MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

Université Saad Dahleb Blida -USDB -

Faculté des sciences

Département Informatique

Mémoire de fin d'étude pour l'obtention de diplôme de Master

Sur le thème

Etude des mécanismes de communication efficaces et peu couteux en énergie dans les réseaux de capteurs sans fil (RCsF)

Présenté par :

SAADA Oussama

BELKHIRI Med Amine

Promoteur :

Mr. Ramdani Mohamed

examinateur : Hadj issa

président de jury : Weld issa

Année universitaire : 2011/2012

Dédicace

Avec un immense plaisir que je dédie ce modeste travail :

A mes très chers parents qui m'ont épanouis de leur amour et leur soutient durant mon parcours du savoir et qui était à mes cotés pendant les moments difficiles.

A Baba el hadj et Baba Makhlouf qui ne cessent de suivre mes pas et mes efforts, a mes oncles Zohir, Tarek sans oublier ma tente et amie Fatima Zohra ainsi que Souad, Nora et Khadidja

A mes chers frères abderraouf, Mohamed Nour, abdelouadoud et ma chére sœur Khouloud.

A tous les membres de ma grande famille qui m'ont souhaités toujours la réussite et le bonheur

A tous mes amis que j'aime et qui m'aiment

Oussama

Dédicace

Avec un immense plaisir que je dédié ce modeste travaille :

A mes très chères parents qui m'ont offert leur amoure et leur soutien durant tout ma carrière et qui m'encouragé pendant mes études.

A mes chers frères.

A tous les membres de ma grande famille qui m'ont souhaites toujours le bonheur.

A tout mes amies que j'aime et qu'ils m'aiment.

Med amine

Remerciement

Nous remercions avant tout le bon dieu qui nous a aidés à réaliser ce modeste travail.

Nos remerciements les plus chaleureux empreints d'une reconnaissance sincères, vont à notre promoteur Mr RAMDANI pour nous avoir dirigés et conseillés tout au long de l'élaboration de ce mémoire, pour sa patience et son aide, qu'il trouve ici l'expression de notre gratitude.

Nous souhaiterons adresser nos remerciements les plus sincères aux personnes qui m'ont apporté leur aide et qui ont contribué à faire de nous des titulaires d'un Master en informatique pour avoir irrigué nos petites cervelles de connaissance et de savoir, depuis l'alphabet arrivant jusqu'a l'ensemble de l'encadrement pédagogique du département d'informatique pour aboutir à élaboration de ce mémoire.

Enfin, nous tenons à remercier de tout cœur tous ceux qui ont contribué de prés ou de loin à la réalisation de ce travail.

Table des matières

Liste des Figures :

Liste des Tableaux :

Liste de Graphes

Introduction générale

Aujourd'hui, les avancées récentes réalisées dans le domaine de la micro-électronique et des technologies de communication sans fil ont permis de créer de petits appareils autonomes, de taille minuscule, à un cout raisonnable. Ces dispositifs sont appelés capteurs ou micro-capteurs. Les capteurs, considérés comme de véritables systèmes embarqués, sont équipés d'une unité de capture, d'une unité de calcul, d'une unité de stockage et d'une radio pour effectuer des communications sans fil avec le monde extérieur. Ces différentes unités ont pour rôle la capture, le traitement, le stockage, la réception et l'émission de données.

Les nœuds capteurs s'organisent et collaborent entre eux pour former un réseau de capteurs sans fil (RcSF) capable de superviser son environnement de déploiement souvent hostile, inaccessible et sans aucune intervention humaine, ce qui peut se révéler très utile pour de nombreuses applications civiles, militaires, environnementales, médicales, agricoles, industrielles…etc.

La collaboration des nœuds capteurs d'un RcSF a pour objectif d'acheminer les données captées d'un nœud source vers une destination sur le réseau (souvent une ou plusieurs stations de base). La haute densité de ce type de réseaux favorise, d'une part, des communications en multi-sauts (sauts multiples) qui consomment moins de ressources, notamment énergétiques, que les communications classiques à un seul saut, et d'autre part, le partitionnement du réseau en plusieurs niveaux hiérarchiques connu sous le nom de routage hiérarchique. Des mécanismes sont conçus pour assurer l'organisation et la gestion du routage d'information et de palier aux limites des RcSF en termes d'énergie et de puissance de traitement.

Plusieurs solutions protocolaires sont présentées dans la littérature afin de faire face aux facteurs et contraintes qui influencent le routage dans les réseaux de capteurs sans fil tels que l'absence d'adressage global, données redondantes, ressources limitées, tolérance aux fautes, passage à l'échelle…etc. et plusieurs classifications ont été retenues ; la conception des protocoles de routage doit se faire selon : la topologie du réseau, l'objectif de déploiement, les paradigmes de communication, la méthode d'établissement de routes, l'initiateur de la communication…etc.

Une solution performante pour un routage efficace doit satisfaire deux critères essentiels : i) une consommation raisonnable d'énergie et ii) des mesures de sécurité adéquates. En effet, la prise en compte de la contrainte d'énergie est une condition nécessaire et non suffisante pour prolonger la durée de vie des nœuds capteurs et par conséquent du réseau entier. De même que l'absence d'une sécurité physique et la nature vulnérable des communications sans fil sont des caractéristiques qui augmentent le risque d'attaques, ainsi, toute solution qui ne comporte aucune mesure de sécurité permet à des agents malicieux de lancer différentes attaques pouvant toucher à l'intégrité et la confidentialité des données échangées, notamment lorsqu'il s'agit de transporter des informations secrètes, et nuire au fonctionnement global du système afin de l'empêcher d'accomplir son objectif de déploiement.

Contribution

Dans ce mémoire, nous avons présenté une étude détaillée sur la problématique du routage d'informations dans les réseaux de capteurs sans fil. On a commencé par définir un RcSF, ses caractéristiques et ses contraintes de conception, puis on s'est intéressé à la fonction du routage et plus particulièrement aux contraintes, à la sécurité des échanges et aux protocoles de routage dans les RcSF. Ensuite, un état de l'art est effectué pour recenser les différentes techniques de conservation d'énergie dans les réseaux de capteurs sans fil. Enfin, nous avons proposé un nouveau protocole de routage hiérarchique, sécurisé et économe en énergie, pour des réseaux de capteurs soumis aux attaques et aux contraintes énergétiques. Notre contribution est récapitulée dans les points suivants :

- Notre protocole de routage permet de conserver un maximum d'énergie dissipée dans le processus de reformation de clusters à chaque déclenchement d'un nouveau round.
- Il sécurise tous les types de liens (nœud-nœud, nœud-nœud chef, nœud chef-nœud puits) entre les entités du réseau, ce qui permet de garantir la confidentialité, l'intégrité et la disponibilité des données.
- Une solution implémentée par un code simple et portable ne nécessitant aucun matériel supplémentaire.

Organisation du mémoire

- Le premier chapitre présente un aperçu général sur les réseaux de capteurs sans fil.
- Le deuxième chapitre présente un état de l'art sur les protocoles de routage dans les RcSF. Plusieurs approches et contraintes sont discutées, des solutions et des métriques de performance sont présentées.
- Le troisième chapitre est entièrement consacré à la problématique de la consommation d'énergie dans les RcSF. Des facteurs de consommation et des techniques d'économie sont étudiées.
- Le quatrième chapitre présente notre contribution dans la problématique de sécurisation des communications et de conservation d'énergie dans les RcSF. On présente les principes et les objectifs de notre solution, son implémentation, ses résultats et ses performances en comparant notre protocole proposé au protocole LEACH. Nos résultats montrent l'efficacité de notre protocole en termes de sécurité et d'énergie par rapport à son vis-à-vis.

Chapitre 1 : Généralités sur les Réseaux de capteurs sans fils (RCSF)

Introduction

L'apparition des réseaux de capteurs sans fils date des années 80 où ils ont connu leurs premiers pas dans le domaine militaire afin de surveiller les zones de combat et rassembler les données distribuées ([JCD10], [KCI10]). De nos jours, l'utilisation des RCSF connait un très grand essor dans des domaines aussi variés que le secteur militaire, la médecine, l'environnement…etc.

Dans le but de connaitre le secret du succès et l'évolution rapide de cette nouvelle technologie qui rassemble à la fois les réseaux sans fils et les systèmes embarqués, nous allons présenter dans ce chapitre une vue générale sur les réseaux de capteurs sans fils, leurs caractéristiques, les contraintes qu'on doit prendre en considération lors de la conception d'un réseau de capteurs sans fils, les stratégies de communication , leurs domaines d'applications ainsi que d'autres notions fondamentales tel que l'énergie, le routage…etc.

1. Définition et architecture d'un RcSF

Un Réseau de capteurs sans fils est un ensemble de dispositifs appelés « nœuds capteurs » dont le nombre varie de quelques dizaines d'éléments à plusieurs milliers, connectés entre eux par une liaison sans fils. Ils sont déployés soit à un endroit précis, soit dispersés aléatoirement sur un champ de captage [YCL08]. Dans ces réseaux, chaque nœud est capable d'effectuer des mesures simples sur son environnement immédiat, comme la température, la vibration, la pression…etc., ou réagir, en cas de besoin, en envoyant l'information collectée à un ou plusieurs points de collecte appelés « station de base ». La station de base peut communiquer les données collectées à l'utilisateur final à travers un réseau de communication, éventuellement l'Internet ou par satellite. L'utilisateur peut à son tour utiliser la station de base comme passerelle, afin de transmettre ses requêtes au réseau.

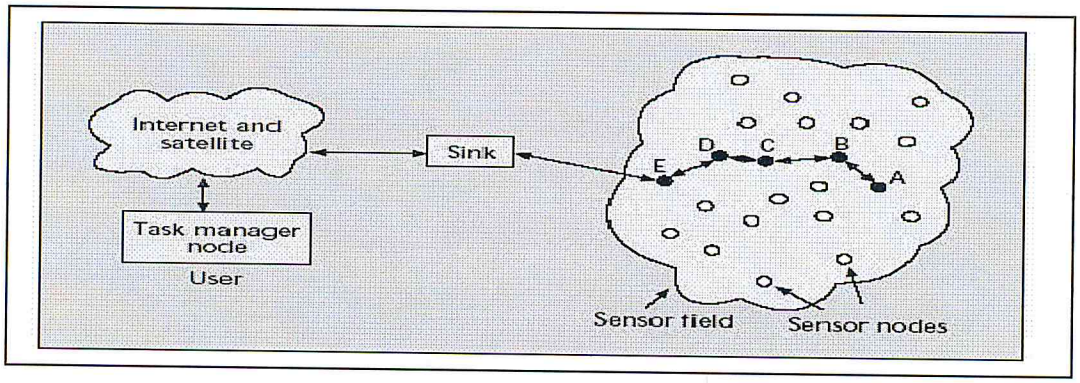


Figure 1: Architecture d'un RCSF [ACA11]

2. Anatomie d'un nœud capteur

Un capteur est un petit appareil autonome assurant trois fonctions principales : prélever, traiter et communiquer. Il est constitué de quatre unités principales comme l'illustre la figure suivante [SEB11] :

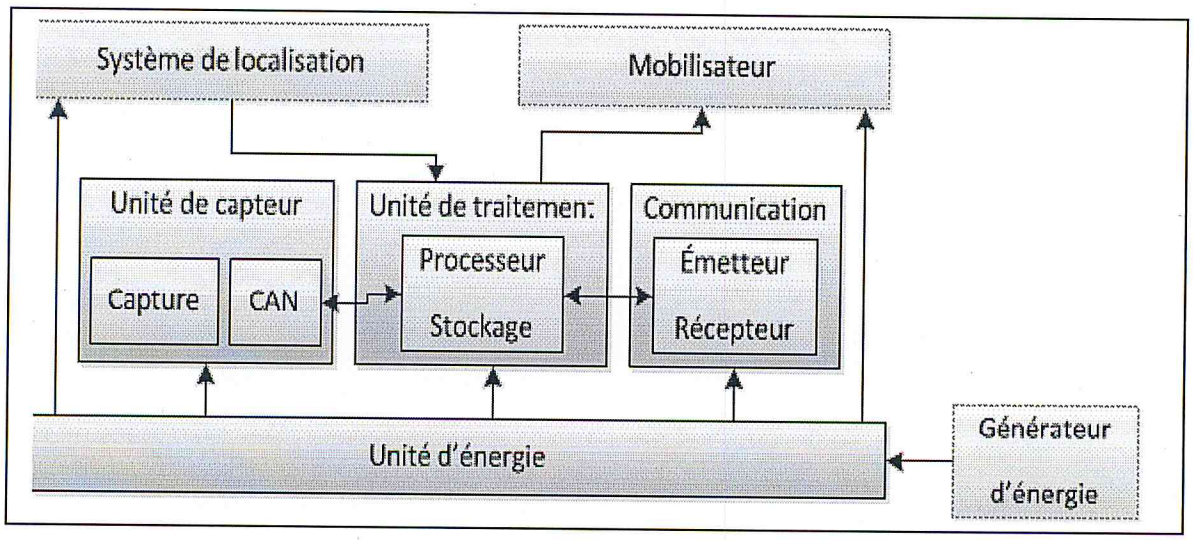


Figure 2 : Architecture d'un nœud capteur [SEB11]

- **Unité de captage « d'acquisition » :** Elle est composée d'un dispositif de capture physique [KCI10] qui mesure l'information de l'environnement : température, pression, image…etc. et un convertisseur analogique/numérique (CAN) qui convertisse les signaux produits lors de la capture afin de les transmettre à l'unité de traitement.

- **Unité de traitement :** Elle est composée d'un processeur avec une petite unité de stockage (RAM pour les données et une ROM pour les programmes et souvent une mémoire flash [ACA11]). Elle acquiert les informations en provenance de l'unité d'acquisition et les stocke en mémoire ou les envoie à l'unité de transmission.
- **Unité de communication :** Elle est responsable de toutes les transmissions et les émissions des données, elle est munie d'un module radio émetteur/récepteur qui permet d'échanger l'information.
- **Unité d'énergie :** Les capteurs sont équipés d'une batterie de taille minuscule (dés fois une pile). Cette batterie est responsable de l'alimentation de tous les composants du capteur. Le problème est que cette unité n'est ni rechargeable et souvent irremplaçable ce qui limite la durée de vie du capteur.

Outre ses quatre unités, le capteur peut contenir d'autres composants supplémentaires [FZB09] tels qu'un système de localisation (GPS), un générateur d'énergie, mobilisateur…etc. Ces composants sont relatifs aux domaines d'application de chaque capteur.

3. Domaines d'applications des RcSF

Les réseaux de capteurs deviennent de plus en plus répandus. Ils sont utilisés dans divers domaines et cela grâce aux évolutions techniques que connaissent les domaines de l'électronique et des télécommunications [DOR10], à la diminution de taille et du coût des capteurs, ainsi que l'élargissement des gammes de capteurs disponibles (mouvement, température, ...) et à l'évolution des supports de communication sans fil. En effet, les applications des réseaux de capteurs peuvent être militaires, médicales, environnementales, commerciales…etc.

3.1. Domaine militaire

Le domaine militaire a été le moteur initial pour le développement des réseaux de capteurs. L'idée était de déployer un réseau de capteurs invisible sur des champs de bataille ou des zones ennemies pour surveiller le mouvement des troupes. Le projet DSN (Distributed Sensor Network) [PRJ03] au DARPA (Defense Advanced Research Projects Agency) était l'un des premiers projets dans les années 80 ayant utilisé les réseaux de capteurs pour rassembler des données distribuées [ACA11].

Ainsi, les RCSF peuvent être utilisés dans la surveillance, la reconnaissance, la détection des mouvements de l'ennemi, le commandement, le contrôle, la communication…etc.

3.2. Domaine médical

Les RcSF peuvent être utilisés pour le monitoring des états de santé des patients [BBC08] (une surveillance permanente), faciliter le diagnostic de quelques maladies, détecter des comportements anormaux (chute d'un lit, choc…) chez les handicapés ou les personnes âgées…etc.

3.3. Domaine de l'environnement

Les réseaux de capteurs sans fil ont beaucoup d'applications dans ce domaine : détecter des incendies, surveiller des catastrophes naturelles, détecter les pollutions et suivre des changements au niveau des forêts, des océans, des activités sismiques…etc.

3.4. Domaine commercial

Les réseaux de capteurs sans fil possèdent plusieurs applications dans ce domaine, parmi lesquelles : la surveillance de l'état du matériel, la gestion des inventaires, le contrôle de qualité des produits, la construction des espaces d'achat intelligents, le contrôle des robots dans les environnements de fabrications automatiques, les jouets interactifs, le contrôle et l'automatisation des processus d'usinage, le diagnostic des machines, la détection et la surveillance des vols de voitures, le dépistage des véhicules, l'instrumentation des chambres blanches consacrées aux traitements des semi-conducteurs[K&N04] …etc.

3.5. Domaine agricole

Dans les champs agricoles, les capteurs peuvent être semés avec les graines. Ainsi, les zones sèches seront facilement identifiées et l'irrigation sera donc plus efficace. D'autre part, un RCSF peut offrir un support important qui permettra la gestion précise des ressources (l'eau, les engrais, etc.), le suivi des développements des maladies, la prédiction du moment adéquat de la récolte…etc.

3.6. Domaine domestique

Les capteurs peuvent être embarqués dans des appareils (fours micro-ondes, magnétoscopes, aspirateurs…) et interagir entre eux et avec un réseau externe via internet pour permettre à un utilisateur de contrôler les appareils domestiques localement ou à distance [ACA11].

4. Notions fondamentales

4.1. Notion de routage

La propagation et la délivrance des données dans un réseau de capteurs sans fils représentent la fonctionnalité la plus importante du réseau. Elle doit prendre en considération toutes les caractéristiques des capteurs afin d'assurer les meilleures performances du système: durée de vie, fiabilité, temps de réponse, ... etc. [YCL08].

Le problème qui se pose dans le routage pour les réseaux de capteurs est l'adaptation de la méthode d'acheminement utilisée avec le grand nombre de nœuds existant dans un environnement caractérisé par de changements de topologies, de modestes capacités de calcul, de sauvegarde et d'énergie [KBN09].

Beaucoup de travaux et des recherches se sont basées sur le routage dans les réseaux de capteur, puisqu'il permet de traiter plusieurs aspects sensibles dans ce type de réseau, Parmi ces aspects on peut citer la mobilité, la tolérance aux pannes, la fiabilité de l'acheminement des messages. Il est ainsi considéré comme un outil très efficace pour la minimisation de la consommation d'énergie afin de permettre la prolongation de la durée de vie du réseau.

4.2. Notion de sécurité

Les RcSF sont utilisés pour des applications vitales et cruciales [CLY08], ils sont souvent dispersés dans des environnements propices à des hostilités où un adversaire peut profiter des vulnérabilités du réseau telles que la vulnérabilité physique (elle permet a l'attaquant de changer en partie un capteur), la vulnérabilité logique (réside dans les programmes et les protocoles) avec l'utilisation des différentes techniques d'attaque : insertion de boucles infinie, brouillage radio…etc. [SEB11].

Le bon fonctionnement du réseau peut être compromis, c'est la raison pour laquelle on doit assurer la sécurité dans ce type de réseau. La sécurisation des RcSF représente un enjeu de taille et ce, notamment en ce qui concerne le bon acheminement des données vers la station de base.

4.3. Notion d'énergie

D'autant qu'un réseau de capteurs est constitué d'un ensemble de capteurs de petite taille qui ne dépasse pas quelques millimètres cube, déployés dans des zones hostiles sans contrôle ni surveillance, cela permet l'apparition de contraintes d'énergie car la batterie, de taille minuscule, est souvent irremplaçable et non rechargeable et son épuisement provoque le dysfonctionnement du capteur d'où une instabilité du réseau.

Pour cela, les recherches sont basées essentiellement sur cette contrainte majeure des RCSF afin de trouver des solutions efficaces et peu coûteuses en énergie, en mettant en œuvre des mécanismes et des techniques qui permettent la conservation d'énergie au niveau du capteur afin de maximiser la durée de vie du réseau.

