



REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE
LA RECHERCHE SCIENTIFIQUE

UNIVERSITE MOULOD MAMMARI DE TIZI-OUZOU
FACULTE DE GENIE ELECTRIQUE ET INFORMATIQUE
DEPARTEMENT D'INFORMATIQUE



Mémoire

de fin d'études

*En vue de l'obtention du diplôme de Master en
Informatique*

Spécialité : SYSTEMES INFORMATIQUES

Thème :

*Implémentation d'une technique d'agrégation dans le
protocole de routage LEACH pour le contrôle de congestion
dans les réseaux de capteurs sans fil*

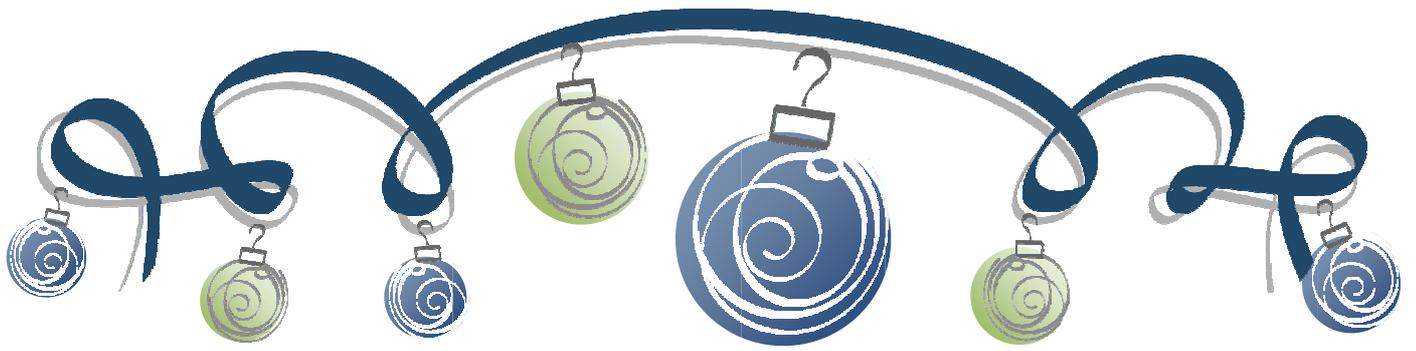
Proposé et dirigé par :

M^{me} R. Aoudjit

Réalisé par :

M^{elle} Samia Zitoun

Promotion : 2010/2011



Dédicaces

Je dédie ce modeste travail :

À mes très chers parents :

À mon fiancé Aghilas

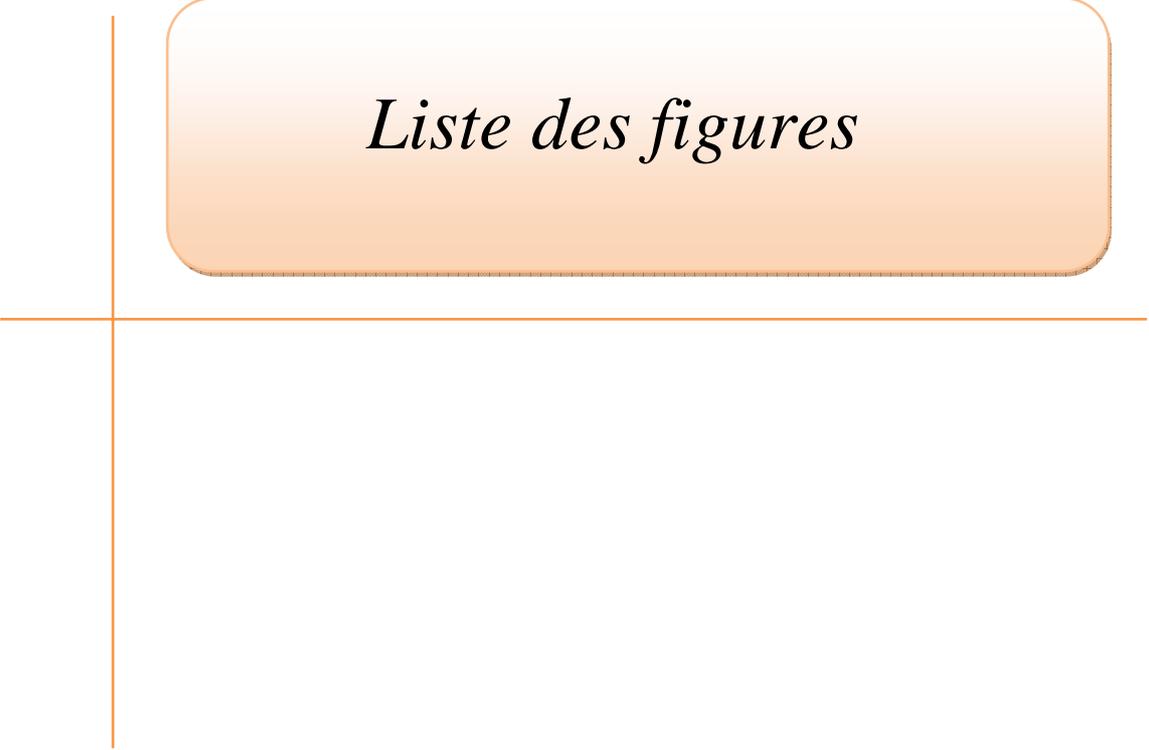
À mes sœurs :

À mes frères :

À mes amies :

Samia





Liste des figures

CHAPITRE I

Figure I.1 : Classification des réseaux mobiles.....	6
Figure I.2 : Schéma d'un réseau cellulaire	8
Figure I.3 : Modélisation du réseau Ad hoc.....	9
Figure I.4: Changement de topologie dans les réseaux Ad Hoc.....	10
Figure I.5 : Architecture général d'un nœud capteur	13
Figure I.6 : Consommation d'énergie en captage, traitement et transmission.....	15
Figure I.7 : Rayons de communication et de sensation d'un capteur.....	16
Figure I.8 : Exemple de capteur intelligent MICA2 de Crossbow.....	17
Figure I.9 : Réseau de capteurs militaire.	20
Figure I.10 : Des capteurs dans des fausses branches.....	20
Figure I.11 : Application des réseaux de capteurs en médecine.....	22
Figure I.12 : Différents type de Sink.....	24
Figure I.13 : Architecture générale d'un réseau de capteurs sans fils.....	24
Figure I.14 : Mobilité du Sink.....	25
Figure I.15 : Mobilité de l'événement.....	26
Figure I.16 : Topologie plate (Flat)	27
Figure I.17 : Topologie Hiérarchique	28
Figure I.18: Pile de protocoles dans les réseaux de capteurs.....	29

CHAPITRE III

Figure.III.1 : Diagrammes représentant le protocole MAC TDMA.....	56
Figure III.2 : Diagrammes représentant le protocole MAC CDMA.....	57
Figure III.3 : Architecture de communication du protocole LEACH.....	58
Figure III.4 : Opérations de l'étape d'initialisation de LEACH.....	59
Figure III.5 : Interférence lors d'une communication dans LEACH.....	61
Figure III.6 : Répartition du temps et différentes phases pour chaque round.	62

CHAPITRE IV

Figure IV.1 : FIFO multiples pour assurer la délivrance équitable de données dans FRA.....70

CHAPITRE V

Figure V.1 : Agrégation de données..... 73

Figure V.2 : Relation entre la technique d'agrégation et d'autres couches de la pile.....74

Figure V.3 : Exemple d'une technique d'agrégation utilisant une structure en anneau.....80

CHAPITRE VI

Figure VI.1 : Diagramme de transition d'états de la phase de collecte des données.....83

Figure VI.2 : Connexions entre les composants dans J-Sim.....87

Figure VI.3 : Vue générale sur trois types de noeuds dans J-Sim.....87

Figure VI.4 : Architecture interne d'un noeud sensor dans J-Sim.....89

Figure VI.5 : Influence de la densité sur le taux d'agrégation 92

Figure VI.6 : Influence de la densité sur la durée de vie de réseau.....93



Liste des tableaux

CHAPITRE II

Tableau II.1: Classification des protocoles de routage.....47

CHAPITRE VI

Tableau VI.1 : les différents champs d'un paquet reçu par un CH.....84

Tableau VI.2 : Les paramètres de simulation.....91

INTRODUCTION GENERALE	1
CHAPITRE I: LES RESEAUX MOBILES ET LES RESEAUX DE CAPTEURS SANS FIL	
I.1 Introduction	3
I.2 Les réseaux mobiles.....	3
I.2.1 Les unités mobiles.....	4
I.2.1.1 Classes d'unités mobiles.....	4
I.2.1.2 Modes de fonctionnement.....	4
I.2.1.3 Les défis des unités mobiles.....	5
I.2.2 Classification des réseaux mobiles.....	6
I.2.2.1 Réseaux personnels sans fil (WPAN)	6
I.2.2.2 Réseaux locaux sans fils (WLAN)	6
I.2.2.3 Réseaux métropolitains sans fil (WMAN)	7
I.2.2.4 Réseaux étendus sans fil (WWAN)	7
I.2.2.5 Les réseaux cellulaires.....	7
I.2.2.6 Les réseaux Ad Hoc (sans infrastructure)	8
I.2.2.6.1 Définition.....	8
I.2.2.6.2 Modélisation d'un système de réseau Ad Hoc.....	9
I.2.2.6.3 Caractéristiques des réseaux Ad Hoc.....	10
I.3 Les réseaux de capteurs	12
I.3.1 Un capteur	12
I.3.1.1 Composants du capteur	13
I.3.1.2 Caractéristiques principales d'un capteur.....	15
I.3.2 Un réseau de capteurs	17
I.3.2.1 Caractéristiques des réseaux de capteurs	17
I.3.2.2 Applications des réseaux de capteurs.....	19
I.3.2.3 Architecture d'un réseau de capteurs	23
I.3.2.4 Types de mobilité dans les réseaux de capteurs sans fils.....	25
I.3.2.4.a Mobilité de nœud	25
I.3.2.4.b Mobilité du Sink	25
I.3.2.4.c Mobilité de l'événement	26

I.3.2.5 Topologies des réseaux de capteurs sans fils.....	26
I.3.2.6 Architecture de communication dans les réseaux de capteurs sans fil	29
I.3.2.7 Contraintes et facteurs influençant l'architecture des WSN.....	34
I.4 Conclusion	38
CHAPITRE II : LE ROUTAGE DANS LES RCSF	
II.1 Introduction	40
II.2 Les considérations de conception d'un protocole de routage dans WSNs.....	40
II.2.1 Déploiement des nœuds.....	40
II.2.2 La consommation d'énergie.....	41
II.2.3 Modèle de délivrance des données.....	41
II.2.4 L'hétérogénéité.....	42
II.2.5 Tolérance aux fautes.....	42
II.2.6 Scalabilité.....	43
II.2.7 La dynamique du réseau.....	43
II.2.8 Media de transmission.....	44
II.2.9 Connectivité	44
II.2.10 Couverture.....	44
II.2.11 Agrégation des données.....	44
II.2.12 Qualité de service.....	45
II.3 Métriques de routages	45
II.3.1 Métriques pour la consommation d'énergétique.....	45
II.3.1.1 Par considération de puissance.....	46
II.3.1.2 Par considération du coût.....	46
II.3.1.3 Par considération de puissance et du coût.....	46
II.3.2 Nombre de sauts.....	46
II.3.3 Perte de paquets.....	46
II.3.4 Délai de bout-en-bout EED.....	46
II.4 Classification des protocoles de routage dans les réseaux de capteurs	47
II.4.1 Classification selon la structure du réseau.....	47
II.4.1.1 Routage à plat.....	47
II.4.1.2 Routage hiérarchique.....	48
II.4.1.3 Les protocoles de routage avec localisation géographique.....	49
II.4.2 Classification selon les fonctions des protocoles.....	50
II.4.2.1 Routage basé sur la QoS.....	50

II.4.2.2 Routage basé sur les requêtes.....	50
II.4.2.3 Routage basé sur la négociation.....	51
II.4.2.4 Routage basé sur multi-chemins.....	51
II.4.3 Classification selon l'établissement de la route	52
II.4.3.1 Protocoles proactifs	52
II.4.3.2 Protocoles réactifs.....	52
II.4.3.3 Protocoles hybrides.....	53
II.4.4 Classification selon l'initiateur de communication.....	53
II.4.4.1 Communication lancée par la source.....	53
II.4.4.2 Communication lancée par la destination.....	53
II.5 Conclusion.....	54
CHAPITRE III : FONCTIONNEMENT DU PROTOCOLE DE ROUTAGE LEACH	
III.1 Introduction.....	55
III.2 Protocoles MAC utilisés par LEACH.....	55
III.2.1 Accès aléatoire	55
III.2.2 Allocation fixe.....	56
III.2.2.1 TDMA.....	56
III.2.2.2 CDMA.....	57
III.3 Architecture de communication de LEACH.....	57
III.4 Algorithme détaillé de LEACH.....	58
III.4.1 Phase d'initialisation.....	58
III.4.1.1 Phase d'annonce	59
III.4.1.2 Phase d'organisation de groupes.....	60
III.4.1.3 Phase d'ordonnancement.....	61
III.4.2 phase de transmission	61
III.5 Avantages et inconvénients de LEACH.....	62
III.5.1 Avantages.....	62
III.5.2 Inconvénients.....	63
III.6 Conclusion.....	64
CHAPITRE IV : CONTROLE DE CONGESTION DANS LES RCSF	
IV.1 Introduction	65
IV.2 Définition et typologies de congestion	65
IV.3 Classification des approches de contrôle de congestion	66
IV.3.1 Mécanisme de détection de congestion	66

IV.3.2	L'objectif du contrôle de congestion	67
IV.3.3	Les mécanismes de contrôle de taux de transfert	67
IV.3.4	Modèle de l'application cible	67
IV.3.5	D'autres métriques.....	67
IV.4	Quelques protocoles de contrôle de congestion dans les RCSF.....	68
IV.4.1	Congestion detection and avoidance: CODA	68
IV.4.2	Fair rate allocation (FRA)	69
IV.5	Conclusion	70
CHAPITRE V : AGREGATION DES DONNEES DANS LES RCSF		
V.1	Introduction.....	72
V.2	Définition	72
V.3	Approches d'agrégation de données	73
V.4	Les éléments de base de l'agrégation de données.....	74
V.4.1	Fonctions d'agrégation de données.	74
V.4.2	Les types d'agrégation.....	75
V.4.3	Protocoles de routage avec agrégation des données	76
V.4.3.1	Approche hiérarchique.....	76
V.4.3.1.1	Tiny AGregation (TAG)	76
V.4.3.1.2	Directed Diffusion	78
V.4.3.1.3	PEGASIS	78
V.4.3.2	Approche basée sur les clusters	78
V.4.3.3	Approche multi-chemins	79
V.4.3.4	Approche hybride	80
V.4.4	La représentation des données	80
V.5	Conclusion.....	81
CHAPITRE VI : IMPLEMENTATION ET SIMULATION		
VI.1	Introduction	82
VI.2	Description générale du protocole LEACHCO.....	82
VI.2.1	Les phases de communication.....	82
VI.2.1.1	Phase de collecte des données	82
VI.2.1.2	Phase d'agrégation des données.....	84
VI.2.1.3	Phase de contrôle de congestion.....	84
VI.3	Implémentation et simulation.....	85
VI.3.1	Environnement de simulation.....	85

VI.3.1.1	Choix du simulateur	85
VI.3.1.2	Le simulateur J-Sim.....	86
VI.3.1.2.1	description générale du simulateur J-Sim.....	86
VI.3.1.2.2	Le langage utilisé pour définir un scénario de simulation	89
VI.3.1.2.3	Installation de J-Sim	89
VI.3.1.2.4	Intégration du code source du protocole dans J-Sim	89
VI.3.1.2.5	Exécution et simulation	90
VI.3.1.2.6	Affichage des résultats de la simulation	90
VI.3.2	Evaluation du protocole LEACHCO.....	90
VI.3.2.1	Paramètres de simulation.....	90
VI.3.2.2	Métriques d'évaluation.....	91
VI.3.2.3	Interprétation des résultats de la simulation.....	92
VI.4	Conclusion	93
	CONCLUSION GENERALE ET PERSPECTIVES.....	95
	REFERENCES BIBLIOGRAPHIQUES.....	97

Résumé

Les progrès réalisés ces dernières décennies dans les domaines de la microélectronique, de la micromécanique, et des technologies de communication sans fil, ont permis de produire avec un coût raisonnable des composants de quelques millimètres cubes de volume. Ces derniers, appelés micro-capteurs, intègrent : une unité de captage chargée de capter des grandeurs physiques (chaleur, humidité, vibrations) et de les transformer en grandeurs numériques, une unité de traitement informatique et de stockage de données et un module de transmission sans fil.

De ce fait, les micro-capteurs sont de véritables systèmes embarqués. Le déploiement de plusieurs d'entre eux, en vue de collecter et transmettre des données environnementales vers un ou plusieurs points de collecte, d'une manière autonome, forme un réseau de capteurs sans fil (RCSF).

En raison des contraintes de miniaturisation, les capteurs sont généralement dotés de ressources très limitées en termes de capacité de calcul, d'espace de stockage de données, de débit de transmission et d'énergie embarquée. L'une des conséquences de cette limitation de ressources est que, dans un réseau de capteurs sans fil, tous les capteurs ne peuvent pas atteindre le collecteur central. Les nœuds proches du collecteur joueront donc le rôle de relais entre le collecteur et les nœuds éloignés.

Etant limité en ressource et jouant le rôle de relais, un capteur peut se trouver dans un état où il ne peut pas traiter ou transmettre les données. Dans cet état on dit que le capteur en question est congestionné, et on parle d'état de congestion. Quand la congestion se présente, elle cause la dégradation des performances d'un réseau avec une perte de données et une consommation inutile de la bande passante. Pour être performant, les protocoles conçus pour les réseaux de capteurs, principalement les protocoles de routage doivent être capables de contrôler la congestion.

Dans les RCSF, les données produites par les nœuds capteurs voisins sont très corrélées. Ceci peut engendrer la réception par la station de base d'informations redondantes. En transmettant ces données redondantes aux nœuds relais, elles peuvent être une source de congestion. La mise en place des techniques capables d'éviter ce type de congestion devient donc une nécessité dans le domaine de la recherche.

Pour répondre à cette problématique, nous proposons une technique d'agrégation appliquée sur le protocole de routage LEACH. Cela consiste à combiner les données redondantes afin de réduire la quantité d'informations transmises par les capteurs et donc pouvoir contrôler la congestion.

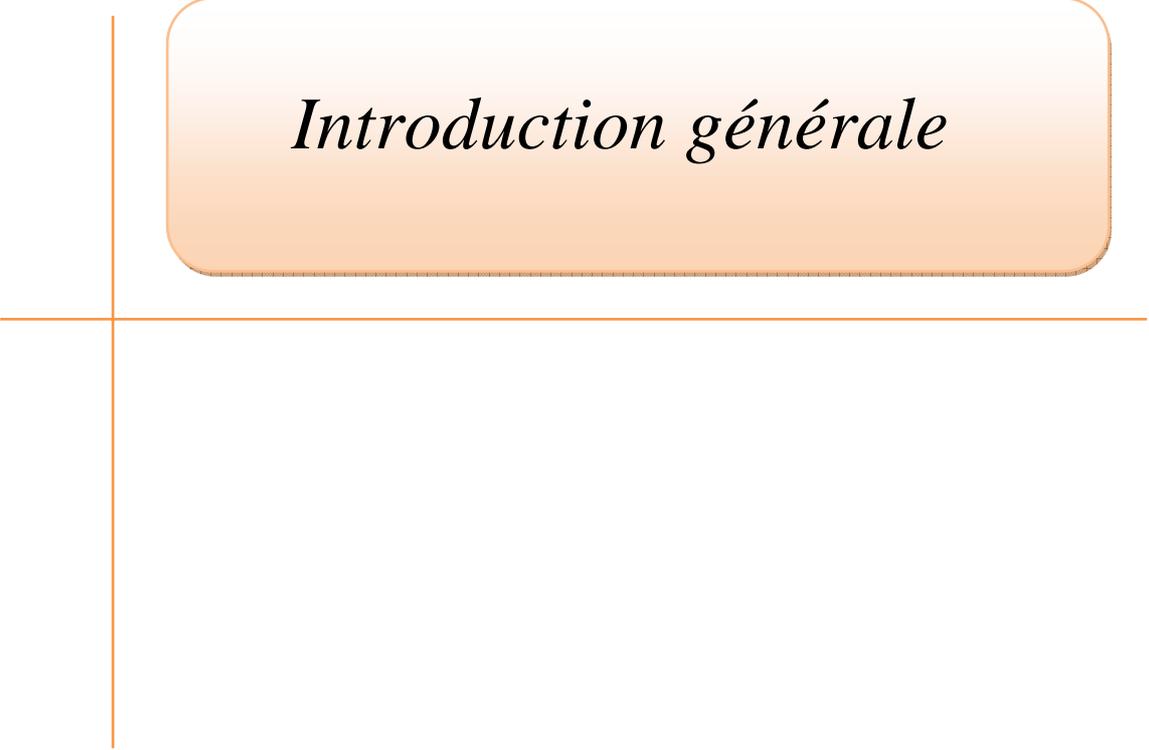
Mots clés :

RCSF : Réseaux de Capteurs Sans Fil.

LEACH: Low-Energy Adaptive Clustering Hierarchy.

CSMA: Carrier Sense Multiple Access.

TDMA: Time Division Multiple Access .



Introduction générale

Les progrès réalisés ces dernières décennies dans les domaines de la microélectronique, de la micromécanique, et des technologies de communication sans fil, ont permis de produire avec un coût raisonnable des composants de quelques millimètres cubes de volume. Ces derniers, appelés micro-capteurs, intègrent : une unité de captage chargée de capter des grandeurs physiques (chaleur, humidité, vibrations) et de les transformer en grandeurs numériques, une unité de traitement informatique et de stockage de données et un module de transmission sans fil.

De ce fait, les micro-capteurs sont de véritables systèmes embarqués. Le déploiement de plusieurs d'entre eux, en vue de collecter et transmettre des données environnementales vers un ou plusieurs points de collecte, d'une manière autonome, forme un réseau de capteurs sans fil (RCSF).

En raison des contraintes de miniaturisation, les capteurs sont généralement dotés de ressources très limitées en termes de capacité de calcul, d'espace de stockage de données, de débit de transmission et d'énergie embarquée. L'une des conséquences de cette limitation de ressources est que, dans un réseau de capteurs sans fil, tous les capteurs ne peuvent pas atteindre le collecteur central. Les noeuds proches du collecteur joueront donc le rôle de relais entre le collecteur et les noeuds éloignés.

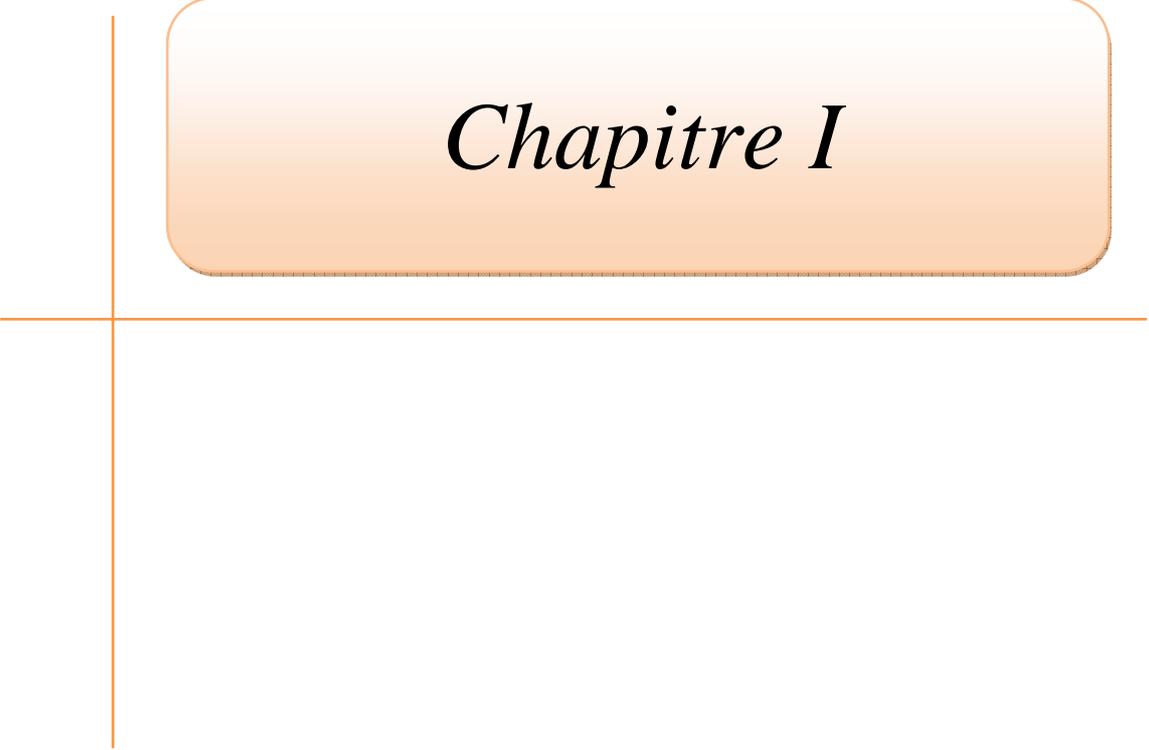
Etant limité en ressource et jouant le rôle de relais, un capteur peut se trouver dans un état où il ne peut pas traiter ou transmettre les données. Dans cet état on dit que le capteur en question est congestionné, et on parle d'état de congestion. Quand la congestion se présente, elle cause la dégradation des performances d'un réseau avec une perte de données et une consommation inutile de la bande passante. Pour être performant, les protocoles conçus pour les réseaux de capteurs, principalement les protocoles de routage doivent être capables de contrôler la congestion.

Dans les RCSF, les données produites par les noeuds capteurs voisins sont très corrélées. Ceci peut engendrer la réception par la station de base d'informations redondantes. En transmettant ces données redondantes aux noeuds relais, elles peuvent être une source de congestion. La mise en place des techniques capables d'éviter ce type de congestion devient donc une nécessité dans le domaine de la recherche.

Pour répondre à cette problématique, nous proposons une technique d'agrégation appliquée sur le protocole de routage LEACH. Cela consiste à combiner les données redondantes afin de réduire la quantité d'informations transmises par les capteurs et donc pouvoir contrôler la congestion.

Pour mener à bien notre travail, nous l'avons organisé en six chapitres selon un plan méthodologique suivant :

Le premier chapitre est une introduction aux réseaux mobile, plus précisément aux réseaux de capteurs sans fils, leurs caractéristiques, leurs domaines d'applications ainsi que leurs architectures. Le second chapitre s'intéresse au routage dans les RCSF ; nous donnerons les classifications, les métriques ainsi que les facteurs de la conception des protocoles de routage. L'un des exemples des protocoles de routage est le protocole LEACH que nous expliquerons en détail dans le troisième chapitre. Le quatrième chapitre est un état de l'art sur les techniques de contrôle de congestion pour les réseaux de capteurs et le cinquième chapitre représente les techniques d'agrégation utilisées. Le dernier chapitre, quant à lui, nous permettra d'exposer notre amélioration que nous avons proposée pour le protocole étudié, baptisé LEACHCO, ainsi que les résultats d'implémentation et de tests de simulation de notre solution. Enfin, nous clôturons par une conclusion générale et des perspectives.



Chapitre I

I.1 Introduction

Les réseaux sans fil (Wireless Networks) connaissent actuellement un succès important et leur utilisation est de plus en plus fréquente. Cela est dû aux nombreux avantages qu'ils procurent. Ils offrent en effet une flexibilité largement supérieure aux réseaux filaires, en s'affranchissant notamment des problèmes de câblage et de mobilité des équipements.

Grâce à cette évolution dans les réseaux sans fil, à la miniaturisation des circuits électroniques ainsi qu'à la réduction de leurs coûts, un nouveau type de réseaux est apparu : les réseaux de capteurs. Ces réseaux sont composés de plusieurs micro-capteurs destinés à la collecte d'informations relatives à l'environnement de déploiement. Chacun des micro-capteurs représente un nœud du réseau et communique avec les autres nœuds via des liaisons optiques ou radios.

Ce chapitre donne un aperçu sur les différentes technologies des réseaux sans fil. Nous y définirons les réseaux ad hoc qui sont des réseaux mobiles sans infrastructure, puis nous nous intéresserons à un type particulier des réseaux ad hoc : les réseaux de capteurs sans fil, qui seront étudiés en détail dans le reste du chapitre.

I.2 Les réseaux mobiles

Comme son nom l'indique, un réseau sans fil, ou réseau mobile, est un réseau dans lequel au moins deux terminaux peuvent communiquer en utilisant des liaisons sans fil, tels que les ondes radioélectriques ou infrarouges, au lieu des câbles habituels (cuivre, fibre optique,...).

Grâce aux réseaux sans fil, un utilisateur a la possibilité de rester connecté tout en se déplaçant dans une zone géographique plus ou moins étendue, à condition toutefois d'être muni d'un module de communication sans fil.

Les réseaux sans fil offrent une multitude d'avantages. En particulier, ils permettent la mise en place de réseaux dans des sites où le câblage serait onéreux ou impossible à cause, par exemple, de la présence d'unités mobiles. Cependant, l'utilisation des ondes radio comme moyen de transmission rend la communication moins fiable par rapport aux réseaux filaires. En effet, les ondes radio sont plus sensibles aux perturbations et aux interférences dues à l'environnement qui peuvent altérer l'information échangée. Par conséquent, les délais de transit des messages augmentent en raison des retransmissions [6].

I.2.1 Les unités mobiles

I.2.1.1 Classes d'unités mobiles

Dans ce qui suit, nous énumérerons les différentes catégories d'unités mobiles, tel que cela a été fait dans [7].

- Les ordinateurs portables (laptops) qui sont munis d'interfaces de communication sans fil tel que les cartes au format PCMCIA.
- Les tablettes à crayon (Pen Tablet), considérées comme des ordinateurs portables sans clavier. Ce dernier est remplacé par un crayon digital.
- Les ordinateurs personnels de poche "Handheld Personal Computers – HPC" caractérisés par l'absence d'une unité de stockage permanente.
- Les assistants numériques "Personal Digital Assistant – PDA" qui sont des appareils numériques portables avec une faible consommation en ressources (RAM, processeurs,...) comparés aux HPCs.
- Les téléphones cellulaires "cellular phones" dédiés principalement aux communications téléphoniques. Plus petits que les HPC et les PDA mais consomment plus d'énergie à cause de la grande portée de communication qu'ils peuvent atteindre.
- Les cartes réseaux sans fil qui sont des cartes qui peuvent être ajoutées aussi bien aux ordinateurs personnels qu'aux autres périphériques pour construire un réseau local sans fil (Wireless Local Area Network - WLAN).

Ces dernières années ont connu l'apparition de micro-capteurs qui permettent la surveillance d'un phénomène donné. Ces micro-capteurs communiquent entre eux via des liaisons sans fil et sont dotés de tous les composants d'un terminal mobile (processeur embarqué, interface de communication sans fil,...). Par conséquent, les capteurs peuvent représenter également un nouveau type d'unités mobiles [2].

I.2.1.2 Modes de fonctionnement

Contrairement aux systèmes distribués classiques où le site est soit connecté soit totalement déconnecté, les unités mobiles peuvent avoir plusieurs formes de liaison avec le reste du réseau.

Afin d'économiser l'énergie consommée, une unité mobile peut fonctionner en mode veille «Doze mode » ou la vitesse du processeur est réduite et aucun calcul n'est effectué, cette unité reste alors en attente de la réception d'un message de contrôle pour reprendre son fonctionnement normal.

A cause de leur mobilité permanente, les unités mobiles prévoient des mécanismes pour détecter la plupart des cas de déconnexion possibles, et exécutent en conséquence des protocoles qui prennent en charge cette phase, en vue d'assurer que l'unité a téléchargé toutes les informations d'états nécessaires lui permettant de continuer son fonctionnement normal indépendamment des autres sites.

Durant son fonctionnement, une unité mobile peut également basculer vers l'état «partiellement connecté » par l'exécution d'un protocole spécifique. Dans ce mode de fonctionnement, toutes les communications avec le réseau doivent être limitées. Finalement, et dans les réseaux mobiles cellulaires [3], une unité mobile exécute un protocole appelé « handoff » quand elle désire sortir de sa cellule courante vers une autre cellule. Ce protocole permet le transfert des informations d'état relatives au calcul mobile en cours à la station de base de la nouvelle cellule.

I.2.1.3 Les défis des unités mobiles

La nature contraignante de l'environnement mobile impose plusieurs défis que doivent surmonter les unités mobiles [4]. En effet, ces unités doivent être efficaces en consommation d'énergie pour permettre la plus longue durée de vie aux batteries utilisées, et ceci, via la production des batteries plus petites et durables, des composants électroniques plus intégrés qui consomment moins d'énergie, et surtout des logiciels qui prennent en compte la contrainte d'énergie.

