- modélisation des réseaux de communication filaires et sans fil
- modélisation de protocole
- modélisation des réseaux de files d'attente
- modélisation de multiprocesseurs et d'autres systèmes matériels distribués
- validation des architectures matérielles
- évaluer les aspects de performance des systèmes logiciels complexes
- en général, la modélisation et la simulation de tout système où l'approche par événements discrets convient et peut être facilement mappée aux entités qui communiquent en échangeant des messages [20].

OMNeT ++ n'est pas un simulateur concret, mais une infrastructure et des outils pour l'écriture de simulations. L'un des ingrédients fondamentaux de cette infrastructure est une architecture de composants pour les modèles de simulation. Les modèles sont assemblés à partir de composants réutilisables appelés modules. Les modules bien écrits sont vraiment réutilisables et peuvent être combinés de différentes manières, comme des blocs LEGO [20].

Les simulations OMNeT ++ peuvent être exécutées sous différentes interfaces utilisateur. Les interfaces utilisateur graphiques et animantes sont très utiles à des fins de démonstration et de débogage, et les interfaces utilisateur en ligne de commande conviennent mieux à l'exécution par lots [20].

3.1 Concepts de modélisation OMNeT ++

Un modèle OMNeT ++ est constitué de modules qui communiquent avec le passage de messages. Les modules actifs sont appelés modules simples ; ils sont écrits en C ++, à l'aide de la bibliothèque de classes de simulation. Les modules simples peuvent être regroupés en modules composés, etc. le nombre de niveaux hiérarchiques

est illimité. L'ensemble du modèle, appelé réseau dans OMNeT ++, est lui-même un module composé. Les messages peuvent être envoyés via des connexions couvrant plusieurs modules ou directement vers d'autres modules. Le concept de modules simples et composés est similaire aux modèles atomiques et couplés de DEVS [20].

Dans la figure ci-dessous, les rectangles représentent des modules simples (fond gris) et des modules composés. Les flèches reliant les petites cases représentent les connexions et les portes [20].

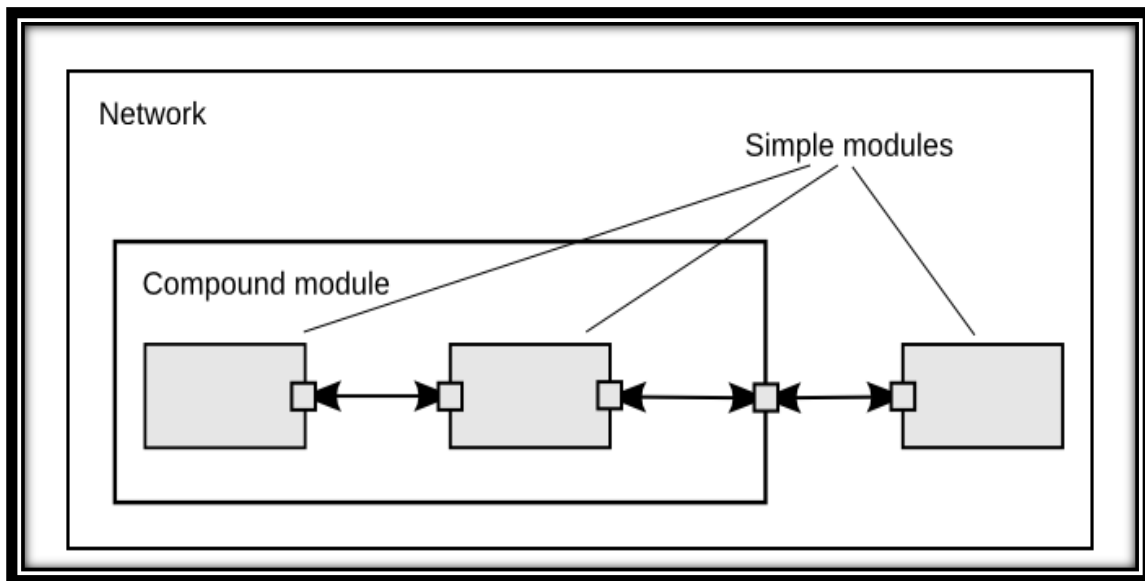


Figure IV.1 : Modules simples et composés [20].