4.4. Environnement de simulation TinyOs

TinyOS est un système exploitation open source développé par l'université américaine Berkley, il est spécialement dédié aux réseaux de capteurs sans fils puisqu'il offre à l'utilisateur une gestion très précise de la consommation d'énergie. Il devient le plus répandu des OS (Operating System) pour les réseaux de capteurs sans fil grâce a ses librairie (TinyOS comprend les protocoles réseaux, les services de distribution, les drivers pour capteurs et les outils d'acquisition de données ainsi que d'autre applications et modules sont développées par des groupe de recherches et des entreprise).

TinyOs travaille sur une base d'association de composants ce qui réduit significativement la taille du code [RHK11]. On peut distinguer quelques propriétés de ce système [YGB10] :

- Il est programmé en NesC (langage dérivé du C conçu pour minimiser l'utilisation de la mémoire des capteurs).
- Il n'est pas nécessaire d'avoir que quelques KOctets de mémoire libre.

- Gestion des événements, des tâches, des interruptions et la mise en veille de capteurs.

Une application écrite en TinyOs c'est l'ensemble de composants qui sont soit des concepts abstraits, soit des interfaces logicielles. L'implémentation de ces composants s'effectue en déclarant des tâches, des événements ou des commandes.

5. Caractéristiques des Réseaux de capteurs sans fils (RCSF)

5.1. Durée de vie limitée

Les nœuds capteurs ayant une batterie de taille minuscule et souvent déployés dans des zones hostiles rendent leur durée de vie dépendante de la durée de vie de leur batterie. Cette dernière est généralement non rechargeable et irremplaçable.

5.2. Ressources limitées

En plus de l'énergie, les capteurs ont une capacité de traitement et de mémoire très limitées à cause de leurs petites tailles.

5.3. Densité des nœuds

Le nombre de capteurs déployé dans un réseau de capteurs sans fil est souvent beaucoup plus élevé que dans un réseau traditionnel et qui peut atteindre des milliers, voire des millions, 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 nœud pour des fonctions de routage notamment ([B&D09],[FMD10]).

5.4. Topologie dynamique

La topologie dans les réseaux de capteurs sans fils est généralement instable donc elle peut changer au cours de temps par la mobilité des nœuds, la défaillance et l'ajout des nouveaux nœuds [DIE07].

5.5. Agrégation des données

La corrélation entre les nœuds déployés dans la même région ainsi que la collaboration entre eux permettent la détection de taches communes, ce qui provoque une redondance des données qui nécessite une agrégation pour réduire la largeur de la bande passante ainsi minimiser la consommation d'énergie ([SRB06],[J&A09]).

5.6. Bande passante limitée

Les nœuds capteurs ne peuvent pas supporter des débits très élevés à cause de leur puissance limitée, pour cela, ils utilisent un débit de quelques dizaines de Kbits/s afin de minimiser la consommation d'énergie ([KCI10], [SRB06]).

6. Contraintes de conception d'un RCSF

Un ensemble de facteurs qu'il faut prendre en considération avant la conception et la mise en œuvre d'un RCSF.

6.1. La tolérance aux pannes

C'est la capacité de maintenir les fonctionnalités du réseau sans interruption lorsqu'une erreur ou une défaillance [YCL08] (manque d'énergie, problème physique...etc.) intervient sur un ou plusieurs capteurs.

6.2. Facteur d'échelle (La scalabilité)

C'est la garantie du bon fonctionnement du réseau en déployant un grand nombre de nœuds capteurs variant de quelque centaines voire de milliers et peut atteindre quelques millions.

6.3. Les coûts de production

Souvent les réseaux de capteurs sont composés d'un nombre de nœuds très important [YCL08]. Donc il faut que le coût de fabrication de ces nœuds capteurs soit tel que le coût globale du réseau ne soit pas supérieur a celui d'un réseau classique afin de pouvoir justifier son intérêt [KHR09].

6.4. Les contraintes matérielles

C'est l'ensemble de conditions et de critères indispensables au capteur afin lui permettre son bon fonctionnement et accomplir les taches qui lui sont dédiées. On peut citer quelques critères : la taille du capteur, la consommation réduite de l'énergie, son adaptation à l'environnement [FZB09].

6.5. La topologie

La topologie d'un RCSF peut changer au cours du temps, elle doit s'adapter a toutes les situations, à savoir les pannes, la mobilité des nœuds, l'ajout des nouveaux nœuds capteurs…etc. Pour cela, il faut gérer avec précision la maintenance de la topologie, cette maintenance consiste en trois phases [YCL08] : i\ déploiement (la mise en place des capteurs : largage par avion, les placer manuellement…etc.), ii\ post-déploiement (le changement de la topologie à cause d'un changement de position, épuisement d'énergie d'où le dysfonctionnement d'un ou de plusieurs capteurs…etc.), iii\ redéploiement des nouveaux capteurs (c'est la réorganisation du réseau et le changement de sa topologie) [K&N04].

6.6. L'environnement de déploiement

Le réseau de capteur est souvent implanté dans des zones hostiles, critiques ou dures (sous haute pression au fond de l'océan, à l'intérieur des grandes machines, champ de bataille…) ce qui rend leur contrôle une tache presque impossible. Donc ils doivent pouvoir fonctionner d'une manière autonome sans surveillance dans les zones ou ils sont déployés.

6.7. Support de transmission

Dans les RCSF, les nœuds capteurs communiquent entre eux via une transmission sans fils. Le faible coût et la facilité d'installation sont deux facteurs principaux qui ont pu attirer une grosse partie d'attention de la communauté scientifique et industrielle sur les RCSF pour utiliser la communication à radio fréquence ainsi que sa basse bande de transmission qui convient avec la consommation réduite d'énergie.

6.8. La consommation d'énergie

Dans un réseau de capteur, chaque nœud capteur déployé consomme l'énergie quand il effectue ses taches habituelles telles que la capture, la communication...etc., on va élaborer en plus de détail la consommation et la dissipation d'énergie dans le chapitre 3. L'épuisement d'énergie d'un capteur conduit à sa mise hors fonction puisque le rechargement et même le remplacement reste très difficile et souvent impossible.

En effet 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 performance telle que la durée de transmission et le débit au détriment du facteur de consommation d'énergie [K&N04].

7. Les stratégies de communication dans les RcSF

La communication dans les réseaux de capteurs consiste à échanger les données entre les capteurs a partir des nœuds sources jusqu'à la station de base « ou le sink en anglais » en passant par plusieurs nœuds capteurs intermédiaires. Les stratégies de communication entre les capteurs dépendent de plusieurs paramètres tels que les applications et les objectifs du réseau à mettre en place. Elle peut être présentée par plusieurs manières [SEB11] :

- La démarche événementielle : la transmission des données dans cette stratégie dépend du déclenchement d'un événement (par exemple : la détection des feux dans les forêts) ou suite à une requête de la station de base (peut être utilisée pour contrôler et reconfigurer les nœuds capteurs par l'envoie des commandes au lieu des interrogations) [DIE07]. Dans cette démarche, les capteurs sont souvent en veille ce qui permettra d'économiser l'énergie.
- La démarche de contrôle continue : elle permet aux nœuds capteurs d'envoyer les données régulièrement d'une manière continue. La stratégie se base suivant un volume de trafic prédéterminé.
- La centralisation des données : le réseau est subdivisé en un ensemble de « clusters » où chaque cluster a un nœuds chef « cluster Head ». Cette stratégie permet d'intercepter les événements et de les envoyer aux clusters-Head qui collectent toutes les données des autres capteurs.
- La distribution des données : elle est utilisé par des nœuds situés dans une région bien déterminée qui collaborent ensemble afin d'avoir une meilleure estimation de l'évènement observé et d'éviter l'émission du même message vers la station de base ce qui contribue à consommer moins d'énergie. Donc elle permet de

localiser les capteurs voisins, d'effectuer des calculs, et de prendre des décisions collectivement. Les capteurs y sont souvent organisés en mailles.

Conclusion

Le succès des réseaux de capteurs sans fils dans tous les domaines est du à sa flexibilité, le déploiement rapide avec un coût réduit, la tolérance aux pannes et d'autres caractéristiques encourageantes. D'autre part, face a ces avantages, il existe des contraintes qui posent des problèmes aux utilisateurs comme la durée de vie du réseau dépendant de l'énergie des capteurs, la sécurité et les changements fréquents de la topologie…etc. ce qui exige a mettre en évidence ces contraintes pour aboutir à des solutions efficaces à ces problèmes.

Le routage dans les RCSF est l'un des axes les plus importants dans les recherches menées par la communauté scientifique puisqu'il touche à une partie intéressante dans les RCSF qui est la communication en utilisant plusieurs techniques et divers protocoles pour un but commun, qui est la minimisation de la consommation d'énergie afin de maximiser la durée de vie du réseau avec des résultats différents.

Nous allons exposer dans le chapitre suivant les différents protocoles de routage existant dans la littérature.

Chapitre 2 : Etat de l'art sur les protocoles de routages dans les RCSF

Introduction

La fonction d'acheminement d'informations entre la source et sa destination représente la fonctionnalité la plus importante dans un réseau informatique en général et dans les réseaux de capteurs sans fil en particulier.

Les caractéristiques des réseaux de capteurs sans fil comme la densité importante des nœuds, leurs autonomies énergétiques limitées, la topologie qu'ils forment, et le passage à l'échelle exigent des moyens et des techniques de routage spécifiques, différentes de celles déployés dans les réseaux classiques usuels.

La stratégie de routage dans les réseaux de capteurs sans fil doit prendre en considération toutes les caractéristiques et les limites des capteurs afin d'assurer les meilleures performances du système comme la fiabilité, le temps de réponse, et surtout la durée de vie. [WEB1]

La minimisation d'énergie consommée pendant la communication est principalement liée aux protocoles développés pour 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) [SRB06]. On définit alors le routage dans un réseau de capteurs comme étant le problème de recherche d'un chemin optimal garantissant un fort taux d'acheminement des messages et une consommation énergétique minimale [CHE09].

Ce chapitre présente l'ensemble des défis et les contraintes qu'il faut prendre en considération lors de la conception d'un protocole de routage pour les RCSF, ainsi qu'une étude sur les principaux protocoles comprenant une classification, comparaison et des métriques mesurant leur l'efficacité. On présente également les principaux algorithmes de routage en conservation d'énergie dans les RCSF avec les avantages et les inconvénients de chacun.

1. Contraintes de routage dans les réseaux de capteurs sans fil [WEB1-DIE07]

Le routage dans les réseaux de capteurs diffère de celui des réseaux Ad Hoc classiques. Les principaux facteurs et contraintes influençant le routage dans les réseaux de capteurs sans fil peuvent être résumés comme suit :

- **Absence d'adressage global :** Il n'est pas possible d'établir un système d'adressage global pour le grand nombre de nœuds du réseau.
- **Réseau à sources multiples / destination unique :** Les applications des réseaux de capteurs exigent l'écoulement de données mesurées depuis des sources multiples vers la destination finale « *Sink* ».
- **Données redondantes :** Les différents nœuds capteurs peuvent capter les mêmes données à proximité d'un phénomène (problème de la redondance des données).
- **Gestion des ressources :** Les nœuds capteurs, limités en ressources, exigent une gestion soigneuse de ces ressources. En raison de ces limites, de nouveaux protocoles de routage respectant ces contraintes ont été proposés dans les réseaux de capteurs.
- **Contraintes d'énergie [SRB06]:** L'optimisation de consommation se fait par le choix de la route à consommation énergétique minimale selon les critères suivante : i) L'énergie maximale disponible : le choix des routes efficaces en consommation d'énergie consiste à prendre celles qui contiennent les nœuds possédant le maximum d'énergie disponible. Cette quantité est égale à la somme des énergies résiduelles des nœuds appartenant à cette route. ii) L'énergie de transmission minimale : le choix se fait sur la route qui consomme le minimum d'énergie pour transmettre un paquet entre le nœud capteur et le nœud puits. iii) Le nombre de sauts minimum : la route sélectionnée est celle qui traverse un nombre minimum de nœuds intermédiaires pour atteindre le nœud puits. iv) Le nœud ayant le maximum des minimums des énergies disponibles : le choix se fait sur la route dans laquelle l'énergie disponible minimale est plus grande que toutes les autres énergies minimales disponibles des autres routes.
- **La tolérance aux fautes** [B&D09, YCL08]: Certains nœuds peuvent générer des erreurs ou ne plus jamais fonctionner à cause d'un manque d'énergie, un

problème physique ou une interférence. Ces problèmes ne doivent pas affecter le fonctionnement du reste du réseau, et c'est le principe de la tolérance aux fautes. La tolérance aux fautes est la capacité de maintenir les fonctionnalités du réseau sans interruptions, suite à une erreur intervenue sur un ou plusieurs capteurs.

2. Les attaques sur les RcSF

Les différents caractéristiques des réseaux de capteur sans fils telles que l'énergie limitée, faible capacité de traitement, la transmission par des ondes radio….etc les exposent à de nombreuses menaces.

Parmi les attaques qui peuvent menacer la sécurité d'un réseau de capteur sans fil, les attaques sur le routage de données profitant de la simplicité des protocoles de routage qui supposent, pour la plus part d'entre eux, un environnement « honnête » [CLY08].

D'autre part, un adversaire peut se baser sur les vulnérabilités des protocoles en utilisant des attaques sur deux niveaux : les données échangées entre les nœuds et la topologie du réseau crée par le protocole ([YCL08],[AOT07]).

Ces attaques peuvent être classées en deux catégories ([YCL08],[B&D09],[D&G08]):

2.1 Attaques actives : Le nœud malicieux émet un certain nombre de paquets pour apporter des modifications aux données circulant sur le réseau et perturber ainsi son bon fonctionnement. Parmi les attaques actives on cite :

- Attaque de « jamming » : Un nœud malicieux émet un signal d'une fréquence proche de celle utilisée dans le réseau afin de brouiller la communication et saturer le médium pour que les nœuds ne puissent pas communiquer entre eux sur ce médium.
- Attaque du trou de la base « sink hole » : Dans ce type de menaces, le nœud malicieux va s'attaquer directement à l'information qui circule de la source vers la base, il consiste d'attirer vers lui le plus de chemins possibles en offrant aux nœuds des routes optimales et en utilisant une connexion plus puissante. En conséquence,

les nœuds vont s'adresser à ce nœud malicieux, considéré comme le plus approprié pour transmettre les données à la station de base, ce qui lui permet de contrôler et de récupérer toutes les informations échangées. Le principe détaillé est comme suit :

Dans ce type d'attaques, un nœud malicieux va s'attaquer directement à l'information circulée par la base, qui est le plus souvent le point qui recueille le plus d'informations sur le réseau [D&G08]. A cet effet, le nœud malicieux va proposer aux autres nœuds du réseau le chemin le plus rapide et l'optimal pour atteindre la station du base en utilisant une connexion plus puissante. L'ensemble des nœuds récepteurs de la proposition du nœud malicieux vont naïvement s'adresser à ce nœud pour router leurs informations à la station de base. Donc il devient comme un nœud puits et peut contrôler et récupérer toutes les informations qui transitent de ces nœuds vers la base, et par la suite, il peut injecter des informations erronées pour perturber le fonctionnement du réseau.

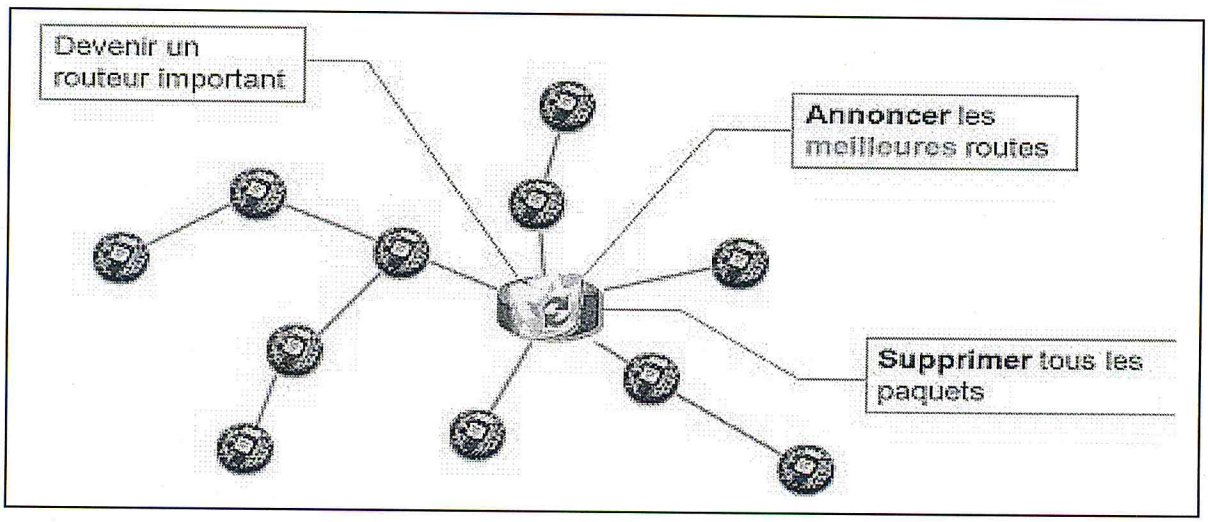


Figure 3 : Attaque Sink Hole [YCL08]

- Attaque de trou de ver « attaque Wormhole » : Le but est de faire tromper les nœuds voisins sur la distance qui les séparent. Elle nécessite l'insertion d'au moins deux nœuds malicieux dont l'un des nœuds reçoit des paquets dans un point du réseau puis les encapsules vers un autre nœud malicieux, soit en multi sauts qui consiste à cacher les nœuds se trouvant entre les deux nœuds malicieux pour

apparaitre comme le plus court chemin, soit dans la communication direct d'où les routes passant par les attaquants sont plus rapide, car il sont à un seul saut.

- Routing table poisoning : Dans cette attaque le nœud malicieux émet un nombre important de fausses informations pour remplir les tables de routage des nœuds, et comme ces tables possèdent des tailles limitées, cela va engendrer un débordement et les tables ne contiendront que de fausses routes.
- Sybil attack : L'attaquant peut altérer les systèmes qui se basent sur l'instauration d'une redondance de chemin pour assurer la fiabilité du routage, en « endossant » plusieurs identités, ce qui permet de créer plusieurs routes passant par le nœud malicieux qui ne sont en réalité qu'un seul chemin.
- Hello flooding : Les protocoles de découvertes sur les réseaux ad hoc utilisent des messages Hello pour s'insérer dans un réseau et pour découvrir ses nœuds voisins, dans ce type d'attaque l'attaquant va utiliser ce mécanisme pour saturer le réseau et consommer l'énergie des nœuds qui le compose. Principe détaillé :

Le principe de cette attaque est d'injecter des messages inutiles et complètement erronées afin de tromper les capteurs de l'emplacement de leurs voisins puisque la topologie des réseaux de capteurs n'est pas déterminée au préalable, donc les capteurs utilisent des messages de type « HELLO » pour découvrir leurs voisins et établir la topologie du réseau.

Ce type de message peut être utilisé par des nœuds malicieux en les envoyés régulièrement avec une forte puissance pour saturer le réseau.

En plus, si un attaquant avec une connexion puissante lui permet d'envoyer des messages « HELLO » a un grand nombre des nœuds distants, afin qu'il croient qu'il fait partie de leurs voisins, donc il vont essayer de lui répondre malgré la distance qui ne permet pas d'atteindre ce nœud malicieux, a force de tenter de répondre a ces messages il vont petit à petit consommer l'intégralité de leur énergie, par conséquent, ces nœud peuvent choisir des routes qui contiennent des voisins imaginaires provoquant ainsi un envoi important de paquets a cet attaquant([D&G08] [B&D09]).