Les unités mobiles doivent avoir également la possibilité de découvrir automatiquement et d'une manière autonome les différents paramètres leurs permettant de s'intégrer dans l'environnement mobile et de s'auto-configurer pour devenir opérationnel sans aucune intervention de l'administrateur. De plus, ces unités doivent avoir toutes les connaissances nécessaires liées à leur localisation et leur contexte de fonctionnement «Location and Context Awareness ».

L'adaptabilité aux changements des conditions des canaux de communication « Time Varying Radio Channels » est une autres caractéristique importantes des unités mobiles qui leurs permet de fonctionner dans les environnements irréguliers.

Enfin, la sécurité, plus qu'elle l'a été dans les réseaux filaires, est d'une importance primordiale dans les réseaux mobiles sans fil. Elle inclus aussi bien la protection des données contre les pertes et la corruption, que leur confidentialité. Cependant, l'application des techniques classiques (cryptage, signature,...) utilisée dans les environnements fixes est loin d'être évidente dans les réseaux mobiles.

I.2.2 Classification des réseaux mobiles

Il y a deux manières pour classer les réseaux sans fil. La première est basée sur la zone de couverture du réseau. Cette classification donne lieu à quatre catégories de réseaux sans fil: les réseaux personnels, les réseaux locaux, les réseaux métropolitains et les réseaux étendus. Dans chaque catégorie sont appliquées des technologies de communication qui se démarquent par le débit, la plage de fréquence utilisée et la portée de communication. La deuxième façon de voir les réseaux sans fil est selon le model et l'infrastructure de communication adoptée. L'infrastructure d'un réseau sans fil comprend toutes les installations servant de relais de communication entre deux unités, telles que les stations de base ou les satellites.

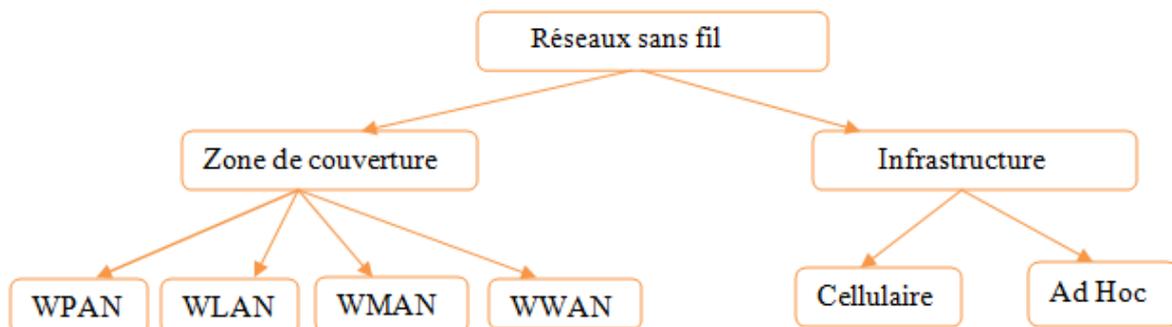


Figure I.1 : Classification des réseaux mobiles

I.2.2.1 Réseaux personnels sans fil (WPAN)

Le réseau personnel sans fil noté WPAN pour Wireless Personal Area Network) concerne les réseaux sans fil d'une faible portée: de l'ordre de quelques dizaines de mètres. Ce type de réseau sert généralement à relier des périphériques (imprimante, téléphone portable, appareils domestiques,...) ou un assistant personnel (PDA: Personal Digital Assistant) à un ordinateur sans liaison filaire ou bien à permettre la liaison sans fil entre deux machines très peu distantes. Les technologies utilisées pour les WPAN sont : Bluetooth, ZigBee (LR-WPAN - IEEE 802.15.4), ...etc

I.2.2.2 Réseaux locaux sans fils (WLAN)

Le réseau local sans fil (WLAN pour Wireless Local Area Network) est un réseau permettant de couvrir l'équivalent d'un réseau local d'entreprise, soit une portée d'environ

une centaine de mètres. Il permet de relier les terminaux présents dans la zone de couverture entre eux. Exemple : Le WiFi (ou IEEE 802.11)

I.2.2.3 Réseaux métropolitains sans fil (WMAN)

Le réseau métropolitain sans fil (WMAN pour Wireless Metropolitan Area Network) est connu sous le nom de Boucle Locale Radio (BLR). Les WMAN sont basés sur la norme IEEE 802.16. La boucle locale radio offre un débit utile de 1 à 10 Mbit/s pour une portée de 4 à 10 kilomètres et utilise les bandes de fréquences entre 2,4 GHz et 3,5 GHz, ce qui destine principalement cette technologie aux opérateurs de télécommunication.

I.2.2.4 Réseaux étendus sans fil (WWAN)

Le réseau étendu sans fil (WWAN pour Wireless Wide Area Network) est également connu sous le nom de réseau cellulaire mobile. Il s'agit des réseaux sans fil les plus répandus puisque tous les téléphones mobiles sont connectés à un réseau étendu sans fil. Les principales technologies sont les suivantes: GSM (*Global System for Mobile Communication*), GPRS (*General Packet Radio Service*), UMTS (*Universal Mobile Telecommunication System*)

I.2.2.5 Les réseaux cellulaires

Un réseau sans fil cellulaire supprime certaines liaisons filaires entre les entités du réseau et substitue le mode de connexion filaire par une technologie nouvelle basée sur les ondes radioélectriques. Ce mode impose de fixer des bornes pour délimiter une région appelée zone de couverture. La figure suivante schématise les principales caractéristiques des réseaux cellulaires (avec infrastructure).

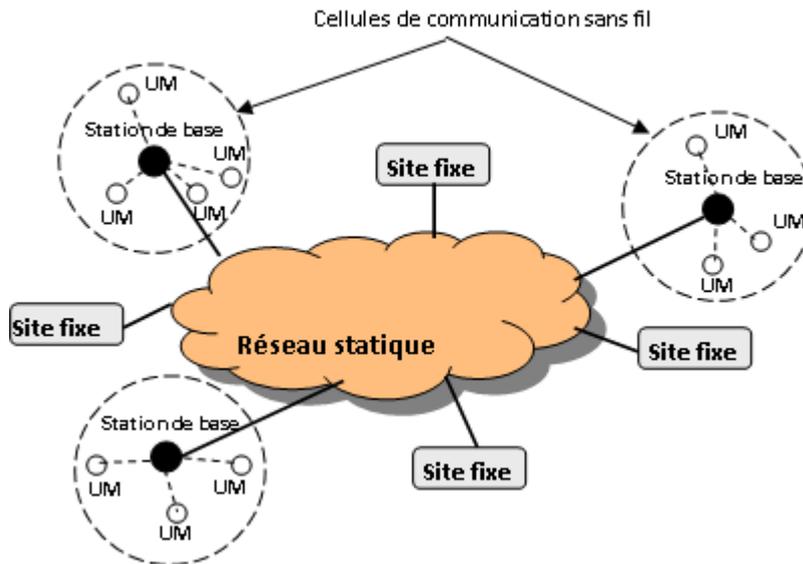


Figure I.2 : Schéma d'un réseau cellulaire

Parmi les sites fixes, on retrouve les stations de bases SB (les cercles noirs sur le schéma), appelées aussi points d'accès. Chaque station de base définit une région appelée *cellule*. Celle-ci correspond à la zone de couverture à partir de laquelle les unités mobiles (UM) peuvent émettre et recevoir des messages via des liaisons sans fil ayant une bande passante limitée qui réduit sévèrement le volume d'informations échangées.

La communication entre deux nœuds (UM) connectés à deux points d'accès différents passe forcément par les SB correspondant aux cellules. Ces SB sont reliées entre elles par des liens filaires.

I.2.2.6 Les réseaux Ad Hoc (sans infrastructure)

Ce sont un type particulier des réseaux sans fil, qui étendent la notion de mobilité pour lui donner un sens beaucoup plus fort. La principale caractéristique qui fait la différence entre ce type de réseaux sans fil et un réseau sans fil classique est l'absence d'une infrastructure préexistante.

I.2.2.6.1 Définition

Un réseau ad hoc, appelé généralement MANET (Mobile Ad hoc Network), est une collection d'unités mobiles munies d'interfaces de communication sans fil, formant un réseau temporaire sans recourir à aucune infrastructure fixe ou administration centralisée [4]. Dans de tels environnements, les unités se comportent comme des hôtes et/ou des routeurs.

Les nœuds des MANETs sont équipés d'émetteurs et de récepteurs sans fil utilisant des antennes qui peuvent être omnidirectionnelles (broadcast), fortement directionnelles (point à point), ou une combinaison de ces deux types. Ils maintiennent d'une manière coopérative la connectivité du réseau, en fonction de leurs positions, la configuration de leurs émetteurs/récepteurs, la puissance de transmission et les interférences entre les canaux de communication. La modélisation de cette connectivité est détaillée dans la section suivante. Un réseau ad hoc peut être isolé, mais il peut aussi avoir des passerelles ou des interfaces qui le relie à un réseau fixe.

I.2.2.6.2 Modélisation d'un système de réseau Ad Hoc

A un instant t , un réseau ad hoc peut être modélisé par un graphe non orienté $G_t = (V_t, E_t)$, où V_t représente l'ensemble des nœuds (c-à-d les unités mobiles), et E_t représente l'ensemble des liens existants entre ces nœuds (la figure).

Si $e = (u, v) \in E_t$, cela veut dire que les nœuds u et v sont en mesure de se communiquer directement à l'instant t .

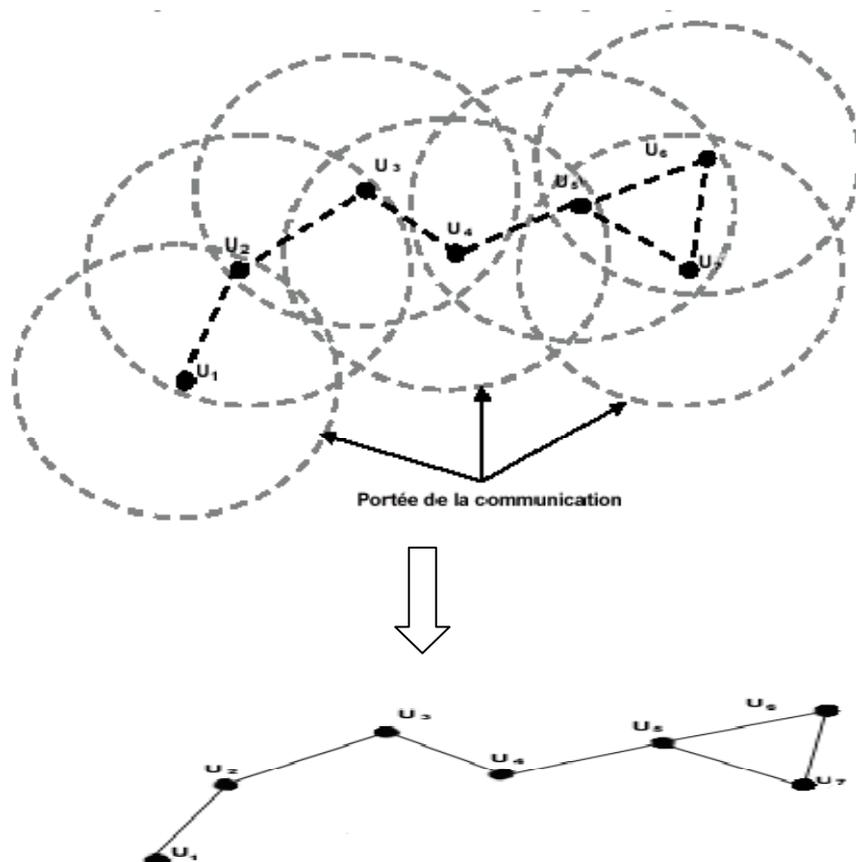


Figure I.3 : Modélisation du réseau Ad hoc

La mobilité des nœuds appartenant à un réseau ad hoc fait que sa topologie peut changer à n'importe quel moment, ce qui entraîne les déconnexions fréquentes (figure I.4).

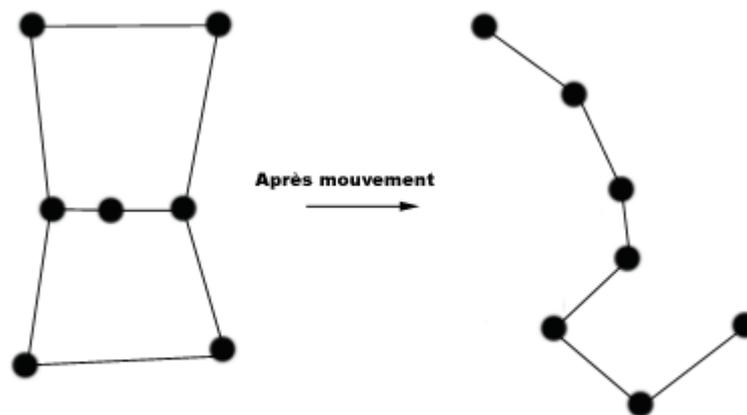


Figure I.4: Changement de topologie dans les réseaux Ad Hoc

I.2.2.6.3 Caractéristiques des réseaux Ad Hoc

Les réseaux ad hoc héritent des mêmes propriétés et problèmes liés aux réseaux sans fil. Particulièrement, le fait que le canal radio soit limité en termes de capacité, plus exposé aux pertes (comparé au médium filaire) et sujet à des variations dans le temps. En outre, les liens sans fil sont asymétriques et non sécurisés.

D'autres caractéristiques spécifiques aux réseaux ad hoc conduisent à ajouter une complexité et des contraintes supplémentaires qui doivent être prises en compte lors de la conception des algorithmes et des protocoles réseaux, à savoir [5]:

❖ Absence d'une infrastructure centralisée

Les nœuds d'un réseau Ad hoc travaillent dans un environnement totalement distribué, ce qui leur permet de se déplacer librement. Cette caractéristique donne plus de liberté aux nœuds, mais ceux-ci doivent assurer des fonctionnalités supplémentaires par rapport aux nœuds d'un réseau sans fil avec infrastructure, puisqu'ils doivent agir en tant que routeurs pour établir les communications entre les autres nœuds.

❖ Les interférences

Il est reconnu que les taux d'erreurs de transmission dans les réseaux radio sont nettement plus élevés que dans les réseaux filaires. Cela est dû, généralement aux problèmes d'interférences, peuvent être de natures diverses.

1. Le nombre limité de canaux disponibles.
2. Les fréquences d'émissions sont proches, ainsi, les émetteurs travaillant à des fréquences trop proches peuvent interférer entre eux.
3. Les bruits produits par l'environnement (certains équipements électriques, certains moteurs...)
4. Phénomènes d'atténuation, de réflexion et des chemins multiples qui rendent le signal incompréhensible en le déformant.

❖ Topologies dynamiques

Une particularité très importante qui distingue les réseaux mobiles ad hoc des autres réseaux est la mobilité des nœuds qui les forment. Ces nœuds se déplacent librement dans le réseau, et à tout moment, des nœuds actifs peuvent quitter le réseau ou de nouveaux nœuds peuvent le rejoindre. Cette caractéristique rend la topologie de ce type de réseaux sans fil très dynamique.

❖ Liaison à débits variables et bande passante limitée

Les liaisons radio présentent des débits variables et ont généralement une bande passante limitée, toujours inférieure à celle des liaisons filaires. La demande sur les applications distribuées dépassera souvent la capacité du réseau. Comme le réseau mobile est souvent une simple extension d'un réseau fixe, les utilisateurs mobiles ad hoc demanderont les mêmes services.

❖ Utilisation limitée de l'énergie

Les nœuds d'un réseau mobile Ad hoc sans généralement des ordinateurs portables, des téléphones portables, des PDA,... Pour un bon fonctionnement du réseau, ces nœuds doivent être les plus autonomes que possible et ce en minimisant leur consommation en énergie. Il faut donc économiser autant que possible les transmissions inutiles.

❖ Sécurité physique limitée

De leur nature, les réseaux sans fil sont très sensibles aux attaques extérieures. La topologie de ces réseaux favorise ce genre de menaces, donc on ne peut appliquer les techniques traditionnelles conçues pour les réseaux filaires. L'implémentation d'une solution pour sécuriser le réseau est plus que nécessaire, surtout en sachant que le premier champ d'application de ces réseaux est les applications militaires qui exigent une confidentialité extrême des informations échangées. Notons cependant un avantage dans le fait que le contrôle des réseaux ad hoc soit décentralisé, évitant ainsi les problèmes pouvant survenir sur les points centraux dans des approches plus centralisées.

I.3 Les réseaux de capteurs

I.3.1 Un capteur

Dans la littérature, un capteur est un dispositif qui transforme l'état d'une grandeur physique observée en une grandeur utilisable, exemple : une tension électrique, une hauteur de mercure, la déviation d'une aiguille, etc. Le capteur se distingue de l'instrument de mesure par le fait qu'il ne s'agit que d'une simple interface entre un processus physique et une information manipulable. Par opposition, l'instrument de mesure est un appareil autonome se suffisant à lui-même. Il dispose donc d'un affichage et peut être d'un système de stockage des données. Ce qui n'est pas forcément le cas du capteur [8].

L'établissement d'un réseau de capteur sans fils exige tout d'abord que les nœuds répondent aux besoins qui viennent des conditions spécifiques qu'une application donnée demande: ils doivent être généralement petits, à faible coût, énergétiquement efficaces, équipés par des sondes appropriés, des ressources de calcul et de stockage nécessaires, et d'équipements de communication adéquats.

Dans le choix des composants matériel pour un nœud de capteur sans fils, l'application joue un facteur décisif surtout pour la taille et la consommation d'énergie du des équipements. A titre d'exemple, un nœud doit être de petite taille, il ne pèse pas plus que 100 g, coûte moins que 1 \$ et consomme moins de 100 μ W. Dans les plus réalistes des applications, la taille d'un nœud n'est pas aussi importante; plutôt, la convenance, l'alimentation simple en énergie, et le coût sont plus importants [9].

I.3.1.1 Composants du capteur

L'architecture d'un nœud est complètement dépendante de l'objectif de son déploiement. Néanmoins, quatre unités de base sont présentes dans chaque capteur : l'unité de captage, l'unité de traitement, l'unité de transmission et l'unité de contrôle d'énergie. En outre, il peut contenir, suivant son domaine d'application, des modules supplémentaires tels qu'un générateur d'énergie pour les cellules solaires, un système de localisation (GPS) ou un système mobilisateur chargé de déplacer les nœuds capteurs en cas de nécessité.

Le schéma suivant représente l'architecture générale d'un nœud capteur :

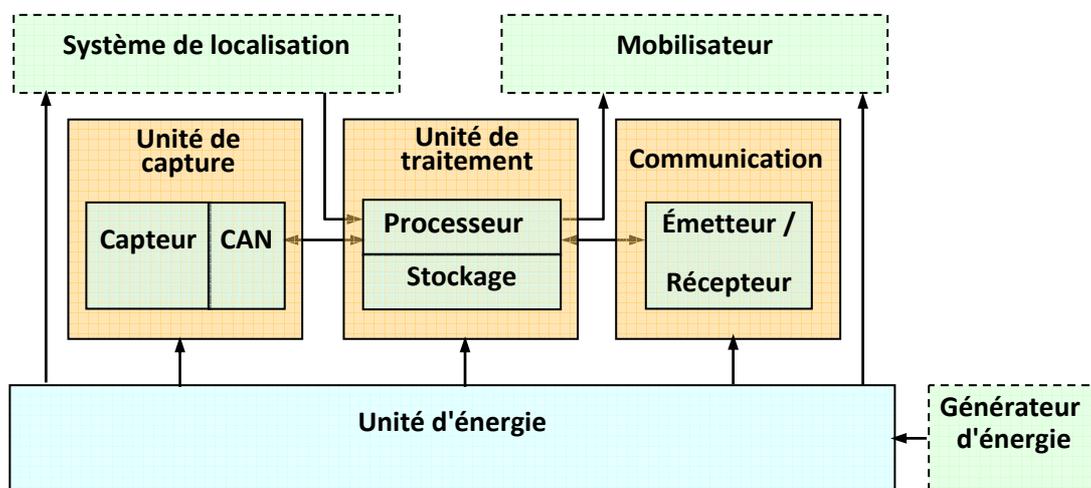


Figure I.5 : Architecture général d'un nœud capteur

➤ L'unité de captage

L'unité de captage est généralement composée de deux sous-unités : le capteur lui-même et un convertisseur Analogique/Numérique. 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.

➤ Unité de traitements

composée d'un processeur et d'une mémoire intégrant un système d'exploitation spécifique (TinyOS , par exemple). Cette unité possède deux interfaces, une interface pour l'unité d'acquisition et une interface pour l'unité de communication. Elle acquiert les informations en provenance de l'unité d'acquisition et les envoie à l'unité de communication.

Cette unité est chargée aussi d'exécuter les protocoles de communications qui permettent de faire collaborer le capteur avec d'autres capteurs. Elle peut aussi analyser les données captées.

➤ **Unité d'émission/réception:**

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 [10], par exemple), ou de type radio-fréquence.

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.

Les unités de transmission de type radio-fréquence comprennent des circuits de modulation, démodulation, filtrage et multiplexage; ce qui implique une augmentation de la complexité et du coût de production du micro-capteur.

Concevoir des unités de transmission de type radio-fréquence avec une faible consommation d'énergie est un véritable défi. En effet, pour qu'un nœud ait une portée de communication suffisamment grande, il est nécessaire d'utiliser un signal assez puissant. Cependant, l'énergie consommée serait importante. L'autre alternative serait d'utiliser de longues antennes, mais ceci n'est pas possible à cause de la taille réduite des micro-capteurs.

Malgré la nécessité de trouver un compromis entre l'élargissement de la portée de communication radio-fréquence et la consommation d'énergie qui en résulte, ce type de communication reste utilisé dans la majorité des projets de recherches portants sur les réseaux de capteurs.

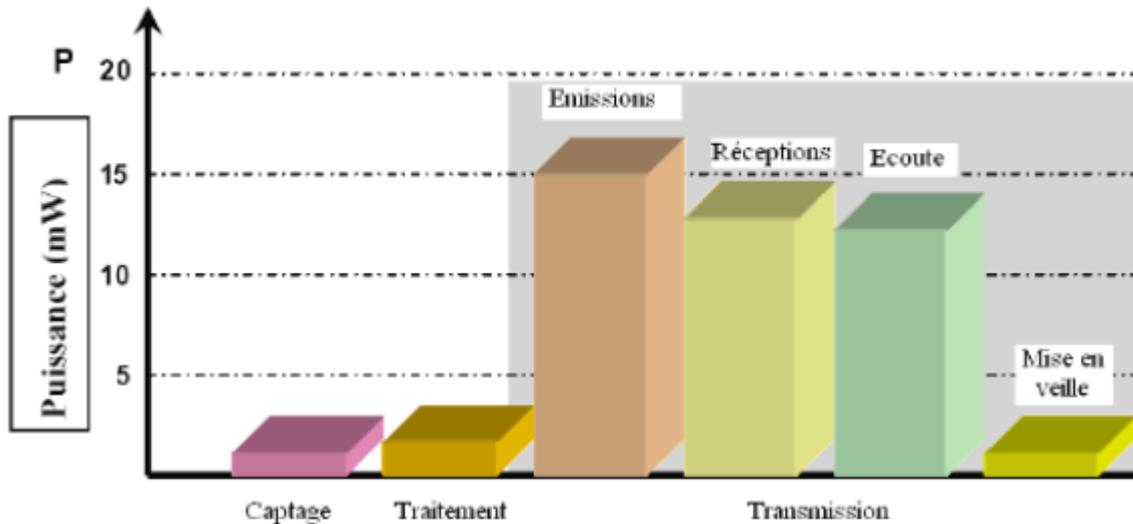


Figure I.6 : Consommation d'énergie en captage, traitement et transmission. [26]

➤ L'unité d'énergie

Un micro-capteur est muni d'une ressource énergétique (généralement une batterie) pour alimenter tous ses composants. Cependant, en conséquence de sa taille réduite, la ressource énergétique dont il dispose est limitée et généralement irremplaçable. Dès lors, l'énergie est la ressource la plus précieuse dans un réseau de capteurs, puisque elle influe directement sur la durée de vie des micro-capteurs et du réseau en entier.

L'unité de contrôle d'énergie constitue donc l'un des systèmes les plus importants. Elle est responsable de répartir l'énergie disponible aux autres modules et de réduire les dépenses en mettant en veille les composants inactifs par exemple. Cette unité peut aussi gérer des systèmes de rechargement d'énergie à partir de l'environnement observé telles que les cellules solaires, afin d'étendre la durée de vie totale du réseau.

Certaines applications ont besoin de savoir l'emplacement du capteur. Pour cette raison, le capteur doit avoir un système de localisation tel qu'un GPS (Global Positioning System). Pour les réseaux de capteurs mobiles, des nœuds doivent se déplacer, donc un mobilisateur doit exister dans les composants du capteur [11].

I.3.1.2 Caractéristiques principales d'un capteur

Deux entités sont fondamentales dans le fonctionnement d'un capteur : l'unité d'acquisition réalise la transmission de celle-ci vers d'autres dispositifs électroniques. Ainsi, fonctionnellement chaque capteur possède un rayon de communication (R_c) et un rayon de

sensation (R_s). La Figure I.7 montre les zones définies par ces deux rayons pour le capteur A. La zone de communication est la zone où le capteur A peut communiquer avec les autres capteurs (le capteur B dans la Figure). D'autre part, la zone de sensation est la zone où le capteur A peut capter l'événement.

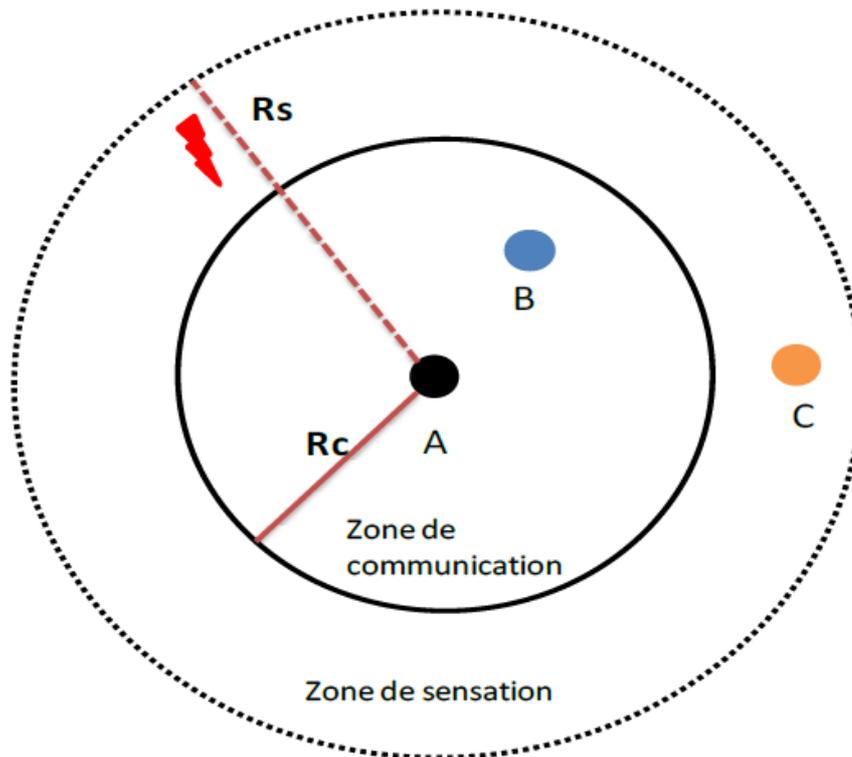


Figure I.7 : Rayons de communication et de sensation d'un capteur

En effet, pour qu'un capteur ait une portée de communication suffisamment grande, il est nécessaire d'utiliser un signal assez puissant. Cependant, l'énergie consommée serait importante [12].

Il existe dans le monde plusieurs fabricants de capteurs. Nous citerons Crossbow, Cisco, Dalsa, EuroTherm, et Sens2B. Parmi ces capteurs, il existe quelques uns qui sont capables de varier la puissance du signal émis afin d'élargir/réduire le rayon de communication et en conséquence la zone de communication. La Figure 1.6 montre un capteur intelligent MICA2 fabriqué par Crossbow [13].

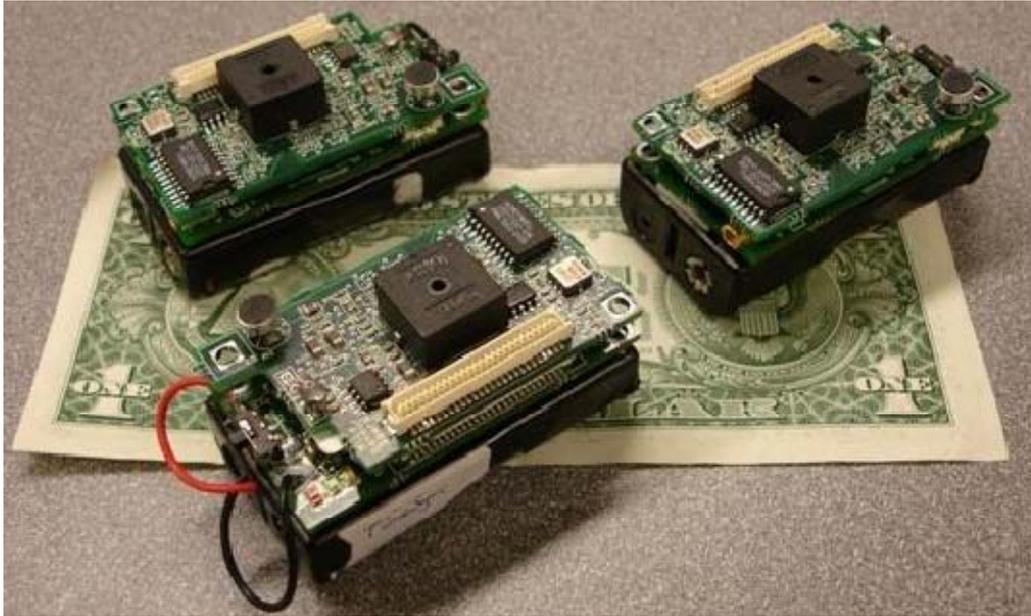


Figure I.8 : Exemple de capteur intelligent MICA2 de Crossbow

I.3.2 Un réseau de capteurs

Un réseau de capteur sans fils (WSN) est constitué d'un nombre plus ou moins grand de nœuds capteurs. Ces nœuds sont autonomes, distribués dans l'espace qui coopèrent pour surveiller des conditions environnementales ou physiques, telle que la température, le bruit, la vibration, la pression, le mouvement, etc. À l'origine, le développement des réseaux de capteur sans fils a été motivé par des applications militaires telle que la surveillance de champ de bataille. Cependant, ce type de réseau est maintenant employé dans plusieurs domaines d'application civils, comme la surveillance d'environnement, d'habitat, la surveillance médicale, l'automatisation des maisons, le contrôle du trafic... [14]

I.3.2.1 Caractéristiques des réseaux de capteurs

- ❖ *Energie limitée* : les réseaux de capteurs sans fil (RCSF) visent la consommation d'énergie puisque l'alimentation de chaque nœud est assurée par une source d'énergie limitée et généralement irremplaçable à cause de l'environnement hostile où il est déployé. De ce fait, la durée de vie d'un RCSF dépend fortement de la conservation d'énergie au niveau de chaque nœud.

- ❖ *Modèle de communication* : Les nœuds dans les RCSF communiquent selon un paradigme plusieurs-à-un (many to one). En effet, les nœuds capteurs collectent des informations à partir de leur environnement et les envoient toutes vers un seul nœud qui représente le centre de traitement [27].
- ❖ *Densité de déploiement* : Elle est plus élevée dans les RCSF que dans les réseaux Ad Hoc. Le nombre de nœuds capteurs peut atteindre des millions de nœuds pour permettre une meilleure granularité de surveillance. De plus, si plusieurs nœuds capteurs se retrouvent dans une région, un nœud défaillant pourra être remplacé par un autre.
Cependant, la densité de déploiement donne naissance à des challenges pour la communication entre les nœuds. En effet, elle provoque des collisions ou des endommagements des paquets transmis.
- ❖ *Absence d'adressage fixe des nœuds* : Les nœuds dans les réseaux sans fil classiques sont identifiés par des adresses IP. Cependant, cette notion n'existe pas dans les RCSF. Ces derniers utilisent un adressage basé sur l'attribut du phénomène capté, on parle donc de l'adressage basé-attribut. En effet, les requêtes des utilisateurs ne sont pas généralement destinées à un seul nœud, mais plutôt, à un ensemble de nœuds identifiés par un attribut. Par exemple, identifier un ensemble de nœuds par « les nœuds qui captent le volume du CO₂ dépassant 0,0375 % dans l'atmosphère » [27].
- ❖ *Limitations de ressources physiques* : A cause de la miniaturisation des composants électroniques, les performances des nœuds capteurs sont limitées. Par conséquent, les nœuds capteurs collaborent en traitant partiellement les mesures captées et envoient seulement les résultats à l'utilisateur. Une autre conséquence [28], ces limitations imposent des portées de transmission réduites contraignant les informations à être relayées de nœud en nœud avant d'atteindre le destinataire. C'est la raison pour laquelle les RCSF adoptent des communications multi-sauts.
- ❖ *Sécurité* : En plus des problèmes de sécurités dans les réseaux Ad Hoc en général, les RCSF rencontrent d'autres handicaps dus à leurs challenges, à savoir l'autonomie et la miniaturisation des capteurs. Cela engendre l'inapplicabilité des mécanismes de défense utilisés dans les réseaux Ad Hoc tout en créant d'autres mécanismes de sécurité pour les RCSF. De plus l'absence d'une sécurité physique dans l'environnement hostile où ils sont déployés expose les nœuds à un danger qui tend vers la falsification de l'information [27].