3.2 Les principaux fichiers d'OMNET++

Le simulateur Omnet++ est composé par des fichiers qui définissent la structure du réseau en global [19].

Fichier (.Ned):

Utilise le langage NED de description de réseau. Il peut être utilisé en 2 modes : Mode Graphique ou Mode Texte qui permettent de décrire les paramètres et les ports du module. Les erreurs commise sont indiquées en temps réel par un point rouge situé à la gauche du code [19].

Fichier (.ini):

Est lié étroitement avec le fichier NED. Permet à l'utilisateur

d'initialisé les paramètres des différents modules ainsi la topologie du réseau[19]

Fichier (.msg):

Les modules communiquent en échangeant des messages. Ces derniers peuvent être déclarés dans un fichier dont l'extension est (.msg) où l'on peut ajouter des champs de données. OMNeT++ traduira les définitions de messages en classes C++ [19].

4. Le plateforme d'OMNET ++ Castalia

Castalia est un simulateur pour les réseaux de capteurs sans fil (WSN), les réseaux de capteurs corporelle (BAN) et plus généralement pour les réseaux de périphériques intégrés à faible consommation. Il est basé sur la plate-forme OMNeT++ et peut être utilisé par les chercheurs et les développeurs souhaitant tester leurs algorithmes et / ou protocoles distribués dans des modèles de canaux et radio sans fil réalistes, avec un comportement de noeud réaliste, notamment en ce qui concerne l'accès à la radio. Castalia peut également être utilisé pour évaluer différentes caractéristiques de plate-forme pour des applications spécifiques, car il est hautement paramétrique et peut simuler une large gamme de plates-formes [21].

Castalia a été conçu dès le départ pour permettre aux utilisateurs d'implémenter / importer facilement leurs algorithmes et protocoles dans Castalia, tout en exploitant les fonctions fournies par le simulateur. Modularisation appropriée et configurable, procédure de construction automatisée aide à cette fin. La modularité, la fiabilité et la rapidité de Castalia sont en partie rendues possibles par OMNeT++, un excellent cadre pour la construction de simulateurs pilotés par les événements [21].

La structure de module de base de Castalia est illustrée dans le schéma ci- dessous :

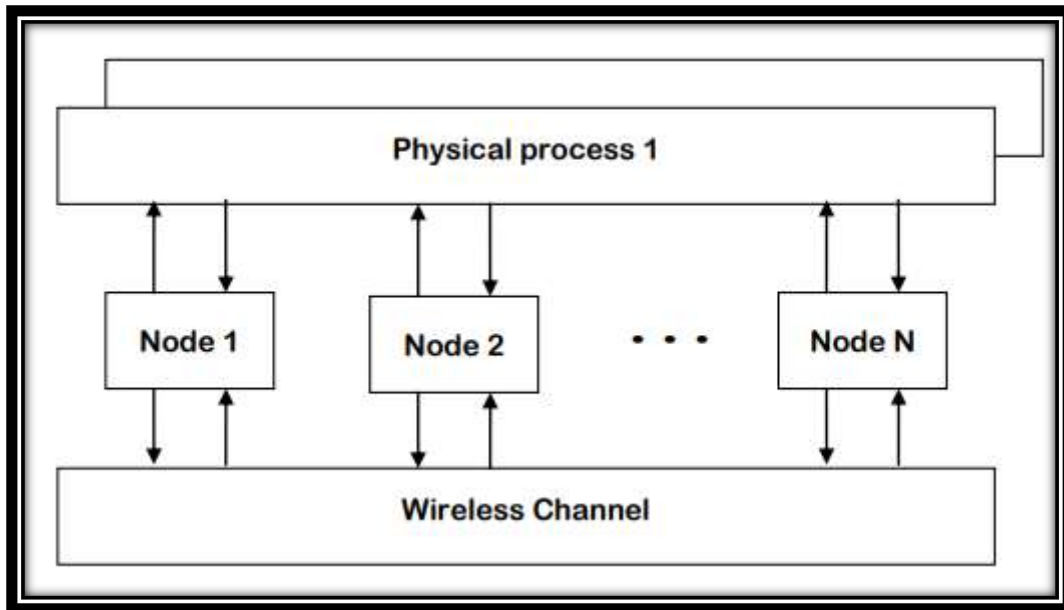


Figure IV.2 : Les modules et leurs connexions à Castalia [21]