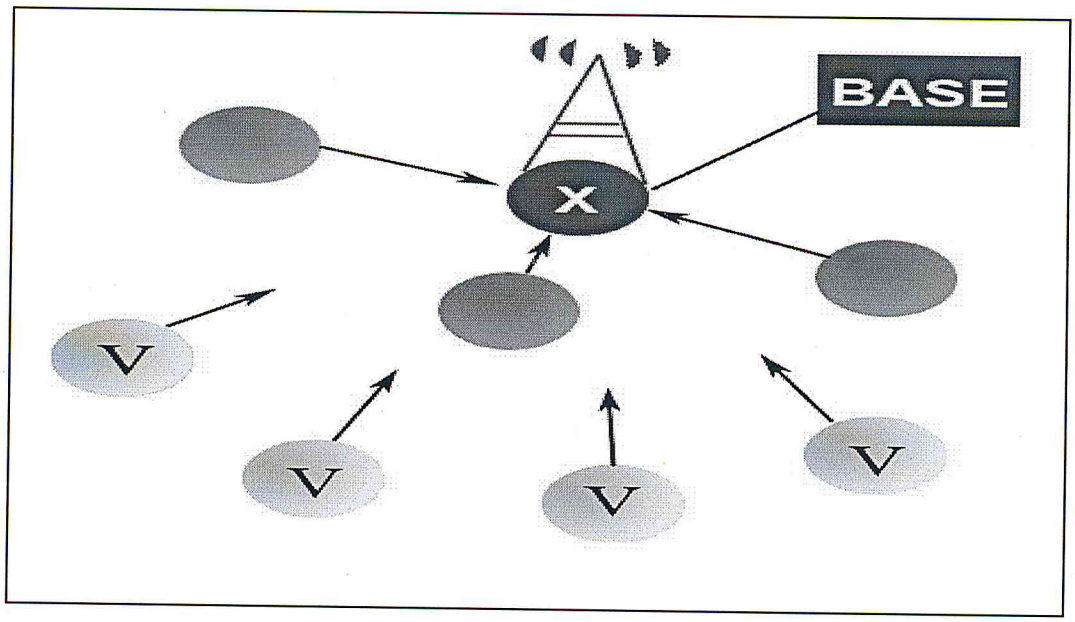


Figure 4: Attaque Hellow flooding

2.2. Les attaques passives

Le nœud malicieux n'utilise pas son énergie puisque ses attaques ne nécessitent aucune émission de paquets, il consiste par ailleurs à obtenir un accès non autorisé à une ressource sans modifier les données ou perturber le fonctionnement du réseau donc il cherche juste à écouter et collecter les informations sur ce fonctionnement qui peuvent, par la suite, être utilisées pour créer une attaque active.

- Attack of cooperation ou selective Forwarding : L'attaquant devient un routeur important dans le réseau dans un premier temps, puis en abandonnant son rôle de routeur, les performances du système seront gravement dégradées.
- Eaversdropping : Dans l'attaque Eaversdropping, le nœud peut analyser toutes les communications de ces voisins car le média sans fil est un média ouvert, cela peut divulguer des informations très importantes comme la localisation des nœuds importants.

3. Solutions de sécurité

Pour contrer les attaques qui menacent les réseaux de capteurs sans fil, les recherches tentent de proposer des solutions simples, prenant en considération les

spécificités des réseaux de capteurs sans fil, afin de permettre une protection efficace couplée à une consommation raisonnable d'énergie.

Parmi les solutions proposées, on distingue les solutions dédiées pour sécuriser le routage [YCL08]:

- La prévention contre les attaques actives en utilisant la cryptographie (le chiffrement, la signature digitale, fonction de hachage…) afin de protéger la communication qui sert à la construction des routes. De plus, les mécanismes d'authentification et de contrôle empêchent les attaquants d'injecter, de modifier et de supprimer une information utile dans le routage. Nous décrivons en particulier les fonctions de hachage et l'authentification pour pouvoir les inclure dans notre solution présentée au chapitre 04.

La fonction du hachage

C'est un mécanisme qui assure l'intégrité de l'information, elle sert à calculer une empreinte de taille fixe avec une fonction a sens unique à partir d'une information du taille arbitraire, la fonction du hachage doit assurer ces conditions [B&D09] :

- Il est facile de calculer l'empreinte a partir du contenu du message
- Il est difficile de trouver le contenu de message a partir de l'empreinte (sens unique)
- Il est difficile de trouver une même empreinte pour deux messages différents pour assurer l'inexistence des collisions.

Le code d'authentification de message MAC

C'est un system de cryptographie qui permet de vérifier l'authenticité de l'origine des informations et leur intégrité en même temps, ce mécanisme fait partie des fonctions du hachage à clés symétriques qui doit vérifier les conditions suivants [Y&B] :

- Etant donné une clé k et un message M, Hk (M) est facile à calculer.
- Etant donné zéro ou plusieurs paires (Mj, Hk(Mj)), il est très difficile de calculer n'importe quelle paire (M,Hk(M)) pour n'importe quel message.

Le mécanisme qui sert de garantir l'authenticité de l'origine se base sur le partage d'une clé public entre l'émetteur et le récepteur.

Cette clé sera utiliser par l'émetteur pour calculer un MAC sur le message à envoyer, ce MAC (code de hachage) est preuve l'authenticité qui accompagnera le message.

Le récepteur utilisera la même clé secrète pour calculer le MAC de nouveau sur le message reçu, le MAC nouvellement calculé sera comparé au MAC accompagnant le message si les deux sont égales alors le message et l'origine sont authentique, sinon le message du l'origine n'est pas authentique.

- La tolérance : En utilisant des mécanismes de tolérance de défaillance des nœuds à cause d'attaques ou de pannes, le routage multi chemin est l'une des solutions typiques de la tolérance aux défaillances.
- La détection de comportements suspects : Consiste à déceler des comportements qui témoignent d'une attaque passive (manque de coopération, refus de relai de paquets…).

4. Les principaux protocoles de routage dans les RCSF

La figure suivante résume les principaux protocoles de routage :

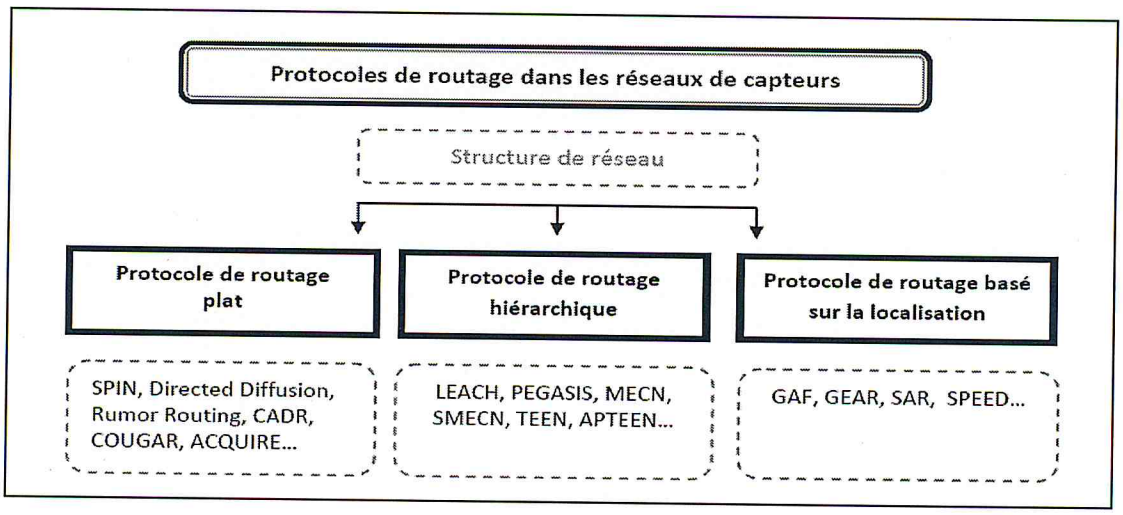


Figure 5 : Les principaux protocoles de routage [YSY10]

On peut classer les principaux protocoles de routage, selon la structure du réseau, sur trois catégories : i) protocoles à plat (Flat based routing) ; ii) protocoles hiérarchiques (Hierarchic based routing/Clusturing based routing) ; et iii) protocoles basés sur la localisation géographique (Location based routing).

4.1 Protocole de routage plat : Dans une topologie dite plate, tous les nœuds possèdent le même rôle [DIE07] et sont semblables en termes d'autonomie et de ressources, communiquant entre eux directement sans faire appel à des nœuds intermédiaires [B&D09].

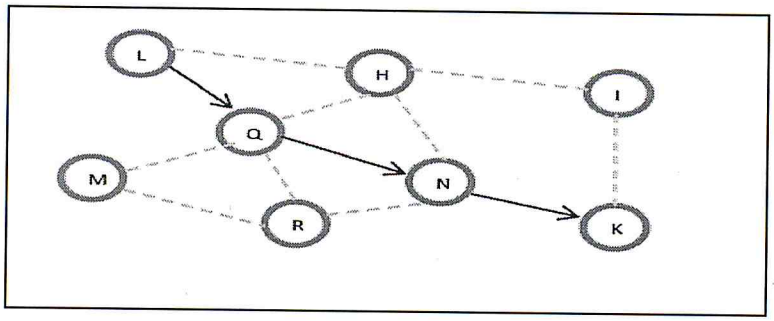


Figure 6 : Routage plat [DIE07]

- **Exemples :** SPIN, diffusion dirigée, routage par rumeur, GBR.
- **Avantages** : Les topologies plates sont caractérisées par la simplicité des algorithmes exécutés par les protocoles de routage. Et comme les RCSF souffrent des changements brusques de la topologie, une organisation plate offre la possibilité de construire différents chemins entre la source vers le nœud puits. [SRB06]
- **Inconvénients** : Les réseaux plats présentent des inconvénients comme l'exemple défini par le problème de *Hotspot*. En effet, tous les nœuds sont homogènes et il n'y a que le nœud puits qui est chargé de la récolte d'informations. Ces dernières passent forcément par les nœuds qui entourent le nœud puits et qui seront de ce fait beaucoup sollicités et rapidement épuisés. Par ailleurs, les nœuds doivent accomplir plusieurs tâches en même temps ce qui pourrait rapidement épuiser leurs ressources énergétiques et dégrader ainsi les performances du réseau. [SRB06]

Quand le nombre de nœuds déployés augmente d'une manière significative, le routage devient de plus en plus ardu et en conséquence il ne serait pas possible d'attribuer des identificateurs globaux à chaque nœud. Cette absence d'identification globale dans un environnement de déploiement aléatoire de nœuds capteurs fait la difficulté de sélectionner un ensemble spécifique de nœuds capteurs à interroger. Par conséquent, les données sont généralement transmises de chaque nœud capteurs avec une redondance importante. Cette réflexion a conduit au routage data-centric [M&K10, YSY10 , GCB10] qui est différent du routage traditionnel où les routes sont créées entre les nœuds adressables et gérées par la couche réseau.

Le destinataire envoi des requêtes à certaines régions et attend la réception des données provenant des nœuds capteurs situés sur les régions ciblées. Comme les données sont exprimées par des requêtes, le nommage est nécessaire pour préciser les propriétés des données. L'exemple d'une approche data-centric est donné par la figure 2.3, où les données provenant des deux sources sont agrégées au nœud N et la donnée combinée (1+2) est envoyée de N vers la destination K.

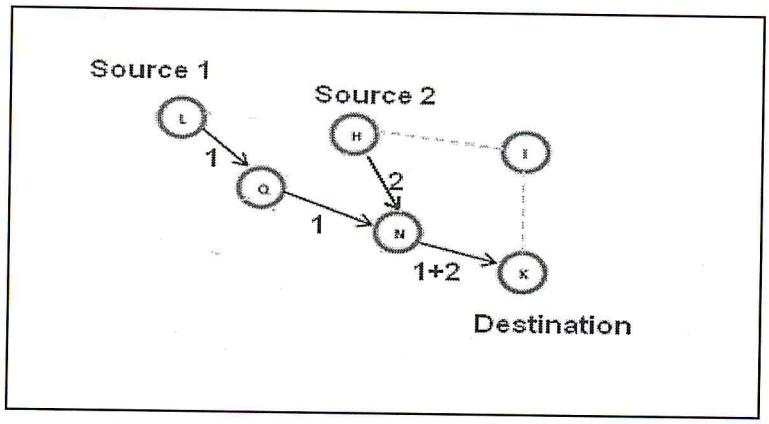


Figure 7 : Le routage data-centric [YSY10]

4.1.1. Le protocole de routage « SPIN »

SPIN (Sensor Protocols for Information via Negotiation) [YCL08] est le premier protocole data centric conçu pour les réseaux de capteurs sans fil. Il présente de nombreuses similitudes par rapport au protocole « la diffusion dirigée ». Son efficacité est dans la réduction des données redondantes et dans la conservation d'énergie [SRB06].

SPIN repose sur un modèle de négociation afin de propager l'information dans un réseau de capteurs sans fil. Son objectif est de pallier aux problèmes de l'inondation. Les tâches confiées aux capteurs sont de recueillir le point de vue complet de l'environnement sous la forme de données et de renforcer la structure du réseau avec la garantie d'une tolérance aux fautes. A la réception d'une nouvelle information, la station informe tous ses voisins de la disponibilité de l'information par des paquets ADV, et les stations intéressées peuvent ensuite envoyer une requête pour obtenir l'information par des paquets REQ [YCL08, SRB06].

La consommation d'énergie durant les calculs et les communications doit être contrôlée afin de prolonger la durée de vie des capteurs au sein du réseau. Lorsque le nœud s'aperçoit que son énergie est passée sous un certain seuil, il change son mode de fonctionnement et ne répond à aucun message ADV [YSY10 , YCL08].

4.1.2. La diffusion dirigée [YSY10 , SRB06, YCL08]

L'idée de base vise à répandre des données aux nœuds capteurs destinataires en employant une appellation combinée « attribut-valeur » définie comme l'ensemble d'intérêts pour les données requises. La raison principale derrière l'utilisation d'un tel système est de se débarrasser des opérations inutiles de routage, de la couche réseau, afin d'économiser l'énergie.

Pour créer une requête, un nœud est défini par une liste de paires « attribut-valeur » comportant, par exemple le nom des objets, l'intervalle, la durée, la zone géographique, etc. Un paquet est diffusé par ce nœud vers la destination à travers ses voisins qui forment un réseau de connexion. Chaque nœud qui reçoit les paquets peut les stocker pour une utilisation ultérieure. Les paquets stockés sont ensuite utilisés pour comparer les données reçues. La requête contient aussi plusieurs champs de gradient. Un gradient est un lien réponse avec un voisin dont le paquet a été reçu et qui est caractérisé par le débit, la durée et la date d'expiration de données. Ainsi, en utilisant les intérêts et les gradients, les routes sont établies entre la destination et les sources. Plusieurs routes peuvent être établies de telle sorte que l'une d'elle est choisie par renforcement. La destination renvoie le message d'intérêt initial à travers la route choisie. Un intervalle plus petit renforce donc le nœud source sur ce chemin pour envoyer des données plus fréquemment.

4.1.3. Le protocole de routage par rumeur [YSY10]

Le routage par rumeur est une autre variante de la diffusion dirigée. Il est principalement prévu pour les contextes de réseaux dans lesquels les critères géographiques de routage ne sont pas applicables. L'idée clé consiste à trouver les routes pour les requêtes vers les nœuds qui ont observé un événement particulier, plutôt que d'inonder tout le réseau pour récupérer des informations sur les événements survenus. Afin de diffuser un événement sur le réseau, l'algorithme de routage par rumeur emploie des paquets appelés « agents ». Quand un nœud détecte un événement, il ajoute cet événement à sa table locale, appelée table d'événements et génère un agent. Cet agent parcourt le réseau afin de propager des informations sur des événements locaux pour les nœuds distants. Quand un nœud génère une requête pour un événement, les nœuds qui connaissent le chemin répondent à la requête en vérifiant leur table événement. Par conséquent, il n'est pas nécessaire d'inonder tout le réseau, ce qui réduit le coût de communication. D'autre part, ce routage n'utilise qu'un seul chemin entre la source et la destination contrairement à la diffusion dirigée où les données peuvent être acheminées par des routes multiples.

Les études ont démontré que le routage par rumeur réalise une économie significative d'énergie par rapport à l'inondation par évènements et peut également assurer la maintenance du routage. Cependant, ce type de routage n'est efficace que si le nombre d'évènements est petit. Pour un grand nombre d'évènements, le coût de maintien des agents et des tables d'évènements dans chaque nœud ne peut pas être compensé s'il n'y a pas assez d'intérêt sur ces évènements de la part d'un destinataire.

4.2. Protocole de routage hiérarchique [SRB06, YSY10]

Suite à l'augmentation de la scalabilité du système, les topologies hiérarchiques ont été introduites en divisant les nœuds en plusieurs niveaux de responsabilité. L'une des méthodes les plus employées est le clustering où le réseau est partitionné en groupes appelés "clusters". Un cluster est constitué d'un chef (cluster-head) et de ses membres.

L'objectif du routage hiérarchique est de maintenir efficacement la consommation d'énergie de nœuds capteurs en les impliquant dans la communication multi-hop au sein d'un cluster et en effectuant l'agrégation et la fusion des données afin de

diminuer le nombre de messages transmis à la destination. La formation de clusters est généralement fondée sur la réserve d'énergie des capteurs et sur les capteurs qui sont à proximité du cluster-head (voir figure 2.4).

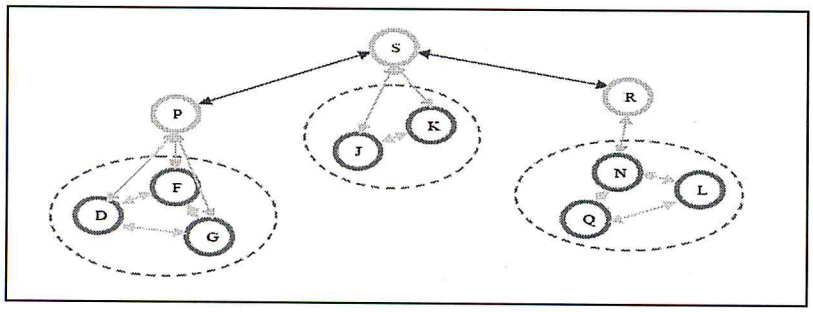


Figure 8 : routage hiérarchique [DIE07]

- **Exemples :** LEACH, PEGASIS, hierarchical-PEGASIS, TEEN et APTEEN.
- **Avantages** : L'agrégation de données est l'avantage du routage hiérarchique puisque les données du cluster entier, généralement similaires et présentent beaucoup de parties communes, peuvent être combinées par le cluster-head et envoyées vers la destination. [SRB06]
- **Inconvénients** : Points chauds (Hotspots), les nœuds élus comme des cluster-heads consomment plus d'énergie que les autres nœuds dans le réseau [SRB06].

4.2.1. Le protocole de routage «LEACH » [SRB06, B&D09]

Le protocole LEACH est considéré comme le premier protocole hiérarchique basé sur l'approche des groupes, il est aussi l'un des algorithmes de routage hiérarchiques les plus populaires pour les RCSF, il combine l'efficacité en consommation d'énergie et la qualité de l'accès au média, il se base sur le découpage en groupe qui va permettre l'utilisation de l'agrégation de données afin de prolonger la duré de vie de réseau.

Le principe de ce protocole consiste à former des groupes a base de l'amplitude du signal, et utiliser des têtes des groupes pour transmettre tous les messages des membres du groupe vers le nœud Puits, l'élection des chefs de groupes se fait d'une manière aléatoire en se basant sur une fonction de probabilité P_i. La figure suivant illustre l'organisation de la communication dans ce protocole.

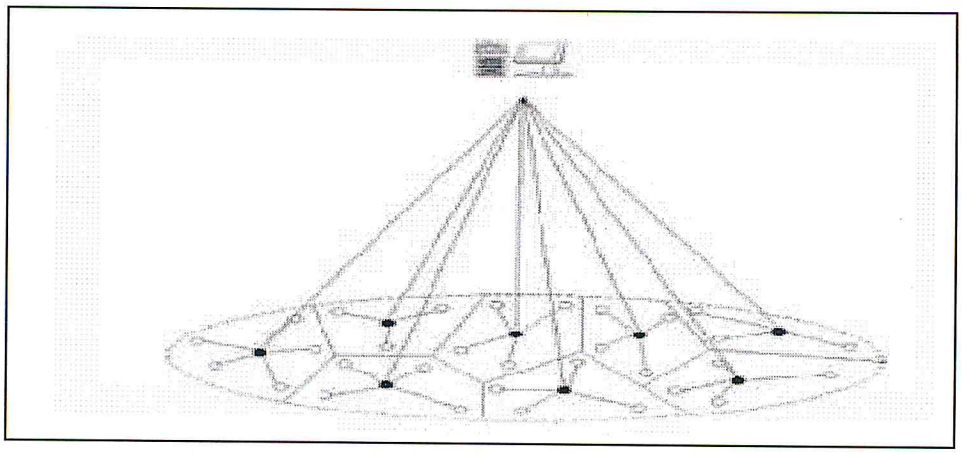


Figure 9 : l'organisation de la communication dans LEACH [B&D09]

Le fonctionnement du protocole LEACH

L'algorithme se déroule en « round » qui ont un même intervalle du temps déterminée au préalable, chaque round est constitue de deux phase [B&D09] :

1) La phase d'initialisation

Cette phase est constituée de trois sous phases : d'annonce, d'organisation des groupes et l'ordonnancement.