I.3.2.2 Applications des réseaux de capteurs

La taille de plus en plus réduite des micro-capteurs, le coût de plus en plus faible, la large gamme des types de capteurs disponibles (thermique, optique, vibrations,...) ainsi que le support de communication sans fil utilisé, permettent aux réseaux de capteurs d'envahir plusieurs domaines d'applications. Ils permettent aussi d'étendre les applications existantes et de faciliter la conception d'autres systèmes tels que le contrôle et l'automatisation des chaînes de montage.

Les réseaux de capteurs ont le potentiel de révolutionner la manière même de comprendre et de construire les systèmes physiques complexes. Les réseaux de capteurs peuvent se révéler très utiles dans de nombreuses applications lorsqu'il s'agit de collecter et de traiter des informations provenant de l'environnement. Parmi les domaines où ces réseaux peuvent offrir les meilleures contributions, nous citons les domaines : militaire, environnemental, domestique, santé, sécurité, etc. Des exemples d'applications potentielles dans ces différents domaines sont exposés ci-dessous.

➤ Les applications militaires

Comme dans le cas de plusieurs technologies, le domaine militaire a été le point de départ du développement des réseaux de capteurs. Nous pouvons citer quelques exemples d'applications dans ce domaine [17].

- **Le contrôle et la gestion des forces:** surveiller le statut et l'emplacement des troupes et des armements afin d'améliorer le contrôle, la communication et le commandement.
- **La surveillance et le contrôle des champs de bataille:** un réseau de capteurs est déployé à partir d'un avion dans un champ d'intérêts, ensuite les capteurs vont se réorganiser afin d'exécuter les tâches prévues (analyser le terrain, détecter et poursuivre des objets ennemis, ...etc.).
- **La protection:** les objets sensibles, par exemple: les stations nucléaires, les ponts, les canaux de pétrole et du gaz, les stations de communications, les réserves d'armes, et les quartiers militaires, peuvent être protégé par un réseau de capteurs intelligent capable de distinguer les différentes classes d'intrus.



Figure I.9 : Réseau de capteurs militaire.

➤ **La surveillance de l'environnement et l'agriculture**

C'est le champ qui apporte le grand intérêt au réseau de capteurs. Plusieurs applications peuvent montrer l'utilité de ce genre de réseaux, parmi lesquelles on cite:

- **La précision d'agriculture:** les informations collectées par un réseau de capteurs, dans un terrain, sur le climat et l'état de la terre, permettent un contrôle précis de l'utilisation de l'eau et des engrais.
- **L'évolution des plantes:** étudier l'évolution des différentes espèces de plantes dans les grandes forêts, ou dans les profondeurs sous marines, où la présence de l'homme est quasi impossible.



Figure I.10 : Des capteurs dans des fausses branches

- **Exploration planétaire:** exploration et surveillance dans les environnements hostiles, par exemple les volcans, les régions toxiques, ... etc.
- **La surveillance géophysique:** les activités sismiques peuvent être détectées et étudiées à l'aide d'un réseau de capteurs implanté dans les régions sensibles.
- **La détection des désastres:** par exemple les feux dans les forêts, les inondations de la neige, une pollution dans l'atmosphère ..., peuvent être détectés et leurs causes peuvent être localisées par le déploiement d'un réseau de capteurs [17].

➤ **La surveillance des Habitats**

L'utilisation des réseaux de capteurs dans ce champs de recherches a permis aux scientifiques d'étudier les comportements des animaux, oiseaux, ou poissons dans leurs milieux, où il était presque impossible avant de le faire. Ce genre de recherches a un grand intérêt pour l'humanité, parce qu'il permet de surveiller et protéger les différentes espèces menacées d'extinction.

Ce domaine peut apporter aussi un grand intérêt aux sociologues. Équiper des personnes avec des capteurs permet d'étudier les interactions humaines et les comportements sociaux.

➤ **L'industrie**

Les réseaux de capteurs sont largement utilisés dans le champ industriel, soit dans les chaînes de production, pour la sécurité, ou même dans les produits.

- **Contrôle et maintenances dans les équipements industriels:** Les robots industriels complexes sont équipés de centaines de capteurs qui sont généralement connectés par des câbles à un ordinateur principal qui assure le contrôle. Puisque les câbles sont plus chers et plus gênants pour les mouvements des robots, ils sont remplacés par des connexions sans fil.
- **La sécurité industrielle:** Les grandes usines de nos jours sont équipées par des appareils très complexes, parfois des équipements pour des produits chimiques qui sont dans la plupart du temps toxiques, donc la moindre mauvaise manipulation peut conduire à une catastrophe. Déployer un réseau de capteurs dans un tel environnement permet de détecter et de réagir rapidement à un tel incendie.
- **Les moyens de transport:** la plupart des moyens de transport de nos jours (véhicule, avion, ...) sont équipés de dizaines même de centaines de capteurs/actionneurs reliés entre eux en réseau communiquant avec des stations de calcul, des bases de données, ou même avec des satellites pour améliorer la sécurité et l'efficacité du trafic [17].

➤ **La santé**

Le champ de contrôle de santé (Health monitoring) représente un grand marché pour les réseaux de capteurs sans fil qui a tendance à croître très rapidement. On peut distinguer deux grandes classes pour les applications de contrôle de santé [28]:

- **La surveillance médicale:** les données physiologique comme la température du corps, la tension artérielle, la quantité de sucre dans le sang, et les pulsations du cœur sont surveillés et automatiquement transmises vers un ordinateur ou un médecin, qui peut les utiliser pour l'exploration et le control médical.
- **La microchirurgie:** où des très petits robots peuvent collaborer pour accomplir une opération chirurgicale microscopique.



Figure I.11 : Application des réseaux de capteurs en médecine.

➤ **Maison, bureau, et vie civile**

Les maisons et les bureaux de travail peuvent être équipés de dizaines de capteurs qui surveillent la température et l'humidité pour contrôler la climatisation et le chauffage. Les PCs peuvent être équipés de claviers et souris sans fil et peuvent être relié entre eux en réseau ad hoc pour faire des travaux collaboratifs et collecter des informations vers une station de calculs pour accomplir un traitement centralisé.

Des réseaux de capteurs peuvent être déployés dans les différentes structures de la ville: ponts, bâtiments, réservoirs d'eau et d'énergie (électricité, carburant, gaz), afin de les surveiller et détecter le moindre danger le plus tôt possible.

Un réseau de capteurs de mouvement peut constituer un système d'alarme distribué qui servira à détecter les intrusions sur un large secteur. Déconnecter le système ne serait plus aussi simple, puisque il n'existe pas de point critique.

Utiliser des réseaux de capteurs dans les routes et les rails permet une meilleure planification urbaine [17].

I.3.2.3 Architecture d'un réseau de capteurs

L'architecture des réseaux de capteurs sans fils utilise beaucoup de sources.

Historiquement, beaucoup du travail relatif a été effectué dans le contexte des réseaux à auto-organisation, mobiles et Ad Hoc.

Un réseau de capteurs est constitué essentiellement de : plusieurs nœuds capteurs, un nœud Sink et un centre de traitement des données [15] :

- **Nœuds**: Ceux sont des capteurs, leur type, leur architecture et leur disposition géographique dépendent de l'exigence de l'application en question. Leur énergie est souvent limitée puisqu'ils sont alimentés par des piles.
- **Sink** : c'est un nœud particulier du réseau. Il est chargé de la collecte des données issues des différents nœuds du réseau. Il doit être toujours actif puisque l'arrivée des informations est aléatoire. C'est pourquoi son énergie doit être illimitée. Dans un réseau de capteur sans fils plus ou moins large et à charge un peu élevée, on peut trouver deux Sink ou plus pour alléger la charge.

Il y a essentiellement trois types de Sink [9] :

- ✓ Un nœud appartenant au réseau comme n'importe quel autre nœud.
- ✓ Une entité extérieure au réseau. Pour ce deuxième cas, le Sink peut être un dispositif extérieur, par exemple, un ordinateur portable ou un PDA interagissant avec le réseau.
- ✓ Une passerelle vers un autre réseau tel que l'Internet, où la demande de l'information vient d'un certain centre de traitement lointain.

La figure I.12 illustre les principaux types de Sink et montre des sources et des Sink en communication directe.

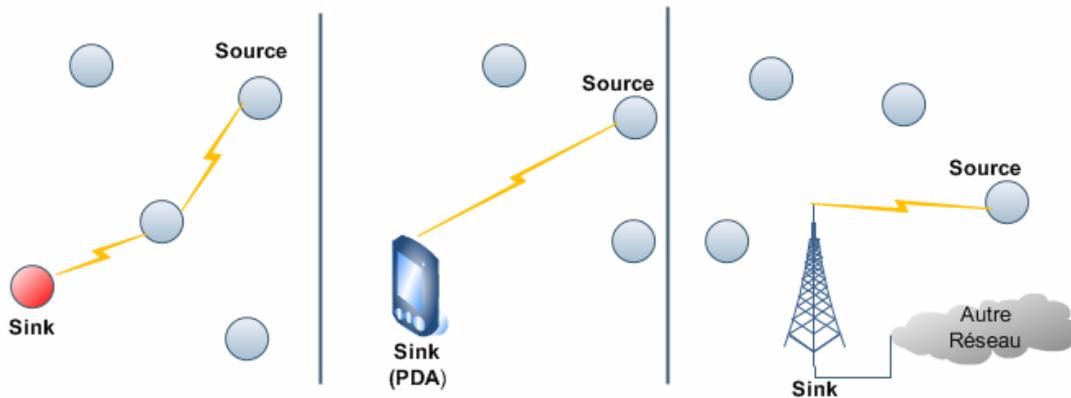


Figure I.12 : Différents type de Sink

- **Centre de traitement des données :** c'est le centre vers lequel les données collectées par le Sink sont envoyées. Ce centre a le rôle de regrouper les données issues des nœuds et les traiter de façon à en extraire de l'information utile exploitable. Le centre de traitement peut être éloigné du Sink, alors les données doivent être transférées à travers un autre réseau, c'est pourquoi on introduit une passerelle entre le Sink et le réseau de transfert pour adapter le type de données au type du canal (comme c'est illustré dans la figure).

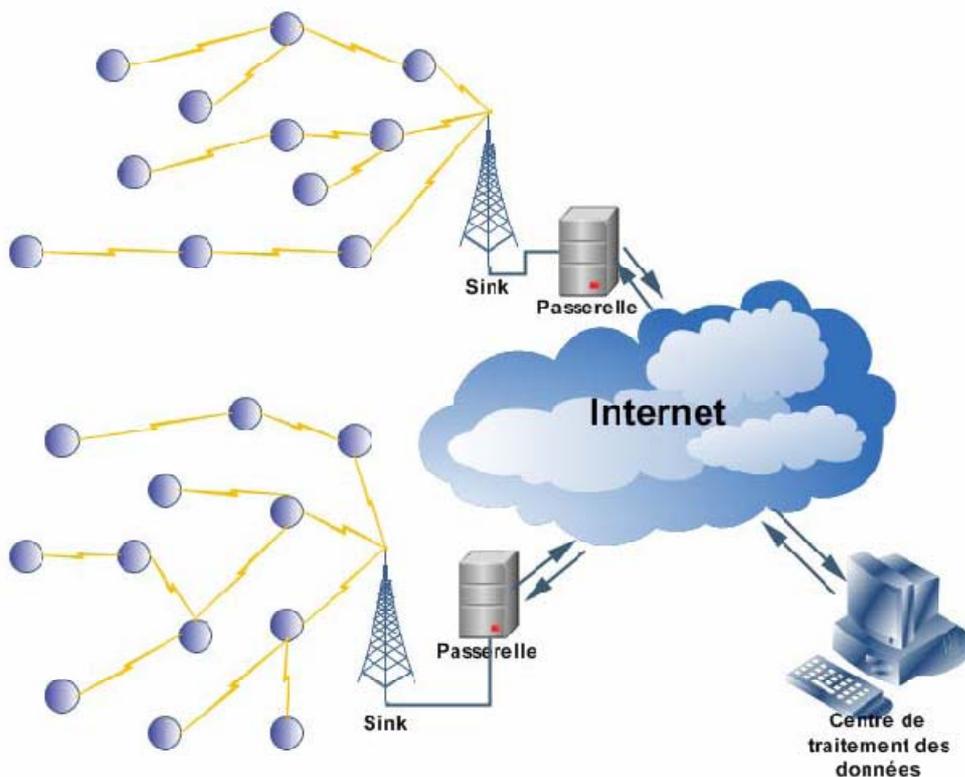


Figure I.13 : Architecture générale d'un réseau de capteurs sans fil

I.3.2.4 Types de mobilité dans les réseaux de capteurs sans fils

La vertu principale de la communication sans fils est sa capacité de soutenir les participants mobiles. Dans les réseaux de capteurs sans fils, la mobilité peut apparaître sous trois formes principales [15] :

I.3.2.4.a Mobilité de nœud

La signification d'une telle mobilité est fortement liée l'application en question. Par exemple, dans le contrôle de l'environnement, la mobilité du nœud n'existe pas, par contre dans la surveillance des animaux (nœud attaché à un animal). Face à la mobilité du nœud, le réseau doit se réorganiser assez fréquemment pour pouvoir fonctionner correctement.

I.3.2.4.b Mobilité du Sink

C'est un cas spécial de mobilité de nœud, l'aspect important c'est la mobilité d'un récepteur d'informations qui ne fait pas partie du réseau de capteurs, par exemple, l'information peut être demandée par un utilisateur via un PDA tout en se déplaçant dans le réseau.

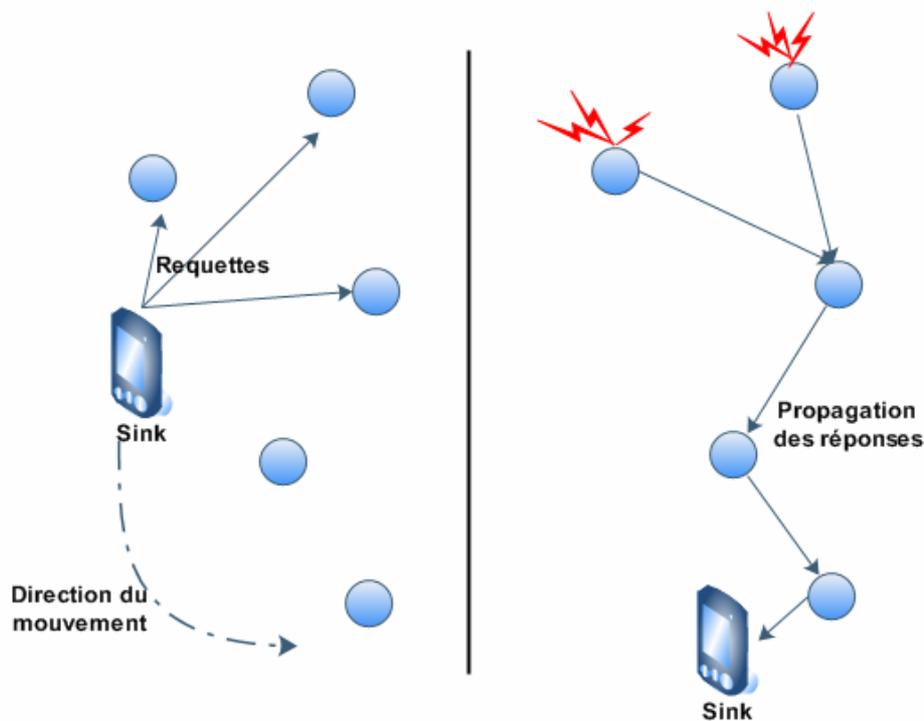


Figure I.14 : Mobilité du Sink

I.3.2.4.c Mobilité de l'événement

Ce type de mobilité existe essentiellement dans les applications de détection des événements et de suivi des cibles. Dans un tel type d'application, il est (habituellement) important que l'événement observé soit couvert par un nombre suffisant de nœuds. Par conséquent, les nœuds vont se réveiller autour de l'objet, pour le surveiller avec un taux d'activité élevée, et puis entrent en sommeil (mode *Sleep*). Pendant que la source d'événement se déplace à travers le réseau, elle est accompagnée d'un secteur d'activité dans le réseau qui le suit (c'est le modèle de *frisbee*).

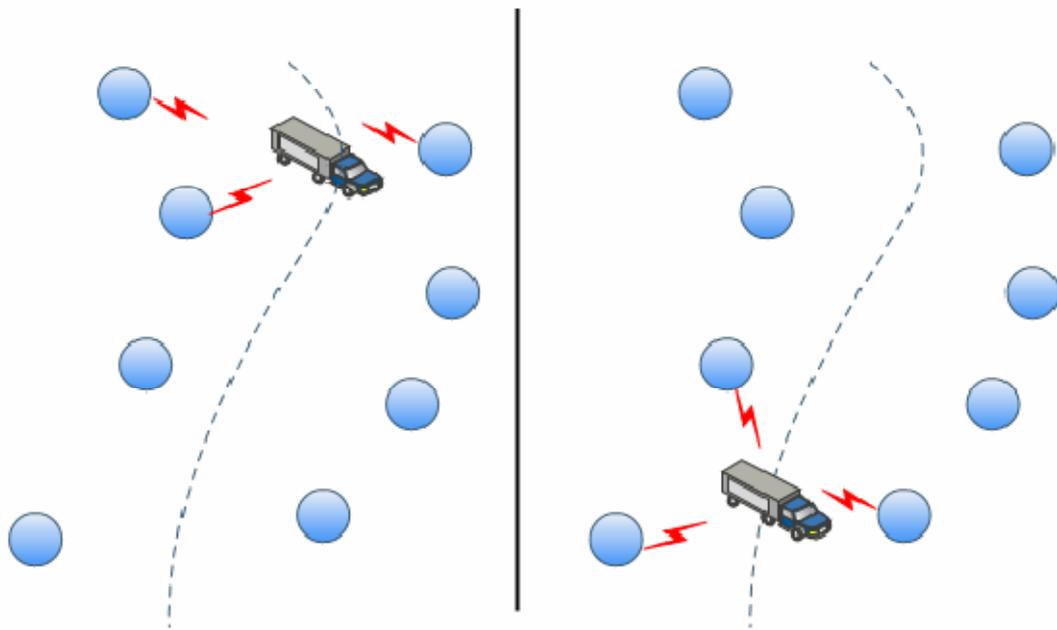


Figure I.15 : Mobilité de l'événement

La figure décrit la notion de la mobilité de l'événement, ceci consiste à détecter un véhicule et de l'observer pendant son déplacement. Les nœuds qui ne détectent rien entrent en sommeil à moins qu'ils soient invités à transmettre de l'information de la zone d'activité à un certain Sink distant.

I.3.2.5 Topologies des réseaux de capteurs sans fils

Les nœuds capteurs sont organisés en réseaux de capteurs. Chacun de ces réseaux a la capacité de collecter des données et de les transférer au nœud de synchronisation central (PUITS) par l'intermédiaire d'une architecture multi saut. Le PUITs transmet ensuite ces données par Internet ou par satellite à l'ordinateur central (gestionnaire des tâches).

Il existe deux types d'architectures pour les réseaux de capteurs : les réseaux de capteurs plats et les réseaux de capteurs hiérarchiques.

❖ **Topologie plate (Flat) :**

Les protocoles à topologie plate (*flat*) considèrent que tous les nœuds sont égaux, ont les mêmes fonctions, et peuvent communiquer entre eux sans devoir passer par un nœud particulier ou une passerelle. Seul un nœud particulier, le *Sink*, est chargé de la collecte des données issues des différents nœuds capteurs afin de les transmettre vers les centres de traitement.

En cas où la destination ne fait pas partie du voisinage de la source, les données seront transmises en utilisant les sauts multiples à travers les nœuds intermédiaires comme c'est illustré dans la figure. Ce type de réseau représente l'avantage de l'existence de différents chemins d'une source vers une destination et c'est pour remédier au problème de changement brusque de topologie ou la défaillance d'un nœud intermédiaire [16].

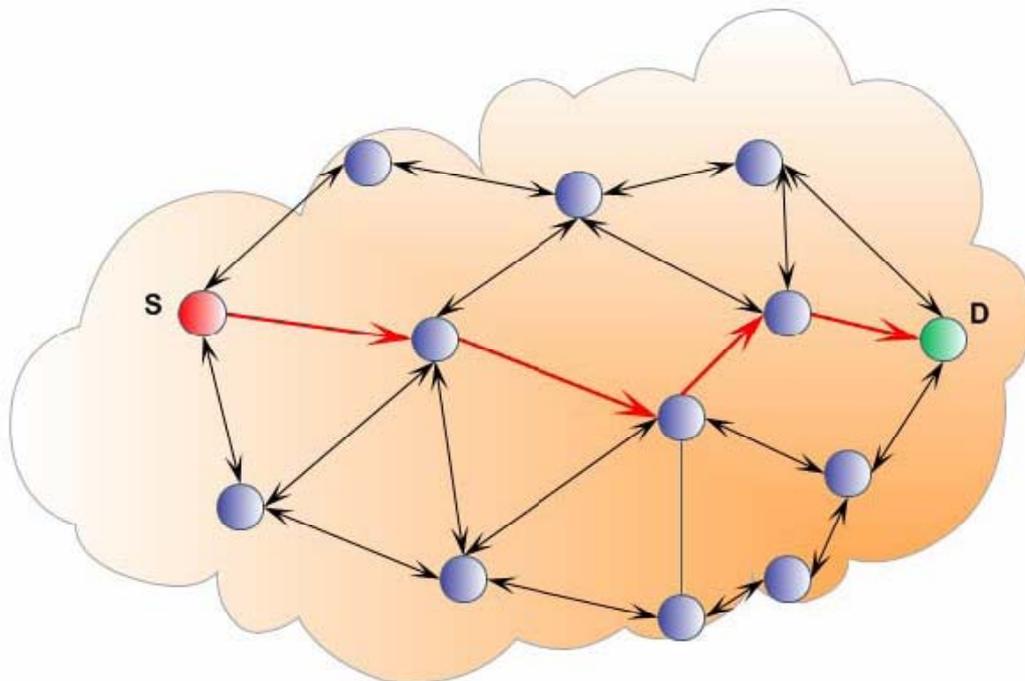


Figure I.16 : Topologie plate (Flat)

À titre d'exemple des protocoles utilisant une topologie plate on peut citer le protocole Direct Diffusion.

❖ Topologie Hiérarchique

Les protocoles à topologie hiérarchique forment des réseaux dans lesquels un noeud central *Sink* (le niveau supérieur de la hiérarchie) est relié à un ou plusieurs autres noeuds qui appartiennent à un niveau plus bas dans la hiérarchie (deuxième niveau) avec une liaison point à point. Aussi, chacun des noeuds du deuxième niveau aura également un ou plusieurs autres noeuds de niveau plus bas dans la hiérarchie (troisième niveau) reliés à lui avec une liaison point à point. Chaque ensemble de noeuds forme une sorte de motif (Cluster). Le noeud central n'a aucun autre noeud au-dessus de lui dans la hiérarchie sauf le centre de traitement des données ou la passerelle si elle existe. Les noeuds du deuxième niveau jouent le rôle des passerelles entre ceux du troisième niveau et le Sink. Dans ce cas, le routage devient plus simple, puisqu'il s'agit de passer par les passerelles pour atteindre le noeud destination.

Un réseau basé sur une topologie hiérarchique doit avoir au moins trois niveaux dans sa hiérarchie, puisqu'un réseau avec un noeud central *Sink* et seulement un niveau hiérarchique au-dessous, forme une topologie en étoile.

Si les noeuds dans un réseau basé sur la topologie hiérarchique doivent effectuer un tel traitement sur les données transmises entre les noeuds dans le réseau, alors les noeuds qui sont à des niveaux plus élevés dans la hiérarchie doivent effectuer plus de traitement que les noeuds de niveau inférieur [15].

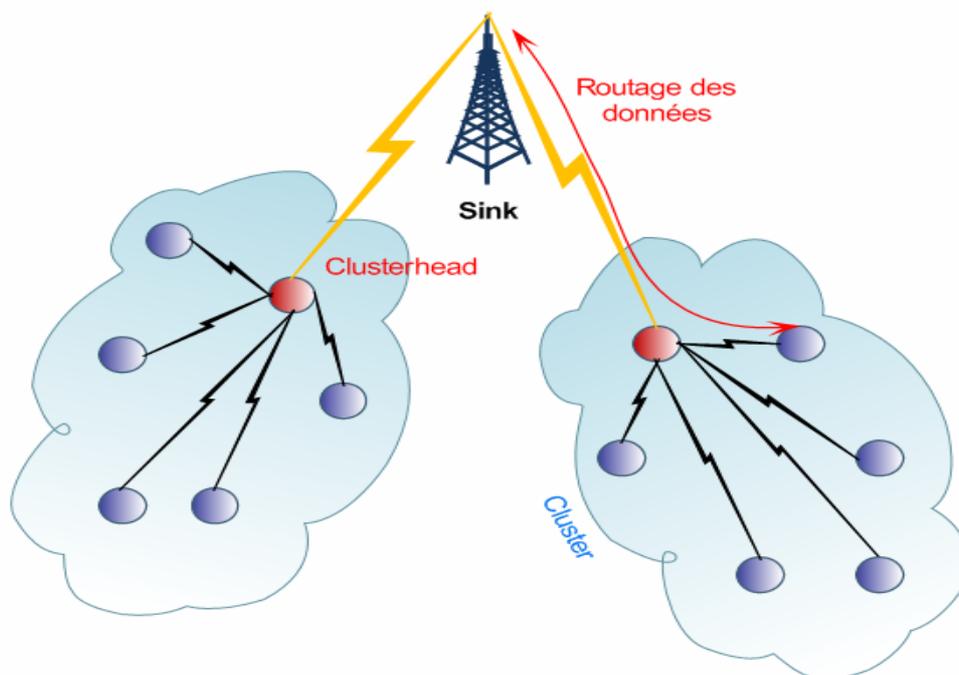


Figure I.17 : Topologie Hiérarchique

À titre d'exemple des protocoles utilisant une topologie hiérarchique on peut citer le protocole LEACH (*Low-energy Adaptive Clustering Hierarchy*), CBRP (*Cluster Based Routing Protocol*).

I.3.2.6 Architecture de communication dans les réseaux de capteurs sans fil

Comme dans les réseaux filaires, l'architecture de communication dans les réseaux de capteurs est divisée en couches. Chaque couche a ses rôles et ses protocoles qui opèrent en dessus. Puisque l'objectif d'un réseau de capteurs n'est pas la communication elle-même et que la consommation d'énergie est un critère très important, d'autres unités doivent exister afin de gérer la consommation d'énergie comme le montre la figure suivante :

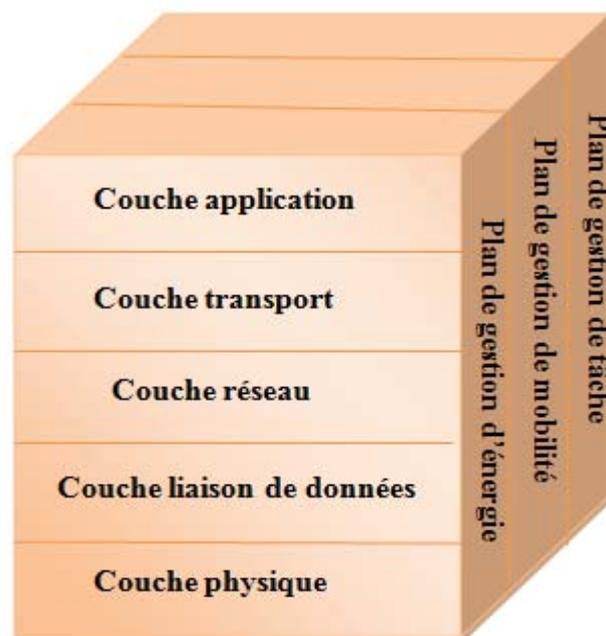


Figure I.18: Pile de protocoles dans les réseaux de capteurs.

➤ Couche application

Elle constitue l'ensemble des applications implémentées sur un réseau de capteurs. Elles doivent fournir des mécanismes pour permettre à l'utilisateur d'interagir avec le réseau (éventuellement, par l'intermédiaire d'un réseau étendu comme Internet) tout en permettant de rendre transparents le matériel et les logiciels utilisés dans les couches inférieures. Ceci, en lui fournissant des interfaces pour la création et la diffusion des requêtes et un moyen d'interpréter les réponses reçues. [17]

Selon les tâches de captage, différents types d'applications logicielles peuvent être implémentés au niveau de la couche application. Nous présentons deux protocoles : SMP, TADAP [18] :

- ✓ **Protocole de gestion de captage SMP** : *Sensing Management Protocol* est un protocole de gestion qui fournit les opérations logicielles nécessaires afin de remplir les tâches administratives suivantes :
 - _ Introduction des règles reliées à l'agrégation de données et au clustering ;
 - _ Echange de données selon les algorithmes de recherche de location ;
 - _ Synchronisation et déplacement des noeuds ;
 - _ Arrêt et démarrage des noeuds ;
 - _ Demande de configuration et reconfiguration du réseau ;
 - _ Authentification, distribution de clé et sécurisation de communication ;
- ✓ **Protocole d'affectation de tâche et d'annonce de données TADAP** : *Task Assignment and Data Advertisement Protocol* fournit aux utilisateurs des applications avec interfaces pour gérer et lancer leur requêtes puis collecter les réponses envoyées. Ces requêtes sont basées sur les attributs (exemple : l'emplacement des noeuds qui captent une température supérieure à 40° ; attribut de température) comme elles peuvent être basées sur la région (exemple : les températures lues par les noeuds de la région A).

➤ **Couche transport**

Cette couche aide à maintenir le flux de données si les applications réseaux le demandent. En général, les principaux objectifs sont :

- _ Relier les applications et la couche réseau ;
- _ Offrir un service de livraison de données entre la source et le collecteur avec un mécanisme de contrôle d'erreur ;
- _ Régulariser la quantité du trafic injecté dans le réseau à l'aide de mécanismes de contrôle de congestion et de flux.

La consommation d'énergie, le traitement de données et les limitations matérielles (ex: mémoire) des noeuds capteurs exigent plus de contraintes pour la détermination du protocole de couche transport. Par exemple, les communications point-à-point conventionnelles, les mécanismes de contrôle d'erreur basé sur la retransmission et le système de fenêtrage qu'adopte le protocole de transport TCP ne peuvent plus être réalisés pour les réseaux de capteurs. [18]

➤ **Couche réseau**

Les capteurs sont déployés avec grande densité dans la surface observée. Ainsi ils peuvent être très proches entre eux. Dans une telle situation une communication multi-saut est la plus adéquate. De plus les noeuds doivent consommer moins d'énergie en transmettant les messages ce qui rend l'utilisation des protocoles de routage traditionnels des réseaux Ad hoc impraticable. Plusieurs techniques sont utilisées dans le routage telles que: le data-centric, l'agrégation des données et le clustering. Dans le chapitre II une taxonomie des différents protocoles de routage sera présentée.

➤ **Couche de liaison de données**

La couche de liaison de données est responsable du multiplexage de données, détection de trame, accès au réseau et contrôle d'erreur. Elle assure la fiabilité des communications point-à-point et multipoint. Toutefois, les contraintes des réseaux de capteurs, les limitations d'énergie et de mémoire déterminent des responsabilités supplémentaires aux protocoles.

Dans ce qui suit, nous détaillons deux principales stratégies de la couche de liaison de données ; protocoles MAC et contrôle d'erreur :

❖ **Medium Access Control « MAC » :**

Puisque l'un des grandes sources de gaspillage de l'énergie et la couche MAC, plusieurs protocoles ont été proposés afin de minimiser la consommation d'énergie dans cette couche. Les méthodes d'accès utilisées par la couche MAC sont divisées en deux classes [19]:

✓ **Accès centralisé:** il existe trois méthodes d'accès centralisé.

• **FDMA (frequency Division Multiple Access)**

En FDMA, la bande passante est découpée en plages de fréquence qui seront allouées aux nœuds communicants de manière équilibrée.

• **TDMA (Time Division Multiple Access)**

En TDMA, les canaux sont multiplexés sous forme d'intervalles de temps de telle manière que chaque utilisateur accède à toute la bande passante allouée pour le système de transmission durant un intervalle donné.

• **CDMA (Code Division Multiple Access)**

En CDMA, chaque utilisateur émet sur une large bande, avec le principe classique de l'étalement de spectre par séquence directe (DSSS), obtenu au moyen d'un code pseudo aléatoire personnel. Ainsi tous les utilisateurs

utilisent simultanément la même bande de fréquences. Cette technique est très souple au niveau des débits transmis, mais relativement complexe car elle peut nécessiter une égalisation sur le récepteur et un contrôle de la puissance d'émission.