Les nœuds ne se connectent pas directement les uns aux autres mais par le biais du ou des modules de canaux sans fil. Les flèches signifient un message passant d'un module à un autre. Lorsqu'un nœud a un paquet à envoyer, cela va au canal sans fil qui décide ensuite quels nœuds doivent recevoir le paquet. Les nœuds sont également liés par les processus physiques qu'ils surveillent. Pour chaque processus physique, il existe un module qui contient la «vérité» sur la quantité représentée par le processus physique. Les nœuds échantillonnent le processus physique dans l'espace et dans le temps (en envoyant un message au module correspondant) pour obtenir les lectures de leurs capteurs [21].

4.1 Le module de nœud

Le module de nœud est composite. La figure 2 montre la structure interne du module composite de nœud. Les flèches en trait plein signifient que le message passe et les flèches en pointillé signifient un appel de fonction simple. Par exemple, la plupart des modules appellent une fonction du gestionnaire de ressources pour signaler que de l'énergie a été consommée. Le module d'application est celui que l'utilisateur changera le plus souvent, généralement en créant un nouveau module pour implémenter un nouvel algorithme. Les modules de communication MAC et de routage, ainsi que le module Mobility Manager, sont également de bons candidats à la

modification par l'utilisateur, généralement en créant un nouveau module pour mettre en œuvre un nouveau protocole ou modèle de mobilité. Castalia prend en charge la création de nos propres protocoles ou applications en définissant des classes abstraites appropriées [21]

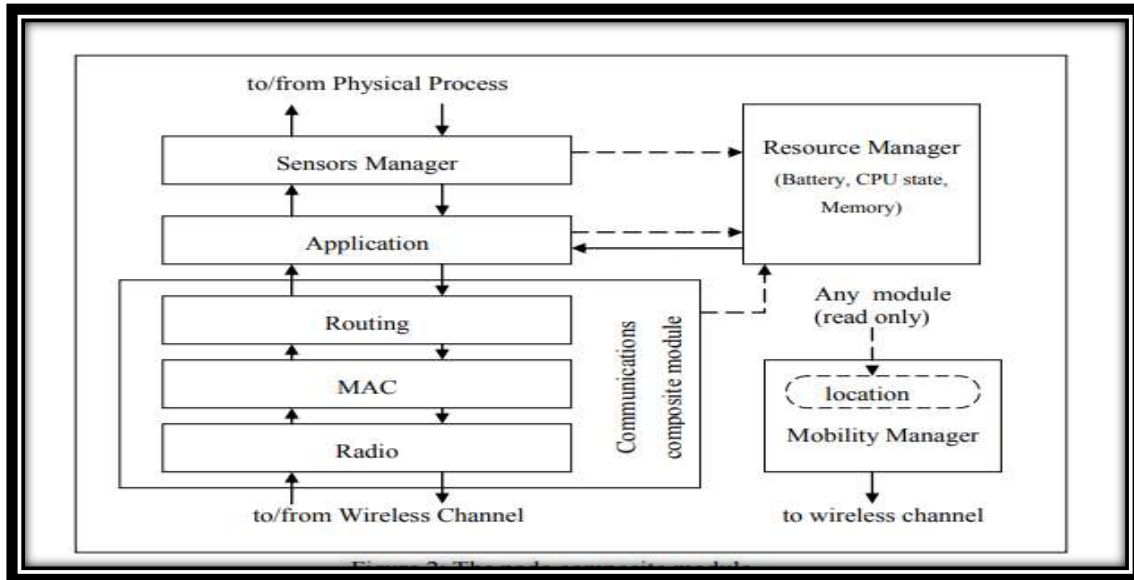


Fig IV.3 : Le module composite de nœud

5. Paramètres de simulation

Nous avons fait la simulation en utilisant OMNET++ 4.6 avec Castalia3.2, les nœuds sont déployés uniformément dans un terrain carré dont sa dimension est variée. La portée de communication ainsi que la valeur initiale de l'énergie sont fixes pour tous les nœuds et le tout peuvent générer les paquets de données.