La phase d'initialisation commence par la phase d'annonce où le nœud Puits informe les nœuds capteurs sur le déclenchement du nouveau round et sur la valeur de probabilité P_i qui désigne l'élection du chef du cluster en fonction du nombre désiré et déterminé au préalable selon le nombre de capteurs du réseau (généralement, le nombre de CHs varie entre 5% et 15%).

Chaque nœud reçoit l'annonce du nouveau round et génère un nombre aléatoire entre le 0 et 1 et vérifie s'il est inferieur à P_i, si oui, le nœud deviendra CH et il doit informer les autres nœuds non-CH dans la phase d'organisation des groupes afin de joindre son cluster. Les nœuds doivent choisir d'appartenir au CH ayant un signal plus fort pour assurer une communication avec un minimum d'énergie.

Après la formation des groupes, chaque CH doit coordonner les transmissions des données au sein de son groupe. Donc il crée un ordonnanceur TDMA dans la phase d'ordonnancement et assigne à chaque nœud membre un slot de temps et un code de

propagation CDMA (généré aléatoirement) afin de minimiser les interférences durant l'envoie des données pendant les slots attribués.

2) La phase de transmission

Cette phase est plus longue que la précédente, elle consiste à ce que chaque nœud envoie les données captées durant son slot en utilisant son code CDMA, ces données sont ensuite agrégées par les CHs qui les fusionnent, les compressent et les envoient au nœud Puits.

Avantages de protocole LEACH

- Protocole auto-organisateur basé sur le groupement adaptatif d'où il est complètement distribué d'une manière que les nœuds prennent leurs décisions de façon autonome
- Rotation des rôles de chefs de groupes
- Faible énergie pour l'accès au média déterminée par l'utilisation de communication sur de petites distances.
- L'agrégation de données effectuées par les CHs afin de réduire la quantité que doivent transmettre au nœud Puits.

Inconvénients

- On pourra ne pas avoir des CH durant un round quelconque si tous les nombres générés aléatoirement sont supérieur à P_i.
- Les nœuds les plus éloignés du CH meurent plus 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 du nœud.
- Il est possible que les CH puissent être concentrés dans une partie du réseau, donc on peut avoir des nœuds isolés.
- L'absence d'un mécanisme de sécurité dans les communications.

4.2.2. Les protocoles de routage «PEGASIS & Hierarchical-PEGASIS»

Power-Efficient GAthering in Sensor Information Systems (PEGASIS) est une version améliorée du protocole LEACH. PEGASIS forme des chaînes plutôt que des clusters de nœuds capteurs afin que chaque nœud transmette et reçoive uniquement des données d'un voisin. Un seul nœud est sélectionné à partir de cette chaîne pour transmettre à la station de base. Le concept de PEGASIS est qu'il utilise tous les nœuds pour transmettre ou recevoir des données avec ses plus proches voisins. Il déplace les données reçues de nœud à nœud, puis les données seront agrégées jusqu'à ce qu'elles atteignent la station de base. Donc, chaque nœud du réseau est tour à tour un chef de file de la chaîne, ainsi que responsable pour transmettre l'ensemble des données recueillies et fusionnées par la chaîne de nœuds au niveau de la station de base [YSY10].

4.2.3. Les protocoles de routage «TEEN et APTEEN» [GCB10, YSY10]

Threshold sensitive Energy Efficient sensor Network protocol (TEEN) et Adaptive Threshold sensitive Energy Efficient sensor Network protocol (APTEEN). Dans les deux protocoles, le facteur clé est la valeur de l'attribut mesuré. La caractéristique supplémentaire d'APTEEN est la capacité de changer la périodicité et les paramètres de TEEN en fonction des besoins des utilisateurs et des applications.

TEEN est conçu pour être sensible à des changements soudains des attributs. L'architecture du réseau de capteurs est basée sur un groupement hiérarchique où les nœuds forment des clusters et ce processus va se répéter jusqu'à ce que la station de base soit atteinte.

APTEEN est une extension de TEEN qui fait à la fois la collection des captures périodique de données et qui réagit aux événements critiques. Quand la station de base forme des clusters, les clusters head diffusent les attributs, les valeurs des seuils, ainsi que le calendrier de transmission à tous les nœuds. Le cluster-head effectue également l'agrégation de données afin d'économiser l'énergie.

4.3. Les protocoles de routage basés sur la localisation [SRB06, B&D09, DIE07]

Les protocoles de routage basés sur la localisation utilisent les informations d'emplacement pour guider la découverte de routage et la transmission des données.

Ils permettent la transmission directionnelle de l'information en évitant l'inondation d'informations dans l'ensemble du réseau.

Tous les nœuds possèdent un moyen de localisation, soit un système natif comme le

GPS (*Global Position System*), soit un système logiciel comme un protocole de localisation.

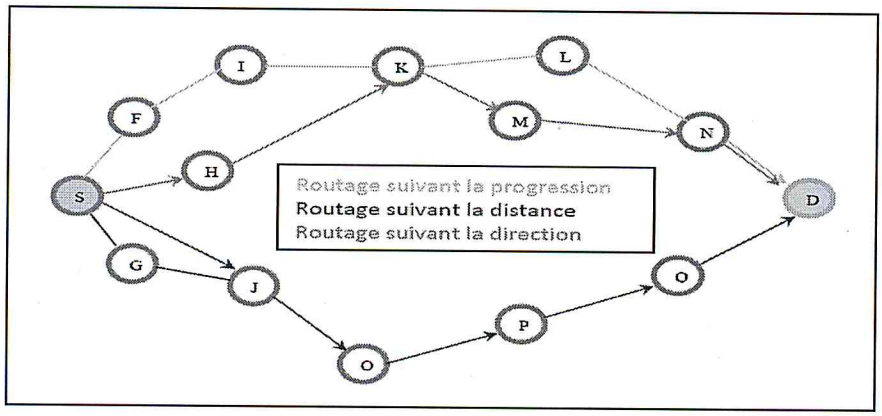


Figure 10 : routage basé sur la localisation [DIE07]

- Routage suivant la progression : La progression d'un nœud correspond à sa projection sur l'axe (SD). Le nœud dont la projection est la plus proche de la destination est choisi comme un prochain nœud.

- Routage suivant la distance : Le nœud le plus proche de la destination D en termes de distance est choisi comme prochain nœud.

- Routage suivant la direction : Le nœud voisin le plus proche de la droite (SD) en direction de D est choisi.

- **Example :** MECN, GAF, GEAR.
- **Avantages** [SRB06, YSY10]**:** Le coût de contrôle de l'algorithme est réduit et le routage est optimisé. De plus, avec la topologie réseau basée sur des informations de localisation des nœuds, la gestion du réseau devient simple. De plus, la région de sensation est connue et la requête peut être donc dirigée uniquement vers cette région, ce qui éliminera le nombre de transmission de manière significative.
- **Inconvénients** [SRB06, YSY10]**:** Chaque nœud doit connaître les emplacements des autres nœuds.

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.

4.3.1. Le protocole de routage « MECN » [SRB06, YSY10]

Minimum Energy Communication Network (MECN) est un protocole de routage qui cherche à établir et à entretenir une énergie minimale pour les réseaux de capteurs sans fil en utilisant des GPS de faible puissance. MECN utilise une station de base comme destination de l'information, ce qui est toujours le cas pour les réseaux de capteurs. MECN identifie une région de relais pour chaque nœud. La région de relais se compose de nœuds dans une zone périphérique où la transmission à travers ces nœuds est plus économe en énergie que la transmission directe. L'idée principale de MECN est de trouver un sous-réseau qui a moins de nœuds et qui nécessite moins d'énergie pour la transmission entre deux nœuds quelconques.

Ceci est effectué en utilisant une recherche localisée pour chaque nœud en prenant en considération sa région de relais.

4.3.2. Le protocole de routage « GAF » [SRB06]

GAF (Geographic Adaptive Fidelity) est un protocole de routage basé sur la localisation, efficace en consommation d'énergie. Ce protocole a été initialement destiné aux réseaux ad hoc, néanmoins il peut être appliqué aux réseaux de capteurs. Il consiste à former des grilles virtuelles de la zone concernée en partitionnant cette zone où les nœuds sont déployés en de petites zones telles que, pour deux grilles adjacentes Gx et Gy, tous les nœuds de Gx peuvent communiquer avec tous les nœuds de Gy. Ainsi, ce système de partitionnement GAF assure la fidélité du routage car il existe au moins un chemin entre un nœud et la station de base.GAF peut augmenter considérablement la durée de vie du réseau. En effet, un seul nœud dans chaque grille reste à l'état actif en faisant passer les autres nœuds de la grille à l'état de sommeil pour une certaine période de temps tout en assurant la fidélité du routage.

4.3.3 Le protocole de routage «GEAR » [SRB06, YSY10]

Le protocole GEAR (Geographic and Energy Aware Routing) consiste à utiliser l'information géographique lors de la diffusion des requêtes aux régions cibles car les requêtes contiennent souvent des données géographiques. L'idée est de restreindre le

nombre de données dans la diffusion dirigée en prenant en considération uniquement une certaine région, plutôt que d'envoyer les données à l'ensemble du réseau. Si le paquet atteint la région, il peut être répondu dans cette région soit par une diffusion géographique récursive, soit par une inondation limitée (des diffusions locales).

Avec le protocole GEAR, chaque nœud maintient le coût pour atteindre la destination en passant par ses voisins (next-hop). Ce coût est divisé en deux parties : un coût estimé et un coût d'apprentissage. Le coût estimé est une combinaison de l'énergie résiduelle et de la distance jusqu'à destination. Le coût d'apprentissage est un raffinement du coût estimé qu'un nœud dépense pour le routage autour des trous dans le réseau. Un trou se forme quand un nœud n'a pas de voisin proche par lequel il peut atteindre la région cible. Ainsi, si une station n'a presque plus de batteries, l'algorithme cherchera à l'éviter. S'il n'y a pas de trous, le coût estimé est égal au coût d'apprentissage. Le coût d'apprentissage se propage d'un saut à chaque fois qu'un paquet atteint la destination.

5. Classification et comparaison des protocoles de routages dans les RCSF

Les protocoles de routage pour les RCSF ont été largement étudiés, et différentes études ont été publiées. Ces protocoles peuvent être classifiés suivant plusieurs critères [B&D09]:

5.1. Classification selon le type de protocole

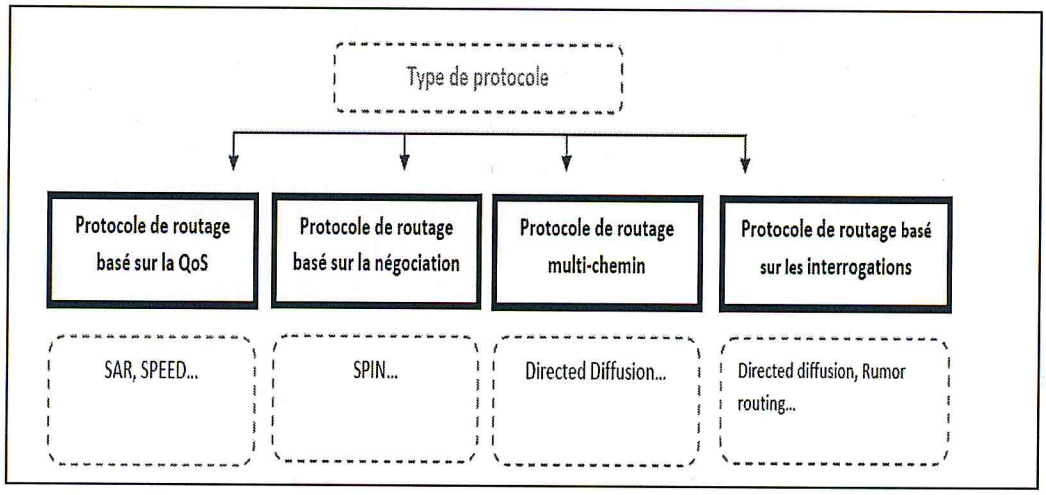


Figure 11 : Classification selon le Type de protocole [DIE07].

5.1.1. Protocole de routage multi-chemin: Dans ce type de routage, les protocoles se basent sur l'adoption de plus qu'un chemin menant vers la destination,

et ce, pour avoir des chemins de secours si jamais le chemin principal serait rompu. [DIE07]

5.1.2. Protocole de routage basé sur la négociation: Dans le cas de détection de même phénomène, les nœuds capteurs inondent le réseau par les mêmes paquets de données. Ce problème de redondance peut être résolu en employant des protocoles de routage basés sur la négociation. En effet, avant de transmettre, les nœuds capteurs négocient entre eux leurs données en échangeant des paquets de signalisation spéciaux, appelés meta-DATA. Ces paquets permettent de vérifier si les nœuds voisins disposent des mêmes données à transmettre. Cette procédure élimine la redondance des données et assure que seules les informations utiles seront transmises. [SRB06, DIE07]

5.1.3. Protocole de routage basé sur les interrogations: [DIE07, YCL08] La collecte des informations sur l'état de l'environnement dans un RCSF dépend de l'application et de l'importance de la donnée. De ce fait, les RCSF peuvent être catégorisés comme time-driven, event-driven ou continous.

- **Application time-driven** : Un réseau time-driven est approprié pour des applications nécessitant un prélèvement périodique des données. Par exemple cela est utile dans des applications de monitoring (feu, météo) afin d'établir des rapports périodiques.
- **Application event-driven** : Dans des applications temps réel, les capteurs doivent réagir immédiatement aux changements soudains des valeurs captées. Un prélèvement périodique des données est inadapté pour ce type de scénarios. Pour cela, le protocole doit être réactif et doit donner des réponses rapides en l'occurrence d'un certain nombre d'évènements.
- **Application a modèle continuous :** Dans ce type d'applications, les nœuds capteurs envoient les informations d'une manière continue au nœud « *sink* » suivant un volume de trafic prédéterminé.

5.1.4. Protocole de routage basé sur la QoS: Dans les protocoles de routage basés sur la Qualité de service, le réseau doit s'équilibrer entre la consommation d'énergie et la qualité de données échangées. Ces protocoles de routage tendent à satisfaire certaines métriques pendant la transmission des données vers la destination finale. Parmi ces métriques, nous citons : i) le délai de bout en bout (les applications

qui ont des exigences temps-réel), ii) la gigue, iii) PDR (*Paquet Delivery Ratio*), iv) bande passante... [SRB06, CLASS].

5.2. Classification selon les paradigmes de communication [DIE07, B&D09, YCL08]

Le paradigme de communication est déterminé par les contraintes sous lesquelles les nœuds du réseau sont interrogés. Dans les RCSF, il peut être classé comme étant centré-nœuds, centré-données ou basés sur la localisation.

5.2.1. Centré-nœuds (Node centric)

Ce paradigme est employé dans les réseaux conventionnels où il est important de connaître les nœuds communicants (à l'aide d'adresses IP). Cependant, ce paradigme ne reflète pas la vision des RCSF quant à leurs applications où la donnée transmise est plus importante que l'émetteur. Néanmoins, le paradigme centré-nœuds n'est pas totalement écarté, car certaines applications nécessitent une interrogation individuelle des nœuds.

5.2.2. Centré-données (Data centric)

Ce modèle est utilisé dans les réseaux où il n'existe pas un système d'identification global, et cela correspond presque à toutes les applications des RCSF. Effectivement, il n'est généralement pas possible d'attribuer les identificateurs globaux (comme les adresses IP) pour chaque nœud à cause du nombre élevé de capteurs déployés. Ainsi, la donnée est plus importante que le nœud lui même. Ce manque d'identification, avec le déploiement aléatoire des nœuds, font qu'il est difficile de sélectionner un ensemble de nœuds pour être interrogé. Par conséquent, les données sont généralement transmises de chaque nœud avec un taux important de redondances à l'intérieur de la région de déploiement. Ainsi, des protocoles de routage centrés-données ont été proposés pour être en mesure de sélectionner un bon ensemble de nœuds demandés, sans l'utilisation d'identifiants globaux. Ils visent également à utiliser l'agrégation de données pour éviter le gaspillage d'énergie dû aux redondances de données.

5.2.3. Basé-localisation (Position centric)

Ce paradigme est utilisé dans les applications où il est plus intéressant d'interroger le système en se basant sur la localisation des nœuds et où on peut tirer profit des

positions des nœuds pour prendre des décisions qui minimisent le nombre de messages transmis pendant le routage. Ces positions représentent le moyen principal d'adressage et de routage, ce dernier s'effectue grâce à des techniques géométriques afin d'acheminer l'information d'une zone géographique à une autre.

5.3. Classification selon la topologie du réseau

La topologie détermine l'organisation logique adaptée par les protocoles de routage afin d'exécuter les différentes opérations de découverte de routes et de transmission de données. Elle joue un rôle significatif dans le fonctionnement d'un protocole. Dans les RCSF la topologie peut être hiérarchique ou plate.

5.4. Classification selon la méthode d'établissement de routes [MLC10, SRB06, B&D09]

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 : protocoles proactifs, réactifs ou hybrides.

5.4.1. Protocoles proactifs

Les protocoles de routage proactifs établissent au préalable les meilleurs chemins pour chaque nœud vers toutes les destinations possibles. Ces protocoles maintiennent en permanence une vision globale de l'état du réseau grâce à une gestion périodique des tables de routage et l'échange des messages de contrôle. Ceci induit un contrôle excessif d'autant plus qu'ils sont particulièrement utilisés pour les réseaux denses. De plus, ils présentent un autre inconvénient dû à la sauvegarde des routes même si elles ne sont pas utilisées.

5.4.2. Protocoles réactifs

Les protocoles de routage réactifs (dit aussi les protocoles de routage à la demande) maintiennent des routes à la demande. Lorsque le réseau a besoin d'une route, une procédure de découverte est lancée. Une fois la route n'est plus utilisée, elle sera immédiatement détruite, ce qui permet une conservation d'énergie. Cependant, le routage à la demande induit une lenteur à cause de la durée nécessaire à la recherche des chemins, ce qui peut dégrader les performances des applications interactives (notamment les applications temps réel).

5.4.3. Protocoles hybrides

Les protocoles hybrides combinant entre les deux techniques précédentes utilisent des méthodes proactives pour l'établissement de la route dans le proche voisinage (par exemple le voisinage à deux où trois sauts) et des méthodes réactives au delà de la zone de voisinage.

5.5. Classification selon l'initiateur de communication [SRB06]

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

5.5.1. 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 évènements.

5.5.2. 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. Le principe est de propager les requêtes à tous les nœuds d'une région topologique et attendre la réception des données du nœud capteur concerné dans cette région.

Remarque : Plusieurs protocoles peuvent appartenir au plus d'une catégorie. À titre d'exemple, PEGASIS est un protocole hiérarchique, proactif, avec qualité de service et de communication lancée par la source.

Le 1er tableau représente une classification de quelques protocoles de routage dans les réseaux de capteurs sans fil (figure 2.7).

Le 2eme tableau représente une comparaison de quelques protocoles de routage dans les réseaux de capteurs sans fil (figure 2.8).

	Structure du réseau	Etablissement de la route	Initiateur de communication	QdS	Multi-chemins	Basé sur la négotiation
SPIN	A plat	réactif	source	non	oui	oui
Direct Diffusion	A plat	hybride	destination	oui	oui	oui
Rumor Routing	A plat	réactif	source	non	non	non
GBR	A plat	réactif	source	non	non	non
LEACH	hiérarchique	proactif	source	non	non	non
TEEN	hiérarchique	hybride	destination	oui	non	non
PEGASIS	hiérarchique	proactif	source	oui	non	non
GAF	LG	proactif	source	non	non	non

Figure 12: Classification des protocoles de routages dans les RCSF [SRB06, YSY10].