✓ **Accès distribué:** il existe deux méthodes d'accès distribué.

- **ALOHA**

ALOHA est une technique d'accès très simple, utilisée au départ par l'université d'Hawaï, pour relier les centres informatiques dispersés sur plusieurs îles. Cette technique est le plus souvent utilisée dans les réseaux satellitaires vu son faible taux d'accès au canal qui avoisine les 20%. Le principe est le suivant: les stations émettent, de façon inconditionnelle, des paquets dès qu'ils sont en leur possession, il n'y a pas d'écoute du support avant la transmission. Dans le cas d'une collision, la station va retransmettre les paquets après un délai aléatoire.

- **CSMA/CA (Carrier Sense Multiple Access - Collision Avoidance)**

Le principe de base du CSMA/CA est d'écouter avant d'émettre puis de tenter d'obtenir l'accès: si le canal est inoccupé lorsqu'une station cherche à transmettre des données, celle-ci envoie ses paquets. Sinon, la station attend la fin de sa temporisation pour gagner le droit d'accès au médium. Lorsque sa temporisation expire, si le canal est inoccupé, la station envoie ses paquets.

❖ **Contrôle d'erreur :**

En plus du contrôle d'accès au média réseau, le contrôle d'erreur dans les données transmises est une autre fonction de la couche liaison de données. En général, les mécanismes de contrôle d'erreur dans les réseaux de communication peuvent être catégorisés en deux principales approches : FEC et ARQ. [18]

L'algorithme ARQ « *Automatic Repeat Request* » est basé sur la retransmission des données perdues. Ce mécanisme encourt donc un coût de transmission et un débordement supplémentaires.

En outre, l'algorithme FEC « *Forward Error Correction* » présente une complexité de décodage inhérente qui exige relativement de ressources de traitement considérables. Or, dans les réseaux de capteurs, ces ressources sont rares et les réserves d'énergie sont

limitées ; d'où, les algorithmes de contrôle d'erreur avec un encodage/décodage peu complexes représentent la meilleure solution pour les réseaux de capteurs.

➤ **Couche physique**

La couche physique est responsable de la sélection de fréquence, génération de porteuse (canal) de fréquence, détection de signal, modulation et cryptage de données. Il est connu que les communications sans fil distantes sont très coûteuses en termes d'énergie et de complexité. La minimisation d'énergie est donc importante pour le choix d'une infrastructure de la couche physique dans les réseaux de capteurs.

Par ailleurs, le choix d'un bon schéma de modulation est critique. L'utilisation d'une modulation m-aire réduit le temps de transmission grâce à l'envoi de plusieurs bits dans un seul symbole. Cependant, elle présente une complexité importante et consomme beaucoup d'énergie. En revanche, la modulation binaire est plus simple et efficace en terme de consommation d'énergie, mais prend plus de temps pour la transmission. Le choix de type de modulation dépend donc du système. L'*Ultra WideBand* (UWB) et la radio impulsion (IR) ont connu une large utilisation dans les applications de communication. L'UWB est caractérisée par une bonne résistance dans les communications multi-sauts, une faible énergie de transmission et de simples circuits d'émission ; ce qui la rend une bonne solution pour les réseaux de capteurs [18].

Le problème de la couche physique dans les réseaux de capteurs est peu exploré. Les nouvelles recherches tentent d'aborder les points suivants :

- _ Schéma de modulation ;
- _ Stratégie de contrôle des effets de propagation de signal ;
- _ Conception d'un matériel trop petit, peu coûteux et économique en énergie.

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 noeuds 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.

○ **Le niveau de gestion d'énergie**

Les fonctions intégrées à ce niveau consistent à gérer l'énergie consommée par les capteurs. Dès lors, un capteur peut par exemple éteindre son interface de réception dès qu'il reçoit un message d'un noeud voisin afin d'éviter la réception des messages

dupliqués. De plus, quand un noeud possède un niveau d'énergie faible, il peut diffuser un message aux autres capteurs pour ne pas participer aux tâches de routage, et conserver l'énergie restante aux fonctionnalités de capture [21].

- **Le niveau de gestion de mobilité**

Ce niveau détecte et enregistre tous les mouvements des noeuds capteurs, de manière à leur permettre de garder continuellement une route vers l'utilisateur final, et maintenir une image récente sur les noeuds voisins. Cette image est nécessaire pour pouvoir équilibrer l'exécution des tâches et la consommation d'énergie [21].

- **Le niveau de gestion des tâches**

Lors d'une opération de capture dans une région donnée, les noeuds composant le réseau ne doivent pas obligatoirement travailler avec le même rythme. Cela dépend essentiellement de la nature du capteur, son niveau d'énergie et la région dans laquelle il a été déployé. Pour cela, le niveau de gestion des tâches assure l'équilibrage et la distribution des tâches sur les différents noeuds du réseau afin d'assurer un travail coopératif et efficace en matière de consommation d'énergie, et par conséquent, prolonger la durée de vie du réseau [21].

I.3.2.7 Contraintes et facteurs influençant l'architecture des WSN

Un ensemble de métriques permet de déterminer le design d'un réseau de capteurs. Ces facteurs influencent sur l'architecture des réseaux de capteurs et le choix des protocoles à implémenter :

- ✓ **La tolérance aux pannes**

La défaillance ou le blocage des noeuds dans un réseau de capteurs peut être engendré par plusieurs causes, notamment l'épuisement d'énergie, l'endommagement physique ou les interférences liées à l'environnement.

La propriété de tolérance aux pannes est définie par l'habilité du réseau à maintenir ses fonctionnalités sans interruptions provoquées par la panne des capteurs. Elle vise donc à minimiser l'influence de ces pannes sur la tâche globale du réseau [22].

- ✓ **L'échelle :**

Le nombre de noeuds déployés pour un projet peut atteindre le million. Un nombre aussi important de noeuds engendre beaucoup de transmissions inter nodales

(implémentation d'une détection d'erreur, d'un contrôle de flux,...) et nécessite que le PUIITS soit équipé de beaucoup de mémoire pour stocker les informations reçues. [23]

✓ **Les contraintes matérielles :**

La principale contrainte matérielle est la taille du capteur. Les autres contraintes sont : que la consommation d'énergie doit être moindre pour que le réseau survive le plus longtemps possible, qu'ils s'adaptent aux différents environnements (fortes chaleurs, eau,...qu'ils soient autonomes et très résistants vu qu'ils sont souvent déployés par avion [23].

✓ **Coût de production :**

Comme les WSN consistent en un grand nombre de nœuds capteurs, le coût d'un seul capteur est très important pour définir le coût total de son réseau. Si ce dernier est plus cher que le déploiement d'un ensemble de capteurs ordinaires, alors le coût du WSN n'est pas justifié. L'état de l'art définit le coût d'un réseau Bluetooth à 10\$, et un nœud capteur à 1\$ [18].

✓ **La topologie de réseau :**

Le déploiement d'un grand nombre de nœuds nécessite une maintenance de la topologie. Cette maintenance consiste en trois phases [18] :

-Phase de pré-déploiement et de déploiement : les nœuds capteurs peuvent être lancés depuis un avion ou placés un par un dans leur champ. Malgré leur grand nombre, l'opération de déploiement initiale doit garantir un faible coût d'installation, augmenter la flexibilité d'arrangement et promouvoir une auto-organisation avec une tolérance aux pannes ;

-Phase de post-déploiement : le déploiement des nœuds capteurs est souvent statique. Cependant, leur panne est régulière et fréquente, due à l'épuisement de batterie ou une destruction intentionnelle. Il est aussi possible d'avoir un ensemble de nœuds mobiles. Par conséquence, la topologie du réseau fréquente souvent des changements après déploiement ;

- Phase de redéploiement de nouveaux nœuds : un ensemble de nœuds capteurs peut être redéployé afin de remplacer les nœuds en panne. L'ajout de nouveaux capteurs exige une réorganisation du réseau et donc des changements dans sa topologie.

✓ 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,... Par conséquent, ils doivent pouvoir fonctionner sans surveillance dans des régions géographiques éloignées [23].

✓ Les médias de transmission

Dans un réseau de capteurs, les nœuds sont reliés par une architecture sans fil. Pour permettre des opérations sur ces réseaux dans le monde entier, le media de transmission doit être normé. On utilise le plus souvent l'infrarouge (qui est licence-free, robuste aux interférences, et peu onéreux), le bluetooth et les communications radio [23].

✓ La consommation d'énergie :

Comme les noeuds capteurs sont des composants micro-électroniques, ils ne peuvent être équipés que par des sources limitées d'énergie (<0.5 Ampère-heure, 1.2 V). De plus, dans certaines applications, ces noeuds ne peuvent pas être dotés de mécanismes de rechargement d'énergie, par conséquent, la durée de vie d'un noeud capteur dépend fortement de la durée de vie de la batterie associée.

Le dysfonctionnement d'un certain nombre de noeuds 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 consomment le minimum d'énergie.

Dans les réseaux de capteurs, l'efficacité en consommation d'énergie représente une métrique de performance significative, qui influence directement sur la durée de vie du réseau en entier.

Pour cela, les concepteurs peuvent, au moment du développement des protocoles, négliger les autres métriques de performances telles que la durée de transmission et le débit, au profit du facteur de consommation d'énergie [24].

En effet, l'énergie totale consommée par un noeud capteur a pour origine trois fonctions principales: la capture, les traitements et la communication.

○ **Energie de capture :**

Cette tâche est effectuée par le composant de la capture (Fig. 1.2) qui traduit les phénomènes physiques en signal électrique et il peut être digital ou analogique. Il existe plusieurs types de ce composant qui mesurent les paramètres de l'environnement comme la température, le son, l'image, la pression, etc. Les sources de consommation d'énergie dans ces composants peuvent être : l'échantillonnage des signaux, la conversion des signaux physiques en signaux électriques, le traitement des signaux et la conversion analogique numérique. La consommation d'énergie par ces composants est dépendante de leurs tâches, les capteurs de température ou de tremblement de terre sont moins consommateurs d'énergie par rapport à ceux d'imagerie ou de vidéo [21].

-Solution

L'énergie consommée lors de la capture peut être réduite en utilisant des composants à faible consommation mais en réduisant ainsi leurs performances. Ou bien par la suppression de la capture inutile en réduisant les durées de capture.

○ **Energie de traitements :**

Cette tâche inclut le contrôle des composants de capture et l'exécution des protocoles de communication et des algorithmes de traitement de signaux sur les données collectées. Elle est effectuée par les microprocesseurs. Le choix de ces derniers est en fonction du scénario de l'application, et il fait en général un compromis entre le niveau de performance et la consommation d'énergie [21].

-Solution

Il existe deux approches pour la minimisation énergétique lors du traitement des données par un noeud capteur :

- L'approche partitionnement du système : 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.
- L'approche DVS "Dynamic Voltage Scaling" : consiste à ajuster de manière adaptative la tension d'alimentation et la fréquence du microprocesseur pour économiser la puissance de calcul sans dégradation des performances [25].

- **Energie de communication :**

L'énergie de communication représente la plus grande proportion de l'énergie totale consommée au niveau d'un noeud . Cette communication est assurée dans la plus part des RCSFs par le support de transmission radio. La consommation d'énergie de ce dernier est affectée par plusieurs facteurs : le type du système de modulation, quantité des données à communiquer, la puissance de transmission (déterminée par la distance de transmission), etc.

En général, les radios peuvent fonctionner dans quatre modes d'opération différents : transmission, réception, actif "idle" et sommeil. Tel que la radio consomme beaucoup plus d'énergie dans les modes transmission et réception. Cependant, le mode actif est également coûteux en énergie. Dans la plupart des cas, la consommation d'énergie est relativement élevée dans le mode actif, puisque ce dernier nécessite que le module radio soit mis sous tension et décode continuellement les signaux radios pour détecter l'arrivée des paquets [21].

-Solution

La minimisation d'énergie pendant la communication est principalement liée aux protocoles développés pour la couche MAC et la couche réseau. Le but des protocoles de cette dernière est de trouver les routes optimales en termes de consommation d'énergie. En effet, la perte d'énergie due à un mauvais acheminement des paquets de données a un impact sur la durée de vie du réseau et peut conduire au partitionnement de ce dernier (dissipation totale de l'énergie des capteurs sur certaines routes) [21].

I.4 Conclusion

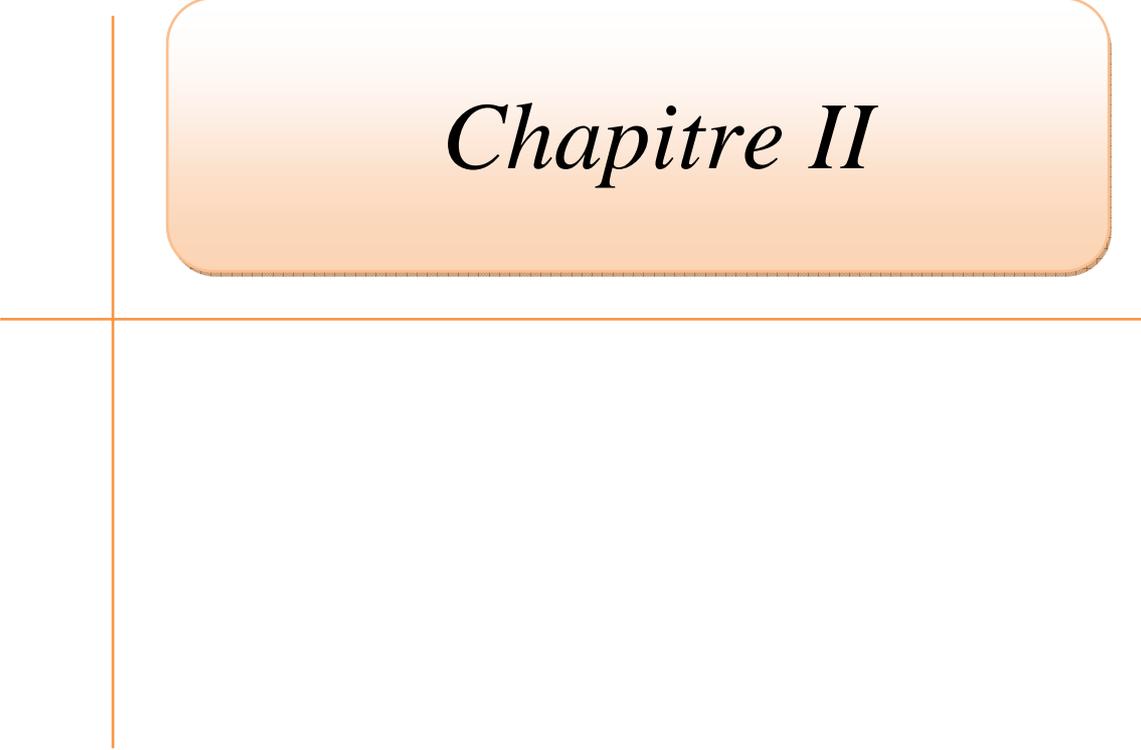
La flexibilité, la tolérance aux fautes, la fidélité élevée de capture, le coût réduit et Les caractéristiques de déploiement rapide des réseaux de capteurs créent de nouveaux domaines d'application pour la capture à distance

Les applications des réseaux de capteurs sont très nombreuses, avec des impacts importants dans des domaines aussi variés que l'industrie, la recherche, l'environnement, ou la médecine. Il paraît évident qu'ils auront des nouveaux effets dans notre vie de tous les jours et peuvent changer considérablement notre vision de notre environnement.

Dans le domaine de la recherche, les réseaux de capteurs posent un certain nombre de défis scientifiques. Les chercheurs électroniciens sont confrontés à de nombreux challenges, au

niveau de la taille des capteurs (miniaturisation maximale), mais aussi au niveau des performances (l'émission de messages la plus performante possible opposée à la consommation la moins importante). En informatique, les enjeux se situent au niveau du routage (détermination du chemin optimal entre deux points du réseau), des protocoles de communication (comme les protocoles TCP et IP de l'Internet) et des architectures logicielles.

Cependant, la réalisation d'un réseau de capteurs requiert la prise en compte de plusieurs facteurs (tel que la consommation énergétique) par les protocoles des différentes couches. Nous donnerons dans le prochain chapitre plus de détails sur ces facteurs. Nous nous intéresserons particulièrement aux problèmes liés au routage dans ce type de réseaux et les différentes techniques proposées.



Chapitre II

II.1 Introduction

En général, le routage est une méthode d'acheminement des informations à la bonne destination à travers un réseau de connexion donné. Le problème de routage consiste à déterminer un acheminement optimal des paquets à travers le réseau, suivant certains critères de performance.

Dans les RCSF, l'utilisation des protocoles de routage conçus pour les réseaux Ad Hoc traditionnels est inappropriée. Ceci est en raison des caractéristiques par lesquelles se distinguent les deux types de réseaux, d'où la nécessité de les améliorer ou de développer de nouveaux protocoles de routage spécifiques aux RCSF.

Dans ce chapitre, nous commencerons par citer quelques facteurs qui influencent sur la conception des protocoles de routage au sein des RCSF. En second lieu, nous décrirons les types de classifications des protocoles de routage. Par la suite, nous étudierons les métriques qui permettent de tester l'efficacité du protocole une fois conçu.

II.2 Les considérations de conception d'un protocole de routage dans WSNs

Ce chapitre présente un certain nombre de considérations qui sont indispensables pour la conception d'un protocole de routage pour *WSNs*. Comme les réseaux capteurs imposent des fonctions spécifiques et des contraintes sur les ressources, leur efficacité et survivabilité dépendent considérablement de la qualité de leurs protocoles. Afin de concevoir un protocole de routage efficace, les facteurs suivants doivent être pris en compte :

II.2.1 Déploiement des nœuds

La méthode de déploiement des nœuds d'un réseau de capteurs dépend de l'application et affecte directement l'exécution du protocole de routage. Cette opération peut se faire d'une manière déterministe, où les nœuds capteurs sont manuellement placés, et les données sont routées par des chemins prédéterminés.

Cependant, vu leur nombre important, les nœuds d'un réseau de capteurs sont généralement dispersés de façon aléatoire, et ne sont pas uniformément réparties sur le champ de captage, ce qui implique que certaines régions du champ de déploiement puissent bénéficier d'une meilleure connectivité par rapport à d'autres et les phénomènes captés dans ces régions peuvent être routés plus facilement.

De plus, certains nœuds capteurs peuvent tomber en panne, pendant le fonctionnement du réseau. Il est donc souvent nécessaire de déployer des nœuds supplémentaires pour combler les "trous" et maintenir la connectivité du réseau, ce qui entraîne le changement de la topologie du réseau.

Par conséquent, les protocoles de routage conçus pour les réseaux de capteurs doivent avoir une capacité d'auto-organisation qui les adapte à la distribution aléatoire des nœuds et à la topologie dynamique du réseau.

II.2.2 La consommation d'énergie

Les nœuds capteurs peuvent utiliser leur approvisionnement en énergie pour calculer et transmettre l'information dans un environnement sans fil. Pour cela, les techniques de conservation d'énergie de communication et de calcul sont essentielles. Car la durée de vie d'un nœud de capteur a une forte dépendance avec la durée de vie de batterie [29]

Dans un WSN de multi-sauts, chaque nœud joue un rôle dual comme un expéditeur de données et un retour de données. Le mal-fonctionnement de quelques nœuds de capteurs dus à la défaillance (à cause la diminution totale d'énergie) peut causer les changements topologiques cruciaux et pourrait exiger le déplacement des paquets ainsi que la réorganisation du réseau.

II.2.3 Modèle de délivrance des données

Le modèle de renvoi des données captées constitue un autre facteur important qui affecte les performances du protocole de routage utilisé. Le modèle de délivrance des données peut être classé dans l'une de ces catégories : continu (time-driven), événementiel (event-driven), orienté requête (query-driven) et hybride [21].

Dans le modèle continu, les nœuds envoient les données environnementales périodiquement. Les modèles événementiel et orienté requêtes génèrent un trafic de données après l'occurrence d'un certain événement (par exemple, détection d'un gaz chimique), ou lors d'une réponse à une requête envoyée par le nœud puits. Le modèle hybride est une combinaison des trois autres modèles.

Le protocole de routage est fortement influencé par les modèles de données rapportées concernant la consommation d'énergie et la stabilité de route [21].

II.2.4 L'hétérogénéité

Dans les premiers travaux liés au routage dans les réseaux de capteurs, tous les nœuds capteurs étaient supposés être homogènes (ayants des capacités égales en termes de calcul, de stockage, de communication et de ressource énergétique). Cependant, les nœuds d'un réseau de capteurs doivent accomplir plusieurs tâches en même temps, telles que l'acheminement des données, le captage et le traitement des données, ce qui pourrait rapidement épuiser leurs ressources énergétiques, et dégrader ainsi les performances du réseau. Une solution proposée à ce problème est d'introduire, dans le réseau, des nœuds spéciaux plus puissants que les autres et qui sont chargés d'effectuer les tâches les plus coûteuses en ressource énergétique afin d'alléger la charge sur les capteurs ordinaires.

Aussi, quelques applications pourraient exiger plusieurs types de capteurs (par exemple, pour surveiller la température, la pression, l'humidité, détecter des mouvements ou prendre des images pour surveiller des objets mobiles).

Cependant, l'intégration d'un ensemble de nœuds hétérogène dans un seul réseau impose de nouvelles contraintes liées au routage de données. En effet, les données récoltées par ces capteurs peuvent être produites à des taux différents, être sujettes à des contraintes diverses de qualité de service, et peuvent suivre des modèles de livraison de données différents.

Par conséquent, un environnement hétérogène rend le routage de données plus difficile. La conception de protocoles de routage doit prendre en compte les différents types de nœuds, et les contraintes qui en résultent.

II.2.5 Tolérance aux fautes

Quelques nœuds capteur peuvent être en panne ou être bloqué dus au manque de puissance, de dommages physiques, ou d'interférence environnementale. La défaillance des nœuds capteurs ne devrait pas affecter la tâche globale du réseau capteurs. Si plusieurs nœuds sont en panne, les protocoles de routage et de MAC doivent s'adapter à la formation de nouveaux liens et router les données collectées aux stations de base. Ceci peut exiger l'activement d'ajustement de puissances de transmission et avertir la vitesse sur les liens existants pour réduire la consommation d'énergie, ou re-router des paquets à travers des régions du réseau où plus d'énergie est disponible [21].

II.2.6 Scalabilité

Le nombre de nœuds capteurs déployés dans une région de sensation peut être dans l'ordre des centaines ou des milliers, ou plus. N'importe quel schéma de routage doit pouvoir travailler avec ce nombre énorme de nœuds capteurs. En outre, les protocoles de routage dans un réseau de capteurs devraient être assez *scalable* pour répondre aux événements dans l'environnement. Jusqu'à ce qu'un événement se produit, la plupart des capteurs peuvent rester dans l'état de sommeil, avec quelques capteurs restants qui fournissent des données d'une qualité brute [30].

II.2.7 La dynamique du réseau

Un réseau de capteurs se compose de cinq composants principaux. Sans une d'entre elles, les WSNs ne fonction pas, ou ils sont inutiles. Ces composants sont [21]:

1. Les capteurs, qui sont des dispositifs pour recueillir et transmettent les données.
2. Le destinataire (ou observateur), qui est employé pour collecter les données stockées.
3. le phénomène, que les capteurs ont été déployés pour le surveiller.
4. L'infrastructure, qui est la manière dont laquelle les capteurs sont actuellement déployées et reliées entre eux.
5. la pile protocolaire qui est responsable de routage et de transfert des données collectées au-dehors du réseau.

Le rôle d'un WSN est de créer un chemin, en utilisant le protocole de routage et l'infrastructure existante entre un phénomène surveillé par un capteur et un destinataire, selon la mobilité de trois premiers composants de réseau (capteur, phénomène, destinataire) les réseaux de capteurs peuvent être classifiés comme dynamiques ou statiques.

Dans les réseaux de capteurs statiques, les composants demeurent stationnaires. C'est habituellement le cas dans la plupart des réseaux de capteurs, exemple un réseau de capteurs fait pour surveiller la température ou l'humidité d'une salle ou bien d'une région.

Dans les réseaux de capteurs dynamiques, au moins l'un des composants est mobile, exemple un mouvement dépistant le système de sécurité.

II.2.8 Media de transmission

Dans un réseau de capteurs multi-saut les nœuds communiquant sont liés par un medium sans fil. Les problèmes classiques liés au canal sans fil (par exemple, effacement, haut taux d'erreur) peuvent également affecter l'opération du réseau de capteurs. En général, la largeur de bande requise des données de capteur sera basse. La transmission médias est liée à la conception MAC. Une approche de conception MAC pour des réseaux de capteurs est d'utiliser les protocoles basés sur TDMA qui conservent plus d'énergie par rapport aux protocoles basés sur la contention comme CSMA (par exemple, IEEE 802.11) [21].

II.2.9 Connectivité

La densité élevée de nœud dans les réseaux de capteurs, exclut complètement l'isolement entre eux. Par conséquent, on s'attend à ce que des nœuds de capteurs soient fortement reliés. Ceci, peut ne pas empêcher la topologie de réseau d'être variable et la taille de réseau d'être craintif aux échecs de nœud de capteurs. En outre, la connectivité dépend probablement de la distribution aléatoire des nœuds [21].

II.2.10 Couverture

Dans les réseaux de capteurs, chaque nœud de capteur obtient une certaine vue de l'environnement. La vue de l'environnement d'un capteur donné est limitée dans la portée et dans l'exactitude, elle peut seulement couvrir un domaine physique limité de l'environnement. Par conséquence, la couverture d'une région est également un paramètre de conception important pour les réseaux de capteurs [21].

II.2.11 Agrégation des données

Puisque les nœuds capteurs peuvent produire des données significatives et superflues, les paquets semblables des différents nœuds peuvent être agrégés de sorte que le nombre de transmissions soit réduit. L'agrégation de données est la combinaison des données de différentes sources selon une certaine fonction d'agrégation, par exemple, suppression, minimum, maximum et moyenne.

Cette technique a été employée pour optimiser la consommation d'énergie lors le transfert de données dans un certain nombre de protocoles de routage. Des méthodes de traitement des signaux peuvent également être employées pour l'agrégation de données. Dans ce cas-là, elle désigné sous le nom de la fusion de données où un nœud est capable de produire un signal de

sortie en employant certaines techniques telles que *beamforming* pour combiner les signaux entrants et réduire le bruit dans ces signaux [21].

II.2.12 Qualité de service

Dans quelques applications, les données devraient être fournies au cours d'une certaine période du moment où elles sont senties, sinon ils sont inutiles, et par conséquent, la latence définie pour la livraison des données est une autre condition pour les applications qui sont soumis sous des contraintes du temps, cependant, dans plusieurs applications, la conservation d'énergie, qui est directement liée à la durée de vie du réseau, est considérée relativement plus importante que la qualité des données envoyées. Pendant que l'énergie s'épuise, le réseau exige de réduire la qualité des résultats afin de réduire la diminution d'énergie dans les nœuds et par conséquent augmenter la vie de réseau. De cela les protocoles énergie-avertis de routage sont exigés pour capturer cette condition [21].

II.3 Métriques de routages

Cette section étudie les métriques communes utilisées pour mesurer l'efficacité des protocoles de routage. Un calcul de métrique est un algorithme qui traite un coût associé à un certain chemin de routage. Les protocoles de routage permettent aux nœuds de comparer les métriques calculées afin de déterminer les routes optimales à emprunter. Plus la métrique est optimale, plus le protocole de routage considère que la probabilité d'atteindre le nœud puits à travers ce nœud intermédiaire est grande [27]. Plusieurs métriques peuvent affecter le routage en termes d'énergie, délai, longueur du chemin, etc. De plus, elles peuvent être considérées seules ou combinées (hybrides) [32].

II.3.1 Métriques pour la consommation d'énergétique

Les protocoles de routage utilisent cet ensemble de métriques pour minimiser la consommation d'énergie pendant le routage [18,24]. L'idée est de calculer l'énergie disponible (ED) pour chaque nœud du réseau et l'énergie nécessaire (EN) pour les transmissions des paquets entre une paire de nœuds.

Les routes entre les nœuds et le puits sont établies et chacune d'elles est caractérisée par la somme des ED des nœuds qui la constituent et par la somme des EN des liaisons qui la construisent. La consommation d'énergie suit plusieurs approches dont on peut citer :

II.3.1.1 Par considération de puissance

La route choisie est celle caractérisée par la somme des ED la plus élevée.

II.3.1.2 Par considération du coût

La route choisie est celle caractérisée par la plus petite somme des EN.

II.3.1.3 Par considération de puissance et du coût

Cette métrique est la combinaison des deux métriques précédentes. La route choisie est celle caractérisée par la plus petite somme des EN et la plus grande somme des ED.

II.3.2 Nombre de sauts

Les protocoles de routage utilisent cette métrique pour minimiser le nombre de sauts pendant le routage. L'idée est de calculer le nombre de nœuds intermédiaire pouvant être traversés lors d'une transmission d'un paquet du nœud source vers le nœud puits. La route choisie est celle qui contient un nombre minimum de nœuds (minimum de sauts) [24].

II.3.3 Perte de paquets

Les protocoles de routage utilisent cette métrique dans le but de minimiser le nombre de paquets de données perdus lors du transfert depuis une source vers une destination pendant le routage [31]. L'idée est de calculer le ratio des paquets perdus et des paquets émis transitant dans le réseau. Autrement dit, on calcule le nombre de paquets perdus sur le nombre de paquets transmis lors d'une transmission. Dans le cas où le taux de perte de paquets est élevé, il est nécessaire de mettre en place des mécanismes qui permettent de minimiser les collisions.

II.3.4 Délai de bout-en-bout EED

L'EED (End-to-End Delay) est le temps moyen nécessaire pour qu'un paquet de données soit acheminé à partir de la source vers la destination [31]. Cette technique est parmi les métriques les plus connues dans les réseaux sans fil. Les protocoles de routage l'utilisent pour minimiser le temps de propagation des paquets de données échangés pendant le routage.

II.4 Classification des protocoles de routage dans les réseaux de capteurs

Récemment, les protocoles de routage conçus pour les RCSF ont été largement étudiés. Les méthodes employées peuvent être classifiées suivant plusieurs critères qui sont illustrés dans le tableau suivant :

Selon la structure du réseau	A plat
	hiérarchique
	Avec localisation géographique
selon les fonctions des protocoles	Basé sur la QoS
	Basé sur la négociation
	Basé sur multi-chemins
Selon l'établissement de la route	Proactifs
	Réactifs
	Hybrides
Selon l'initiateur de communication	Source
	Destination

Tableau II.1: Classification des protocoles de routage

II.4.1 Classification selon la structure du réseau

Les protocoles de routage basés sur la structure du réseau peuvent être classifiés en trois catégories : protocoles à plat (Flat based routing), protocoles hiérarchiques (Hierarchic based routing/Clustering based routing) et protocoles basés sur la localisation géographique (Location based routing) [21].

II.4.1.1 Routage à plat

Dans cette catégorie de routage, les protocoles sont basés sur le principe centrés données où tous les nœuds ont le même rôle et ils collaborent entre eux pour accomplir la tâche de routage.

- **Avantages**

- *Scalabilité* : les réseaux à plat sont scalables du fait que chaque nœud participe également à la tâche de routage et puisque les nœuds ont besoin seulement des informations sur leurs voisins directs.

- *Simplicité* : les réseaux à plat permettent aux protocoles de routage d'être simples, ainsi que nous n'avons besoin d'aucun algorithme complexes pour faire le choix d'un cluster head.

- **Inconvénients**

- *Points chauds (Hotspots)* : si les nœuds capteurs sont uniformément distribués dans tout le réseau et il y a un seul nœud puits. Alors, les nœuds au tour de ce dernier épuiseront leurs énergies plus tôt que les autres nœuds. Parce que tout le trafic du réseau passe par les nœuds entourant le nœud puits.

II.4.1.2 Routage hiérarchique

Les protocoles du routage hiérarchiques sont chargés généralement d'établir des clusterheads et de définir la manière dont laquelle les nœuds décident quel cluster-head à joindre. Le but principal de routage hiérarchique est de maintenir l'efficacité de consommation d'énergie des nœuds capteurs en les impliquant dans la communication multi-sauts avec un cluster particulier et en performant l'agrégation de données afin de diminuer le nombre de messages transmis à la destination. La formation des clusters est typiquement basée sur l'énergie réservée dans les nœuds capteurs et de la proximité de ceux-ci au cluster-head.

- **Avantages**

- *L'agrégation de données* : l'avantage du routage hiérarchique est que les données du cluster entier peuvent être combinées par le cluster-head et envoyées vers la destination.

- **Inconvénients**

- *Points chauds (Hotspots)* : les nœuds élus comme des cluster-heads consomment plus d'énergie que les autres nœuds dans le réseau. Si les cluster-heads ne changent pas régulièrement, le réseau va être partitionné, c'est à dire le découpage du réseau en secteurs.