Paramètre	valeur
Nombre des nœuds	[30,50,70]
Somme du nombre de valeurs détectées	6400
Temps de simulation	200 s
Zone de simulation	[100,200,300]
Plage de transmission	50 m
Énergie initiale	12 Joules
Tx Power	-5 dbm
Modèle radio	CC2420
Temps de pause de la mobilité	[1..5]
Vitesse de mobilité	[1,2,4]
Répétitions de simulation	20

Tableau IV.1 : Paramètres de simulation

6. Scénarios de simulation, résultats et discussion

Pour l'évaluation de performance des protocoles GeRaF et SIF La simulation se faite en terme d'énergie consommé par le nœud et la latence dans chacun des scénarios suivants :

6.1 1^{er} scénario : zone de simulation (Field length)

Dans un premier temps, nous verrons la valeur d'énergie consommé par un nœud capteur pour l'acheminement du paquet tout le temps de simulation où le déploiement des nœuds se varie dans un champ de 100,200 et 300 mètres.

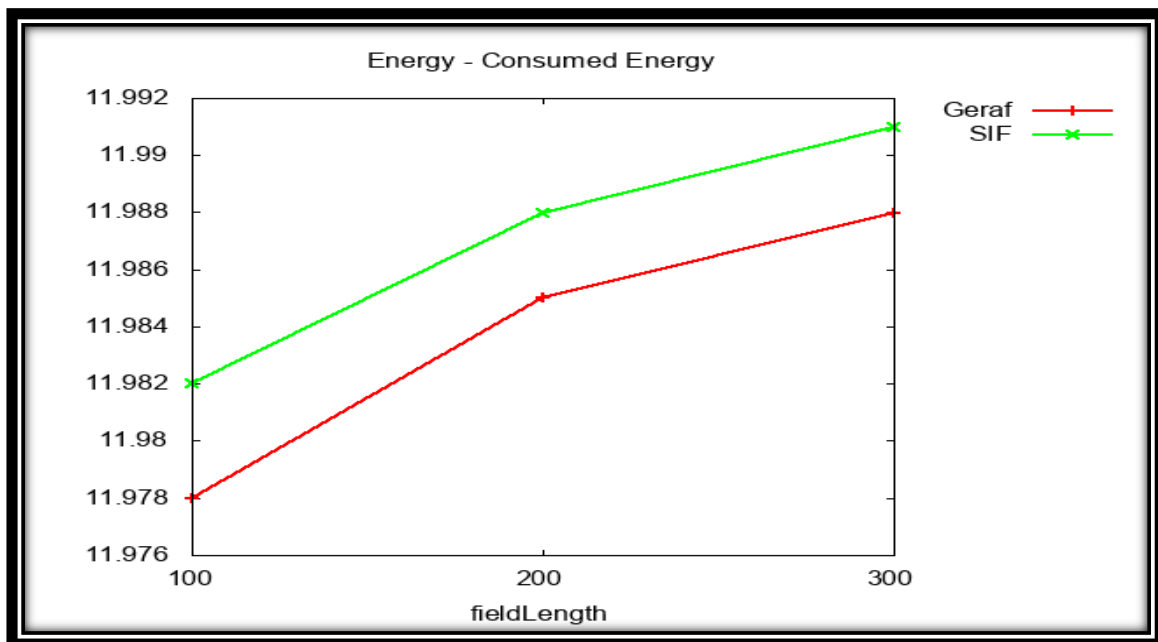


Fig IV.4 : énergie consommé vs field length

Le rapport d'énergie consommé est presque en parallèle entre GeRaF et SIF, en variant le field length. Cependant, GeRaF marque une consommation moindre par rapport à SIF comme indiqué sur la figureIV.4, et cela peut être dû au mécanisme utilisé par GeRaF pour l'auto-sélection du prochain saut qui est basé seulement sur le taux d'avancement du paquet, ce qui minimise le nombre de saut total. Contrairement au protocole SIF qui combine le taux d'avancement avec l'énergie résiduelle ce qui peut

être influé sur le nombre de saut total. Et cela implique directement la consommation énergétique.