	Agrégation	Utilisation de puissance	Informations de localisation	Mobilité	Scalabilité	Simplicité
SPIN	oui	limitée	non	possible	limitée	bonne
Direct Diffusion	oui	limitée	non	limitée	limitée	bonne
Rumor Routing	oui	minimale	non	trés limitée	bonne	bonne
GBR	oui	minimale	non	limitée	limitée	bonne
LEACH	oui	maximale	non	puits fixe	bonne	cluster-heads
TEEN	oui	maximale	non	puits fixe	bonne	cluster-heads
PEGASIS	non	maximale	oui	puits fixe	bonne	bonne
GAF	non	limitée	oui	possible	bonne	bonne
GEAR	non	limitée	oui	non	limitée	bonne
MECN	non	minimale	oui	non	limitée	moyenne

Figure 13: comparaison des protocoles de routages dans les RCSF [SRB06, YSY10].

6. Critères de performance des protocoles de routage : [SRB06, B&D09]

Cette section présente les critères de performances pris en considération pour les protocoles de routage. Certains critères sont significatifs notamment pour les environnements soumis à des contraintes d'énergie.

- **Le nombre de sauts**

C'est le critère le plus typique qui est utilisée dans la gestion des réseaux. Il représente le nombre des nœuds traversés par une transmission pendant le transfert des données depuis la source à la destination. L'inconvénient principal de ce critère est qu'il ne tient pas compte de la largeur de la bande passante disponible entre les nœuds. Toutefois, on ignore les longs chemins (qui ont un nombre élevé de sauts) malgré qu'il existe des chemins parmi eux qui peuvent avoir une bande passante plus large que la bande passante des courts chemins.

- **Le temps de traverser un saut**

Ce critère mesure le temps d'aller-retour des requêtes envoyées aux nœuds voisins.

Ce critère peut être calculé en ayant un nœud qui va envoyer un paquet de requête avec un estampille "timestamped" à l'un de ses voisins chaque 500 ms. Quand le voisin reçoit le paquet, il le transmet de nouveau à l'expéditeur. En comparant le timestamped avec la durée du retour, la qualité du lien peut être évaluée. Naturellement, les résultats de ce test peuvent être altérés par le temps d'attente "queuing delay" ou la charge sur les deux nœuds.

- **La différence en temps d'arrivée de deux paquets par saut**

Ce critère est une amélioration du critère précédent car elle réduit le temps d'attente qui peut modifier les résultats. Ce critère peut être calculé, en ayant un nœud examinateur qui va envoyer à l'un de ses voisins deux requêtes toutes les deux secondes, tel que la première requête doit être envoyée avant la deuxième. Le récepteur calculera la différence de temps entre la réception des deux paquets et fera un rapport à l'expéditeur, ce dernier va maintenir ces différences de temps.

- **La notion du coût**

"Cost awareness" représente une technique pour minimiser la consommation d'énergie dans le routage dans laquelle nous essayons de prolonger au maximum la durée de vie d'un nœud. Les choix des opérations de routage que le nœud fera sont

une fonction relative à son énergie de batterie restante. Afin d'utiliser "cost awareness", on doit calculer la quantité d'énergie consommée pour chaque route imposée au réseau. Plus la consommation d'énergie est minime plus les tâches de routage peuvent être accomplies par le réseau/nœud avant qu'il soit défaillant.

- **La notion de puissance**

"Power Awareness" représente une technique pour minimiser la consommation d'énergie.

Elle essaye de réduire au minimum l'énergie totale qui a été dépensée lors de l'envoi d'un message depuis une source à sa destination. Afin d'utiliser "power awareness" en tant qu'une métrique, on doit attribuer un poids, basé sur la distance, sur chaque saut possible entre les nœuds du réseau.

- **La notion de coût-puissance**

Ce critère est la combinaison des deux critères précédents. Il vise à réduire au minimum l'énergie consommée dans tout le réseau et, en même temps, il évite qu'un nœud ait une quantité d'énergie limitée.

- **Le temps du premier nœud à mourir**

Ce critère détermine le temps auquel le premier nœud épuise complètement son énergie. Elle n'est pas concernée par la défaillance d'un nœud dû à des raisons techniques.

- **Le temps du dernier nœud à mourir**

C'est l'opposé exact du critère précédant, celle-ci enregistre le temps où le dernier nœud du réseau a consommé toutes ses ressources en énergie. En d'autres termes, ce critère mesure la durée de vie du réseau.

- **Perte de paquets**

Les protocoles de routage utilisent ce critère dans le but de minimiser le nombre de paquets de données perdus lors du transfert depuis une source vers une destination pendant le routage. 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.

- **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. Ce critère 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.

Conclusion

Dans ce chapitre, nous avons situé les contraintes de routage et de sécurité dans un réseau de capteurs sans fil. Puis, nous avons décrit brièvement les principaux protocoles de routages dans les RCSF. Nous les avons classés selon la topologie du réseau en trois catégories principales : les protocoles hiérarchiques, les protocoles basés sur la localisation et les protocoles data centric. Puis, on a fait d'autres classifications selon d'autres critères. Enfin, Nous nous sommes concentrés sur les protocoles de routage qui gérent au mieux la consommation d'énergie. Ces protocoles utilisent des stratégies différentes pour obtenir leurs routes. Certains de ces protocoles utilisent le clustering, les fonctions, les équations, les arbres de routage, les recherches multi-paths etc. Par exemple, le protocole LEACH utilise les clusters-head comme des routeurs pour assurer ses communications avec une consommation énergétique raisonnable.

Dans le prochain chapitre, nous allons présenter quelques techniques de minimisation de la consommation d'énergie exploitées dans le processus de routage de données dans les réseaux de capteurs sans fil.

Chapitre 3 : Présentation des différentes techniques de conservation d'énergie

Introduction

Comme les capteurs sont des petits appareils microélectronique, ils ne peuvent être équipés que d'une source d'énergie limitée, souvent des petites batteries ou des piles. Pour cela, il est nécessaire que les nœuds suivent un plan de gestion d'énergie efficace en préservation d'énergie afin de prolonger leurs durée de vie et ainsi rester fonctionnels pour des mois voire des années. Ce schéma de gestion est imposé par des difficultés de remplacement des batteries d'autant que les RcSF, composés de milliers de nœuds, sont souvent déployés dans des zones hostiles et inaccessibles. [KHR09].

Nous allons présenter dans ce chapitre la contrainte majeure (et la plus importante) dans les réseaux de capteurs sans fils qui est « la conservation d'énergie ».

1. Problématique de la consommation d'énergie dans les RCSF

L'objectif d'une application de réseau de capteurs sans fil, pour plusieurs domaines, est de profiter de son fonctionnement autonome, de la taille minuscule de ses entités et du médium sans fil utilisé dans les communications afin d'accomplir des taches vitales. L'autonomie ne peut être éternelle car le capteur n'est pas en mesure de fonctionner avec des ressources énergétiques illimitées.

Pour comprendre l'aspect consommation d'énergie et pouvoir y développer des mécanismes et des techniques de minimisation, on doit d'abord savoir pour quelles taches un capteur utilise son énergie. Assurément, l'énergie consommée par un nœud capteur est due aux opérations suivantes : la capture, le traitement et la communication.

- **L'énergie de capture :** C'est l'énergie consommée pour le prélèvement d''informations sur l'environnement surveillé. Elle comprend les taches suivantes : échantillonnage, traitement du signal, conversion analogique / numérique et l'activation de la sonde de capture.

- **L'énergie de traitement :** Elle dépend du fonctionnement du microprocesseur, elle peut être dissipée de deux façons :
  - L'énergie de commutation déterminée par la tension d'alimentation et la capacité totale commutée au niveau logiciel.
  - L'énergie de fuite correspondant à l'énergie consommée lorsque le microprocesseur n'effectue aucun traitement.
- **L'énergie de communication :** C'est l'énergie consommée lors des échanges de données entre les capteurs eux-mêmes ou entre les capteurs et le nœud « sink ». Elle concerne l'énergie de transmission et l'énergie de réception. Elle est déterminée par la quantité de données à communiquer et la distance de transmission, ainsi elle dépend de la puissance de transmission.

Remarque : La communication est la tache qui consomme le plus d'énergie par rapport à la capture et traitement. Elle représente environ 80% des besoins en ressources énergétiques d'un nœud capteur.

2. Facteurs intervenants dans la consommation d'énergie

Plusieurs facteurs provoquent la consommation inutile de l'énergie d'un nœud capteur, on cite ([SMD08] [KHR09]) :

a. Etat du module radio : C'est le composant qui consomme plus d'énergie puisqu'il assure la communication entre les capteurs. Le module radio joue un rôle dans la configuration de la quantité d'énergie à consommer selon ses différents états :

- **Etat actif** : C'est l'état qui provoque une perte d'énergie due à l'écoute inutile du canal de transmission d'autant que la radio est allumée sans utilité.
- **Etat sommeil** : La radio est mise hors tension et le capteur n'est pas en mesure de recevoir ou de transmettre. Cet état sert d'alternative pour conserver l'énergie du capteur.
- **Etat transmission** : La radio est allumée afin de transmettre des paquets de données.
- **Etat réception** : La radio est en marche pour recevoir des paquets de données.

Notes importantes sur l'état du module radio

- La consommation d'énergie dans l'état actif est presque égale à la consommation d'énergie en état de réception donc il est préférable d'éteindre complètement le module radio que de le laisser à l'état actif en l'absence d'opérations de transmission ou de réception de données.

- Le passage de la radio d'un état a un autre peut engendrer une dissipation d'énergie importante appelée « l'énergie de transmission » due à l'activité des circuits électroniques.

b. Phénomènes au médium de transmission : Pendant les communications entre les nœuds capteurs du réseau, plusieurs phénomènes peuvent apparaitre et engendrent une perte d'énergie importante. On les cite dans ce qui suit :

- Les collisions : Elles sont la première source de perte d'énergie, ce phénomène peut survenir lors d'une transmission simultanée de paquets par plusieurs nœud capteurs, ce qui les rend inexploitables et provoque leurs retransmission synonyme d'une nouvelle consommation d'énergie du capteur.
- L'écoute à vide (idle listening) : Ce phénomène se produit lorsque le capteur est en état actif ou prêt à recevoir un paquet qu'il ne recevra jamais, la durée de cette écoute à vide provoque une perte d'énergie.
- L'écoute abusive (overhearing) : Ce phénomène se présente lorsqu'un nœud capteur reçoit des paquets qui ne lui sont pas destinés et cela peut lui causer une dissipation d'énergie importante si le trafic est élevé et la densité des nœuds est très grande.
- La surémission (overmitting) : Elle se produit quand un nœud capteur envoie des paquets de données à son destinataire qu'il n'est pas prêt à les recevoir, donc c'est une perte d'énergie additionnelle puisque les messages envoyés sont considérés inutiles.
- La surcharge (l'overhead des paquets de contrôle) : C'est la surcharge du canal de transmission à cause des messages de contrôle utilisés par les protocoles MAC (ACK, ID, SYNC, DATA…etc.) qui nécessitent une énergie additionnelle.

c. La taille de paquets

La taille des paquets échangés entre les capteurs a un effet sur la consommation de leur énergie. En effet, si la taille est petite, on provoque l'augmentation de l'overhead causé par le nombre de paquets de contrôle générés, et si la taille est grande, cela nécessite puissance de transmission importante et gourmande en ressources énergétiques des capteurs.

d. Modèle de propagation radio

Le modèle de propagation présente une estimation de la transmission de la puissance moyenne reçue du signal radio à une distance donné d'un émetteur.

La propagation du signal radio est généralement soumise à différents phénomènes : la réflexion, la dissipation et la diffraction par divers objets.

e. Routage de données

La consommation d'énergie d'un nœud capteur en cours de communication est utilisée soit pour transmettre des données, soit pour relayer les paquets des autres nœuds capteurs d'autant que le routage dans les réseaux de capteurs est en multi-sauts.

Dans ce contexte, les protocoles de routage cherchent à mettre en œuvre des mécanismes permettent garantissant la conservation d'énergie car toute mauvaise stratégie de routage peut conduire à des pertes d'énergie et à la limitation de la durée de vie du réseau.

3. Techniques d'économie d'énergie

3.1. Planification optimisée des états des capteurs

La planification optimisée des états des capteurs cherche un ordonnancement optimal des activités en alternant entre les états des capteurs car dans le cas où le capteur est activé consomme beaucoup plus d'énergie que dans le cas où il est éteint (la consommation considéré dans ce cas comme négligeable [ACA11]).

Nous présentons quelques mécanismes proposés dans la littérature et qui mettent les capteurs en veille. Les travaux sont cités dans [ALM09] :

- Un algorithme d'ordonnancement de transmission dans une topologie hiérarchique avec un seul niveau de TG (tête de grappe). Il attribue à chaque capteur un ensemble optimal d'intervalles temporels (Time slots) de transmission durant une période T, ce qui minimise l'énergie dissipé dans cette période.
- Un algorithme reparti s'intéresse à la planification spatiale des états de capteurs, il se base sur une activation sélective d'un sous ensemble de capteurs offrant une couverture optimale (ou la minimum des points non couverts) qui permet aux capteurs dont la portée est couvertes par leurs voisins direct, de se mettre en veille. Cet algorithme utilise un temps back-off aléatoire qui garantit que deux capteurs ne prendront pas la décision de se mettre en veille en même temps.
- Un mécanisme d'allocation des états dans une topologie hiérarchique avec une garantie de couverture. On définit dans chaque grappe des sous-ensembles de capteurs qui peuvent être à l'état actif, simultanément, pour assurer la couverture totale de la zone à surveiller. Parmi tous les sous-ensembles, un seul sera activé et les autres seront mis en veille jusqu'à l'épuisement complet de l'énergie des capteurs du sous-ensemble activé. Dans ce cas, un autre sous-ensemble sera choisi.

3.2. Méthodes d'accès au canal

La conservation d'énergie dans les méthodes d'accès au canal se réalise principalement par deux techniques : i) la limitation du temps d'accès au canal, moyennant des mise en veille des capteurs, et ii) une gestion très efficace des transmissions afin de limiter les collisions. On peut distinguer différentes méthodes ([YWH03], [PUJ05]) :

- L'accès multiple par répartition temporelle (TDMA) : Cette méthode est basée sur un multiplexage temporel où les nœuds utilisent la même fréquence et occupent des slots de temps différent ce qui permet à chaque capteur d'utiliser toute la bande passante durant un slot donné. La méthode TDMA permet au capteur de passer à l'état « endormi » durant les slots inactif afin d'éviter la dissipation d'énergie due aux phénomènes « écoute abusive »(overheaving) et « écoute passive » (idle).

La synchronisation est obligatoire pour éviter les collisions, donc la station de base doit émettre périodiquement des paquets de synchronisation aux différents nœuds pour mettre à jour leurs horloges malgré que cette réinitialisation de l'horloge consomme

une quantité d'énergie considérée moins importante que l'énergie dissipée dans la retransmission des paquets de données engendrées par les collisions et les pertes de données.

- L'accès multiple par répartition fréquentielle (FDMA) : La méthode FDMA est basée sur le multiplexage fréquentielle. Cela signifie que la bande passante est partagée entre les différents canaux auxquels sont affectés les nœuds ce qui leur permet de transmettre des paquets de données simultanément. La conservation d'énergie dans cette méthode est présentée par l'élimination des temps d'attente nécessaires au nœud avant qu'il puisse accéder au support (cas du TDMA) et la minimisation des collisions puisque chaque nœud occupe sa propre bande de fréquence.

D'autre part, la bande passante assez étroite attribuée à chaque nœud (la bande passante totale étant partagée par plusieurs nœuds), provoque un temps de transmission assez lent et une augmentation de la consommation d'énergie.

- L'accès multiple par répartition de code (CDMA) : Elle est basée sur la distribution d'un code aléatoire unique à chaque nœud. Le nœud émetteur émet ses données à travers le canal de transmission en utilisant son code unique, le nœud récepteur regroupe les données reçues et essaye d'extraire uniquement les données provenant du nœud émetteur. Ce type d'échange peut réduire la bande passante du canal de transmission mais l'augmentation du temps de transmission entraine une augmentation de la consommation d'énergie.
- L'accès multiple avec écoute de la porteuse (CSMA/CA) : CSMA/CA est une technique aléatoire dans laquelle chaque capteur doit rester à l'écoute du médium avant de transmettre ses données pour éviter les collisions. L'inconvénient de cette méthode est que les nœuds doivent rester réveillés pour l'écoute du médium ce qui accroit leur consommation d'énergie. Egalement et dans le cas d'une densité importante du réseau, elle provoque une augmentation de risque de collision.

3.3. L'ajustement optimisé des puissances de transmission

La communication dans le RCSF est définie comme l'échange d'informations (émission/réception) entre les nœuds capteurs du réseau. La transmission est la partie de la communication qui consomme beaucoup plus d'énergie que la réception.

L'énergie de transmission dépend directement de la puissance de transmission. Pour cela, les capteurs sont équipés de plusieurs puissances de transmission, ou d'une puissance ajustable [ACA11]. Si on prend l'exemple d'une topologie hiérarchique, chaque nœud utilise une puissance de transmission minimale qui lui permet d'atteindre au moins une TG voisine.

3.4 Distribution des charges entre les capteurs

La technique de distribution des charges entre les capteurs est une solution très efficace au problème de congestion de charges où les paquets émis empruntent toujours les mêmes chemins, ce qui provoque l'épuisement rapide des ressources énergétiques des nœuds intermédiaires constituant ces routes.

En effet, dans le but de maximiser la durée de vie de ces nœuds et du réseau entier, la technique de distribution des charges permet de faire un équilibrage de charges dans le réseau basé sur un routage multi-chemin, qui consiste à choisir le chemin moins encombrés. [BBY11] propose un protocole du routage basé sur la création d'un arbre des plus courts chemins ayant la station de base comme racine. On a utilisé une fonction de cout basé sur l'énergie résiduelle au sein des nœuds, l'idée de base consiste à pondérer les couts des liens proches a la station de base plus que les autres nœuds ce qui permet un meilleur équilibrage de charge entre les nœuds voisins.

3.5. La formation des grappes (clustering)

La structuration du réseau est l'une des techniques principales de conservation d'énergie notamment ceux ayant une densité importante de nœuds [KBN09]. La technique de formation des grappes (cluster) consiste à partitionner le réseau en sous ensembles afin de faciliter la gestion du réseau. Le routage se réalise sur plusieurs niveaux.

Chaque sous ensemble (cluster) est constitué d'un ensemble de nœuds regroupés autour d'un nœud nommé tête de grappe ou bien nœud-chef (cluster-head) appartenant au cluster. Chaque nœud transmet ses données a son nœud-chef, qui à son tour, les achemine jusqu'au centre de traitement, soit directement c'est-à-dire en un seul saut, soit en multi sauts via d'autres nœuds-chef voisins.

Les nœuds-chefs peuvent effectuer certaines opérations comme le filtrage et l'agrégation des données collectées, ce qui permet d'éliminer des redondances et de limiter la quantité de données transmises à la station de base, ainsi alléger la bande passante et sauvegarder l'énergie des nœuds collecteurs [ACA11]

Par ailleurs, la formation des grappes permet de coordonner et d'ordonnancer au mieux les taches des capteurs dans un RCSF. L'ordonnancement des activités des capteurs par leurs nœuds-chef qui, autorisent certains nœuds de passer en mode vielle, limitent leur puissance de transmission, organisent les instances de transmission des capteurs de leurs grappes respective afin d'éviter les collisions et par conséquent les retransmissions [ALM09].

Toutes les caractéristiques et les avantages cités de la technique de formation de clusters lui accorde le privilège d'être une solution très efficace en conservation d'énergie et l'une des techniques les plus utilisées, et cela malgré ses quelques inconvénients tel que le risque d'épuisement d'énergie des nœuds chefs ne possédant pas une source d'énergie plus élevée que les autres nœuds.