- *Condition physique* : plusieurs protocoles exigent que les nœuds cluster-heads aient des ressources énergétiques plus élevées que les autres nœuds dans le réseau.
- *Complexité* : si les nœuds cluster-heads ont la même capacité que les autres nœuds dans le réseau, donc, la méthode utilisée pour faire le routage et le choix des clusterheads doit prendre en considération la contrainte de consommation d'énergie d'une manière équitable. Cela va augmenter le nombre des messages consommant l'énergie dans le réseau.
- *Non scalable* : les protocoles hiérarchiques ne sont pas scalables puisque le nombre des cluster-heads augmente quand la taille du réseau augmente. Et par conséquent, le nombre des messages overhead augmente lors de l'établissement de ces clusterheads.

II.4.1.3 Les protocoles de routage avec localisation géographique

Un routage est dit géographique lorsque les décisions de routage sont basées sur la position des nœuds. La plupart des protocoles de routage dans les réseaux de capteurs nécessitent la localisation des nœuds capteurs. En général, ces informations sont nécessaires pour calculer la distance entre deux nœuds particuliers de sorte que la consommation d'énergie puisse être estimée.

Puisque il n'y a aucun système d'adressage pour les nœuds dans les réseaux de capteurs (comme les adresses IP) et comme ils sont déployés dans une région d'une manière aléatoire, l'information de localisation de ces nœuds peut être utilisée dans le routage des données d'une manière efficace en termes d'énergie.

- **Avantages**

- L'utilisation des GPSs permet d'améliorer la connaissance de la position au centimètre près. Des traitements du signal dans des récepteurs plus sophistiqués permettent d'améliorer la précision de positionnement (résolution de la distance).
- Dans le routage basé sur la localisation géographique, la région de destination est connue et la requête peut être donc dirigée uniquement vers cette région, ce qui éliminera le nombre de transmission de manière significative.

- **Inconvénients**

- Les nœuds doivent être équipés d'un système de localisation par satellite.
- Le routage basé sur la localisation géographique n'est pas un bon choix pour les applications qui exigent une livraison fiable à des intervalles réguliers des paquets de données.

II.4.2 Classification selon les fonctions des protocoles

Les protocoles de routage peuvent être classifiés selon leurs fonctionnalités en quatre catégories: routage basé sur la Qualité de Service "QoS" (Quality of Service "QoS" based routing), Routage basé sur les requêtes, routage basé sur des multi-chemins (Multi-path based routing), et routage basé sur la négociation (Negociation based routing).

II.4.2.1 Routage basé sur la QoS

Les protocoles de routage basé sur la qualité de service (QoS) sont utilisés dans les applications qui ont des exigences temps-réel. Par exemple, dans le domaine de la sécurité, la détection d'intrusion doit être acheminée au plus bref délai vers le nœud puits. Ce type de protocoles essaye de répondre à quelques exigences de qualité de service (délais de transmission ou niveau de fiabilité) et doit faire l'équilibre avec la consommation d'énergie [27].

- **Avantages**

- La prise en compte des délais de transmissions rend les protocoles de cette approche très recommandés à des applications de surveillance (centres nucléaires, monitoring médical, applications militaires, etc).
- La qualité des liaisons dans la communication assure la fiabilité des transmissions.
- Augmentation du taux d'arrivée des paquets au nœud puits [21].

- **Inconvénients**

- L'approche doit prendre en considération la contrainte d'énergie en parallèle avec les critères de la QoS [21].

II.4.2.2 Routage basé sur les requêtes

Dans ce type de routage, les nœuds destinataires propagent une requête de données de la part de la station de base à travers le réseau et le nœud qui détient ces données les envoie au nœud demandeur en suivant le chemin inverse de la requête.

Tous les nœuds détiennent des tables qui se composent des requêtes sur les tâches de capture, et envoient les données correspondantes aux requêtes quand ils les reçoivent. Les protocoles Directed Diffusion et rumor routing sont deux exemples de ce type de routage [17].

II.4.2.3 Routage basé sur la négociation

Ce genre de protocole utilise des méta-données afin de décrire la donnée avant de l'émettre. Ainsi, le récepteur éventuel pourra décider de recevoir ou pas le paquet. Cela permet d'éliminer le problème de la transmission des données redondantes.

- **Avantages**

- Le mécanisme de négociation utilisé permet de réduire le taux de données redondantes transmises.
- La négociation entre les nœuds permet à eux de prendre des décisions adéquates suivant leurs ressources énergétiques disponibles [21].

- **Inconvénients**

- L'échange de messages de contrôle entre les nœuds cause la congestion du réseau ainsi qu'une perte additionnelle d'énergie.
- Le scénario de négociation entre les nœuds (déterminer les données et les acheminer) produit un retard pour délivrer les données au nœud puits [21].

II.4.2.4 Routage basé sur multi-chemins

Dans cette sous-section, les protocoles de routage utilisent des chemins multiples plutôt qu'un chemin simple afin d'augmenter la performance du réseau. La tolérance aux fautes d'un protocole est mesurée par la probabilité qu'un chemin alternatif existe entre une source et une destination quand le chemin primaire soit défaillant. Ceci peut être augmenté en maintenant les chemins multiples entre la source et la destination aux dépens d'une consommation d'énergie et d'une génération du trafic. Ces chemins alternatifs sont maintenus par l'envoi périodique des messages.

Par conséquent, la fiabilité du réseau peut être augmentée en maintenant les chemins alternatifs les plus récents [21].

- **Avantages**

- Un mécanisme d'équilibre de charge peut être utilisé pour la répartition du trafic sur les routes, ce qui permet de répartir l'utilisation des ressources des nœuds intermédiaires (énergie) et le débit sur les liens.
- L'augmentation de la fiabilité et de la robustesse par la possibilité d'existence de plusieurs routes entre la source et la destination.

- **Inconvénients**

- Les chemins alternatifs sont maintenus en vie par l'envoi de messages périodiques.

Par conséquent, un overhead et une perte additionnelle d'énergie viennent s'ajouter pour maintenir ces chemins alternatifs.

- Le risque de perte des paquets augmente dans le cas où ces derniers sont envoyés sur des chemins ayant des nœuds communs qui peuvent tomber en panne.

II.4.3 Classification selon l'établissement de la route

Suivant la manière de création et de maintenance de routes lors de l'acheminement des données, les protocoles de routage peuvent être séparés en trois catégories : les protocoles proactifs, les protocoles réactifs et les protocoles hybrides.

II.4.3.1 Protocoles proactifs

Le principe de base est de maintenir à jour les tables de routage périodiquement par l'échange de trames de contrôle, de sorte que lorsqu'un nœud désire envoyer un paquet à un autre, une route sera immédiatement connue. Par exemple: le protocole DSDV, le protocole OLSR et le Protocole FSR [17].

- **Avantages**

- Les routes sont établies à priori, ce qui facilite l'acheminement des données.

- **Inconvénients**

- Les routes sont sauvegardées mêmes si elles ne sont pas utilisées.

- Les nœuds du réseau maintiennent des tables de routage pour toutes les destinations indépendamment de l'utilité des routes.

II.4.3.2 Protocoles réactifs

Les protocoles de routage réactifs (dit aussi, les protocoles de routage à la demande) créent et maintiennent des routes selon les besoins. Lorsque le réseau a besoin d'une route, une procédure de découverte de route est lancée [21].

- **Avantages**

- La conservation d'énergie par rapport aux protocoles proactifs.

- **Inconvénients**

- Le routage à la demande induit une lenteur à cause de la recherche des chemins, ce qui peut dégrader les performances des applications interactives.

- Il est impossible de connaître au préalable la qualité du chemin (en terme de bande passante, délais, etc).

II.4.3.3 Protocoles hybrides

Les protocoles hybrides combinent les deux idées des protocoles proactifs et réactifs. Ils utilisent un protocole proactif pour apprendre le proche voisinage (par exemple le voisinage à deux ou à trois sauts), ainsi, ils disposent des routes immédiatement dans le voisinage. Au-delà de la zone de voisinage, le protocole hybride fait appel à un protocole réactif pour chercher des routes.

II.4.4 Classification selon l'initiateur de communication

La communication dans un réseau de capteurs peut être lancée par les nœuds sources ou par les nœuds destinataires [21].

II.4.4.1 Communication lancée par la source

Dans les protocoles de communication lancée par la source, les nœuds envoient des données à la destination quand ils les ont capturées. Ces protocoles utilisent les données rapportées avec time-driven ou avec event-driven. Ceci signifie que les données sont envoyées à certains intervalles ou quand les nœuds capturent certains événements.

- **Avantages**

- L'établissement de la communication dans le réseau évite le problème d'overhead.
- L'efficacité énergétique due à l'absence des requêtes qui consomment beaucoup d'énergie générées par le nœud puits.

- **Inconvénients**

- Les capteurs doivent avoir des informations sur les chemins qui conduisent au nœud puits.
- Pour cette approche, l'énergie n'est pas la seule préoccupation, des exigences de QoS doivent en général être respectées (latence, fiabilité).

II.4.4.2 Communication lancée par la destination

Les protocoles de communication lancée par la destination utilisent les données rapportées avec query-driven, et dans ce cas, les nœuds répondent aux requêtes envoyées par la destination ou un autre nœud différent. C'est-à-dire propager les requêtes à tous les nœuds d'une région topologique et attendre la réception des données du nœud capteur concerné dans cette région.

- **Avantages**

- L'envoi des requêtes décrivant les données requises par le nœud puits élimine les transmissions inutiles.

- **Inconvénients**

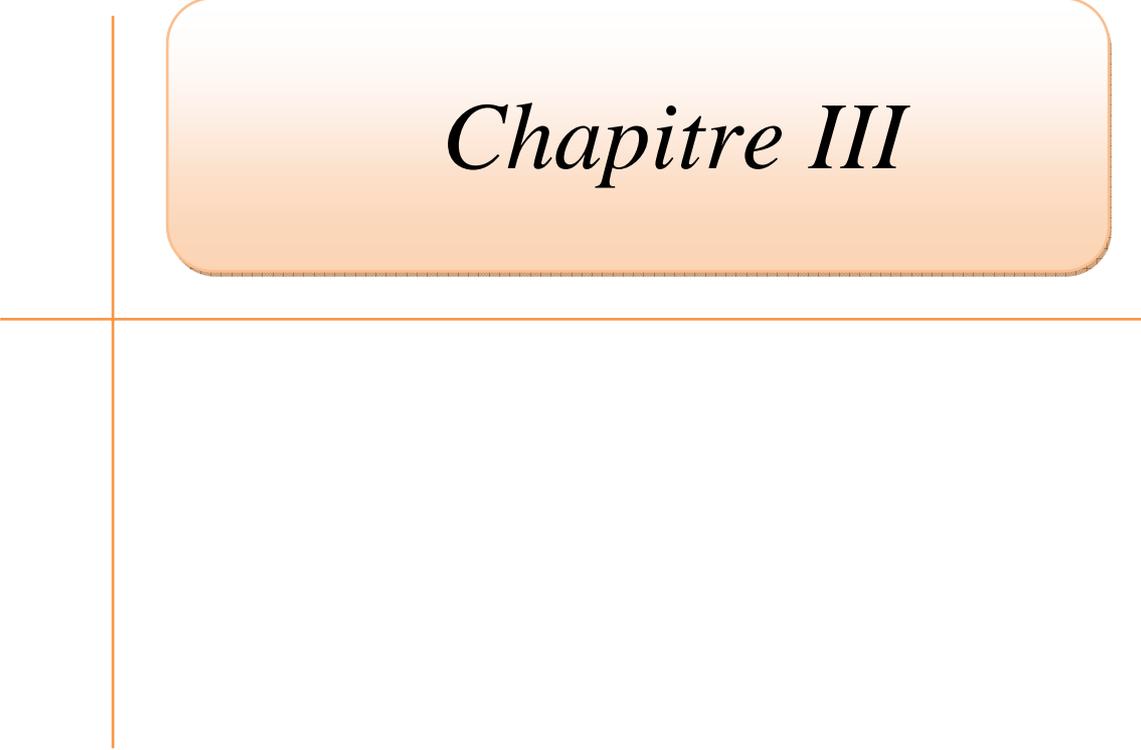
- Les délais entraînés par l'établissement des routes.

- La circulation de messages requêtes de grande taille tend à épuiser les batteries des capteurs.

II.5 Conclusion

La propagation et l'acheminement de données dans un RCSF représentent une fonctionnalité très importante. Ils doivent prendre en considération toutes les caractéristiques du réseau afin d'assurer les meilleures performances du système. C'est pourquoi le routage dans les RCSF est un problème complexe. Ainsi, la conception d'un protocole de routage se fait selon des facteurs qui doivent être satisfaits pour atteindre une communication efficace. Le taux de satisfaction de ces facteurs peut être mesuré par des métriques qui permettent de tester les performances du protocole de routage après sa réalisation.

Plusieurs protocoles de routage ont été proposés pour les RCSF grâce aux avantages qu'ils présentent. Bien que les techniques de routage semblent prometteuses, elles restent un sujet à surmonter. Parmi ces protocoles, on distingue LEACH qui suit une architecture hiérarchique et qui est particulièrement intéressant pour les RCSF. En effet, il constitue un standard sur lequel est basée la conception de plusieurs protocoles de routage. LEACH constitue l'objet principal de notre étude. Ainsi, le chapitre suivant sera consacré pour son étude détaillée.



Chapitre III

III.1 Introduction

Les protocoles de routage hiérarchiques sont considérés comme étant des protocoles très favorables en termes d'efficacité énergétique. Deux grandes approches sont dérivées de ce type de protocoles: l'approche basée sur les chaînes (chaine-based approach) dont l'idée de formation de chaînes a été proposée pour la première fois dans l'algorithme PEGASIS, et l'approche basée sur les groupes (cluster-based approach). LEACH est considéré comme étant le premier protocole de routage hiérarchique basé sur la seconde approche. Il est aussi l'un des algorithmes de routage hiérarchiques les plus populaires pour les RCSF, proposés dans le cadre du projet μ AMPS [33]. Il combine l'efficacité en consommation d'énergie et la qualité de l'accès au média, et ce en se basant sur le découpage en groupes, en vue de permettre l'utilisation du concept de l'agrégation de données pour une meilleure performance en termes de durée de vie.

L'architecture, l'algorithme et les caractéristiques du protocole LEACH sont expliquées ci-dessus.

III.2 Protocoles MAC utilisés par LEACH

Pendant son fonctionnement, le protocole LEACH appelle certains schémas des protocoles MAC qui seront détaillés dans cette section pour mieux comprendre son déroulement. Les nœuds doivent avoir une certaine capacité de calcul pour supporter différents protocoles MAC. Comme les RCSF ont des caractéristiques distinctes de tout autre type de réseaux sans fil, les protocoles MAC conçus pour ces derniers ne sont pas toujours applicables dans les RCSF. Deux versions des protocoles MAC pour l'accès au media sont alors proposées pour les RCSF : l'accès aléatoire et l'allocation fixe [24].

III.2.1 Accès aléatoire

Les schémas à accès aléatoire sont à base de contention. Dans ces schémas, les nœuds qui possèdent des données à transmettre doivent essayer d'obtenir l'autorisation pour l'accès au media tout en réduisant les collisions avec les transmissions des données des autres nœuds. Le schéma d'accès multiple avec surveillance de porteuse CSMA (Carrier Sense Multiple Access) sur lequel se base le protocole LEACH est l'un des schémas d'accès aléatoire [34]. Lorsqu'un nœud veut transmettre un message, il examine le média pour vérifier s'il est libre ou occupé par un autre nœud. Dans le cas où le media est libre, ce nœud pourra émettre son message afin d'éviter les collisions. Cela dit, des nœuds peuvent émettre des données en

même temps, ce qui mène à des collisions. Il est nécessaire donc que celles-ci soient détectées et que la récupération de données soit effectuée et que ces données soient retransmises.

Si les retransmissions se passent encore en même temps, d'autres collisions vont se produire.

Une solution à ce problème consiste à introduire que chaque nœud attende un délai aléatoire avant de retransmettre ses données, ce qui réduit la probabilité d'une autre collision. [35]

III.2.2 Allocation fixe

Les schémas à allocation fixe permettent d'allouer pour chaque nœud le media de transmission suivant des intervalles de temps (schéma TDMA) ou un schéma de codage particulier (schéma CDMA).

Étant donné que chaque nœud est attribué en exclusivité à un intervalle, il n'y a presque pas de collisions entre les données. Toutefois, les schémas à allocation fixe s'avèrent inefficaces lorsque tous les nœuds n'ont pas de données à transmettre. En effet, ces intervalles sont affectés à des nœuds qui n'ont pas besoin de les utiliser. [36]

III.2.2.1 TDMA

Le schéma d'accès multiple à répartition de temps ou TDMA (Time Division Multiple Access) permet de diviser le temps en intervalles (time-slot) attribués à chaque nœud (voir figure III-1). Ainsi, un seul nœud a le droit d'accès au canal (il utilise toute la plage de la bande passante du canal), mais doit émettre ses données pendant les intervalles de temps qui lui sont accordés. [35]

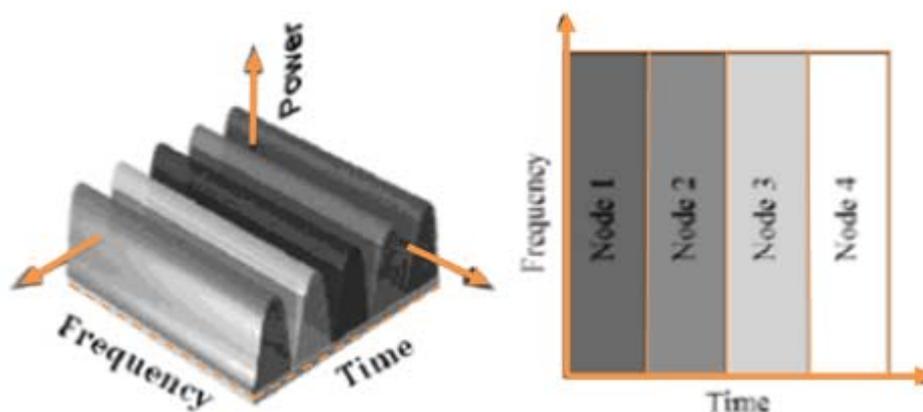


Figure.III.1 : Diagrammes représentant le protocole MAC TDMA.

III.2.2.2 CDMA

Le schéma d'accès multiple par répartition en code ou CDMA (Code Division Multiple Access) permet de côtoyer plusieurs nœuds simultanément (voir figure III.2). En effet, il ne divise ni la plage de fréquences ni l'intervalle de temps. Ainsi, des nœuds peuvent émettre leurs données continuellement et selon une large plage de fréquence. Le protocole CDMA utilise des techniques d'étalement de spectre afin d'éviter les collisions entre les transmissions simultanées des nœuds. [37]

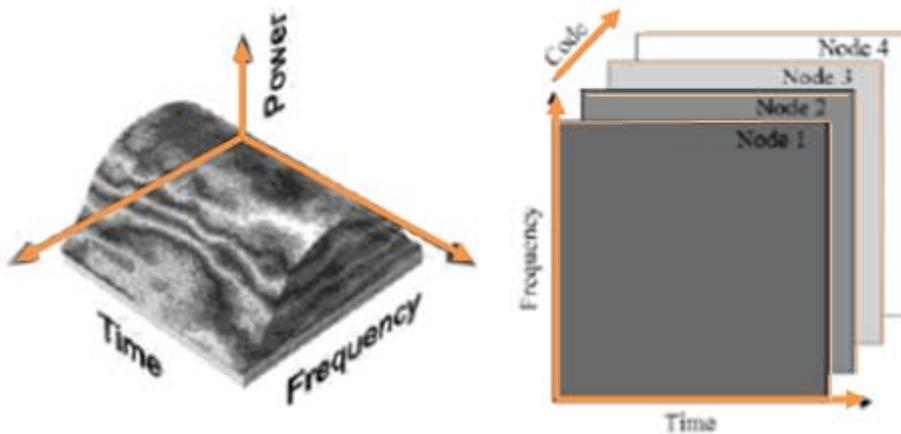


Figure III.2 : Diagrammes représentant le protocole MAC CDMA. [37]

III.3 Architecture de communication de LEACH

L'architecture de communication de LEACH consiste, de façon similaire aux réseaux cellulaires, à former des cellules basées sur l'amplitude du signal, et utiliser les têtes de cellules comme routeurs vers le nœud puits. Ces cellules sont appelées groupes (clusters), quant aux têtes : chefs de groupes (cluster-heads CH). Les chefs de groupes sont choisis de façon aléatoire selon un algorithme spécifique d'élection basé sur une fonction de probabilité qui prend en compte différents critères comme l'énergie disponible des nœuds. Comme la figure III.3 l'indique, les nœuds sont chargés de collecter des données, les envoyer à leurs CH qui les agrègent et transmettent, à leur tour, les résultats d'agrégation au nœud puits selon une communication unicast (à un seul saut).

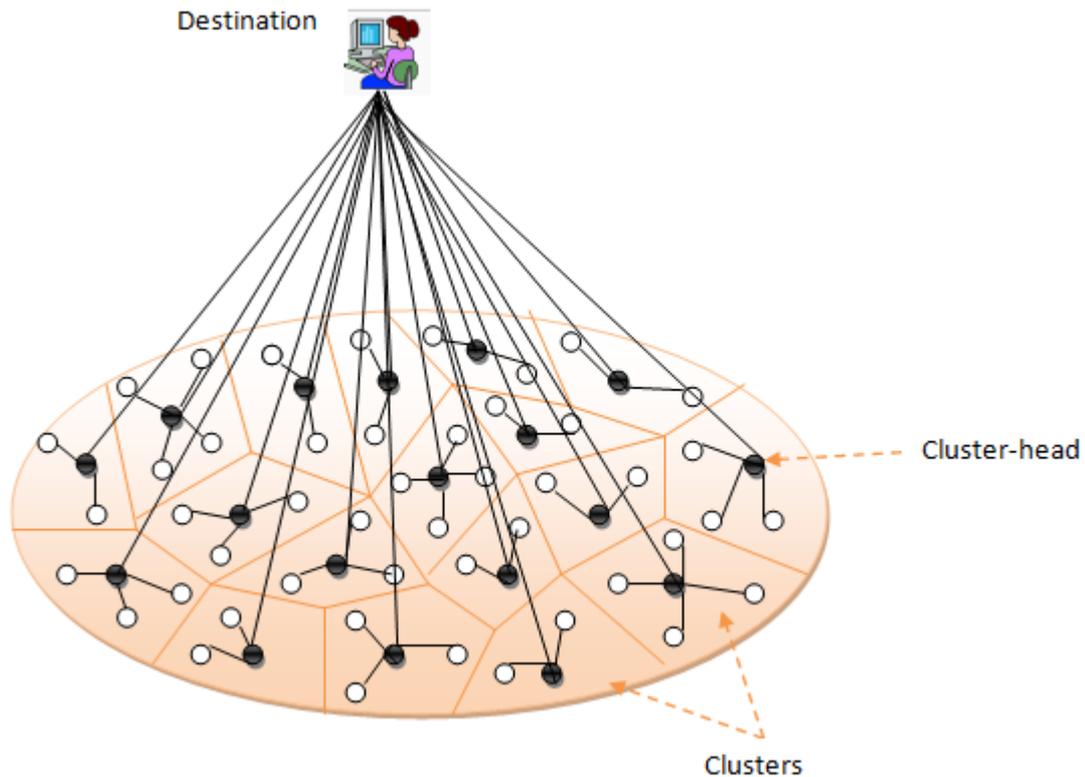


Figure III.3 : Architecture de communication du protocole LEACH

Les CH ont pour mission d'assurer les fonctions les plus coûteuses en énergie, à savoir la communication avec le nœud puits qui est supposé éloigné, ainsi que tous les traitements de données (agrégation, fusion et transmission de données) afin de réduire la quantité des données transmises. Ce dispositif permet d'économiser l'énergie puisque les transmissions sont uniquement assurées par les CH plutôt que par tous les nœuds du réseau. Par conséquent, LEACH réalise une réduction significative de la dissipation d'énergie [21].

III.4 Algorithme détaillé de LEACH

L'algorithme se déroule en « rounds » qui ont approximativement le même intervalle de temps déterminé au préalable. Chaque round est constitué d'une phase d'initialisation et d'une phase de transmission.

III.4.1 Phase d'initialisation

Comme l'indique la figure III.4, la phase d'initialisation est composée de 3 sous-phases: d'annonce, d'organisation des groupes et enfin d'ordonnancement, et qui seront détaillées ci-dessous.

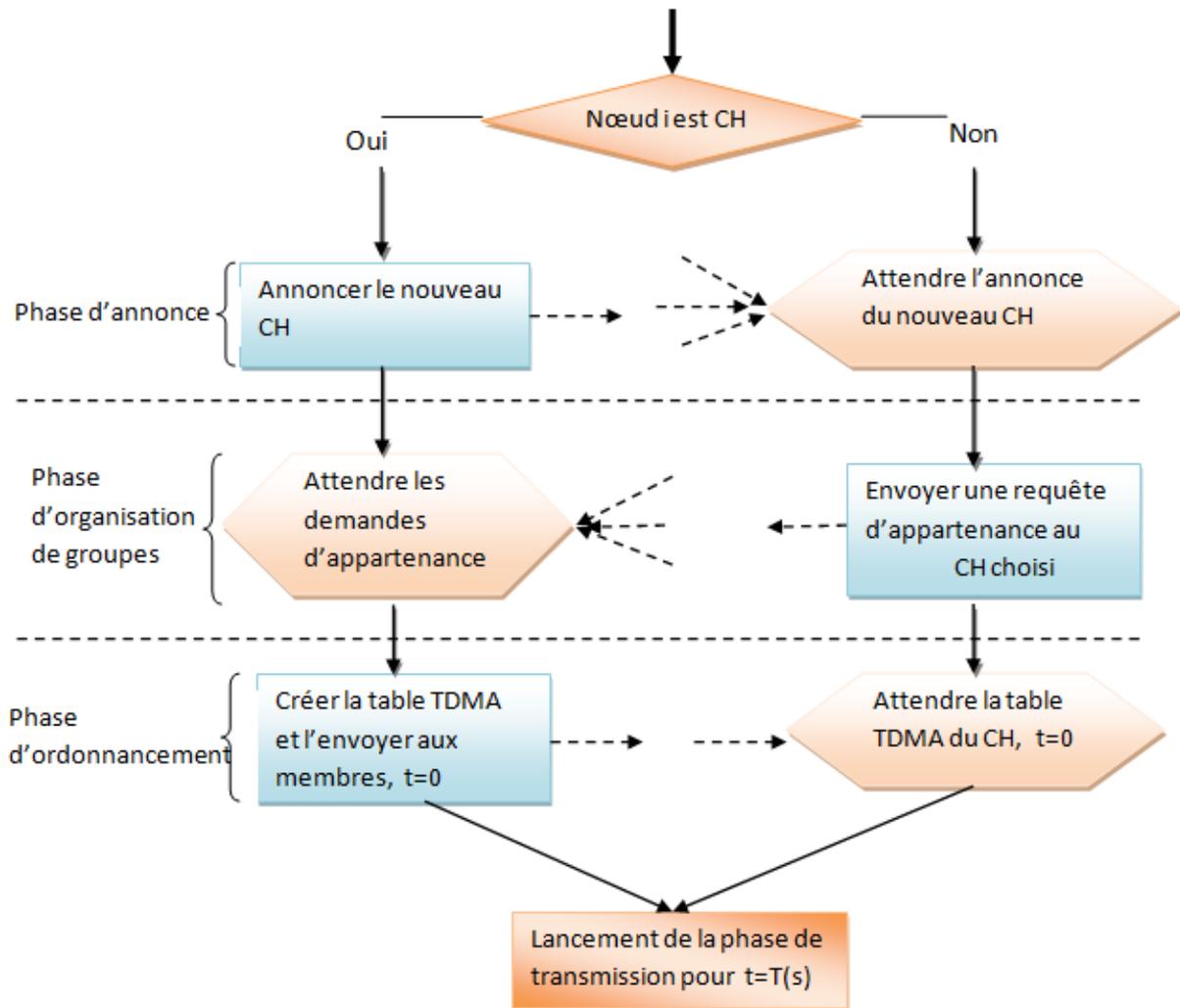


Figure III.4 : Opérations de l'étape d'initialisation de LEACH

III.4.1.1 Phase d'annonce

Avant de lancer cette phase, on désire avoir un certain nombre de CH. Ce nombre, que l'on note K , est fixe et il est inchangé durant tous les rounds. On estime que le pourcentage optimal du nombre de CH désirés devrait être de 5% à 15% du nombre total de nœuds [38]. Si ce pourcentage n'est pas respecté, cela mènera à une grande dissipation d'énergie dans le réseau. En effet, si le nombre de CH est très élevé, on aura un nombre important de nœuds (CH) qui se consacrent aux tâches très coûteuses en ressources énergétiques. Ainsi, on aura une dissipation d'énergie considérable dans le réseau. De plus, si le nombre de CH est très petit, ces derniers vont gérer des groupes de grandes tailles. Ainsi, ces CH s'épuiseront rapidement à cause de travail important qui leur est demandés.

Cette phase commence par l'annonce du nouveau round par le nœud puits, et, par la prise de décision locale d'un nœud pour devenir CH avec une certaine probabilité $P_i(t)$ au début du round $r+1$ qui commence à l'instant t . Chaque nœud i génère un nombre aléatoire entre 0 et 1. Si ce nombre est inférieur à $P_i(t)$, le nœud deviendra CH durant le round $r+1$. $P_i(t)$ est calculé en fonction de K et de round r [39]:

$$\text{Nombre(CH)} = \sum_{i=1}^N P_i(t) = K$$

Où N est le nombre total de nœuds dans le réseau. Si on a N nœuds et K CH, alors, il faudra N/K rounds durant lesquels un nœud doit être élu seulement une seule fois autant que CH avant que le round soit réinitialisé à 0. Donc la probabilité de devenir CH pour chaque nœud i est :

$$P_i(t) = \frac{\text{le nombre de CH désirés}}{\text{Le nombre de noeuds qui n'ont pas encore été élus CH durant les } r \text{ rounds précédents}}$$

$$P_i(t) = \begin{cases} \frac{K}{N - K * (r \bmod \frac{N}{K})} & : C_i(t)=1 \\ 1 & : C_i(t)=0 \end{cases} \dots (1)$$

Où $C_i(t)$ égal à 0 si le nœud i a déjà été CH durant l'un des $(r \bmod N/K)$ rounds précédents, et, il est égal à 1 dans le cas contraire. Donc, seuls les nœuds qui n'ont pas encore été CH, ont vraisemblablement une énergie résiduelle suffisante que les autres et ils pourront être choisis.

Le terme $= \sum_{i=1}^N C_i(t)$ représente le nombre total des nœuds éligibles d'être CH à l'instant t .

Il est égal à : $\sum_{i=1}^N C_i(t) = N - K * (r \bmod N/K) \dots (2)$

Utilisant l'équation (1) et (2), le nombre de CH par round est :

$$\text{Nombre (CH)} = \sum_{i=1}^N P_i(t) * C_i(t) = K$$

III.4.1.2 Phase d'organisation de groupes

Après qu'un nœud soit élu CH, il doit informer les autres nœuds non-CH de son nouveau rang dans le round courant. Pour cela, un message d'avertissement ADV contenant l'identificateur du CH est diffusé à tous les nœuds non-CH en utilisant le protocole MAC

CSMA pour éviter les collisions entre les CH. La diffusion permet de s'assurer que tous les nœuds non-CH ont reçu le message. Par ailleurs, elle permet de garantir que les nœuds appartiennent au CH qui requière le minimum d'énergie pour la communication. La décision est basée donc sur l'amplitude du signal reçu; le CH ayant le signal le plus fort (i.e. le plus proche) sera choisi. En cas d'égalité des signaux, les nœuds non-CH choisissent aléatoirement leur CH [39].

Chaque membre informe son CH de sa décision. Une fois que le CH ait reçu la demande, il lui envoie un message d'acquiescement Join- REQ.