6.2 2^{ième} scénario : scalabilité (nombre des nœuds)

Dans le deuxième test, on va contrôler l'influence de la taille du réseau en variant le nombre des nœuds qui forment le réseau. Ils se varient entre 30,50 et 70 nœuds.

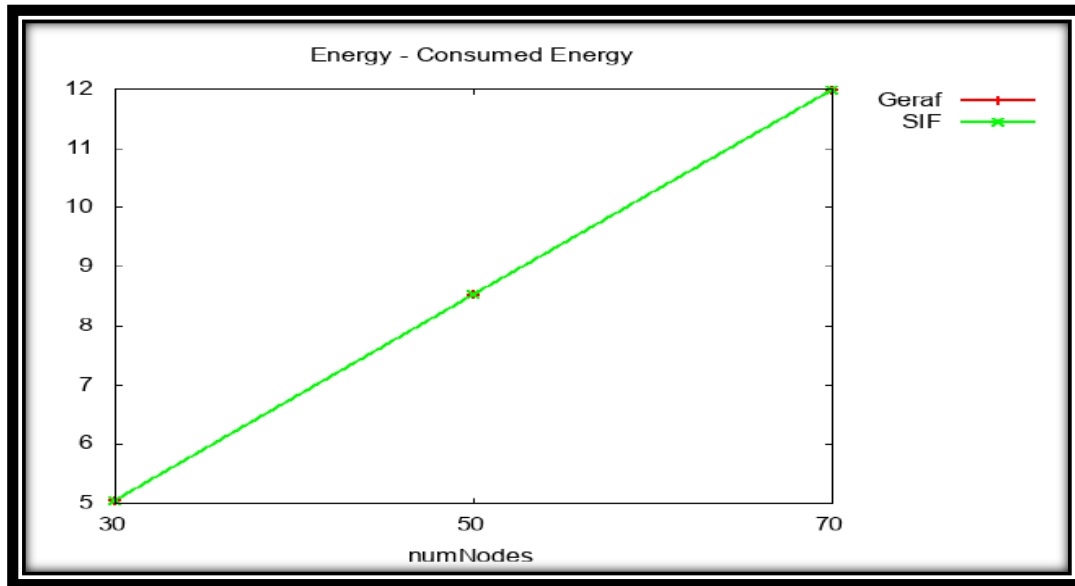


Fig IV.5 : énergie consommé vs nombre des nœuds

La figure IV.5 montre que plus le nombre des nœuds est élevé, plus l'énergie consommée est élevée, d'une part c'est parce que le nombre de collision augment avec la densité des nœuds.

De l'autre part, la performance en terme d'énergie consommé entre GeRaF et SIF est identique.