Plusieurs protocoles et travaux se basant sur la formation des grappes sont présentés dans littérature :

- LEACH est un protocole reparti qui offre une distribution équitable de la consommation d'énergie des nœuds capteurs via une rotation aléatoire des têtes de grappes durant une période de temps appelée « round ». Chaque nœud capteur détermine la possibilité d'être le chef, et s'il décide de l'être, il le fait savoir à tous ses nœuds voisins. Les autres nœuds qui décident de ne pas être un chef de groupe se joignent à l'un des chefs élus. la sélection du chef de groupe adéquat se base sur plusieurs paramètres : tels que son niveau d'énergie et le rapport signal/bruit.

L'agrégation locale des données au niveau des clusters se fait uniquement par les nœuds-chefs ce qui permet aux autres nœuds membres du cluster de conserver leur énergie [K&N04]. Cette réduction d'énergie est le fruit de la diminution du nombre de communications agrégées au niveau des nœuds-chef.

- Weighted Clustering Algorithme (WCA) est un algorithme réactif de formation des grappes, il se base sur une fonction score appelé « pondération combiné » pour l'évaluation de chaque capteur. Cette fonction est une combinaison linéaire pondérer du degré du niveau de mobilité, de la puissance de transmission et de l'énergie résiduelle d'un capteur, chaque nœud capteur diffuse sa pondération combiné a ses voisins et le nœud ayant le score le plus bas sera élu nœud-chef [ALM09].

3.6. Agrégation de données

L'agrégation de données est une technique efficace en termes de conservation d'énergie dans RCSF, son principe est que deux ou plusieurs capteurs qui couvrent une même zone du réseau peuvent transmettre des données décrivant un même événement [MIN11], ce que provoque une redondance des données capturées. En effet, l'idée de base de cette technique consiste à combiner les données prévenante de différents nœuds sources en éliminant les redondances existantes selon une fonction d'agrégation (suppression, minimum, maximum et moyen…) [SRB06] et minimisant aussi le nombre de transmission possibles pour économiser la quantité d'énergie consommée ([K&N04], [MBA07]).

L'agrégation de données peut se réaliser soit par des programmes incorporés (intégrés) dans le capteur (l'inconvénient de cette approche est que l'utilisateur ne peut pas changer le comportement du système), soit par des requêtes diffusées par l'utilisateur semblables à celles utilisées en SQL. La requête peut contenir des clauses comme SELECT, GROUPE BY, HAVING et des clauses d'agrégation : MAX, AVG, MIN, COUNT et SUM, comme on peut ajouter d'autres clauses comme DURATION et EVERY qui permettent au capteur, pendant la période prédéfinie par la clause, de se mettre en veille, ceci peut conserver l'énergie d'où la durée de vie du réseau.

Les différentes techniques d'agrégation de données dans les RCSF sont classées en deux approches :

- Approche centralisée : Le nœud-chef agrège uniquement les données récoltées par ses membres. Cette approche est utilisée dans les protocoles hiérarchiques tels que LEACH, PEGASIS, TEEN, APTEEN…etc.

- Approche distribuée (agrégation dans un arbre) : C'est une approche centrée-données autorisant les nœuds intermédiaires à consulter le contenu des messages reçus par les autres nœuds-chef et agréger les données transportées par les différents paquets qu'ils réceptionnent. Elle implique le décalage d'une partie de calcule des clients aux nœuds capteurs agrégeant les résultats ou filtrant les données inutiles, ceci permet de réduire le transfert des messages et l'utilisation efficace de la bande passante pour conserver l'énergie pour une plus longue durée de vie d'un RCSF.

3.7. Tolérance aux pannes

Les vulnérabilités des RCSF sont avantagées par leurs caractéristiques, comme l'absence de sécurité physique, la source d'énergie limitée, la perte de connexion entre les capteurs…etc. ils impliquent une nécessité de mise en œuvre de techniques qui prennent en considération ses vulnérabilités et qui peuvent assurer le bon fonctionnement du réseau.

Le but de la tolérance aux pannes est d'éviter la faille totale du système malgré la présence de failles dans un sous ensemble de ses composants élémentaires [YCL08]. L'impact de la tolérance aux pannes dans les RcSF est lié aux ressources limitées des capteurs notamment en énergie et à l'environnement de déploiement.

Les techniques préventives tentent de retarder ou d'éviter tout type d'erreur afin de garder le réseau fonctionnel le plus longtemps possible. Parmi les mécanismes de ces techniques, on distingue :

- La gestion de la batterie à travers une distribution uniforme pour la dissipation d'énergie entre les différents capteurs définit par les protocoles afin de gérer la consommation et augmenter aussi la durée de vie. Le mécanisme de mise en vielle est une technique de gestion de la batterie.
- Le routage multi chemins : Consiste à déterminer plusieurs chemins depuis les capteurs sources vers les stations de base pour garantir la disponibilité de plus d'un chemin fiable pour la transmission et offre une reprise rapide des transferts en cas de panne sur le premier chemin sélectionné.
- Mobilité : Consiste à déplacer un ensemble de nœuds collecteurs (menée d'une batterie plus puissante que celle des capteurs) entre les capteurs et collecter les

données captées. Ceci permet de limiter la puissance de transmission des capteurs et donc une réduction de la consommation d'énergie.

- Gestion des données : On s'appuie sur les deux techniques citées auparavant qui sont l'agrégation des données et le clustering qui permettent une réduction des communications d'où une consommation minimisée de la bande passante et de l'énergie.

3.8. Solutions algorithmiques

L'objectif principal de tous les protocoles de routage est de trouver des routes économes en énergie afin de maximiser la durée de vie du réseau. Pour atteindre cet objectif, de nombreux protocoles ont été développés avec différentes stratégies pour créer un cheminement intéressant entre la source et sa destination telles que la formation des grappes, les équations, les fonctions, la construction des arbres de routage optimales, les chaines, les multi-chemins…etc. et avec différents mécanismes de gestion efficace d'énergie tels que l'ajustement de puissance de transmission, la mise en veille des capteurs, la mobilité des nœuds collecteurs…etc.

Dans cette section, on décrit quelques solutions algorithmiques de préservation d'énergie intégrées dans les algorithmes cités auparavant.

- EAR, proposé par shah [SRB06], est basée sur la création d'un chemin multi-routes à modifier de façon aléatoire. Les routes sont choisies au moyen d'une fonction de probabilité qui dépend de la consommation énergétique de chacune d'elles. Ainsi, la route la plus économe est sélectionnée. Si des changements surviennent au cours du processus de routage, le chemin sera modifié selon les nouvelles données énergétiques des routes.
- GAF est un protocole de routage basé sur la localisation, efficace en énergie, dont le principe est d'éteindre l'ensemble des nœuds inutiles sans toutefois affecter le niveau de fidélité du réseau (le niveau de précision dans l'opération de routage). Il se base sur une grille virtuelle sur le champ de captage, où chaque nœud s'associe à un point particulier de la grille construite. Les nœuds se trouvant dans la même zone de la grille sont considérés équivalents en terme du cout lié au routage des paquets, cette

équivalence permet à certains nœuds associés au même point de la grille de se mettre en veille afin de conserver l'énergie consommée.

- MCFAC (Minimum Cost Forwarding Algorihtme) est un algorithme qui consiste à chercher un chemin minimal entre la source et le puits, tout en prenat en considération les limites de réseau de capteur. Chaque nœud maintient une variable de cout qui détermine une valeur minimale du chemin optimal vers le puits. L'algorithme se déroule en deux phases : le calcul des couts et le relais des paquets.

Pour prendre en considération les contraintes d'énergie des capteurs, MCFA utilise une méthode qui emploie moins de messages de contrôle selon un mécanisme de backoff. Le backoff permet de retarder la prise de décision sur la valeur locale du cout en attendant la valeur optimale globale. L'intervalle du backoff dépend du cout du lien de réception : plus le cout est grand, plus on a la chance de recevoir une valeur plus optimale donc on doit attendre plus de temps.

- [M&K10] ont proposés un algorithme de routage hiérarchique appelé « MHEED » à plusieurs sauts pour les grands réseaux de capteurs. Cet algorithme est une amélioration de l'algorithme HEED (protocole de routage hiérarchique basé sur deux paramètres : l'énergie résiduelle et le cout de communication intra-grappe). L'algorithme MHEED basé sur deux variantes pour la minimisation de la consommation d'énergie, la première variante se base sur l'utilisation du meilleur chemin construit pour véhiculer les données, et la seconde a pour principe que l'émetteur choisit son prochain relais de manière probabilisée pour équilibrer la charge entre les différents relais.

4. Les principaux algorithmes de conservation d'énergie [YSY10]

De nombreux algorithmes de routage ont été spécifiquement conçus pour les réseaux de capteurs où la consommation d'énergie est un facteur primordial. Ce facteur a posé de nombreux défis à la conception et à la gestion des réseaux de capteurs. Ces défis nécessitent une gestion efficace de l'énergie pour toutes les couches de la pile du protocole réseau. L'objectif principal de ces protocoles est de trouver des moyens pour une mise en œuvre efficace de l'énergie et pour une diffusion fiable des données de la source vers la destination de sorte que la durée de vie du réseau soit maximisée. Quelques algorithmes ont été développés pour prendre

soin du contrôle de la capacité. Certains se concentrent sur l'utilisation effective du temps d'activation des nœuds capteurs. Plusieurs paramètres tels que la distance de transmission, le nombre de sauts et le retard ont été pris en compte pour économiser l'énergie dans les réseaux de capteurs.

La recherche dans le domaine des protocoles efficaces en gestion d'énergie dans les réseaux de capteurs sans fil est relativement nouvelle. L'objectif principal de tous ces protocoles et algorithmes est de trouver les routes qui sont économes en énergie et donc de maximiser la durée de vie du réseau. Les algorithmes d'énergie efficace les plus connus sont:

4.1. L'algorithme de routage « EARLEAHSN »

L'algorithme Energy Aware Routing for Low Energy Ad Hoc Sensor Networks (EARLEAHSN) utilise un ensemble de sous-chemins optimaux afin d'augmenter la durée de vie du réseau. Ces chemins sont choisis au moyen d'une fonction de probabilité qui dépend de la consommation d'énergie de chaque route. La survie du réseau est la mesure principale de cette approche qui propose d'éviter l'utilisation permanente de la route la plus économe en énergie car cela épuise l'énergie des nœuds sur cette route. Au lieu de cela, l'un des trajets multiples est utilisé avec une certaine probabilité de sorte que la vie entière du réseau se prolonge. Le protocole suppose que chaque nœud est adressable par le biais d'une classe d'adresse qui comprend l'emplacement et les types de nœuds.

4.2. L'algorithme de routage «EARCBSN »

Energy-Aware Routing in Cluster-Based Sensor Networks (EARCBSN) propose un algorithme de routage hiérarchique basé sur une architecture à trois niveaux.

Les capteurs sont regroupés en clusters avant l'exploitation du réseau. L'algorithme emploie les clusters-head comme des passerelles et ces clusters-head possèdent de l'énergie plus que les autres capteurs et connaissent l'emplacement des tous les capteurs.

Le routage nécessite une maintenance d'un cluster-head qui inclut tous les paramètres qui influent sur la décision de routage. Dans cet algorithme, ces paramètres sont l'état du capteur, sa localisation, l'énergie restante et le trafic des messages. Il y a une certaine imprécision dans le modèle d'énergie des passerelles

due à la surcharge, la perte des paquets et au retard de propagation des messages. Le nœud passerelle agit comme un gestionnaire de cluster de réseau centralisé qui achemine les routes pour les données des capteurs, qui contrôle la latence dans tout le cluster et qui arbitre les accès entre les capteurs.

Le nœud passerelle trace l'utilisation d'énergie de chaque nœud capteurs et contrôle aussi les changements dans l'environnement. De plus, il permet de configurer les capteurs et le réseau efficacement afin de prolonger sa vie du réseau.

4.3. L'algorithme de routage « GBR »

L'algorithme Gradient-Based Routing (GBR) ou le routage par gradient est une version légèrement modifiée de la diffusion dirigée. L'idée de ce protocole est de maintenir le nombre de sauts lorsque le paquet est diffusé à travers le réseau. Ainsi chaque nœud peut découvrir le nombre minimal de sauts jusqu'à la destination. Ce nombre est appelé hauteur du nœud. La différence entre la hauteur d'un nœud et celui de son voisin est considérée comme le gradient sur ce lien. Un paquet est transmis sur un lien avec le gradient le plus grand. Le routage par gradient vise à utiliser certaines techniques auxiliaires telles que l'agrégation des données afin d'équilibrer le trafic de manière uniforme sur le réseau.

Trois techniques différentes pour gérer les données ont été présentées:

- **Stochastic Scheme** : Quand il y a deux sauts ou plus avec le même gradient, le nœud choisit l'un d'eux au hasard.
- **Energy-based scheme :** Lorsque l'énergie d'un nœud tombe en dessous d'un certain seuil, il augmente sa hauteur afin que les autres capteurs soient découragés d'envoyer des données à ce nœud.
- **Stream-based scheme** : L'idée est de détourner les nouveaux flux à partir de nœuds qui font actuellement parti de la trajectoire des autres filières. Les données s'efforcent alors de parvenir à une répartition égale de la circulation à travers l'ensemble du réseau, ce qui contribue à équilibrer la charge sur les nœuds capteurs et augmente la durée de vie du réseau. Les techniques employées pour équilibrer la charge de trafic et la fusion de données sont également applicables aux autres protocoles de routage pour des performances améliorées.

Conclusion

La conservation d'énergie dans les RCSF est un défi indéniable qui continue à attirer l'intérêt de la communauté scientifique. De nombreux algorithmes, mécanismes et protocoles ont été proposées dans la littérature scientifique pour traiter les problématiques de la minimisation de l'énergie dissipée par les capteurs et la maximisation de la durée de vie du réseau [ALM09]. Les différentes techniques présentées dans ce chapitre ont eu des résultats très efficaces, avec des portions différentes, dans la minimisation de la consommation d'énergie. Pour cela les protocoles de routage utilisent ces techniques pour offrir une circulation d'information fiable et économe en énergie en gardant les performances du réseau et en prolongeant tout de même sa durée de vie.

Dans le chapitre suivant, nous allons présenter notre solution qui consiste à améliorer l'un des protocoles présenté ci-dessus, considéré comme simple et efficace en énergie, mais moins sécurisé.

Chapitre 4: Présentation et implémentation de la solution proposée

Introduction

La souplesse du domaine des réseaux de capteurs ouvre la porte devant les recherches afin de proposer des solutions efficaces pour les différents problèmes (routage, localisation, consommation d'énergie, sécurité…etc) connus par ce type spécial de réseau.

La consommation d'énergie et la sécurité sont deux facteurs très importants qu'il faut prendre en considération lors du déploiement d'un RCSF, et ainsi faire le maximum d'efforts pour assurer une consommation réduite de l'énergie et sécuriser les communications pour le bon fonctionnement du réseau entier.

La forte dépendance entre la sécurité du réseau et la consommation réduite de l'énergie permet d'offrir un RCSF plus performant et presque optimal, par contre l'absence d'un des deux rend l'autre a moins d'importance ou bien minimise la performance du réseau, d'où une attaque sur un réseau peut engendrer une large dissipation d'énergie conservée, d'autre part un réseau sécurisé qui consomme beaucoup d'énergie peut aboutir a la fin du sa durée de vie.

Dans ce chapitre, on a essayé de coupler les deux contraintes par l'implémentation d'un protocole de routage sécurisé et économe en énergie.

1. Motivations

Le routage est l'un des axes les plus sensibles et les plus importants dans les réseaux de capteurs sans fils car il constitue la colonne vertébrale du réseau par le bon fonctionnement de ces mécanismes en termes de fiabilité d'acheminement des messages, de sécurité, de la tolérance aux pannes et de la maximisation de la durée de vie du réseau.

Les protocoles de routage hiérarchiques se présentent comme l'une des solutions les plus efficaces face aux contraintes du routage (la redondance de donnée, l'absence

d'adressage, la consommation d'énergie…etc.) qui sont considérées comme des problèmes de base pour le routage.

Pour cela, on a choisi cette approche de routage hiérarchique pour ses nombreux avantages (agrégation de données, la répartition des charges par les tours de rôle des nœuds-chef…etc.). LEACH est considéré comme une référence des protocoles hiérarchiques du fait qu'il est le premier protocole conçu pour ce type d'approche de routage. On a commencé par étudier ce protocole, son fonctionnement, ses avantages et ses inconvénients devant lesquelles nous nous sommes arrêtés pour présenter quelques inconvénients :

- Le risque d'absence des CHs (nœuds-chef) si le nombre aléatoire générés par tous les nœuds est supérieur à la probabilité P_i, comme il est possible d'avoir un nombre supérieur a celle désirée auparavant si les nombre générés par plusieurs nœuds sont inferieurs à P_i, ce qui provoque une large consommation d'énergie par les capteurs qui jouent le rôle de CH.
- L'instabilité du réseau suite au changement de la topologie à chaque nouveau round, cette restructuration implique une dissipation énorme d'énergie.
- La rotation du rôle des CHs se fait sans aucune contrainte, elle est totalement aléatoire (puisqu'elle dépend du nombre aléatoire généré par les nœuds et la valeur de probabilité P_i) donc il est possible d'avoir un CH avec une faible capacité énergétique ce qui provoque le dysfonctionnement du réseau.

Tous ces inconvénients et bien d'autres nous laissent à repenser à concevoir un protocole hiérarchique différent de LEACH (sous forme d'une variante) contenant des solutions efficaces aux insuffisances du protocole LEACH tout en étant efficace en terme d'énergie et de sécurité.

2. Présentation et objectifs du protocole

Le protocole proposé est un protocole hybride, centralisé dans le premier round ou le nœud puits désigne aléatoirement les Clusters Head selon le nombre désiré, et reparti dans les rounds qui suivent le premier jusqu'à ce que tous les nœuds passent par le rôle du Cluster Head. Dans ce cas, le protocole sera centralisé et réparti par cette alternance.

La sélection du Cluster Head, dans notre protocole, est basé principalement sur l'énergie résiduelle du nœud capteur. Cette sélection est faite d'une manière aléatoire puisqu'on considère que tous les nœuds capteurs sont homogènes donc ils possèdent une même énergie résiduelle initiale lors du déploiement, et elle sera presque la même après le tournement du rôle du Cluster Head.

L'idée principale de notre proposition (solution) consiste à garder la stabilité du réseau en évitant de reformer les clusters a chaque nouveau round, donc la formation du cluster se fait uniquement lors du déploiement et lors du tournement du rôle du Cluster Head par tous les nœuds capteurs.

Une autre solution est inclut dans notre approche, elle concerne le choix du prochain Cluster Head pour le prochain round par le Cluster Head du round courant. Cette élection basée sur l'énergie résiduelle envoyée par les nœuds avec la donnée captée dans leurs slots, le Cluster Head choisi le nœud ayant le plus grand taux d'énergie résiduelle pour jouer le rôle du Cluster Head dans le prochain round, cela va réduire les messages échangés pendant la phase d'initialisation (formation des grappes) au niveau de chaque nœud dans le cas d'une reformation des clusters. Le principe est de répondre aux questions suivantes :

- Comment que chaque nœud puisse connaitre son Cluster Head dans le prochain round ?
- Comment se fait le processus de changement de rôle entre l'ancien et le nouveau Cluster Head ?
- Comment (ré) attribuer à l'ancien CH son slot et son code CDMA d'autant que la procédure se fait uniquement lors de l'invitation des nœuds à former les clusters ?

Afin de palier à ces insuffisances, on va classer (numéroter) les clusters dans la phase d'initialisation du round 0 et à chaque nouveau round, chaque nœud doit garder le rang de son cluster jusqu'au nouveau déploiement ou reformation de clusters (quand tous les nœuds ont joués le rôle du Cluster Head, la valeur du round doit être à 0).

Lorsque le Cluster Head reçoit les données captées de son cluster, il compare l'énergie résiduelle du nœud émetteur à celles des autres nœuds ayant déjà transmis leurs données et si elle est la plus grande, le Cluster Head désigne l'émetteur comme le prochain Cluster Head tout en gardant la valeur de son slot et de son code CDMA pour la transmission de ses données avec les autres nœuds capteurs membres de son cluster lors du prochain round.