III.4.1.3 Phase d'ordonnement

Après la formation des groupes, chaque CH agit comme un centre de commande local pour coordonner les transmissions des données au sein de son groupe. Il crée un ordonnanceur (schedule) TDMA et assigne à chaque nœud membre un slot de temps durant lequel il peut transmettre ses données. L'ensemble des slots assignés aux nœuds d'un groupe est appelé frame. La durée de chaque frame diffère selon le nombre de membres du groupe. Par ailleurs, afin de minimiser les interférences entre les transmissions dans des groupes adjacents, chaque CH choisit aléatoirement un code dans une liste de codes de propagation CDMA. Il le transmet par la suite à ses membres afin de l'utiliser pour leurs transmissions. [40]

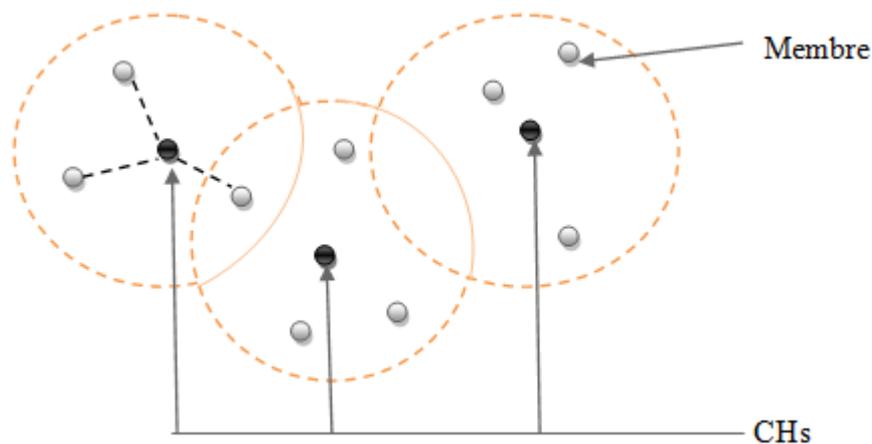


Figure III.5 : Interférence lors d'une communication dans LEACH

III.4.2 phase de transmission

Cette phase est plus longue que la phase précédente, et permet la collecte de données captées. En utilisant l'ordonnanceur TDMA, les membres émettent leurs données captées pendant leurs propres slots. Cela leur permet d'éteindre leurs interfaces de communication en

dehors de leurs slots afin d'économiser leur énergie. Ces données sont ensuite agrégées par les CH qui les fusionnent et les compressent, et, envoient le résultat final au nœud puits.

Après un certain temps prédéterminé, le réseau va passer à un nouveau round. Ce processus est répété jusqu'à ce que tous les nœuds du réseau seront élus CH, une seule fois, tout au long des rounds précédents. Dans ce cas, le round est réinitialisé à 0.

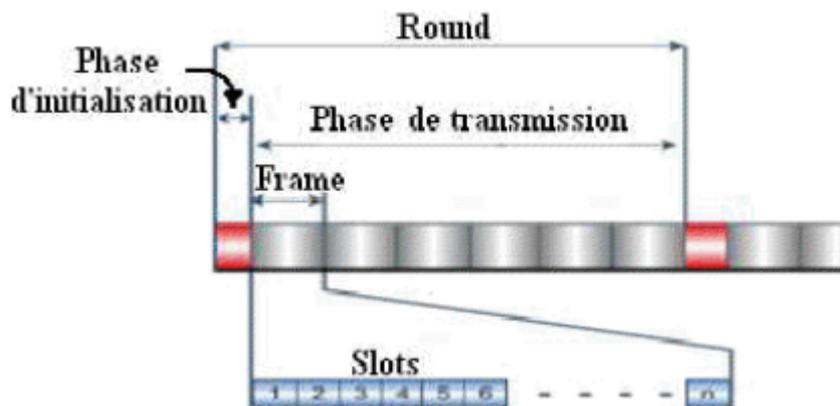


Figure III.6 : Répartition du temps et différentes phases pour chaque round.

III.5 Avantages et inconvénients de LEACH

Le protocole LEACH engendre beaucoup d'avantages en ce qu'il offre comme bonne manipulation de ressources du réseau en respectant plusieurs contraintes telle que la consommation d'énergie. Bien que LEACH économise la consommation d'énergie comparé à la transmission directe, grâce à l'agrégation de données et la réutilisation de largeur de bande, un nombre d'inconvénients restent plus ou moins apparents. Dans ce qui suit, on cite quelques avantages et inconvénients du protocole LEACH.

III.5.1 Avantages

- *Protocole auto-organisateur basé sur le groupement adaptatif:*

LEACH est complètement distribué, autrement dit, les nœuds prennent leurs décisions de façon autonome et agissent de manière locale et n'ont pas besoin d'une information globale ni d'un système de localisation pour opérer de façon efficace. De plus, la collection de données est faite périodiquement (l'utilisateur n'a pas besoin de toutes les données immédiatement). Pour exploiter cette caractéristique, ce protocole introduit un groupement adaptatif, c'est-à-dire, il réorganise les groupes après un intervalle de temps aléatoire, en

utilisant des contraintes énergétiques afin d'avoir une dissipation d'énergie uniforme à travers tout le réseau. [27]

- **Rotation des rôles de chefs de groupes:**

La rotation des rôles de chefs de groupes s'avère un facteur important pour l'organisation des nœuds. Ce rôle est épuisant en termes de d'énergie car les CH sont actifs tout au long de leur élection. Puisque le nœud puits est généralement loin du champ de surveillance, les CH diffusent une quantité plus importante d'énergie pour lui transmettre leurs données. Donc, si les CH sont choisis d'une manière fixe, leur énergie s'épuisera rapidement ce qui induit à leur défaillance. Par conséquent, tous les autres nœuds seront sans CH et donc inutiles. C'est pourquoi, les algorithmes de groupement (clustering) étudiés jusqu'ici adoptent la rotation du rôle de chefs de groupes. [27]

- **Faible énergie pour l'accès au média:**

Le mécanisme de groupes permet aux nœuds d'effectuer des communications sur des petites distances avec leurs CH afin d'optimiser l'utilisation du média de communication en la faisant gérer localement par un CH pour minimiser les interférences et les collisions.

- **Compression locale (agrégation) :**

Les CH compressent les données arrivant de leurs membres, et envoient un paquet d'agrégation au nœud puits afin de réduire la quantité d'informations qui doit lui être transmise. Cela permet de réduire la complexité des algorithmes de routage, de simplifier la gestion du réseau, d'optimiser les dépenses d'énergie et enfin de rendre le réseau plus évolutif (scalable).

III.5.2 Inconvénients

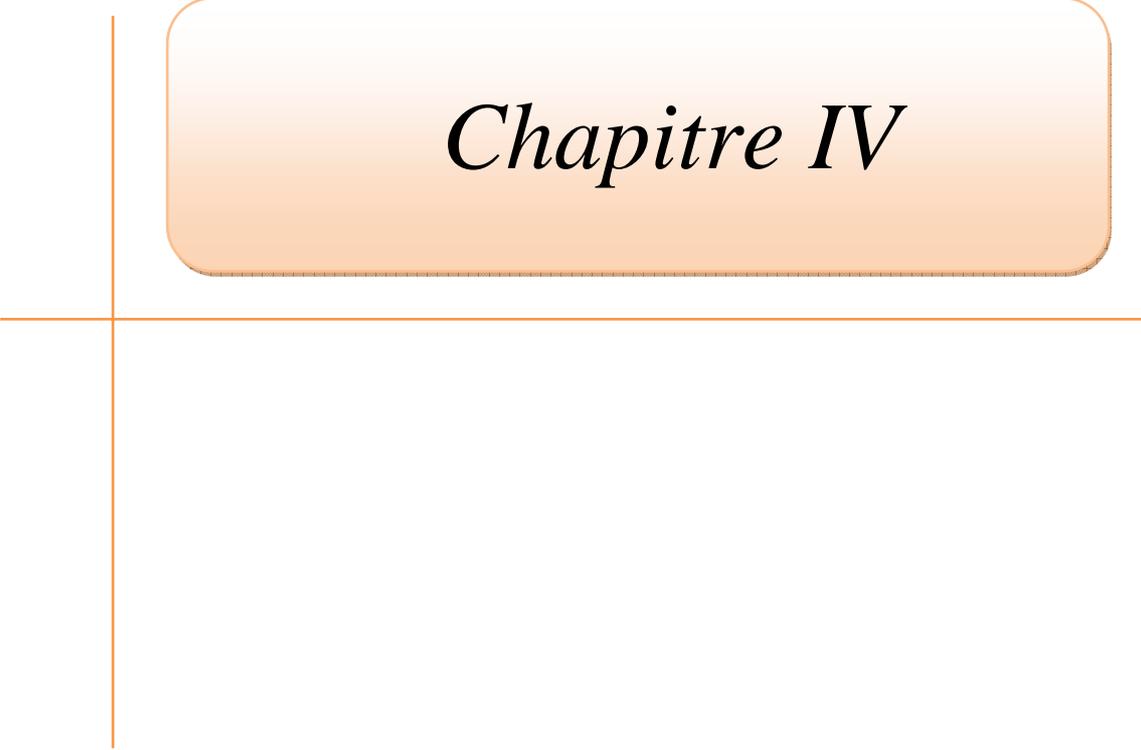
- On pourra ne pas avoir des CH durant un round si les nombres aléatoires générés par tous les nœuds du réseau sont supérieurs à la probabilité $P_i(t)$.
- Les nœuds les plus éloignés du CH meurent rapidement par rapport aux plus proches.
- L'utilisation d'une communication à un seul saut au lieu d'une communication multi-sauts diminue l'énergie des nœuds.
- Le protocole LEACH ne peut pas être appliqué à des applications temps-réel du fait qu'il résulte en une longue latence.

- La rotation des CH permet de ne pas épuiser les batteries. Cependant, cette méthode n'est pas efficace pour de grandes structures de réseaux à cause de la surcharge d'annonces engendrées par le changement des CH, et qui réduit le gain d'énergie initial.
- Il n'est pas évident que les CH soient uniformément distribués. Donc, il est possible que les CH puissent être concentrés dans une partie du réseau. Par conséquent, certains nœuds n'auront pas des CH dans leurs voisinages.
- Le protocole LEACH n'est pas sécurisé. Aucun mécanisme de sécurité n'est intégré dans ce protocole. Ainsi, il est très vulnérable même aux simples attaques. Donc, un attaquant peut facilement monopoliser le réseau et induit à son dysfonctionnement.

III.6 Conclusion

Dans ce chapitre, nous avons présenté le protocole de routage hiérarchique LEACH qui suit une approche basée sur les groupes. Cette approche a montré son efficacité, comparée aux autres approches (par exemple, la topologie plate), en termes de consommation et de dissipation uniforme d'énergie prolongeant ainsi la durée de vie du réseau. Nous avons vu que le protocole LEACH est soumis à certaines contraintes et suppositions qui engendrent toutefois des inconvénients. Par exemple, la communication unicast, établie entre le nœud puits et les CH et entre ces derniers et leurs membres, n'est pas toujours efficace par rapport à la communication multi-sauts.

Le protocole LEACH comme d'autres protocoles de routage proposés pour les RCSF, à un objectif commun : Assurer l'acheminement des données collectées par les nœuds capteurs tout en essayant d'étendre la durée du réseau. Cela nécessite la prise en compte des caractéristiques des RCSF et des exigences des applications pour lesquelles ces réseaux sont destinés. Parmi ces exigences on cite le contrôle de congestion qui est le principe de notre étude dans le chapitre suivant.



Chapitre IV

IV.1 Introduction

Le modèle de communication many-to-one dans les RCSF crée un trafic intense de flux de données dans la région proche du puits que dans le reste du zone de captage (à la périphérie). Ainsi, les noeuds proches du puits devront effectuer plus de tâches que les autres. Etant limités en ressources, il n'est pas rare que ces noeuds (proches du puits) se trouvent dans l'état où ils ne peuvent plus effectuer toutes ces tâches. Le terme utilisé pour désigner cette situation est la *congestion*.

Dans les réseaux sans fil, particulièrement dans les RCSF, il existe plusieurs sources de congestion [54] ; comme le débordement des mémoires tampon, les transmissions concurrentes, collision des paquets. Parmi les problèmes causés par la congestion, on peut citer : le retarder l'information, perte de paquets qui contiennent parfois les informations critiques, gaspillage de la bande passante. Il est facile de constater que la congestion dégrade les performances du réseau en l'empêchant de garantir certaines exigences de Qos comme le temps réel, le routage de bout en bout, la maximisation de la durée de vie du réseau. Ce problème motive le besoin de mise en place des mécanismes de contrôle de congestion

Notre objectif dans ce chapitre est de faire une étude sur les techniques de contrôle de congestion proposées dans la littérature, afin de voir leur comportement dans certaines applications. Pour cela, nous donnons quelques notions sur la détection et le contrôle de congestion dans les RCSFs. Ensuite nous présenterons quelques protocoles et techniques de contrôle de congestion.

IV.2 Définition et typologies de congestion

Dans un réseau informatique, la congestion est provoquée par les sources excédant le lien de communication ou la capacité (de stockage ou de traitement) des éléments du réseau. Pour cela, deux types de congestion pourraient se produire dans un RCSF [55] : la congestion au niveau du noeud (node-level congestion) et la congestion au niveau du lien (link-level congestion).

La congestion au niveau du noeud, qui est répandue dans les réseaux conventionnels, est provoquée par le débordement des tampons dans le noeud et peut causer la perte et le retard des paquets.

Dans les RCSFs, le canal de communication sans fil est partagé par plusieurs noeuds en utilisant les protocoles de contrôle d'accès au média de la famille CSMA. Les collisions pourraient se produire quand les noeuds capteurs essaient de transmettre en même temps suite à la détection d'un événement critique (incendie dans la forêt, séisme, etc.).

Dans cette situation, on parle de congestion au niveau du lien. Cette congestion conduit à un gaspillage de la bande passante et à un taux d'erreur élevé des paquets lors de leur réception.

La limitation de congestion suit généralement deux étapes [54]: détection de congestion et contrôle de congestion. La détection exacte et efficace de congestion joue un rôle essentiel dans le contrôle de congestion dans les RCSF [54].

Généralement il existe deux approches de contrôle de congestion [55] : La gestion des ressources du réseau et la régulation du trafic. La gestion des ressources du réseau essaie d'augmenter ses ressources (mémoire tampon, puissance d'émission de l'interface de communication, vitesse de traitement, etc) pour atténuer la congestion quand elle se produit.

La régulation du trafic implique le contrôle de congestion par ajustement du taux de circulation des paquets afin qu'il s'adapte aux noeuds sources ou intermédiaires. La plupart des protocoles de contrôle de congestion existants appartiennent à ce type. La régulation du trafic peut être « bout en bout » ou « saut par saut ». Dans le bout en bout, la régulation s'effectue au niveau du noeud source pour simplifier la tâche aux noeuds intermédiaires ; il en résulte une réponse lente et dépend fortement du temps d'aller-retour. En « saut par saut » la réponse est très rapide. Il est généralement difficile d'ajuster le taux de transmission des noeuds intermédiaires car ce taux dépend du protocole MAC et peut être variable.

IV.3 Classification des approches de contrôle de congestion

Nous pouvons différencier les protocoles de contrôle de congestion à travers plusieurs axes [55] qu'on va décrire dans cette section.

IV.3.1 Mécanisme de détection de congestion

Le mécanisme de détection de congestion peut être local ou global. La détection de congestion locale est réalisée aux noeuds intermédiaires en contrôlant des indicateurs locaux de congestion tels que l'occupation de la file d'attente ou l'état de canal. D'autre part, la détection de congestion globale est réalisée au niveau du puits où les attributs de bout en bout

tels que les retards inter-paquets (inter-packet delays) et la fréquence de pertes peuvent être utilisés pour déduire la congestion.

IV.3.2 L'objectif du contrôle de congestion

Dans leur nature, les RCSF sont orientés application (application specific). Donc, les protocoles de congestion seront différents selon l'application visée par un RCSF où ils sont appliqués. Pour cette raison, les protocoles de contrôle de congestion sont aussi orientés application.

IV.3.3 Les mécanismes de contrôle de taux de transfert

Les mécanismes de contrôle de taux dans les RCSF peuvent être centralisés (centralised), contrôle de la source (source-control) et *hop-by-hop backpressure*. Le mécanisme de contrôle de la source est réalisé par le puits). Essentiellement, quand la congestion (ou le premier signe de congestion) est découvert, le puits donne l'ordre aux noeuds sources de régler leurs taux. Alors que, dans *hop-by-hop backpressure* le mécanisme est réalisé aux noeuds intermédiaires, dans lesquels le noeud intermédiaire donne l'ordre aux noeuds qui sont en son amont de régler leurs taux en se basant sur son état de congestion local.

IV.3.4 Modèle de l'application cible

La plupart des protocoles se basent sur le modèle de communication many-to-one. Cependant, quelques protocoles diffèrent sur leurs hypothèses dans ce modèle, telles que la supposition du flux à haut débit (high-rate flows), ou multiples requêtes à multiples puits (multiple queries to multiple sinks), etc.

IV.3.5 D'autres métriques

D'autres métriques peuvent différencier les protocoles de contrôle de congestion. Par exemple, quelques protocoles nécessitent un support additionnel (MAC spécialisé, ou capacité réseau supplémentaire). De plus, quelques protocoles font l'attention spéciale à l'efficacité énergétique.

IV.4 Quelques protocoles de contrôle de congestion dans les RCSF

Dans le passé récent, de nouveaux protocoles de contrôle de congestion ont été proposés [56]. Le nombre élevé des protocoles de contrôle de congestion ne nous donne pas la possibilité de les explorer tous. Dans le paragraphe suivant nous allons faire une étude un peu détaillée sur certains d'entre eux.

IV.4.1 Congestion detection and avoidance: CODA

CODA [57] est une technique de contrôle de congestion pour les RCSF qui comprend trois mécanismes :

1) *Détection de congestion basée sur le récepteur(Receiver-based congestion detection)*

L'occupation du tampon a été abondamment utilisée dans les algorithmes de détection de congestion traditionnels comme une mesure de niveau de congestion. Dans leur algorithme, les auteurs démontrent que l'occupation du tampon seule n'est pas une bonne mesure de congestion dans les réseaux sans fil à cause de la nature partagée du canal. La file d'attente peut se décongestionner potentiellement même si les paquets sont perdus en raison de la collision. Il est possible aussi pour les noeuds de déterminer la congestion en écoutant le canal et déterminer comment il est occupé/chargé .Cependant, cela peut avoir un coût énergétique significatif.

Cependant, l'écoute continue encourt le haut prix d'énergie. Donc, la CODA utilise un plan d'échantillonnage qui active la surveillance du canal local surveillant seulement sous de certaines conditions, par exemple seulement quand le tampon d'envoi n'est pas vide, pour économiser l'énergie.

2) *Open-loop hop-by-hop back-pressure*

Quand le récepteur détecte une congestion, il envoie un message de suppression (une notification de congestion explicite), appelé « backpressure signal », en anglais, vers la source. Le message de suppression est envoyé à plusieurs reprises tant que l'état de congestion persiste. Les noeuds peuvent répondre à ce message en supprimant des paquets ou en réduisant leur taux. Le message de suppression peut se propager entièrement jusqu'à

la source, ou atteindre seulement les noeuds intermédiaires selon leur état de congestion local.

3) *Closed-loop multi-source regulation*

Ce mécanisme de contrôle de congestion est utilisé par le puits pour intervenir dans la régulation des sources multiples, dans le cas où la congestion est persistante.

Essentiellement, quand le taux de transmission d'une source excède le débit théorique maximum, S_{max} , la source informe le puits par un bit qu'elle met dans chaque paquet qu'elle transmet au puits tant que le taux de transmission reste supérieur à S_{max} .

En réponse, le puits commence à envoyer les ACKs à la source jusqu'à ce qu'il détecte la congestion. Quand le puits détecte la congestion, il arrête d'envoyer les ACKs jusqu'à l'atténuation de la congestion, pour implicitement informer l'expéditeur de baisser son taux de transmission. En général, les sources maintiennent, diminuent, ou augmentent leurs taux selon la fréquence de réception des ACKs.

IV.4.2 Fair rate allocation (FRA)

Fair rate allocation, ou allocation équitable de taux de transmission Est une approche explicite au contrôle de congestion avec garantie d'équité proposée par Ee et Bajcsy [58]. Le mécanisme de FRA comprend les trois démarches suivantes :

Déterminez le taux moyen, r , de transmission d'un paquet : En supposant que les paquets ont la même taille, le taux de transmission du paquet peut être estimé comme l'inverse de l'intervalle de temps de transmission d'un seul paquet. L'intervalle est mesuré à partir du moment où la couche transport envoie le paquet à la couche réseau jusqu'à au moment où la couche réseau signale que le paquet a été transmis.

Assignez le taux r aux noeuds en amont (c-à-d les noeuds fils dans l'arbre de collecte de données) : Le taux moyen de transmission de paquet est divisé par le nombre, n , de noeuds fils pour assigner le taux de génération de paquet de données comme $r_{data} = rn$

Pour calculer n , chaque noeud inclut la taille de son sous-arbre (le nombre de ses noeuds fils) dans un paquet et l'envoie au parent. Le parent décompte les nombre de ces descendants, y ajoute un (si le parent lui-même produit des données) et inclut le total dans le paquet avant de l'envoyer vers le puits.

Quand les files d'attente débordent ou sont au point de déborder, le noeud assigne un taux de génération de paquet inférieur aux noeuds qui sont en son amont.

Obtenir le taux du noeud parent $r_{\text{data_parent}}$ par l'écoute du canal ou via un message de contrôle. Comparer r_{data} avec $r_{\text{data_parent}}$ et propager le plus petit taux aux noeuds du sous-arbre.

L'équité proportionnelle est obtenue en mesurant et en divisant le taux par le nombre de noeuds en aval. Il s'agit donc de l'équité proportionnelle. Pour réaliser cela, chaque noeud maintient une file d'attente de type FIFO pour chaque noeud fils comme le montre la figure IV.1. Alors, un mécanisme de sélection probabiliste est employé pour mesurer le poids du choix des paquets. Le choix de la file d'attente à partir de laquelle le paquet sera transmis est proportionnel au nombre de noeuds entretenus par cette file d'attente.

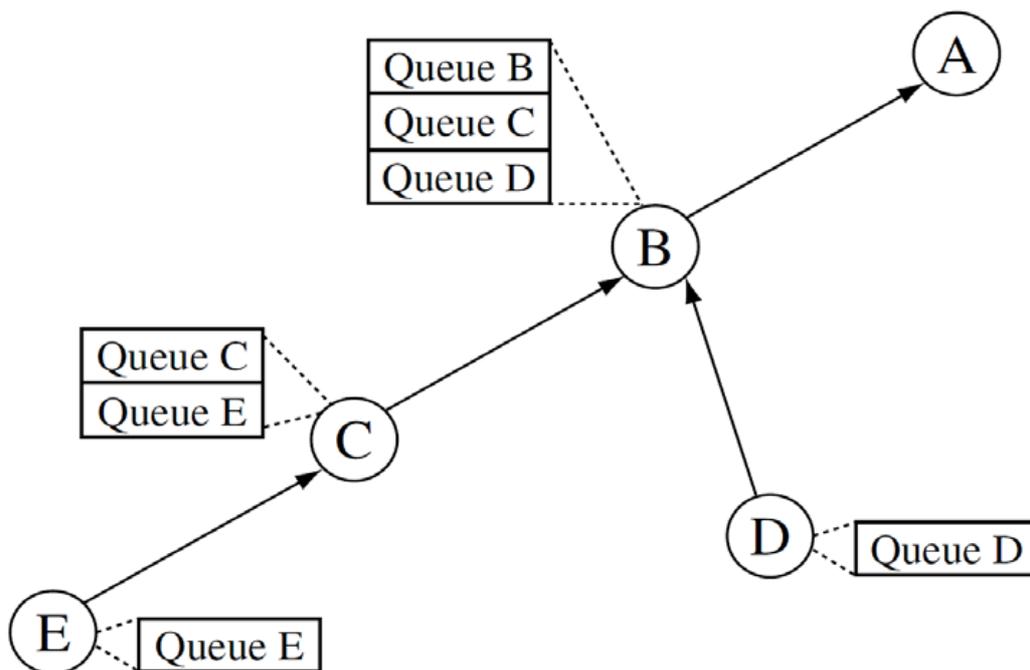


Figure IV.1 : FIFO multiples pour assurer la délivrance équitable de données dans FRA

IV.5 Conclusion

La congestion, lorsqu'elle existe dans un réseau, dégrade les performances du système et peut causer beaucoup de problèmes. Dans ce chapitre nous avons identifié quelques

problèmes parmi lesquels une perte des paquets, parfois contenant l'information critique. Nous avons aussi étudié quelques protocoles proposés pour détecter et/ou contrôler la congestion dans les RCSF.

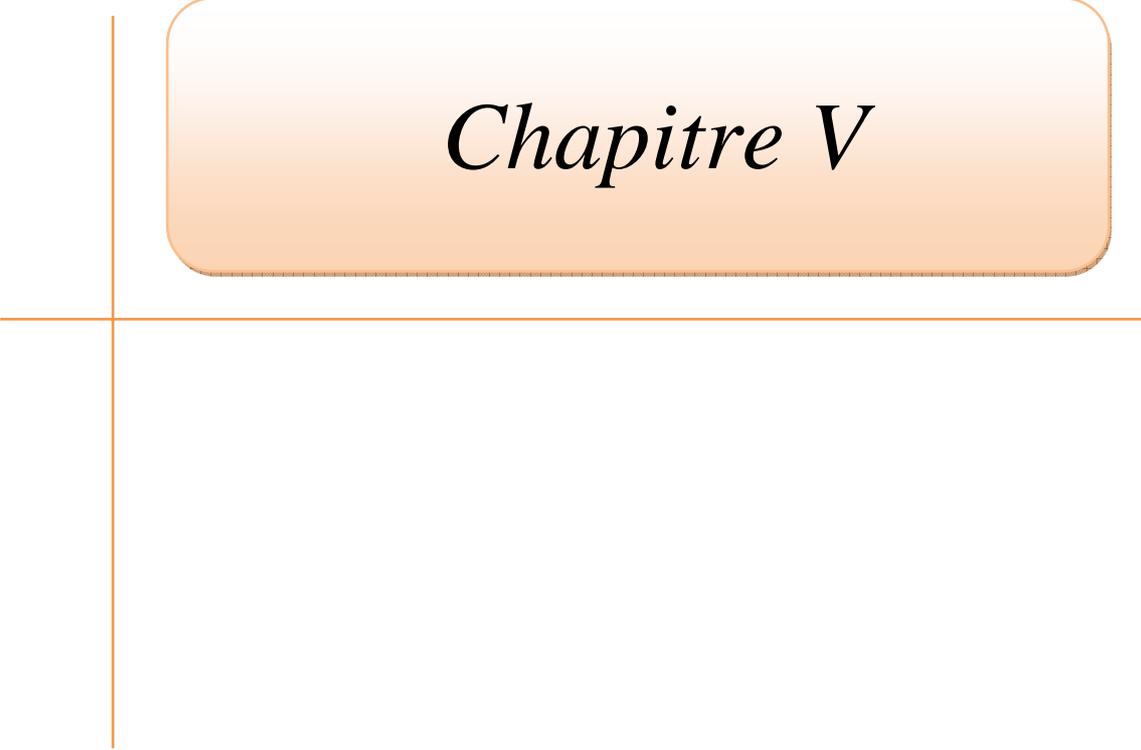
Le point commun de ces protocoles est que, lorsqu'une congestion ou le premier signe de congestion apparaît au niveau d'un noeud, ce dernier procède à une régulation du taux d'activité des noeuds sources des messages dont il est le destinataire.

Malgré que ces protocoles ont proposé une amélioration significative aux techniques classiques de contrôle de congestion qui se basaient presque uniquement sur le taux d'occupation du tampon de données au niveau du destinataire des messages pour détecter la congestion, ces protocoles peuvent ne pas garantir la non perte des paquets.

En effet, dans ce genre de protocoles, quelques noeuds amont (fils dans l'arbre de collecte de données) peuvent réduire leur taux de transfert jusqu'à ne pas transmettre pendant un certain temps.

Nous avons vu que selon le phénomène mesuré, ces noeuds sont susceptibles de capter et de transmettre la même donnée ou les données présentant un écart de valeur non significatif. La redondance de ces données peut être une source sérieuse de congestion.

Le problème qui se pose dans les protocoles étudiés dans ce chapitre, est que, à notre connaissance, aucun d'entre eux ne prend en considération cette redondance. Ce qui nous motive à proposer une technique d'agrégation dans le protocole LEACH exploitant cette propriété des RCSF pour contrôler la congestion. La technique utilisée pour réduire ou éviter cette redondance est connue sous l'appellation d'agrégation des données et va être décrite en détails dans le chapitre V avant de proposer notre solution.



Chapitre V

V.1 Introduction

Dans un capteur, la problématique principale concerne la consommation d'énergie : en effet, ces derniers doivent restés opérationnels le plus longtemps possibles, dans des conditions parfois difficiles. Il a été montré dans plusieurs publications scientifiques que la transmission d'un bit est équivalent, en terme d'énergie, à l'exécution d'environ 1000 instructions [41]. Cette valeur augmente avec la portée de la radio. Plus le capteur devra transmettre loin, et par conséquent augmenter sa puissance d'émission, plus il va consommer de l'énergie, et par conséquent réduire sa durée de vie. Il convient donc de réduire en compressant ou en agrégeant les données lors de leur routage.

Les techniques d'agrégation des données, c'est à dire de traitement des données par le réseau, permettent de réduire le nombre de messages (et de bits transmis sur les liens sans-fil) et par conséquent réduire la consommation en énergie.

L'objectif de ce chapitre est d'avoir quelque notion sur l'agrégation des données dans les réseaux de capteurs et pour cela nous allons présentés quelques techniques d'agrégation utilisé par des protocoles de routage dans les RCSF.

V.2 Définition

L'agrégation de données dans les réseaux de capteurs consiste à remplacer les lectures individuelles de chaque capteur par une vue globale, collaborative sur une zone donnée (clustering). [42]

L'agrégation de données est une technique qui permet de réduire le coût global des communications dans un réseau où les messages envoyés entre les noeuds ont des contenus « similaires ». Des paquets venant de plusieurs noeuds qui arrivent sur un noeud dit « agrégateur », le long du chemin vers la station de base, peuvent être agrégés (avec une fonction spécifique suivant l'application). [43]

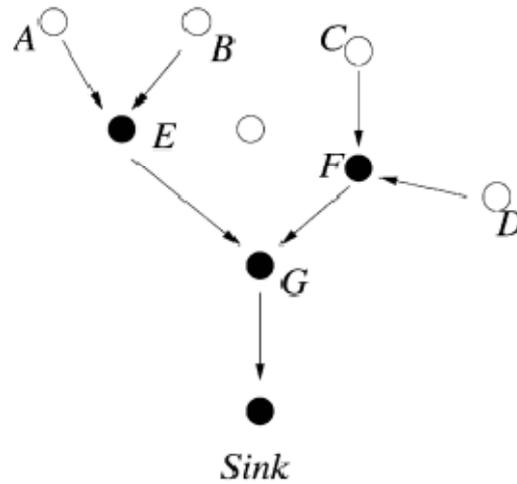


Figure V.1 : Agrégation de données

V.3 Approches d'agrégation de données

Dans un RCSF on distingue deux approches d'agrégation de données [44][45] : agrégation sans et avec réduction de la taille des données .

- **Agrégation avec réduction de la taille (*In-network aggregation with size reduction*)** : fait allusion au processus de combinaison des données venant de différentes sources pour réduire la quantité de données à envoyer dans le réseau. Comme exemple, supposez qu'un nœud reçoit deux paquets de deux différentes sources contenant les températures localement mesurées. Au lieu d'envoyer les deux paquets, le capteur peut calculer la moyenne des deux lectures et l'envoyer dans un seul paquet.
- **Agrégation sans réduction de la taille (*In-network aggregation without size reduction*)** : fait allusion au processus de fusion des paquets venant de différentes sources dans le même paquet sans aucun traitement sur les données. Supposez par exemple qu'un nœud reçoit deux paquets contenant les données qui décrivent les phénomènes physiques différents, par exemple, l'humidité et l'acidité du sol. Ces deux valeurs ne peuvent pas être traitées ensemble mais elles peuvent être transmises dans un seul paquet simple et réduire ainsi l'overhead.

L'avantage de la première approche est qu'elle permet de réduire au maximum la quantité de données échangées. Son principal inconvénient est que après l'opération d'agrégation, il n'est pas toujours possible de reconstituer tous les paquets originaux¹. La seconde approche, par contre, préserve les paquets originaux (c.à.d., au niveau du puits, les paquets originaux

peuvent être reconstruits). Le choix de l'approche à utiliser dépend de plusieurs facteurs dont : type d'application, taux de transfert de données, les caractéristiques du réseau.

V.4 Les éléments de base de l'agrégation de données

Les techniques d'agrégation dans le réseau exigent trois éléments fondamentaux [44] : un protocole de routage convenable, les fonctions d'agrégation efficaces et une façon efficace de représenter les données, voir figure V.2 ci-dessous. Dans le reste de cette section nous décrivons chacun de ces aspects.

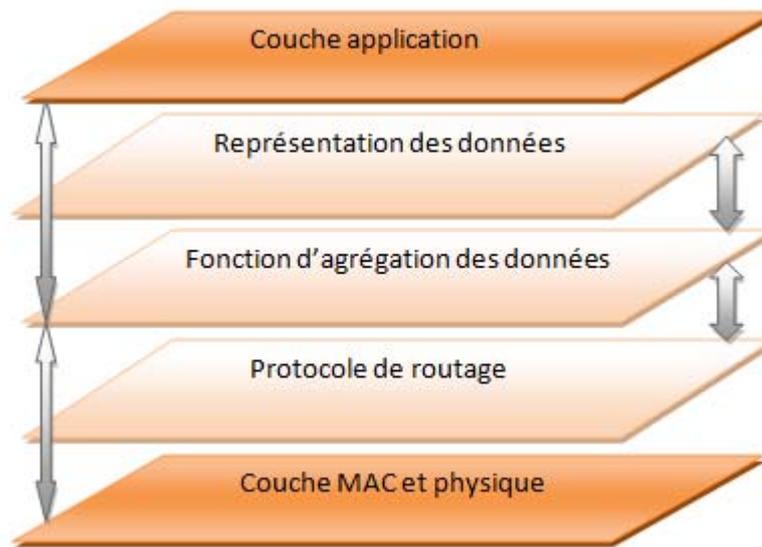


Figure V.2 : Relation entre la technique d'agrégation et d'autres couches de la pile

Notons que dans la plupart des cas, la technique d'agrégation interagit avec les couches application, Physique et MAC, comme le montre la figure.