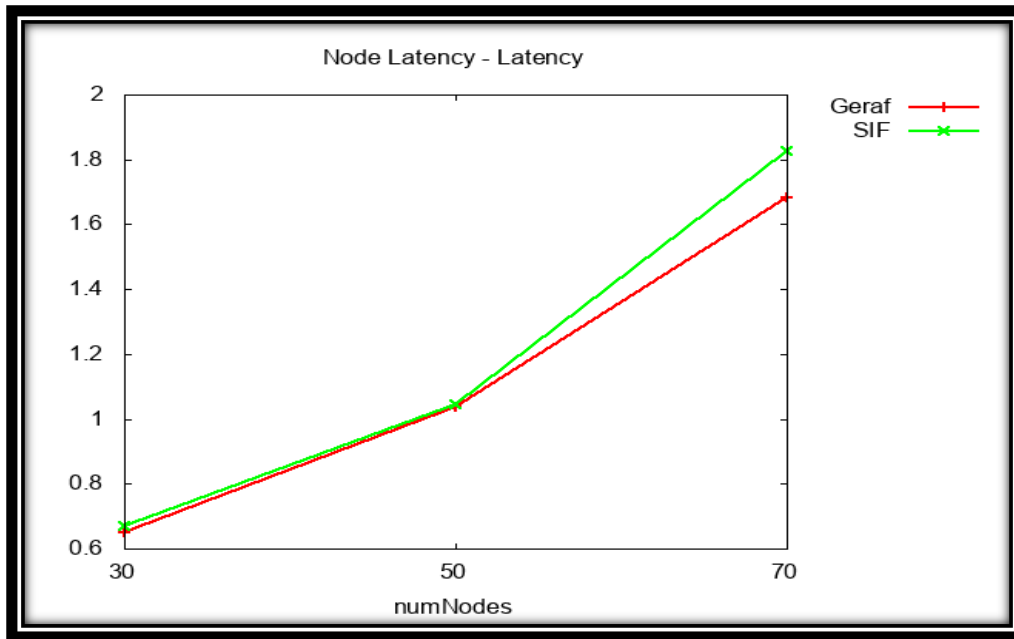


Figure IV.6 : la latence vs nombre des nœuds

Comme mentionné précédemment pour l'énergie, la taille du réseau affect aussi bien la latence soit pour GeRaF ou SIF et ceci présenter dans la (figure) qui montre que GeRaF est plus efficace à partir de 50 à 70 nœuds (Figure IV.6).

Cette résultat c'est à cause de politique utilisé dans GeRaF qui s'appuie sur l'utilisation d'une deuxième radio pour la signalisation d'occupation et l'élimination du DISF ce qui lui permet de gagner en délai de livraison des paquets.

6.3 3^{ième} scénario : Node speed

Dans ce cas, nous avons effectué la simulation avec une variation de la vitesse de mobilité entre 1,2 et 4 m/s.

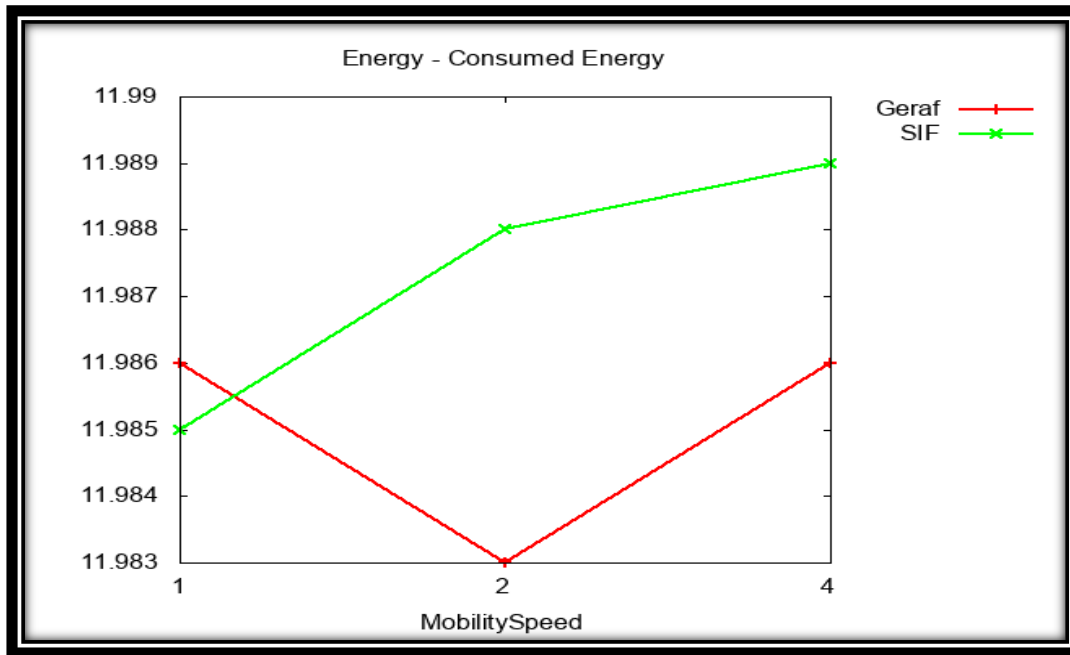


Fig IV.7 : énergie consommé vs mobility speed

La figure 15 montre que La vitesse de mobilité aussi influe à la performance des deux protocoles dans les RCSFs et que GeRaF est beaucoup plus efficace que le protocole SIF en terme de l'énergie (figure) et de latence (Figure IV.7).