Dès que le round courant soit terminé, le nœud puits lance le déclenchement d'un nouveau round et informe les nœuds du réseau de ce déclenchement en leur envoyant les coordonnées de leurs prochains Cluster Head. Chaque nœud reçoit le message du puits, il procède au changement de l'adresse de son Cluster Head et il garde son slot et son code CDMA qui lui a été attribué.

2.1. Fonctionnement du protocole

1- round =0

a) la phase initialisation

- Le nœud puits initialise le round à 0 et choisi aléatoirement les Clusters Head selon le nombre des clusters désiré (généralement 10% est le pourcentage des Clusters Head sur le nombre totale des nœuds), après il lance le message de déclenchement du nouveau round 0 correspond a la formation des grappes contenant les adresses des Clusters Head sélectionnés.
- Chaque nœud reçoit le message du déclenchement du round, il vérifie s'il est élu comme Cluster Head, et si c'est le cas, il invite les nœuds à joindre son cluster.
- Le nœud qui reçoit des invitations pour rejoindre les Clusters, il choisit le Cluster Head le plus proche (pour implémenter l'amplification du signal) et lui envoie une demande d'adhésion.
- Le Cluster Head reçoit les demandes d'adhésion a son cluster, il les confirme et il attribue un slot et un code CDMA pour chaque nœud accepté pour pouvoir envoyer ses données dans son slot et avec son code pour éviter les collisions.
- Après la réception du slot et du code CSMA par chaque nœud demandeur d'adhésion à un cluster, les clusters seront formés et la phase d'initialisation sera achevée.

b) La phase transmission

- chaque nœud doit attendre son tour, selon les slots, pour envoyer ses données (la donnée captée et son énergie résiduelle).
- Les Clusters Head reçoivent les données captées et l'énergie résiduelle des nœuds, agrègent la donnée selon une fonction d'agrégation (moyenne, somme, suppression des redondances…etc.) et gardent les informations (ID, énergie, slot, code) du nœud ayant une énergie résiduelle plus grande pour le désigner comme le prochain Cluster Head.
- Le nœud puits reçoit les données agrégées ainsi que les ID des prochains Clusters Head envoyées par les nœuds-chef.
- A la fin de la durée du la phase de transmission, le nœud puits lance le déclenchement du nouveau round et informe les nœuds sur l'identité de leurs prochains Cluster Head selon la dernière mise à jour (dernière agrégation reçue) effectuée.

2- round ≠ 0

C'est le cas des rounds qui suivent le premier round, et comme il n'existe pas une phase d'initialisation, puisque la structure du réseau ne change pas, il n'y a que la phase de transmission.

- Chaque nœud reçoit le déclanchement du nouveau round, vérifie s'il est choisi comme Cluster Head pour ce round, sinon change l'adresse de Cluster Head.
- Après que tous les nœuds exécutent le déclenchement du nouveau round, chaque nœud commence à envoyer ses données selon son slot et son code attribué.

Pour rendre le protocole plus efficace et économe en énergie et assurer tout de même sa stabilité et sa continuité, surtout devant les attaques abusives, on a implémenté un mécanisme simple basé sur l'authentification et l'intégrité des données afin d'empêcher un attaquant d'emprunter l'identité des nœuds légitimes pour s'approprier leurs données. Pour cela on a utilisé des outils cryptographiques afin de sécuriser la communication dans le réseau et bloquer ainsi toute tentative de perturbation du réseau.

Ce nouveau mécanisme implémenté permet d'assurer la sécurité des communications dans les différents liens (Puits-Membre, Membre-CH, CH-Puits…etc.) d'une manière similaire, c'est-à-dire le mécanisme fonctionne de la meme sorte pour tous les liens du réseau.

La solution est présentée sous forme de code d'authentification de message MAC qui sera calculé par une fonction de hachage mais sans l'utilisation de clés symétriques qu'on a préféré éviter, malgré leur efficacité et leur fiabilité en terme de sécurisation des liens, mais qui conduisent à une gestion des clés, différente pour chaque lien, qui nécessite plus d'espace mémoire et peut, par conséquent, augmenter la complexité du programme avec une dissipation d'énergie additionnelle suite aux échanges des tables des clés entre les différents liens.

Le calcul du message d'authentification MAC dépend de l'ID de l'émetteur et le round courant (lors la transmission et/ou la réception) d'où chaque nœud voulant émettre un message doit calculer ce message en utilisant cette fonction :

$$Mac\ (m) = (IDemt+1)*(round\_courant+1)\ mode\ N$$ où :

N : nombre totale des nœuds capteurs du réseau.

Le récepteur recalcule le MAC en utilisant le contenu du message reçu (IDemt), et si le mac recalculé est égal au mac reçu dans le message, le nœud accepte ce message et sera traité, sinon il le rejette et considère l'émetteur comme un attaquant.

2.2. Intérêts et objectifs du protocole proposé

L'intérêt principal de notre protocole est la réduction du nombre de messages échangés et cela par l'annulation de la reformation des clusters à chaque round, puisqu'on a remarqué que cette reformation itérative à chaque round engendre une dissipation considérable et conséquente d'énergie. Cette contribution permet d'atteindre bien d'autres objectifs :

- Elle rend le réseau plus stable par la minimisation des changements de la topologie dans chaque round.

- Elle offre une distribution de charge par la rotation du rôle du Cluster Head, cette rotation basée sur l'énergie résiduelle évite l'épuisement rapide de la source d'énergie lors la sélection du Cluster Head d'une maniéré aléatoire et sans aucune contrainte.
- Le choix des Clusters Head d'une maniéré centralisé dans le round 0 permet de garantir l'existence des Clusters Head et donc l'existence des Clusters.
- Elle permet d'éviter les collisions grâce aux slots et aux codes CDMA attribués (on peut avoir deux nœuds dans des clusters différents ayant un même slot mais pas avec le même code CDMA pour l'accès au canal).
- Elle peut assurer une planification de mise en vielle des capteurs lorsqu'il est hors de son slot donc une conservation d'énergie.
- La mise en œuvre d'un mécanisme de sécurité simple ne nécessitant aucune ressource additionnelle ni de traitements supplémentaires.
- L'efficacité de l'authentification par message MAC assure l'isolation du réseau de toute tentative d'accès externe au réseau.

3. Implémentation

Cette partie est l'étape la plus intéressante de notre travail, c'est la partie pratique où se réalise notre protocole pour tester son efficacité et décider son succès ou son échec avant sa mise en œuvre sur le terrain. Pour cela, on simule le protocole proposé pour le routage des données dans un réseau de capteur sans fils avant son déploiement, en utilisant des outils mis à la disposition des développeurs et des chercheurs du domaine pour évaluer leur travail.

3.1. Environnement de simulation

Ces outils sont représentés par le système d'exploitation des réseaux de capteur sans fils TinyOs, le langage de programmation avec lequel nous avons programmé notre protocole Nesc, le simulateur TOSSIM, l'interface graphique TinyViz pour visualiser le déroulement de la simulation, le simulateur POWER TOSSIM pour évoluer la consommation d'énergie.

a) TinyOs

Ce système est considéré comme le plus répandu et le plus utilisé par les universités et les centres de recherche dans le monde de la recherche scientifique dédiée aux systèmes embarqués en général et aux réseaux ad hoc et réseaux de capteurs en particulier, vu les caractéristiques qu'il détient et qu'on a cité plus haut en chapitre 1, il nous apparait comme le meilleur choix devant notre nécessité d'utiliser un système qui offre des outils, des fonctions, des bibliothèques prédéfinies pour répondre aux objectifs de notre travail, ainsi la programmation orienté composant et orienté événement qu'il supporte, nous facilite le travail puisqu'elle permet au programmeur d'arranger et de contrôler son code source grâce aux composant indépendants sans toutefois oublier la possibilité de leur réutilisation dans d'autres programmes. Encore, la programmation orienté événement convient aux RCSF car elle permet au capteur de se réveiller suite au déclenchement d'un événement sinon il est en veille et son énergie sera conservée.

b) Le Langage de programmation NesC

Ce langage de programmation orienté composants conçu pour la réalisation des systèmes embarqués distribués et en particuliers les RCSF.

Le NesC supporte trois types de fichiers source : les fichiers interfaces, les fichiers configuration et les modules. Une configuration définit les composants et/ou les interfaces utilisés ainsi que la description de la liaison entre eux, le module constitue la brique élémentaire du code et implémente une ou plusieurs interfaces, cette dernière définit d'une manière abstraite les interactions entre deux composants et elle définit un fichier décrivant les commandes et les événements proposés par le composant qui les implémente, une commande doit être implémentée par le fournisseur de l'interface et l'événement doit être implémenté par l'utilisateur de l'interface [RHK11].

c) Le simulateur TOSSIM

L'intérêt de la simulation est d'assurer le bon fonctionnement de tous les protocoles de communication avant leur mise en place afin de minimiser au maximum les

erreurs de conception et éviter une perte financière puisque la densité du réseau de capteur est généralement importante et ils sont souvent déployés dans des zones hostiles, et tout dysfonctionnement serait fatal pour l'utilisateur.

TOSSIM est l'un des simulateurs qui sont crées pour permettre une simulation très proche de ce qui se passe réellement dans les RCSF du monde concret. C'est un outil très puissant avec une économie d'efforts et une préservation du matériel. Il possède également une interface graphique TinyViz pour une compréhension moins complexe du déroulement de l'activité du réseau.

d) Le simulateur POWER TOSSIM

Le simulateur POWER TOSSIM est un simulateur conçu par l'université Haward pour palier à l'incapacité de TOSSIM face à la vérification d'énergie dissipée pendant l'exécution des applications. POWER TOSSIM est intégré dans TOSSIM, il permet de générer un fichier de l'extension *.trace qui enregistre les détails de la simulation notamment l'énergie consommée par les nœuds du réseau.

3.2. Implémentation et déroulement

Pour un aperçu clair et complet du bon fonctionnement de notre protocole, on va présenter d'abord son déroulement dans un état normal (absence des attaques) et tester par la suite sa réaction face à des attaques quelconques.

3.2.1. Structure de données

Les structures de données sont différentes selon l'initiateur du message (Puits, Membre, Cluster Head), un paquet est envoyé dans une structure appelée TOS_Msg contenue dans un champ « uint8_t data [TOSH_DATA_LENGTH] ». Voici les différentes structures de données implémentées pour notre protocole.

a) **Le nœud Puits**

```
typedef struct PUITS
{
uint16_t ID_Pro_ch[10]; //tableau contient les ID des prochains CH
uint16_t ID;            //l'identificateur de chaque noeud qui correspond à
TOS_LOCAL_ADRESS
uint8_t round;          //le round courant
uint16_t MAC;           //message d'authentification MAC
uint8_t Depth;          //la profondeur du neoud dans le réseaux
}PUITS;
```

b) **Le nœud MEMBRE :**

```
typedef struct MEMBRE
{uint16_t ID_MEMBRE;            //l'identificateur de chaque nœud qui correspond à
TOS_LOCAL_ADRESS
uint16_t ID_CH;         //l'identificateur du CH dont lequel appartiendra le nœud membre
uint8_t  temp;                  //variable qui contient la température captée
uint8_t  req;           //si req=1 alors le neoud membre préviend le CH qu'il fais partie de son
groupe,si il est égal à 2 sa veut dire qu'il a envoyé la valeur captée
uint16_t enrg_res;     // énergie résiduelle du noeud
uint8_t mon_slot;   // slot attribué au noeud
uint16_t MAC;       //message d'authentification MAC
uint8_t rangcluster;  //le némuro du cluster ou le nœud appartient
uint8_t round_courant;   //la valeur du rond courant
}MEMBRE;
```

c) **Le nœud CH (Cluster Head) :**

```
typedef struct CLUSTER_HEAD
{
uint16_t ID_MEMBRE;      //l'identificateur de chaque noeud qui correspond à TOS_LOCAL_ADRESS
uint16_t ID_CH;    //l'identificateur du CH dont lequel appatiendra le noeud membre
uint8_t  donne_aggreger;            //la donnée aggreger à envoyer au noeud PUITS
uint16_t FREQ;           //La fréquence avec laquelle les membre d'un memebre Cluster envoi
uint16_t  SLOT_ATTRIBUER;          //le slot attribuer à chaque membre
uint8_t  NBR_MBR;                  //Calcul le nombre de membre utiliser pour la connectivité
uint8_t rang;        //le némuro du cluster
uint8_t max_energ;   //la grande valeur d'énergie résiduelle envoyé par les nœuds
uint16_t ID_Proch_CH;   // ID du prochain CH
 uint16_t MAC;        //message d'authentification MAC
uint8_t round_courant; //la valeur du rond courant
}CLUSTER_HEAD;
```

3.2.2. Evénements et commandes

Nous citons dans cette section les principaux événements utilisés pour l'implémentation du notre solution.

Evénement	**Sortie**	**Fonction**
Sol_ReceiveMsg.receive(TOS_MsgPtr pmsg)	TOS_MsgPtr	Réception du round
ANNONCE_ReceiveMsg.receive(TOS_MsgPtr pmsg)	TOS_MsgPtr	Annonce du CH
ORGANISATION_ReceiveMsg.receive(TOS_MsgPtr pmsg)	TOS_MsgPtr	Formation de groupes

SLOT_ReceiveMsg.receive(TOS_MsgPtr pmsg)	TOS_MsgPtr	Réception des slots
Temperature_ReceiveMsg.receive(TOS_MsgPtr pmsg)	TOS_MsgPtr	Réception du CH des températures captées et les énergies résiduelles
AGGREGATION_ReceiveMsg.receive(TOS_MsgPtr pmsg)	TOS_MsgPtr	Réception du puits des résultats d'agrégation
ReqRelayTimer.fired()	result_t	Relai des annonces du round
RoundTimer.fired()	result_t	Envoi du nouveau round par le nœud puits

3.3 Implémentation des attaques

Afin de tester la réaction des deux protocoles face aux attaques abusives et vérifier ses effets sur leur déroulement et fonctionnement ainsi que sur la consommation d'énergie, nous implémentons deux attaques qui nous permettent d'atteindre les objectifs attendus.

a) Attaque Sink Hole

Dans notre cas, on a implémenté cette attaque de telle façon que le nœud malicieux éjecte des données pour perturber le fonctionnement du réseau et ainsi provoque une consommation additionnelle d'énergie, l'attaquant prend le rôle d'une station de base (Puits), il désigne une valeur de probabilité très élevé pour augmenter le nombre des Clusters Heads (dans le cas du protocole LEACH) , ceci provoque beaucoup de messages échangés correspondants aux invitations envoyées par les Clusters Heads pour joindre leur clusters, les demandes d'admission, l'envoi des slots et du code CDMA …etc.

b) Attaque Hellow floods :

Dans cette attaque, l'attaquant envoi des paquets inutiles vers les Clusters Heads pour les tromper, en envoyant des demandes d'admission aux plusieurs Clusters Heads, ce qui engendre une perturbation du fonctionnement et une augmentation de la consommation d'énergie relativement aux nombre de messages d'organisations envoyés (l'envoi des solts).

4. Résultats et Performances

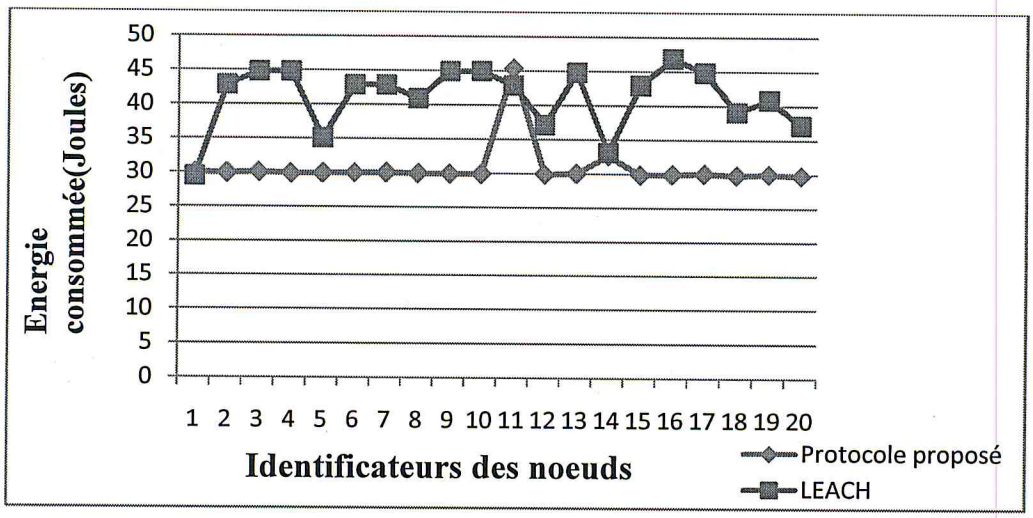
Pour évaluer les performances du protocole proposé en terme d'efficacité en consommation d'énergie ainsi que la fiabilité de la sécurité du protocole, nous avons procéder à le comparer au protocole LEACH (puisqu'il est la référence des protocoles hiérarchiques). Nous avons effectué des simulations avec les mêmes paramètres pour les deux protocoles afin d'évaluer la consommation énergétique de chacun des deux, de plus, nous vérifions l'effet de la dégradation de s ressources en énergie des capteurs due au attaques simulées.

4.1. Paramétrage de la simulation

Nous avons effectué des tests sur des réseaux de petite taille pour montrer l'efficacité de la consommation d'énergie qui n'a aucune dépendance avec la taille de réseau, ce qu'on va prouver plus tard. Donc nous avons simulé des réseaux de taille de 10, 20, 30, 40 nœuds durant 500 secondes, 700 secondes et 900 secondes, et ainsi l'écart de la consommation va apparaitre et prendre une valeur significative à

partir du 3iem round initialement proche ou presque de celle enregistrée sur LEACH durant les premiers rounds.

4.2. Consommation d'énergie sur un échantillon de 20 nœuds



Graphe 1 : Energie consommée par nœud

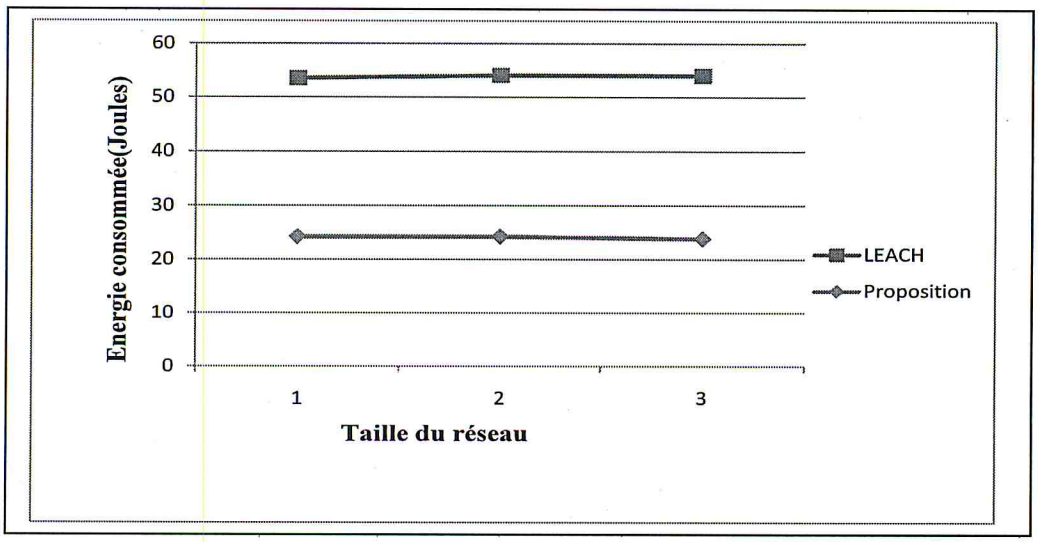
Nous pouvons vérifier, en analysant le résultat de ce graphe, la consommation réduite par chaque capteur dans le protocole proposé par rapport aux capteurs qui utilisent le protocole LEACH. D'autre part, les sommets du graphe représentent les Clusters Heads puisqu'ils consomment beaucoup plus d'énergie pour leurs rôles supplémentaires (agrégation, l'organisation du cluster avec l'envoi des slots et code CDMA aux membres…). On remarque également deux sommets du graphe de notre protocole qui représentent les Cluster Heads du premier round a cause de l'étape de formation des grappes associée a ce round, par contre les Clusters Heads qui suivent le premier round ne font qu'agréger les données captées et transmises par les membres du cluster et envoyer le résultat de cette agrégation aux nœud puits. Une autre remarque apparait dans le graphe approprié à la solution proposée présente l'un de ses sommets, le plus éloigné, a une consommation d'énergie élevée par rapport à la consommation des autres, c'est le cas aussi d'un cluster qui contient beaucoup plus de membres dans son cluster, donc ce que provoque logiquement un nombre de message échangés plus élevé que les autres.