V.4.1 Fonctions d'agrégation de données.

L'une des fonctionnalités les plus importantes que les techniques d'agrégation dans le réseau devraient fournir est la capacité de combiner des données venant de différents noeuds. Il y a plusieurs types de fonctions d'agrégation et la plupart d'entre elles sont fortement dépendantes de l'application cible. Néanmoins, nous pouvons identifier quelques paradigmes communs pour leur classification [44][45] :

- ***Insensibles à la duplication Vers sensible à la duplication***

Dans un réseau de capteur sans fil, un noeud intermédiaire peut recevoir des copies multiples d'une même information. Dans ce cas, il arrive que cette même information soit considérée plusieurs fois lors de l'agrégation la fonction d'agrégation utilisée est sensible à la duplication (duplicate sensitive), le résultat final dépendra du nombre de fois que la même valeur a été considérée. Dans le cas contraire, la fonction d'agrégation est dite insensible à la duplication (duplicate insensitive).

- ***Sans perte Vs Avec perte***

L'agrégation de données peut se faire avec ou sans perte d'information. L'agrégation avec perte ne permet pas de reconstruction parfaite mais l'agrégation sans pertes garantit une récupération complète de toutes les données de capteur individuelles à la station de base (puits) [46].

De bonnes fonctions d'agrégation pour les réseaux de capteur sans fil ont besoin de satisfaire des besoins supplémentaires. En particulier, elles devraient tenir compte du traitement très limité et des capacités d'énergie des noeuds intermédiaires et devraient être donc implémentées au moyen des opérations élémentaires.

V.4.2 Les types d'agrégation

Selon la stratégie utilisée pour choisir le moment où un noeud doit retransmettre la donnée agrégée, nous pouvons distinguer trois types d'agrégation : [47] : Agrégation périodique simple, Agrégation périodique par saut et Agrégation périodique par saut ajusté.

- ***Agrégation périodique simple (Periodic simple aggregation) :***

Chaque noeud doit attendre une période de temps prédéterminé, pour agréger tous les paquets reçus avant de transmettre le résultat de l'agrégation.

- ***Agrégation périodique par saut (Periodic per-hop aggregation) :***

Quand on considère un arbre de collection et un noeud agrégateur envoi le paquet fusionné seulement quand il a reçu un paquet de tous ses enfants. De nouveau cette approche est très simple, mais peut mener aux temps d'attente inefficaces quand quelques noeuds sont moins actifs que d'autres et envoient des données tout à fait rarement.

- ***Agrégation périodique par saut ajustée (Periodic per-hop adjusted aggregation)***

Il utilise le même principe de base que périodiques par saut, mais la durée de temporisation d'un noeud est basée sur sa position dans l'arbre de distribution.

V.4.3 Protocoles de routage avec agrégation des données

L'ingrédient le plus important pour l'agrégation dans le réseau est un protocole de routage bien conçu [44]. Comparativement au routage classique, la prise en compte d'agrégation des données exige de nouveaux paradigmes pour acheminer les données. Par exemple, les techniques d'agrégation dans le réseau peuvent exiger une forme de synchronisation parmi les noeuds. En particulier, la meilleure stratégie d'un noeud donné n'est pas toujours d'envoyer des données aussi tôt que c'est disponible. L'attente d'information venant des noeuds voisins peut mener à de meilleures techniques d'agrégation des données et, ainsi, améliorer la performance.

Dans ce qui suit, nous essayons de donner un aperçu sur quelques protocoles de routages avec agrégation des données en les classifiant quatre catégories : hiérarchique, basés sur les clusters, multi-chemins et hybrides.

V.4.3.1 Approche hiérarchique

La plupart des travaux faits sur l'agrégation de données dans les RCSFs ont proposé des solutions exploitant une structure hiérarchique (arborescente) [53]. En effet, la façon la plus simple d'agréger des données venant des sources vers le puits est d'élire quelques noeuds spéciaux qui travaillent comme les points d'agrégation et définissent une direction préférée à être suivie en envoyant des données.

Selon l'approche hiérarchique [51] [52], un arbre s'étendant à partir du puits est construit d'abord. Par la suite, une telle structure est exploitée en répondant aux requêtes produites par le puits. Ceci est fait en performant l'agrégation le long de l'arbre d'agrégation en procédant niveau par niveau de ses feuilles à sa racine. Ainsi, puisque au moins deux messages arrivent à un noeud donné, le résultat de leur agrégation peut être calculé exactement.

Dans les paragraphes suivants, nous considérons les principaux algorithmes de routage basés sur les arbres d'agrégation de données.

V.4.3.1.1 Tiny AGregation (TAG)

TAG [50] est un protocole data centric basé sur les arbres d'agrégation et est spécifiquement conçu pour l'application de surveillance. Cela signifie chaque noeud devrait produire l'information périodiquement. Donc, il est possible de classifier TAG comme un protocole à Agrégation périodique par saut ajustée. TAG se compose de deux phases : une phase de *distribution* (distribution phase), dans laquelle les requêtes sont disséminées et une

phase de *collecte* (collection phase), où les valeurs agrégées sont continuellement routées vers le haut.

Pendant la phase de distribution, le puits diffuse un message en demandant aux noeuds de s'organiser dans un arbre de routage et envoie ensuite ses requêtes. Dans chaque message il y a un champ spécifiant le niveau (level), ou la distance depuis racine, qui est incrémenté à chaque fois qu'un noeud reçoit un message et le rediffuse aux autres noeuds voisins. Le niveau du puits est égal à zéro. Ce processus continue jusqu'à ce que tous les noeuds aient été assignés identificateur et un parent.

TAG adopte la sélection et l'agrégation offertes par les langages d'interrogation de bases de données (SQL). Par conséquent, les requêtes de TAG ont la forme suivante :

```
SELECT{agg(expr), attrs} from SENSOR
WHERE{selPreds}
GROUP BY{attrs}
HAVING{havingPreds}
EPOCH DURATION i
```

En pratique, le puits envoie une requête, où il spécifie les quantités qu'il veut recueillir (le champ *attrs*), comment celles-ci doivent être agrégées (*agg (expr)*) et les capteurs qui devraient être impliqués dans l'extraction de données. Cette dernière demande est spécifiée par les clauses *WHERE*, *GROUP BY* et *HAVING* [50]. Finalement, un champ de durée *EPOCH* spécifie le temps (en secondes) que chaque capteur devrait attendre avant d'envoyer de nouvelles lectures de captage. Cela signifie que les utilisées pour calculer le résultat de l'agrégation appartiennent toutes au même intervalle de temps, ou epoch.

Pendant la phase de collecte de données, en raison de la structure arborescente, chaque parent doit attendre des données de tous ses enfants, pendant un temps égal à epoch, avant qu'il puisse envoyer le résultat de l'agrégation à son parent. Les *epochs* sont divisés en intervalles plus courts appelés slots de communication. Le nombre de ces slots est égal à la profondeur maximum de l'arbre de routage et l'agrégation de données est exécutée par tous les noeuds intermédiaires.

Exemple de requête utilisée dans TAG :

```
SELECT AVG(temperature),chambre FROM capteurs
WHERE etage = 10
GROUP BY chambre
```

```
HAVING AVG(temperature) > 25  
EPOCH DURATION 60s
```

Cette requête partitionne les capteurs se trouvant au dixième étage d'un immeuble suivant les chambres dans lesquelles ils se trouvent. La requête renvoie toutes les chambres dans lesquelles la température moyenne est supérieure à 25 unités de température. Les résultats mis à jour sont envoyés après chaque minute (60secondes).

V.4.3.1.2 Directed Diffusion

Dans Directed Diffusion, l'agrégation de données est exécutée, quand les données sont envoyées au puits, au moyen des méthodes convenables, qui peuvent être choisies selon les exigences de l'application. L'arbre de collecte de données (renforcement des chemins) doit être périodiquement rafraîchi par le puits. Cela peut être cher en cas de topologies dynamiques.

V.4.3.1.3 PEGASIS

Rappelons que dans PEGASIS les noeuds sont organisés en chaînes avec un chef (leader) par chacune et qu'il est le seul noeud autorisé, parmi tous les noeuds qui forment la chaîne dont il est leader, à transmettre directement au puits. L'agrégation dans PEGASIS se fait selon la procédure suivant :

Chaque noeud reçoit la donnée de son voisin (son prédécesseur dans la chaîne), l'agrège avec sa propre donnée en générant un seul paquet de même taille et envoie le résultat à son successeur. Ce processus continue jusqu'à ce que le paquet atteigne le leader de la chaîne courante. A ce stade, le leader inclut sa propre donnée dans le paquet et l'envoie au puits.

V.4.3.2 Approche basée sur les clusters

Dans les protocoles basés sur les clusters tels que LEACH et COUGAR, l'agrégation est exécutée par les cluster-heads. Le cluster-head collecte les données des membres de son cluster, les agrège avec sa propre donnée et envoie le résultat au puits (si il se trouve dans la portée du puits) ou transmet le résultat à un autre cluster. Le processus est donc semblable à celui vu dans l'algorithme PEGASIS, en comparant le cluster-head au chef de la chaîne et les membres du cluster aux noeuds appartenant à la même chaîne.

V.4.3.3 Approche multi-chemins

L'idée principale de cette approche est que chaque noeud peut envoyer à ses (si possible) multiples voisins en exploitant la nature broadcast du média sans fil. Une structure qui convient bien à cette approche s'appelle topologie en anneaux où les noeuds capteurs sont divisés en plusieurs niveaux selon le nombre de sauts les séparant du puits. L'agrégation de données est exécutée sur les chemins multiples puisque les paquets se déplacent niveau par le niveau vers le puits (voir figure V.3).

Dans ce qui suit, nous allons voir Synopsis Diffusion qui appartient à cette classe de protocoles.

Dans Synopsis Diffusion [49] la topologie de diffusion de données est organisée en anneaux concentriques autour du puits. Synopsis Diffusion comprend deux phases : la phase de distribution des requêtes (distribution of the queries) et la phase d'extraction de données (data retrieval). La topologie en anneau est formée quand un noeud envoie une requête dans le réseau. En particulier, deux différentes structures, énumérées ci-dessous, peuvent être prises en compte.

Le premier type de topologie consiste en structure d'anneau simple.

Pendant la phase de distribution des requêtes, les noeuds du réseau forment un ensemble d'anneaux autour du noeud émetteur de la requête q , qui est le seul capteur appartenant à l'anneau R_0 . Un noeud est dans l'anneau R_i s'il est à i sauts du noeud q .

Le deuxième type de topologie a quelques améliorations qui le rendent plus robuste que le précédent et capable de faire face aux changements dans le réseau. Cette topologie s'appelle *anneaux adaptatifs* (adaptive rings). La phase de distribution ne change pas mais cette fois-ci un noeud n dans l'anneau i garde la trace du nombre de fois, n_{ov} , que les transmissions de n'importe quel noeud n_{i-1} dans l'anneau $i-1$ ont inclus ses propres données pendant quelques derniers epochs. Si le nombre est petit, n essaie de trouver un meilleur anneau pour avoir plus de ses propres données incluses dans les transmissions ultérieures.

Dans l'exemple de la figure V.3, les données générées au noeud A peuvent atteindre le puits par sept chemins : {A, B, F, I, S}, {A, B, F, H, S}, {A, B, F, G, H, S}, {A, C, D, E, I, S}, {A, C, F, H, S}, {A, C, F, I, S} et {A, C, G, H, S}.

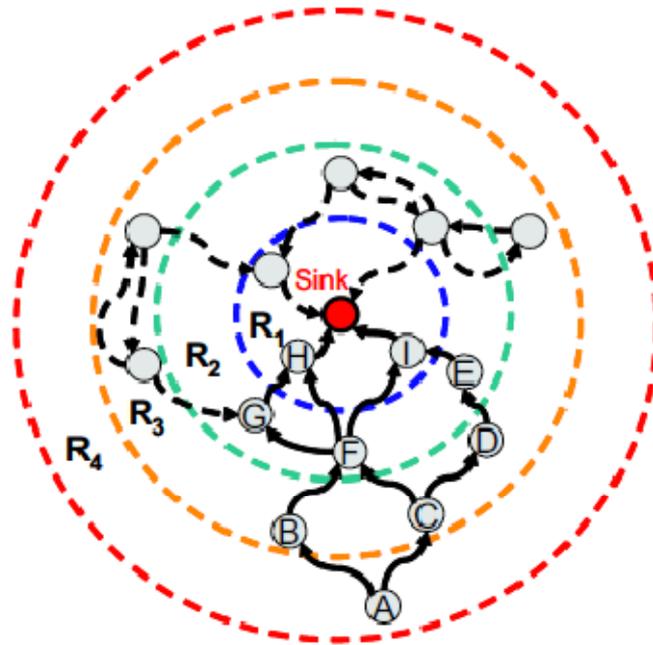


Figure V.3 : Exemple d'une technique d'agrégation utilisant une structure en anneau

V.4.3.4 Approche hybride

Pour profiter des avantages de deux approches (hiérarchique et multi-chemins), il est possible de définir des approches hybrides. L'exemple typique est présenté dans [48] et est expliqué ci-après.

Dans le protocole Tributaries and Deltas [48] les structures d'agrégation des données peuvent circuler simultanément dans de différentes régions du réseau. L'idée consiste en ce que sous les taux faibles de perte de paquets, un arbre d'agrégation de données est la structure la plus convenable. D'autre part, quand ces taux deviennent, une approche multi-chemins peut être la meilleure. Pour cela, les noeuds sont divisés en deux catégories : les noeuds utilisant l'approche hiérarchique pour envoyer les paquets (appelés aussi les noeuds T) et les ceux utilisant l'approche multi-chemins (Les noeuds M). Cela signifie que le réseau est organisé dans les régions en exécutant l'une des deux approches.

V.4.4 La représentation des données

En raison de ses capacités de stockage limitées, un noeud peut ne pas être capable de conserver tous les paquets reçus et générés dans sa mémoire tampon. Il a besoin de décider donc s'il faut les conserver, les supprimer, les compresser, ou les transmettre. Toutes ces opérations exigent une façon convenable de représenter les données. La structure de données correspondante peut varier selon les exigences de l'application, du noeud ou même de la

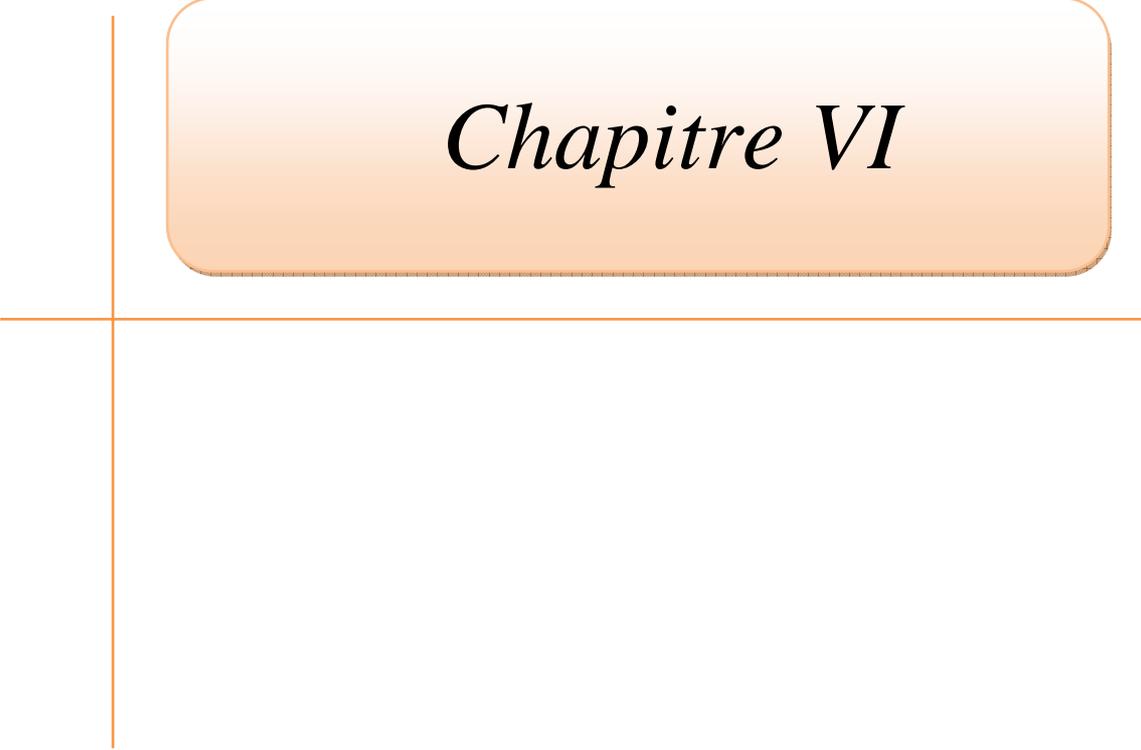
position du noeud. Ces structures exigent aussi qu'il y ait des fonctions d'agrégation capables de les exploiter. Actuellement, beaucoup de travaux de recherche ont proposé des modèles de représentation de données dans les réseaux de capteurs. Exemple : *Synopsis Diffusion Framework*.

V.5 Conclusion

L'agrégation de données dans les réseaux de capteur sans fil est une approche prometteuse pour neutraliser la perte de ressources causées par la redondance voyageant partout dans le réseau.

Dans ce chapitre, nous avons étudié les protocoles d'agrégation des données utilisés dans les réseaux de capteurs sans fil. Nous avons constaté que ces protocoles utilisent les fonctions variées allant des fonctions de calcul de la moyenne des données collectées à des fonctions utilisant les requêtes semblables à celles des langages d'interrogation des bases de données.

Les messages réduits par la fonction d'agrégation peuvent causer la congestion et donc la technique d'agrégation des données peut être utilisée pour contrôler la congestion. Le chapitre suivant explique bien notre technique d'agrégation pour le contrôle de congestion appliquée sur le protocole LEACH étudié dans le troisième chapitre. Et afin de montrer notre amélioration de protocole LEACH, une implémentation des deux versions sur un simulateur réseau est nécessaire. Les détails de l'implémentation sur le simulateur J-Sim et une comparaison entre notre amélioration et la version originale de LEACH seront présentés toujours dans le chapitre VI.



Chapitre VI

VI.1 Introduction

Les protocoles de contrôle de congestion ne sont pas toujours efficaces dans les applications où il y a beaucoup de redondances des données. L'agrégation de données est une bonne solution pour ce problème. C'est une collection des lectures de capteurs, elle représente une vue collaborative d'un ensemble de noeuds. Généralement, elle est appliquée sur une zone très spécifique limitée par le noeud PUIITS. Ce dernier envoie la valeur de l'agrégation à la station de base en utilisant un protocole de routage. Le nombre de noeuds qui envoient leurs lectures peut être important et les informations envoyées par ces noeuds peuvent être redondantes. L'agrégation de données conserve l'énergie par la réduction du nombre de données acheminées par les noeuds intermédiaires.

Après la démarche générale de prise de conscience de l'importance de la réduction du nombre de données acheminées par les noeuds dans le protocole LEACH, et la conservation de l'énergie, et, après l'étude de quelques techniques d'agrégation des données, nous allons dans ce chapitre introduire au protocole LEACH le contrôle de congestion utilisant la technique d'agrégation des données. Nous allons renommer ce protocole par LEACHCO.

Le but de ce chapitre est d'effectuer une étude de la solution proposée et présentée l'ensemble des simulations effectuées sur les deux protocoles afin de voir l'amélioration apportée.

VI.2 Description générale du protocole LEACHCO

Le protocole que nous allons décrire introduit une autre métrique de qualité de service qui est le contrôle de congestion dans le réseau de capteur. Le protocole LEACHCO utilise une technique d'agrégation de données pour réduire le nombre de paquets transmis au noeud puits dans le but d'éviter la congestion qui peut être causée par la présence des données redondantes dans le réseau.

VI.2.1 Les phases de communication

VI.2.1.1 Phase de collecte des données

La collecte des données se fait au niveau du noeud puits et au niveau des capteurs incluant le cluster-head (CH).

Nous avons vu dans le troisième chapitre que la collection des données au niveau des capteurs se fait au niveau de la phase de transmission où les membres du cluster émettent leurs données captées au CH pendant leurs propres slots.

La collection des données au niveau des CHs est différente à celle des autres nœuds capteurs. Chaque CH maintient une structure de données (buffer) d'une taille qui dépend de l'espace mémoire dont dispose le capteur et de la taille des paquets échangés. Ce buffer permet de stocker les paquets de données envoyés par les membres du cluster.

Lorsque la phase de collecte commence, le CH initialise un timer, *aggregTimer*.

A chaque réception d'une donnée, le CH calcule le taux d'occupation du buffer. Si ce taux dépasse un certain seuil ou bien atteint son niveau maximal, un capteur arrête le timer et commence la phase d'agrégation. Si non il stocke la donnée reçue et la phase continue. A l'expiration du timer, le CH commence la phase d'agrégation et enfin, envoie le résultat final au nœud puits pour les collectés.

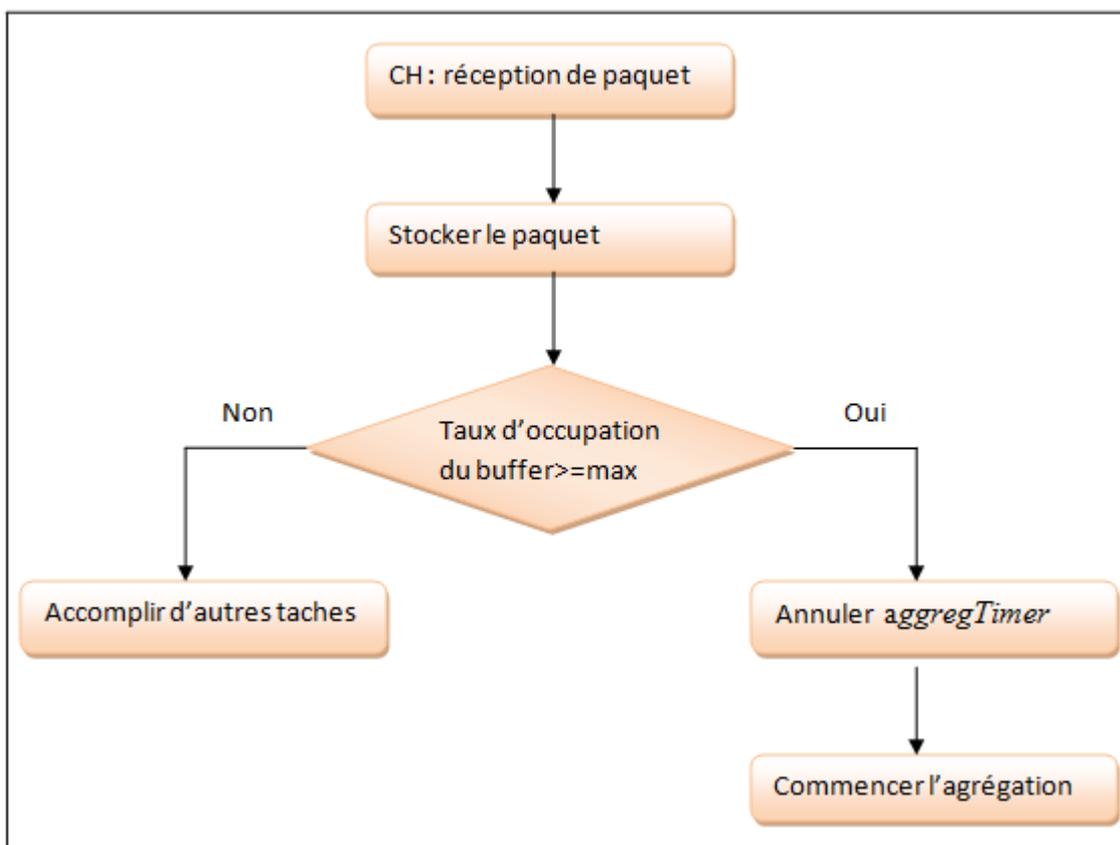


Figure VI.1 : Diagramme de transition d'états de la phase de collecte des données.

Le format d'un paquet de données est décrit dans le tableau ci-dessous.

Champs	description
sender_id	L'identifiant du nœud source
CH_id	L'identifiant du CH destinataire
sensedData	La donnée ou le phénomène étudié
timeStamp	Unité de temps utilisé par le schedule
size	La taille de la donnée

Tableau VI.1 : les différents champs d'un paquet reçu par un CH

VI.2.1.2 Phase d'agrégation des données

A partir des données stockées dans le buffer et la donnée issue de l'unité de captage, cette fonction se base sur la corrélation entre ces données pour former les paquets à envoyer. Pour cela, nous définissons une variable de sensibilité *seuilData*. Tous les paquets de données dont le champ *sensedData* diffère d'une valeur inférieure ou égale à *seuilData* seront agrégés en un seul paquet dont le champ *sensedData* du paquet final à envoyer au nœud puit par le CH, est la moyenne arithmétique des données agrégées. La formule est donnée comme suit :

$$\text{dataToSend} = \text{finalData} / \text{numberOfDataAggregated}$$

Où *finalData* est le résultat de l'agrégation des deux données ;

numberOfDataAggregated est le nombre de données agrégées ;

dataToSend la données final à envoyer au nœud puit.

Le nombre de paquets à envoyer après l'agrégation dépendra de la corrélation entre les données reçues.

VI.2.1.3 Phase de contrôle de congestion

Pour assurer le contrôle de congestion au niveau du nœud, nous avons dit qu'on a introduit à chaque CH un buffer de réception des données de taille limitée, *bufferSize*, égale

au nombre maximum des noeuds dont les paquets de données peuvent être stockés avant qu'un noeud déclare un état de congestion. Ce type de contrôle est effectué chaque fois qu'un noeud reçoit un paquet de données. *BufferSize* est configurable et dépend de l'espace mémoire dont dispose un capteur.

Chaque CH utilise un compteur *bufferSizeOccup* pour vérifier le niveau d'occupation du buffer de données.

Le contrôle de congestion se fait comme suit :

A la réception des paquets de données, le CH ajoute à *bufferSizeOccup* la taille du paquet reçu. Si le pourcentage d'occupation du buffer dépasse un certain seuil, le noeud commence l'agrégation. Si non il sauvegarde le paquet dans le buffer et continue les autres traitements.

VI.3 Implémentation et simulation

Afin de vérifier les performances de notre amélioration par rapport à celles du protocole original, nous avons recouru à la simulation. Pour ce faire, les deux protocoles ont été implémentés sur un simulateur réseau.

VI.3.1 Environnement de simulation

Pour tester les performances d'une solution apportée à un problème de communication dans un réseau, il n'est pas toujours possible d'accéder aux infrastructures nécessaires en raison de leurs coûts élevés. De plus, les expérimentations réelles n'offre souvent pas une grande souplesse. Par exemple, il est difficile de gérer la distribution des nœuds déployés d'une manière ad hoc dans un terrain de plusieurs kilomètres carrés. Pour remédier à ce problème, on a recours à la simulation, qui met à la disposition de l'utilisateur un environnement d'expérimentation.

VI.3.1.1 Choix du simulateur

Plusieurs environnements de simulation sont utilisés pour évaluer les protocoles et des architectures proposés pour les WSNs. Certains sont libres et parfois Open source par contre il y en a d'autres qui sont commercialisés. Aucun de ces simulateurs n'est parfait ni ne répond à tous les besoins.

Nous avons choisi le simulateur *J-Sim* pour simuler notre protocole. L'architecture et le code utilisé par J-Sim sont suffisamment bien structurés pour permettre une prise en main relativement aisée.

Concernant l'analyse des résultats, il est plus aisé que pour le cas du simulateur NS2. J-Sim permet d'utiliser, comme générateur de trafic, n'importe quelle application Java et semble gérer correctement l'aspect consommation d'énergie.

VI.3.1.2 Le simulateur J-Sim

VI.3.1.2.1 description générale du simulateur J-Sim

J-SIM J-Sim [59] (appelé autrefois JavaSim) a été développé par une équipe du laboratoire Distributed Realtime Computing Laboratory (DRCL) de l'université d'État d'Ohio. Ce simulateur, développé entièrement en langage Java, repose sur une architecture logicielle basée sur les composants autonomes, appelée « Autonomous Component Architecture » (ACA). Un composant est une entité indépendante représentant un objet physique (une batterie, un module radio, une couche logicielle, etc.) ou logique (un protocole de routage, un modèle de mobilité, etc.). Ces composants seront ensuite connectés à l'aide de ports afin de générer un réseau simulé.

La simulation du fonctionnement d'un réseau de capteurs, qui exige la définition des composants et leur mise en relation, est réalisée grâce à un langage spécifique, TCL (Tool Command Line) [60]. Il s'agit d'un langage de script dans lequel on spécifie l'architecture du réseau ainsi que les paramètres de simulation et d'analyse. Les commandes de script peuvent également être fournies en ligne de commande, instruction par instruction.

A l'aide de TCL, on définit les composants puis on les connecte. Tous les composants sont hébergés dans un conteneur, qui est à son tour un composant. La définition des composants est en fait la création des objets. Cette création est réalisée par la commande TCL *mkdir*. Chaque composant est d'une entité indépendante qui fonctionne indépendamment des autres entités. Les composants possèdent des ports par défaut pour qu'ils puissent communiquer entre eux. D'autres ports peuvent être créés pour un composant. Une connexion entre deux composants est réalisée par l'intermédiaire de deux ports dédiés, un dans chaque composant (voir la Figure VI.2). Cette connexion est matérialisée par la commande TCL *connect*. Il suffit de suivre un schéma qui indique l'interconnexion entre les différents types de composants que l'on veut utiliser. On obtient ainsi l'architecture du noeud.

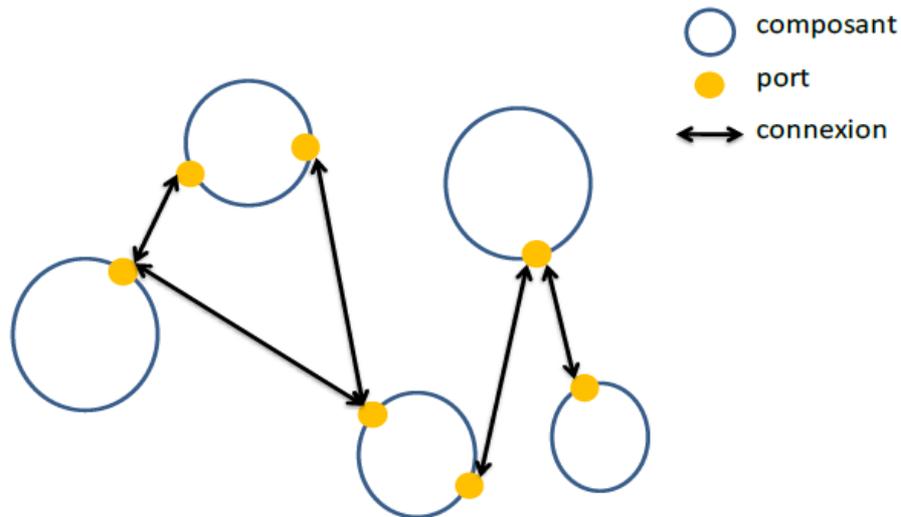


Figure VI.2 : Connexions entre les composants dans J-Sim

On distingue trois types de noeuds dans J-Sim (voir figure VI.3): *target*, *sink* et *sensor*. Les noeuds target ont pour fonction de générer des signaux (stimuli) qui peuvent être, par exemple, une secousse sismique, un bruit, etc. Le noeud sink est quant à lui le noeud cible, celui où les informations doivent arriver. Le reste du réseau est formé par les noeuds sensor qui captent le signal généré par target, forment les paquets contenant l'information de mesure et acheminent ces paquets jusqu'au noeud sink.