Plus précisément, GeRaF donne un meilleur fonctionnement pour une mobilité du 2 m/s.

7. Conclusion

Dans ce chapitre, nous avons simulé les deux protocoles BLR « GeRaF » et « SIF » dans l'environnement OMNET++.

Notre objectif, à travers les simulations effectuées était de tester les performances de notre protocoles d'où nous avons pu montrer l'avantage de l'utilisation des protocoles de routage BLR dans les RCSFs pour assurer la conservation d'énergie au sein du réseau ce qui augmente la durée de vie du réseau.

Dans ce contexte, nous avons montré par les simulations effectuées que GeRaF est plus efficace par rapport à SIF.

Suite à tous ces avantages réalisés avec le routage BLR, les recherches futures sont plus favorisées vers des approches multi objectif, plus facile à mise en œuvre d'une part, et qu'ils donnent une meilleur performance pour prolonger la durée de vie de la batterie d'un nœud capteur d'une autre.

Conclusion générale

Conclusion générale

Les RCSFs sont applicables dans plusieurs domaines. Puisque la plupart des applications utilisent des capteurs dont leurs batteries sont limitées d'énergie, il est essentiel de choisir un protocole de routage approprié. En outre, les RCSFs avec nœuds mobiles nécessitent des protocoles de routage personnalisés. Comme nous avons mentionné dans les chapitres précédents, les protocoles BLR sont très efficaces pour prolonger la durée de vie de réseau en termes d'énergie. Parmi ces protocoles quel est le plus efficace ?

Parmi les protocoles mentionnés dans le chapitre III, nous avons choisi l'étude et l'évaluation des deux protocoles de routage « GeRaF » et « SIF » et de déterminer le plus performant. Le principe de fonctionnement des deux protocoles est presque le même, la différence la plus importante c'est comment calcule le CTS_timer qui représente le temps d'attente pour envoyer un CTS ?

L'implémentation des RCSFs exige un outil spécialisé comme NS2 ou Omnet++. Nous avons utilisé le simulateur Castalia qu'il est construit à la base d'Omnet++.

Nous avons évalué les performances en termes d'énergie consommée avec une variation de fieldlength, nombre des nœuds et mobility speed. En général, tous ces facteurs influent d'une façon spécifique sur les performances des protocoles.

Le cas de différentes valeurs de fieldlength, GeRaF donne des bons résultats par rapport à SIF.

Pour un nombre du nœud varié, nous avons observé que la performance de GeRaF et SIF sont la même en terme d'énergie consommée, mais en terme de latence, GeRaF était le mieux.

Le dernier test était de simuler les performances de GeRaF et SIF en termes d'énergie consommée et avec des mobility speeds différents. On a trouvé que GeraF est le plus efficace, les nœuds se déplacent avec une vitesse de 2m/s. Comme un résultat général GeRaF donne de meilleures performances.

Comme perspectives, nous allons évaluer les performances de tous les protocoles BLR en d'autres termes (duplication de paquets, rapport de livraison...). Ensuite, on va comparer tous ces protocoles pour déterminer quel sont les protocoles les plus adaptés à certaines applications.

Références bibliographiques

[1] : Rezki, y .Bouordjah, S . (2014). Etude des mécanismes de localisation dans les réseaux de capteurs sans fil. Mémoire Master Recherche: Réseaux et Système Distribuée. Béjaia: Université A/Mira de Béjaia.

[2] : Belkacem, N. Benchallal, K. (2015). Mise en place d'un réseau de capteurs sans fil pour le suivi d'une chaîne de production. Mémoire Master Recherche Opérationnelle : Fiabilité et Evaluation des Performances des Réseaux. Béjaia: Université Abderrahmane Mira de Béjaia.

[3] : Abdelfatah, F. (2008). Développement d'une bibliothèque de capteurs. Master Informatique: Informatique professionnelle et Recherche en Informatique. Montpellier: Université Montpellier 2.