4.3. Variation de consommation d'énergie moyenne au nombre de nœuds du réseau

On va présenter les résultats des tests effectués sur des réseaux de taille différentes pendant une même durée de 700 secondes afin d'évaluer la variation de la consommation d'énergie en fonction de la taille du réseau.

Nombre de nœud	10	20	30
La consommation moyen d'énergie dans LEACH (joules)	29,299	29,791	30,865
La consommation moyenne d'énergie dans le Protocole proposée	24,239	24,271	23,865

Tableau 1 : Variation de la consommation selon le nombre de nœuds dans le réseau



Graphe 2 : Variation de la consommation selon le nombre de nœuds dans le réseau

Comme l'illustre les résultats des tests effectués sur le tableau et interprétés dans le graphe, la consommation d'énergie au niveau de chaque capteur n'a aucune dépendance avec la taille du réseau puisque la topologie du protocole hiérarchique les rend trop scalable, et cela quand le nombre des nœuds déployées augmente, le

nombre des Clustrs Heads augmente et les nouveaux nœuds vont être affectés aux nouveaux CHs pour former des nouveaux clusters indépendants aux clusters visités déjà, donc chaque capteur garde la même consommation due a ses opérations effectuées quelque soit la taille du réseau.

4.4. Comparaison de la consommation d'énergie dans les deux protocoles

Ce tableau montre la consommation d'énergie totale par chaque protocole durant (500secondes, 700secondes, 900secondes) dans des réseaux de tailles différentes.

	10 nœuds			20 nœuds			30 nœuds		
LEACH (joules)	500	700	900	500	700	900	500	700	900
	196,58	292,992	384,82	396,82	595,82	823,37	603,20	904,45	1193,03
Protocole Proposée	165,74	246,753	317,43	349,76	485,42	617,81	532,37	715,97	936,69
% du conservation d'énergie	%18,68	%15,78	%17,41	%11,85	%18,32	%24,96	%11,74	%20,83	%21

Tableau 2 : Variation de consommation entre les deux protocoles

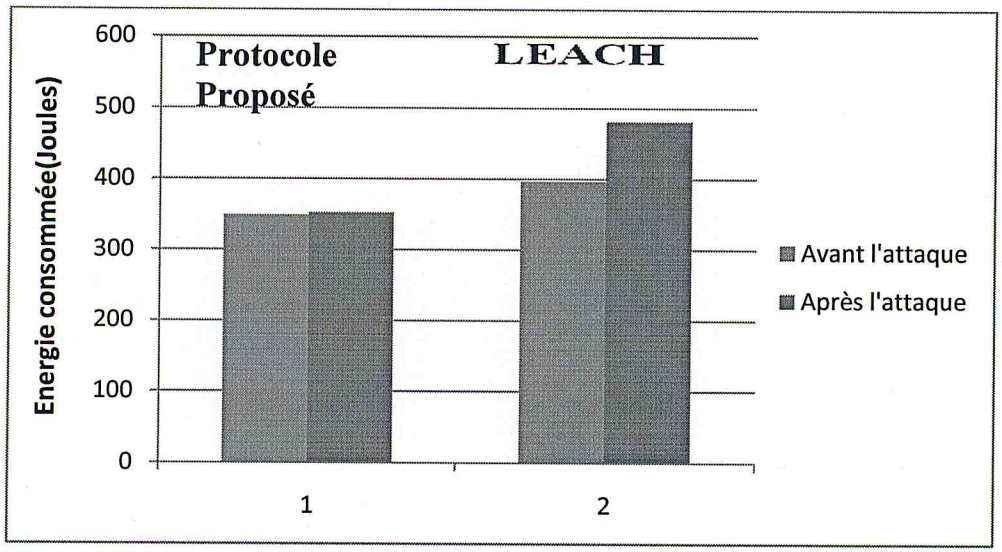
Les résultats obtenues prouve l'efficacité de la stratégie présentée dans le protocole proposé vu l'écart étendu au cours du temps a cause des messages échangés durant la phase d'initialisation lors de la formation des grappe qui se répète à chaque round dans LEACH donc ils provoquent une consommation additionnelle, par contre, dans le protocole proposé les capteurs attendent leurs slots pour envoyer leurs données directement puisque les Clusters Heads sont déjà formés.

4.5. Simulation de l'attaque Sink Hole

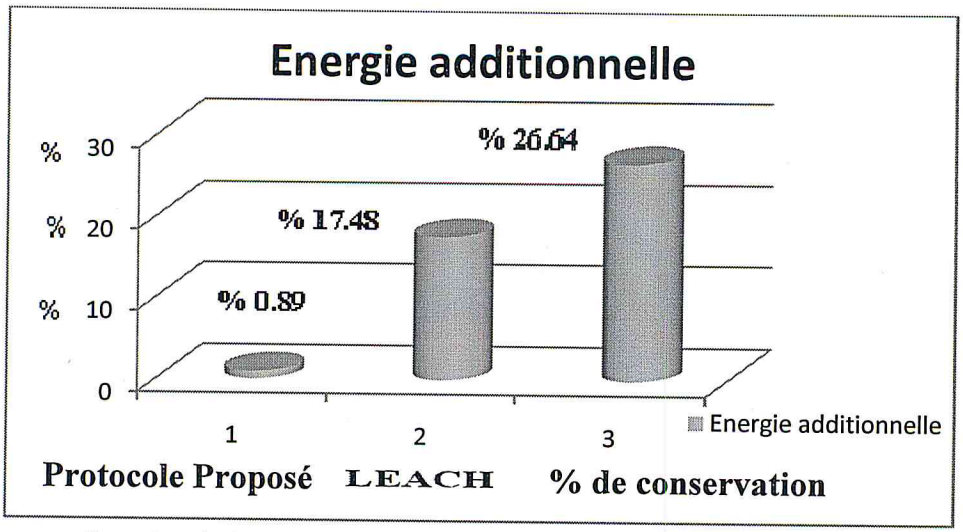
Dans cette partie, nous étudions les conséquences d'attaques de type sink hole sur les deux protocoles afin de comparer leurs consommations énergétiques.

N=20 nœuds t=500 seconds	Solution	Sink Hole contre solution	LEACH	Sink hole contre LEACH
Consommation totale (joule)	349.599	352.788	396.826	480.911
Energie additionnel consommée après l'attaque	% 0.89		%17.48	
Différance de consommation entre les deux protocoles après l'attaque	%26.64			

Tableau 3 : la consommation d'énergie avant et après l'attaque Sink Hole



Graphe. 3 : La consommation d'énergie avant et après l'attaque Sink Hole



Graphe 4 : L'énergie additionnelle due à l'attaque Sink Hole

Comme l'illustre le tableau et le graphe 4, nous pouvons apercevoir clairement la stabilité de la consommation d'énergie approximativement, avant et après l'attaque, car les nœuds ignorent le contenu des messages de l'attaquant grâce au service d'authentification utilisé, d'autre part, on remarque l'effet de cette attaque sur le protocole LEACH qui ne contient aucun mécanisme de sécurité traduite par une augmentation de la consommation d'énergie due aux messages d'annonces lancés par chaque capteur causés par la valeur des probabilité fausses déclarées par le nœud malicieux (l'attaquant) permettant aux capteurs d'être des Clusters Heads.

Conclusion

Dans ce chapitre, nous avons commencé par analyser des difficultés de notre problématique qui consiste a trouver une solution protocolaire sécurisée et efficace en énergie et choisir des solutions qui présentent de nombreux avantages, et on les a comparées au protocole LEACH. Nos solutions exploitent les insuffisances du protocole LEACH dans la gestion de la topologie du réseau et son comportement naïf contre les attaques sur ses nœuds.

Par la suite, on a présenté notre protocole proposé en expliquant ses contributions, son intérêt et ses objectifs, son implémentation ainsi que son déroulement dans les deux cas qui nous intéressent (absence et existence des attaques).

Enfin et après différents scénarios de simulation, nous avons constaté l'efficacité du protocole en terme de la consommation énergétique et de sécurité en effectuant des tests sur des réseaux de taille dissemblable et durant des délais différents.

Conclusion générale et perspectives

Dans ce travail, nous avons mis en avant les caractéristiques essentielles et les notions fondamentales des réseaux de capteurs sans fil. Nous avons étudié plus particulièrement les notions de routage, de sécurité et d'énergie par une définition complète des contraintes, des besoins, des défis et des moyens, de chacune d'elles, mis à disposition des nœuds capteurs du réseau pour acheminement correct, sécurisé et économe en énergie.

Plusieurs protocoles sont présentés et plusieurs classifications ont été établies. Nous étions intéressés très particulièrement aux protocoles hiérarchiques pour leur gestion du réseau d'une manière à minimiser l'énergie consommée et la bande passante allouée. Nous avons tout de même exploités les insuffisances de ce type de protocoles, notamment en reformation des clusters, pour proposer une solution capable de résoudre ce problème et permettre ainsi au réseau de conserver une énergie considérable. Egalement, une taxonomie d'attaques et de solutions sont étudiées, et à partir des failles détectées, une solution simple et efficace est dégagée. Notre solution de sécurité utilise les fonctions de hachage pour calculer le code d'authentification MAC, facile à mettre en œuvre et très difficile à recalculer par un nœud malicieux.

Les résultats obtenus par notre protocole de routage hiérarchique ont montré l'intérêt de nos méthodes d'organisation et de sécurisation du réseau sur l'énergie totale consommée. Malgré ces résultats encourageants, il ne nous empêche pas d'envisager plusieurs perspectives pour des travaux futurs, parmi lesquels :

- Améliorer la conservation d'énergie en mettant les nœuds capteurs en mode veille pendant les périodes hors slot.
- Trouver des mécanismes qui détectent les nœuds capteurs isolés lors du déploiement ou après un cycle de vie du réseau provoqués par des attaques (compromission des nœuds) ou l'épuisement des ressources en énergie.
- Minimiser le nombre de messages échangés lors du processus d'adhésion des nœuds aux clusters au lancement de chaque nouveau round.

- Développer le mécanisme de sécurité, qui reste assez simple malgré son efficacité, pour prendre en charge des attaques avancées.

Bibliographie :

[YCL08] : Yacine Challal « Réseau de capteur sans fils » livre, version 1, pages : 11-26, 37-97, 2008.

[J&A09] : Jun Zheng, Abbas Jamalipour « Wireless Sensor Networks-A Networking Perspective » livre,version1, pages-229-237, 2009.

[JCD10] : Jacquot Aurélien, Chanet Jean-Pierre, De Sousa Gil « Les réseaux de capteurs sans fil au service des applications agro-environnementales » Séminaire Réseaux de capteurs sans fils, LabSTICC, Faculté de sciences Brest, pages : 1-11,2010.

[B&D09] : Berrachedi Amel, Diarbakirli Amina « Sécurisation du protocole de routage hiérarchique LEACH dans les réseaux de capteurs sans fil », Thèse d'ingéniorat, Ecole nationale Supérieure d'Informatique (E.S.I) Oued-Smar, Alger, pages : 17-96, 2009.

[DIE07] : Dhib Eya « Routage avec QoS temps réel dans les réseaux de capteurs », Thèse d'ingéniorat, Ecole supérieur de communication de Tunis, pages 7-25 : 2007.

[YSY10] : Yousef Yaser « Routage pour la Gestion de l'Energie dans les Réseaux de Capteurs Sans Fil », Thèse doctorat, Université de Haute Alsace Faculté des Sciences et Techniques, pages : 8-32, 2010.

[KCI10] : Kaci BADER « Détection d'intrusion dans les réseaux de capteurs sans fils », Rapport de stage, Université IFSIC-Rennes 1, pages : 9-12, 2010.

[ACA11] : Adel Chouha « Traitement et Transfert d'images Par Réseau de Capteurs sans Fil » Mémoire de Magister, Université de Batna pages : 14-39, 2011.

[FZB09] : Fatima Zohra Ben Hamida « Tolérance aux pannes dans les réseaux de capteurs sans fils », Mémoire de Magister, Ecole nationale Supérieure en Informatique Oued-Smar Alger, pages : 5-15, 2009.

[BBC08] : Hatem Bettahar, Abdelmadjid Bouabdallah, Yacine Challal « Les Réseaux de capteurs (GCB10 Wireless Sensor Networks) », Cours, Université de Technologie de Compiègne, France, pages : 1-31, 2008.

[K&N04] : Lyes Khelladi & Nadjib Badache « Les réseaux de capteurs : état de l'art » rapport, laboratoire de systèmes informatique USTHB, pages :7-35, 2004.

[CLY08] : Yacine Challal « Réseau de capteur sans fils -Sécurité» Cours, Université de Technologie de Compiègne, France, pages : 4-16, 2008.

[SEB11] : Salah-Eddine Benbrahim «Défense contre l'attaque d'analyse de trafic dans les réseaux de capteurs sans fil (GCB10) », Mémoire présenté pour l'obtention de diplôme de Maîtrise ès sciences appliquées, Université de Montréal, pages : 25-49 2011.

[RHK11] : Rahim Kacimi « Premiers pas avec TinyOS », Tutoriel, ENSEEIHT Télécommunications et Réseaux, pages : 1-7, 2011.

[YGB10] : Yong, Aguilar Andres, Gonzalez Andres, Barroux Mickael « agrégation de données dans les réseaux de capteurs », Thèse d'ingéniorat, Université de technologie Compiègne, pages : 1-15, 2010.

[SRB06] : Samra Boulfekhar « Approches de minimisation d'énergie dans les réseaux de capteurs » Mémoire de Magister, Université Abderahmane Mira de Bejaïa, pages : 7-63, 2006.

[KHR09]: Rahim Kacimi « Techniques de conservation d'énergie pour les réseaux de capteurs sans fils » Thèse doctorat, Université de Toulouse, pages : 13-30, 2009.

[PRJ03]: Chong, Kumar « Sensor Networks: Evolution, Opportunities, and Challenges. In Proceedings of the IEEE », vol.91, no.8, pages : 1247-1256, 2003.

[DOR10] : Mohammed El Mehdi Diouri « Proposition d'un mécanisme de lutte contre les attaques Sybille dans les réseaux de capteurs sans fil » Thèse d'ingéniorat, INSA Lyon, pages : 5-35, 2010.

[FMD10] : Fatima Mourchid « Nouveau modèle pour le positionnement des senseurs avec contraintes de localisation » Mémoire présenté pour l'obtention de diplôme de Maîtrise ès sciences appliquées Université Montréal, école polytechnique de Montréal, pages : 5-21,2010.

[SMD08] Sofiane Moad « Optimisation de la consommation d'énergie dans les réseaux de capteurs sans fil », Rapport de stage, Université : IFSIC-Rennes 1, pages : 6-15, 2008.

[ALM09] : Chamam Ali « Mécanisme optimisés de planification des états des capteurs pour la maximisation de la durée de vie dans les réseaux de capteurs sans fil », Mémoire présenté pour l'obtention le grade philosophie docteur, l'école polytechnique de Montréal, pages : 26-44, 2009.

[PUJ05] **:** Pujolle, « Les réseaux Editions 2005 », Livre, éditions Eyrolles, pages :117-136, 2005.

[YWH03]**:** Ye W., Heidmann J., « Medium Access Control in Wireless Sensor Networks», These, USC/ISI Technical Report ISI-TR-580, pages: 57-66, 2003.

[BBY11] : Walid Bechkit, Abdelmadjid Bouabdallah et Yacine Challal « Un Prototype de Réseaux de Capteurs sans Fils pour l'Agriculture et le Contrôle de l'Environnement » conférence CFIP 2011 - Colloque Francophone sur l Ingénierie des Protocoles (2011), Université de Technologie de Compiègne, pages : 1-4, 2011.

[KBN09] : Kamal Beydoun « Conception d'un protocole de routage hiérarchique pour les réseaux de capteurs » Thèse doctorat, Université de Franche Comte, pages : 37-59, 2009.

[MIN11] : Mohamed Aissani « Optimisation du routage dans les réseaux de capteurs pour les applications Temps-Réel » Thèse doctorat, Université Pris-Est et l'Université USTHB, pages : 7-32, 2011.

[MBA07] : 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 USTHB, pages : 7-25, 2007.

[M&K10] : Naourez Meriji, Farouk Kamoun « Algorithme de routage Hiérarchique MHEED à Plusieurs Sauts pour les Grands Réseau de capteur » Conférence SETIT 2007, Ecole nationale des sciences informatique (ENSI), pages :2-7, 2007.

[D&G08] : David Martins, Hervé Guyennet, « Etat de l'art : Sécurité dans les réseaux de capteurs sans fil » rapport, *SAR*-SSI , pages :1-15 ,2008.

[AOT07] : Abdelraouf Ouadjaout « La sécurité et la fiabilité´e du routage dans les réseaux de capteurs sans fils » Thèse d'ingéniorat, Université USTHB Alger, pages : 3-36, 2007.

[CHE09]: Samia Chelloug , Mohamed Benmohamed, « Prédiction de la Mobilité pour un Routage Efficace en Energie dans les Réseaux de Capteurs Mobiles », Conférence JDIR'09: 10èmes Journées Doctorales en Informatique et Réseaux Université Mentouri, pages : 1-5, 2009.

[RBM10]: Rajashr, Biradar, Patil, Sawant, Mudholkar « Classification and comparison of routing protocols in wireless sensor networks », UbiCC Journal, Kolhapur (India) pages: 3-8, 2010.

[MLC10]: Mickaël Cartron, « Vers une plate-forme efficace en énergie pour les réseaux de capteurs sans fil », Thèse doctorat, Ecole Nationale Supérieure de Sciences Appliquées et de Technologie, Rennes, pages : 13-18, 2006.

[GCB10] : Gerard Chalhoub « Routage et MAC dans les réseaux de capteurs sans fil », Thèse doctorat, Clermont Université, pages 26-30, 2010.

[WEB1]:Yassine Chellal, Réseaux de Capteurs SansFils, http://www4.utc.fr/~sit60/co/Module_RCSF_48.html, (2012)

Annexe

Installation du SE TinyOs 1.x sous Linux

Deux façons sont possibles pour installation TinyOs. Soit installer une VM (machine virtuelle) ou bien installer TinyOs sur un système d'exploitation hôte. Lors d'une installation sur un système hôte (tel est notre cas avec une installation de tinyos sur le SE Ubuntu), soit, on utilise un paquet Debian ou on l'installe manuellement avec RPM. Pour notre cas, nous allons nous intéresser à une installation sur un Os avec un paquet Debian. La méthode est la suivante :

i. Retirez tout ancien référentiel TinyOs du fichier : / etc / apt / sources.list et ajoutez la ligne suivante : Un ensemble commun prend en charge toutes les distributions basées sur Ubuntu Debian Squeeze. Spécifiant la version lucide devrait bien fonctionner :

deb http://tinyos.stanford.edu/tinyos/dists/ubuntu **lucid main**

ii. Mettez à jour votre cache de dépôts : **sudo apt-get update**

iii. Exécutez la commande suivante pour installer la dernière version de TinyOs et tous ses outils pris en charge : **sudo apt-get install tinyos**

Ceci vous donnera probablement un message vous invitant à choisir entre plusieurs versions disponibles. Un exemple à exécuter ensuite est : **sudo apt-get install tinyos-1.x**

Ajoutez la ligne suivante à votre fichier ~ /. Bashrc ou ~ /.profil dans votre répertoire home afin de mettre en place l'environnement pour le développement TinyOS lors de la

Connexion **#Sourcing the tinyos environment variable setup script**

source /opt/tinyos-2.1.1/tinyos.sh