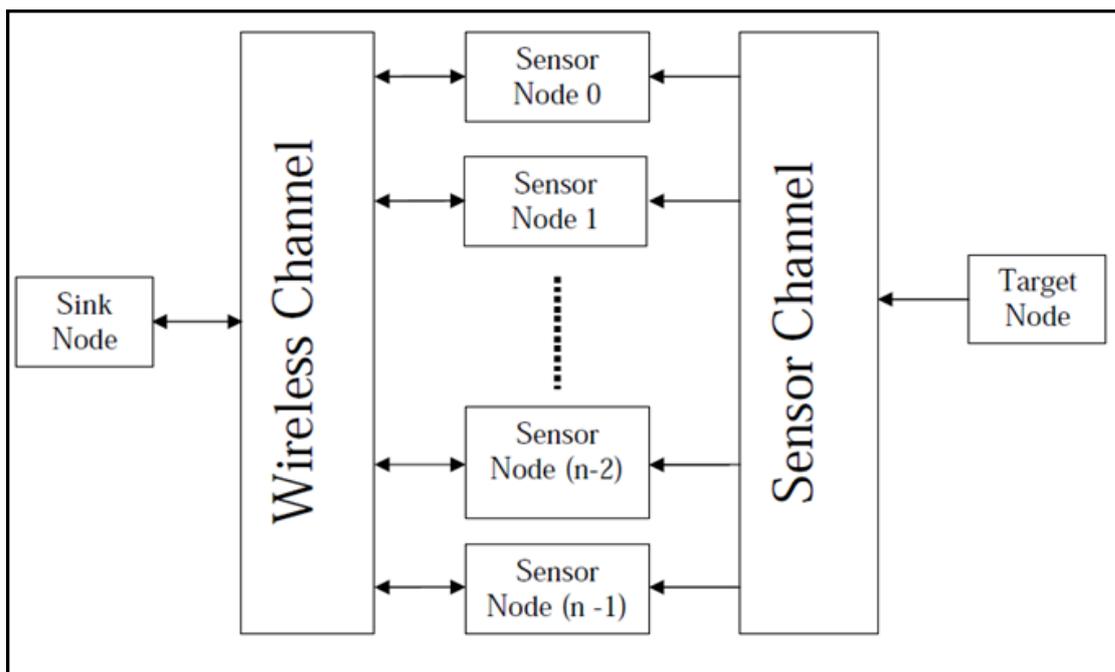


Figure VI.3 : Vue générale sur trois types de noeuds dans J-Sim

La Figure VI.4 suivante (partie en pointillé) montre l'architecture interne d'un noeud sensor dans J-Sim. On y distingue notamment les composants CPU et Radio qui définissent les modèles de la consommation énergétique du microcontrôleur et de l'antenne radio. Le composant CPU décrit en principe le coût de traitement des instructions. Le composant Radio décrit le coût de l'envoi et la réception des signaux et la mise en veille. Le composant Battery définit le modèle de la batterie d'un noeud. Ce composant calcule la consommation énergétique due au traitement des instructions, envois et réceptions des signaux en se basant sur les modèles du CPU et de Radio. Un programmeur peut facilement créer ses propres modèles (CPU, Radio, Battery) et les insérer dans un scénario de simulation afin de les tester.

La Figure VI.4 montre aussi que les composants des différentes couches d'un noeud sont séparés (Network layer, Mac Layer, Physical Layer). Ils communiquent entre eux via des ports. Les connexions (désignées par des flèches) entre les composants peuvent être unidirectionnelles ou bidirectionnelles. Une connexion unidirectionnelle d'un composant C1 vers un composant C2 signifie que les informations peuvent être envoyées dans une seule direction (de C1 à C2). D'autre part, une connexion bidirectionnelle signifie un échange d'information dans les deux directions. Le composant Wireless Channel est le composant commun pour tous les noeuds sensor du réseau. Il fait communiquer tous les noeuds sensor entre eux. Chaque noeud sensor du réseau doit avoir une connexion, réalisée par le programmeur, avec ce composant. Le cas échéant, le noeud ne peut pas communiquer avec les autres noeuds. Le composant Sensor Channel est responsable de la communication entre les noeuds target et les noeuds sensor. De même, chaque noeud (sensor ou target) doit avoir une connexion avec ce composant. Si, par exemple, un tel événement est créé par un noeud target, ce composant envoie l'information à tous les noeuds sensor qui entourent le target (la distribution des noeuds et leurs positions dans le champ de simulation sont définies dans le fichier TCL).

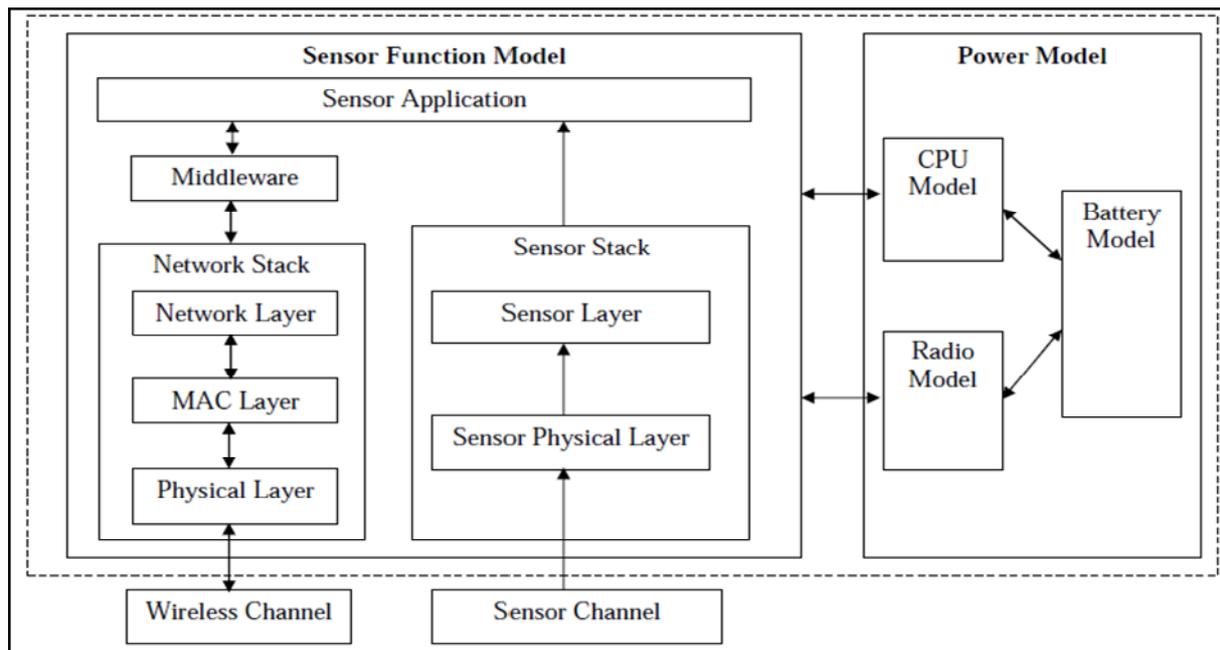


Figure VI.4 : Architecture interne d'un noeud sensor dans J-Sim

VI.3.1.2.2 Le langage utilisé pour définir un scénario de simulation

Bien que J-Sim soit écrit en Java, les scénarios de simulation ne sont pas décrits en Java. La combinaison des langages Java et TCL ne facilite pas cette tâche. Pour développer un grand projet, il peut devenir encombrant d'employer des commandes TCL/Java parce que les références des objets Java doivent être stockées dans des variables TCL afin d'y accéder.

VI.3.1.2.3 Installation de J-Sim

Le fait que J-Sim soit développé en java lui offre l'avantage d'être un simulateur multiplateforme. Cela veut dire qu'il s'installe sur toute plateforme (Système d'exploitation) disposant d'une machine virtuelle Java (JVM : Java Virtual Machine). Pour cela nous avons disposé de la machine virtuelle sur notre système d'exploitation Windows7 avant d'installer JSim. Le guide d'installation de J-Sim sous Windows et UNIX/Linux, est disponible sur le site officielle de J-Sim [59].

VI.3.1.2.4 Intégration du code source du protocole dans J-Sim

Le code source du protocole à simuler, qui doit être écrit en langage Java est copié dans l'un des sous-répertoires du répertoire `/src` de J-Sim, à condition de respecter le principe de développement imposé par le langage Java (notion de packages).

Pour faciliter le développement du code source, il est nécessaire de choisir l'un des environnements de développements pour le langage Java. Il en existe plusieurs mais les plus populaires sont Eclipse IDE [61] et NetBean IDE [62]. Nous avons choisi NetBeans IDE pour sa facilité à créer les projets qui nous a permis d'ailleurs d'installer J-Sim dans le répertoire */project* de NetBeans IDE.

VI.3.1.2.5 Exécution et simulation

Pour lancer la simulation, nous avons deux possibilités :

Charger le fichier de configuration de notre protocole via l'interface RUV, ou utiliser la commande « *java drcl.ruv.System -u nom_fichier_de_configuration* ».

Le nom du fichier de configuration est de format **.tcl*

VI.3.1.2.6 Affichage des résultats de la simulation

J-Sim intègre un outil d'affichage des résultats de la simulation, appelé « plot ». Les utilisateurs de J-Sim peuvent choisir d'autres outils d'affichage ou d'interprétation des résultats non fournis par J-Sim.

VI.3.2 Evaluation du protocole LEACHCO

Dans cette phase, nous allons évaluer le comportement du protocole en fonction des différents paramètres de configuration pour voir s'il répond bien à notre problématique.

VI.3.2.1 Paramètres de simulation

Les paramètres pouvant être utilisés pour simuler notre protocole sont nombreux. La plupart d'entre eux sont les paramètres de configuration du protocole J-Sim. Le tableau ci-dessous donne un certain nombre de paramètres que nous avons utilisés pour évaluer notre protocole.

Zone de déploiement	100x100 m
Nombre de noeuds capteurs	10, 20, 30,40
Nombre de noeuds puits	1
Nombre de Cluster	3
Données du domaine étudiées	Varié entre 0 et 100
Nombre de noeuds target	5
Sensibilité	1
Rayon de transmission wireless channel	100m
Rayon de transmission sensor channel	100m
Durée du agregTimer	3s
Temps de simulation	1000 s

Tableau VI.2 : Les paramètres de simulation.

VI.3.2.2 Métriques d'évaluation

Le choix des métriques de performance pour évaluer un protocole dépend de l'objectif de l'évaluation et des relations entre ces métriques.

Dans un protocole de contrôle de congestion par la technique d'agrégation des données, nous avons jugé important de définir une métrique appelée « *taux d'agrégation globale* » (**Tg**) pour mesurer la performance de notre protocole.

Le taux d'agrégation globale est défini comme étant le rapport entre le nombre de paquets de données générés par l'ensemble des noeuds sources du réseau sur le nombre de paquets de données reçus par le noeud puits.

Ces taux sont toujours supérieurs à un .Plus le taux d'agrégation globale augmente, plus l'algorithme d'agrégation des données est performant et donc plus on évite la congestion.

$$Tg = \frac{\text{Nombre de paquets de données générés par les noeuds sources}}{\text{Nombre des paquets de données reçus par le noeud puit}}$$

Nous allons aussi définir une autre métrique qui est la durée de vie de réseau. Cette durée représente le temps **dans lequel meure** le dernier nœud dans le réseau.

VI.3.2.3 Interprétation des résultats de la simulation

Nous allons étudier l'impact de la densité du réseau sur les performances des protocoles LEACH et LEACHCO.

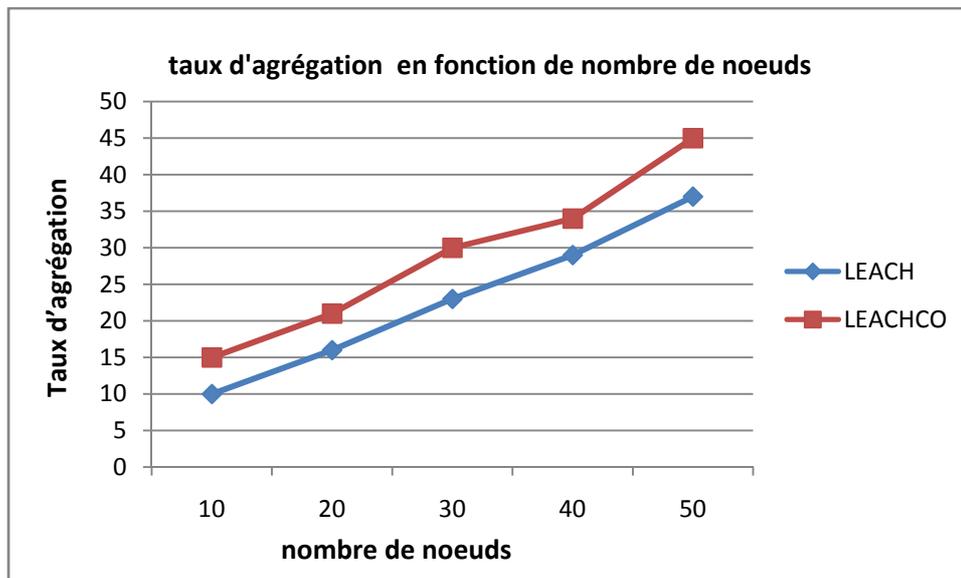


Figure VI.5 : Influence de la densité sur le taux d'agrégation

D'après les résultats obtenus nous observons que le taux d'agrégation global est proportionnel au nombre de noeuds du réseau. Le protocole proposé est donc plus performant avec un certain grand nombre de noeuds capteurs.

Avec un taux d'agrégation global égal à x , cela signifie qu'en moyenne x paquets produits par l'ensemble des noeuds capteurs du réseau ont été combinés en un seul paquet. Ce taux varie en fonction de quelques autres paramètres comme la corrélation entre les données du domaine étudié, la taille du buffer de données, etc. En réduisant le nombre de transmission (x augmente), on réduit en même temps le taux d'occupation du média sans fil qui peut être causé par la sur-écoute (overhead) et donc on réduit la congestion au niveau du canal sans fil.

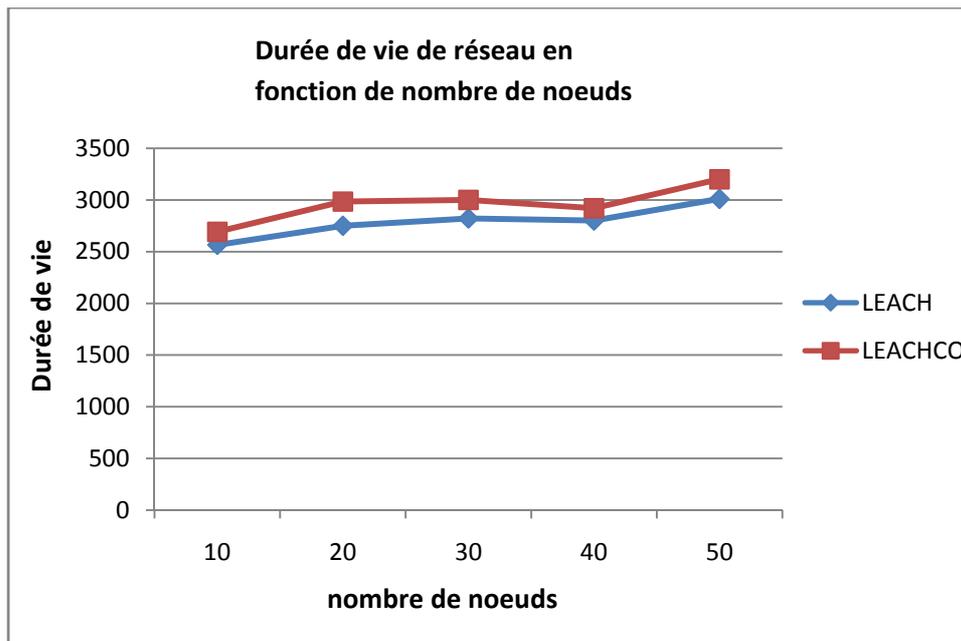


Figure VI.6 : Influence de la densité sur la durée de vie de réseau

Comme l'illustre le résultat du graphe VI.6, nous remarquons que la durée de vie de réseau est indépendante du nombre de nœuds déployés à cause de la topologie hiérarchique du protocole LEACH. En effet, quand la taille du réseau augmente, le nombre de CH augmente. Donc, les nouveaux nœuds vont être affectés aux nouveaux CH.

Par ailleurs, nous constatons que le protocole LEACHCO maximise la durée de vie de réseau par rapport à LEACH. Ceci est interprété par la consommation d'énergie par les CHs qui est inversement proportionnelle au taux x , puisque les modules radio des nœuds capteur vont passer la plus part de temps dans l'état d'attente, qui consomme moins d'énergie par rapport à l'état de réception et encore moins par rapport à l'état de transmission.

Ainsi, lorsqu'on réduit le taux de transmission, le taux d'agrégation augmente, ceci minimise la consommation énergétique.

VI.4 Conclusion

Dans ce chapitre, nous avons présenté la solution ainsi que l'environnement de notre simulation et les outils de programmation utilisés. Par la suite nous avons interprété les résultats en fonction des métriques d'évaluation.

L'étude comparative entre le protocole LEACH et LEACHCO a montré que ce dernier réalise une meilleur agrégation. Vu le degré de congestion pouvant être causée par les données redondantes, les résultats de simulation montre que ce protocole permet d'éviter cette congestion. D'où le protocole LEACHCO répond bien aux critères souhaités.

Conclusion générale

Les réseaux de capteurs constituent un axe de recherche très fertile et peuvent être appliqués dans plusieurs domaines différents. Cependant, il reste encore de nombreux problèmes à résoudre dans ce domaine afin de pouvoir les utiliser dans les conditions réelles.

Les RCSF vont sans doute dans les années à venir constituer un développement technologique majeur apportant des solutions aux différents problèmes dans plusieurs domaines d'applications liés à la santé, l'agronomie, la sécurité, etc.

L'un des problèmes qu'on peut rencontrer dans ce genre de réseau est la congestion causée par les données redondantes. Cette congestion est liée à la nature des réseaux de capteurs, principalement leur mode de déploiement. Quand un réseau est congestionné, il y a un gaspillage des ressources dont la bande passante et l'énergie qui est une ressource critique dans les réseaux de capteurs. Cette congestion est causée principalement par le nombre important de messages circulants dans le réseau, qui sont parfois inutiles.

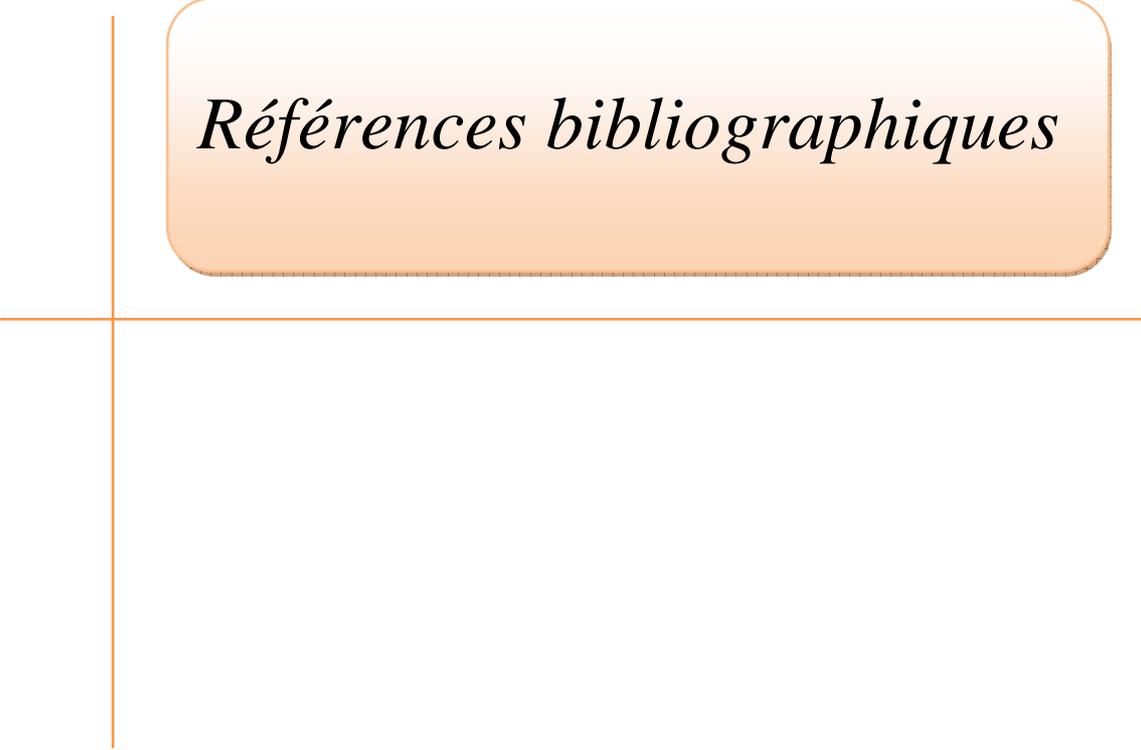
Il est donc important de mettre en place des techniques d'agrégation afin de réduire le nombre de paquets reçu par le nœud destinataire, et donc assurer le contrôle de congestion et le bon fonctionnement de réseau.

Dans ce projet, nous avons proposé une technique d'agrégation pour le contrôle de congestion dans les RCSF. L'agrégation de données intervient dans le transport des informations captées d'une manière généralement hiérarchique. Le paradigme de l'agrégation remplace les lectures des nœuds par une vue collaborative sur une zone spécifique. Cette collaboration implique que plusieurs nœuds participent, afin de calculer le résultat final de l'agrégation, qui permet aux nœuds agrégateurs de manipuler n'importe quelle valeur reçue dans sa région.

Nous avons décidé d'appliquer notre technique d'agrégation sur le protocole de routage LEACH vu de sa topologie hiérarchique. Le protocole résultant est nommé LEACHCO. Après avoir effectué plusieurs simulations et analysé les résultats obtenus, nous avons constaté que le protocole LEACHCO répond bien à nos besoins.

En effet nous aimerions comparer les performances de notre protocole avec celles de quelques protocoles de contrôle de congestion existant. Cela n'a pas été fait puisque non seulement il nous fallait avoir le code source de ces protocoles, mais aussi il fallait trouver un protocole qui utilise la technique d'agrégation des données.

Comme perspectives de notre travail, nous allons continuer à l'améliorer et surtout en prenant en compte d'autres métriques comme le taux de perte des paquets et le niveau de congestion au niveau de chaque noeud du réseau. Nous envisageons tous cela dans nos futurs travaux de recherche qu'ils soient d'ordre individuels, professionnels ou académiques.



Références bibliographiques

- [1] N.Badache, « *La mobilité dans les systèmes répartis* », Techniques et sciences informatique, Volume 17-n°8, pp 969-997, 1998.
- [2] L.Khelladi, N.Badache, « *Réseaux de capteurs : état de l'art* », Rapport de recherche, Université des sciences et de la technologie houari Boumediene. Février 2004.
- [3] N.D.Tripathi, « *Handoff in cellular systems* », IEEE Personal Communication, pp.26-37, December 1998.
- [4] O.derhab, « *Le problème d'exclusion mutuelle dans les réseaux mobiles Ad Hoc* », thèse de magistère, université des sciences et de la technologie houari Boumediene, 2003.
- [5] Scott Carson and Joseph Macker. « *Mobile ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Consideration* ». RFC 2051. 1999.
- [6] T.Lemlouma, « *Le Routage dans les Réseaux Mobiles ad hoc* », Mini Projet, Université des sciences et de la technologie houari Boumediene. Septembre 2000.
- [7] P.Lettierra et M.B.Srivastava, « *Advances in wireless terminals* », IEEE personal communications, 1999.
- [8] www.wikipedia.org
- [9] Holger Karl and Andreas Willig, « *Protocols and Architectures for Wireless Sensor Networks* », John Wiley & Sons 2005.
- [10] <http://www-bsac.eecs.berkeley.edu/archive/users/warneke-brett/SmartDust/>
- [11] Ian F, Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci. « *A Survey on Sensor Networks* », Georgia Institute of Technology, Pages 102-114, IEEE Communications Magazine. August 2002.
- [12] Kamal Beydoun, « *conception d'un protocole de routage hiérarchique pour les réseaux de capteurs* », thèse, UFR des sciences et techniques de l'université de Franche Compté, décembre 2009
- [13] <https://www.xbow.com/Products/productdetails.aspx?sid=158>.

- [14] Holger Karl and Andreas Willig, « *Protocols and Architectures for Wireless Sensor Networks* », John Wiley & Sons 2005.
- [15] M. Yasser ROMDHANE, « *Evaluation des performances des protocoles S-MAC et Directed Diffusion dans les réseaux de capteurs* », thèse, école supérieur des communications de Tunis, 2007
- [16] Jamal N. Al-Karaki Ahmed E. Kamal, « *Routing Techniques in Wireless Sensor Networks: A Survey*», Dept. of Electrical and Computer Engineering Iowa State University, Ames, Iowa
- [17] Abdelhakim HAMZI, « *Plateforme basée agents pour l'aide à la conception et la simulation des réseaux de capteurs sans fil* », Mémoire de magister, Institut National de formation en Informatique (I.N.I) Oued-smar Alger,2007
- [18] BENHAMIDA Fatima Zohra, « *La tolérance aux pannes dans les réseaux de capteurs sans fil* », Rapport du mini projet, Institut National de Formation en Informatique INI – Alger, 2007
- [19] Mounir Achir. « *Technologies basse consommation pour les réseaux Ad Hoc.* » Thèse pour obtenir le grade de Docteur de l'INPG. Institut National Polytechnique de Grenoble. juillet 2005.
- [20] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. I. Cayirci. «*A survey on sensor networks*», IEEE Communications Magazine, Vol. 40, No. 8, pp. 102-116, Août 2002.
- [21] Samra BOULFEKHAR, « *Approches de minimisation d'énergie dans les réseaux de capteurs* », Mémoire de Magistère, Université Abderahmane Mira de Béjaïa, 2006
- [22] Y. Wang, G. Attebury et B. Ramamurthy, « *A Survey of Security Issues in Wireless Sensor Networks* », 2005 .
- [23] Miloud BAGAA, « *La sécurité de l'agrégation dans les réseaux de capteurs sans fil* », Mémoire de Magister, Université des sciences et de la technologie Houari Boumediene, 2007

- [24] L. Khelladi et N. Badache. «*Les réseaux de capteurs : état de l'art*». Rapport de Recherche, Faculté Electronique et Informatique Bab Ezzouar-Algérie, Février 2004.
- [25] S. Zhuang and C. G. Cassandras. «*Optimal dynamic voltage scaling for wireless sensor networks with real-time constraints* », Proceedings of SPIE Conference on Intelligent Systems in Design and Manufacturing VI, pp. 8-16, Octobre 2005.
- [26] Amhammedi Ahmed, Targui Mohamed, « *Conception et realization d'un simulateur pour la surveillance d'un réseau de capteurs sans fil* », Projet de fin d'étude, Institut des science exactes , department d'informatique, centre universite de Bechar, juin 2007
- [27] BERRACHEDI Amel & DIARBAKIRLI Amina, « *Sécurisation du protocole de routage hiérarchique LEACH dans les réseaux de capteurs* », Projet de fin d'étude, Ecole nationale Supérieure d'Informatique Oued-Smar, Alger,2009
- [28] Mohammad Ilyas and Imad Mahgoub, «*Handbook of sensor networks: compact wireless and wired sensing systems*». CRC Press 2004.
- [29] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan. «*Energy-efficient communication protocol for wireless sensor networks*». Proceedings of the IEEE Hawaii International Conference on System Sciences, pp. 3005-3014, Janvier 2000.
- [30] K. Akkaya and M. Younis, «*A survey on routing protocols for wireless sensor networks*» Ad Hoc Networks, Vol. 3, No. 3, pp. 325-349, 2005.
- [31] Hani Hadjammam, Naouel Doufene. «*Routage dans les réseaux de capteur :optimisation du protocole Directed Diffusion* », Projet de fin d'étude, Institut National de formation en Informatique INI, Algérie, 2006
- [32] Prométhée Spathis, Serge Fdida, Yosra Barouni, « *Modèle générique pour le routage orienté contenu* ». Document scientifique, Laboratoire d'informatique de Paris 6, Université Pierre et Marie Curie, Mars 2008

[33] Mounir Achir, « *Technologies basse consommation pour les réseaux Ad Hoc* », Thèse, institut National Polytechnique de Grenoble, Juillet 2005.

[34] Isabelle Guérin Lassous, « *Autonomic Computing : Accès au médium radio* » Cours M2 Recherche RTS, RTS5, pages :43-95, Université de Lyon, 15 septembre 2007

[35] Sébastien Tixeuil, Ted Herman, « *Un algorithme TDMA réparti pour les réseaux de capteurs* », INRIA Projet Grand Large, Universités Iowa et Paris-Sud XI, 2004

[36] Preetha Radhakrishnan, « *Enhanced routing protocol for graceful degradation in wireless sensor networks during attacks* », Thèse d'ingénieur, Université de Madras, Chennai, décembre 2005

[37] Eric Lawrey, « *The suitability of OFDM as a modulation technique for wireless telecommunications, with a CDMA comparison* », Projet d'ingénieur, Université James Cook, Australie, 2001

[38] Mr Boubiche Djallel Eddine, « *protocole de routage pour les réseaux de capteurs sans fil* », mémoire de magister, Université de l'Hadj Lakhdar-Batna, 2008

[39] Wendi Beth Heinzelman, « *Application-Specific Protocol Architectures for Wireless Network* », IEEE Transaction on Wireless Communications, Massachusetts Institute of Technology, june 2000

[40] Sachin Mujumdar, « *Prioritized Geographical Routing In Sensor Networks* », Thèse, Université Vanderbilt, Mai 2004

[41] Aldar CHAN et Claude CASTELLUCCIA, « *On the security of concealed data aggregation* », dans le Colloque européen sur la recherche dans le domaine de la sécurité d'ordinateur (ESORICS 2007), Septembre 2007, Dresden, Allemagne.

[42] AGUILAR Andrs and BARROUX Mickael, « *Agrégation des données dans les réseaux de capteurs* », Projet SR04, Université de Technologie Compiègne, 2010

[43] Alexandre Brianceau Jérémie Christin, « *Sécurité de l'agrégation de données dans les réseaux de capteurs* », rapport de projet M1, Université de Versailles Saint-Quentin-en Yvelines

[44] Elena FASOLO, Michele ROSSI, Jörg WIDMER et Michele ZORZI, « *In-network Aggregation Techniques for Wireless Sensor Networks: A Survey* ».

[45] Kiran MARAIYA, Kamal KANT et Nitin GUPTA, « *Wireless Sensor Network: A Review on Data Aggregation* », revue internationale de la recherche scientifique et technologique, Vol. 2, N°4, Avril 2011.

[46] T. ARAMPATZIS , J. LYGEROS et S. MANESIS, « *A Survey Of Applications Of Wireless Sensors And Wireless Sensor Networks* », dans la conference méditerranéenne sur la commande et l'automatisation MED05, 2005, Nicosia, Cyprus.

[47] I. SOLIS et K. OBRACZKA, « *The Impact of Timing in Data Aggregation for Sensor Networks* » , dans IEEE ICC 2004, Juin 2004, Paris, France.

[48] A. MANJHI, S. NATH et P. B. GIBBONS, « *Tributaries and Deltas: Efficient and Robust Aggregation in Sensor Network Stream* », dans ACM SIGMOD 2005, Juin 2005, Baltimore, MD, US.

[49] S. NATH, P. B. GIBBONS, Z. R. ANDERSON et S. SESHAN, « *Synopsis Diffusion for Robust Aggregation in Sensor Networks* », dans ACM SenSys 2004, Novembre 2004, Baltimore, MD, US.

[50] S. MADDEN, M. J. FRANKLIN, J. M. HELLERSTEIN et W. HONG, « *TAG: a Tiny AGgregation Service for Ad-Hoc Sensor Networks* », dans OSDI 2002, Décembre 2002 Boston, MA, US.

[51] S. LINDSEY, C. RAGHAVENDRA et K. M. SIVALINGAM, « *Data Gathering Algorithms in Sensor Networks using Energy Metrics* », IEEE Trans. Parallel Distrib. Syst., vol. 13, N°. 9, pp. 924–935, Septembre 2002.

- [52] Y. XU, J. HEIDEMANN et D. ESTRIN, « *Geographic-Informed Energy Conservation for Ad Hoc Routing* », dans ACM/SIGMOBILE MobiCom 2001, Juillet 2001, Rome, Italie.
- [53] K. AKKAYA et M. YOUNIS, « *A Survey of Routing protocols in wireless Sensor networks* », revue Elsevier Ad Hoc Network, vol. 3, N° 3, pp. 325–349, Mai 2005.
- [54] Rekha CHAKRAVARTHI, C. GOMATHY, Suraj K. SEBASTIAN, K. PUSHPARAJ et Vinu Binto MON, «*A Survey on Congestion Control in Wireless Sensor Networks*», Revue internationale de l'informatique et de la communication, Vol. 1, N°1, pp. 161-164, Janvier-Juin 2010.
- [55] R.THEN MALAR « *Congestion Control in Wireless Sensor Networks Based Multi-Path Routing In Priority Rate Adjustment Technique*»
- [56] G. Bianchi «*Performance analysis of the IEEE 802.11 distributed coordination function*»,IEEE Journal on Selected Areas in Communications, March 2000.
- [57] C.Y. WAN, S. B. EISENMAN et A. T. CAMPBELL, « *CODA: Congestion Detection and Avoidance in Sensor Networks* » démarches de ACM SenSys, Novembre 2003.
- [58] C.-T. EE et R. BAJCSY, « *Congestion Control and Fairness for Many-to-One Routing in Sensor Networks* », démarches de ACM SenSys, November 2004.
- [59] <http://sites.google.com/site/jsimofficial/>
- [60] <http://www.tcl.tk/>.
- [61] <http://www.eclipse.org/>
- [62] <http://netbeans.org/>