[4] : Kaci , B (2010). Détection d'intrusion dans les réseaux de capteurs sans fils. Master Recherche 2 en Informatique. Bretagne: institut de formation supérieure en informatique et communication.

[5] : Lounes, A. Ghersa, E (2017). Réalisation d'un parking intelligent. Mémoire de master professionnelle: Administration et Sécurité des Réseaux. . Béjaia: Université A/Mira de Béjaia.

[6] : Boukhecheba , S. Ben esseddik, K(2015). Protocoles Cross-Layer pour l'économie d'énergie dans les réseaux de capteurs sans fil. Mémoire Master Recherche: Réseau Convergence et Sécurité. ouargla: kasdimerbahouargla.

[7] : Makhmoukh. D, Melouk. S. (2017). « Approche de minimisation de la consommation d'énergie dans les réseaux de capteurs sans fil ». Mémoire Master : Administration et Sécurité des Réseaux. Université A/Mira de Béjaia.

[8] : Mekki. N, Mohammedi. K. (2018). « Techniques de conservation d'énergie

pour les réseaux de capteur sans fil ». Mémoire Master :RISR. UNIVERSITE Dr. TAHAR MOULAY SAIDA.

[9] : Korichi.W, «Partage de données en environnements mobiles Ad hoc »,. MémoireMagistère : Réseaux et Systèmes d'Information Multimédia. Université KasdiMerbah Ouargla.

[10] : W. Ye, J. Heidemann, and D. Estrin. "An Energy-Efficient MAC Protocol for Wireless Sensor Networks". pp 1567-1576, June 2002

[11] :Dhoutaut D.(2003).Etude du standard IEEE 802.11 dans le cadre

desréseaux ad hoc : de la simulation a l'expérimentation. Thèse doctorat : L'Institut National des Sciences Appliquées de Lyon.

[12] :Amadou.I.(2012). Protocoles de routage sans connaissance du voisinage

pour réseaux radio multi-sauts ».thèse doctorat. École doctorale : Informatique et Mathématiques de Lyon.

[13]: C. Mehmet, Vuran, F. Ian Akyildiz.(2010). XLP: A Cross-Layer Protocol for Efficient Communication in Wireless Sensor Networks. , *IEEE Transactions On Mobile Computing*, vol. 9, no. 11.

[14] ; B. M. Blum.(2003). *IGF: A Robust State-Free Communication Protocol for Sensor Networks*

[15]: D. Chen, J. Deng, P. K. Varshney. (2005). A State-Free Data Delivery Protocol for Wireless Sensor Networks", *Proc. IEEE WCNC*.

[16] :. H. F'ußler, J. Widmer, M. K'asemann, M. Mauve, and H. Hartenstein. (2003). ContentionBased Forwarding for Mobile Ad-Hoc Networks. Elsevier's Ad-Hoc Networks.

[17] :. M. Zorzi, R. R. Rao. (2003). Geographic Random Forwarding (GeRaF) for Ad Hoc and Sensor Networks : Multihop Performance", *IEEE Trans. Mobile Computing*, vol. 2, no. 4.

[18]; Heissenbüttel. M. (2004) . BLR: Beacon-Less Routing Algorithm for Mobile Ad-Hoc Networks", *Elsevier Computer Commun. J.*, vol. 27, no. 11.

[19] : NIAR L I (2012). Analyse Graphique pour la surveillance dans un réseau de capteurs sans fils (RCSF) Simulateur : OMNET++. Mémoire Magister : Analyse, Commande et Surveillance des Systemes. Université d'Oran.

[20]: Andrés Varga and OpenSim Ltd. OMNeT++ User Manual Version 4.3.1.

[21]:Athanasios Boulis. Castalia A simulator for Wireless Sensor Networks and Body Area Networks Version 3.2. NICTA March 2

[22] : Schurgers C, Tsiatsis .V, Ganeriwal .S, and Srivastava .M.(2002).Optimizing Sensor Networks in the Energy-Latency-Density Design Space. IEEE Trans. Mobile Computing, vol. 1, no. 1,pp. 70-80