RÉPUBLIQUE ALGERIENNE DÉMOCRATIQUE ET POPULAIRE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ ABOU BEKR BELKAID - TLEMCEN
FACULTÉ DE TECHNOLOGIE
DÉPARTEMENT DES TÉLÉCOMMUNICATIONS

T H È S E

pour obtenir le titre de

Docteur en Télécommunications

Option : Systèmes et Réseaux de Télécommunications

Présentée par

TABET HELLEL Chifaa Fouzia

Mécanismes d'auto-organisation pour la tolérance aux pannes dans les réseaux de capteurs sans fil

soutenue le 30 Juin 2015 devant le jury composé de :

Président :	FEHAM Mohammed	Professeur	Université de Tlemcen
Examinateurs :	BOUKLI HACENE Sofiane	MCA	Université de Sidi Bel Abbès
	MANA Mohamed	MCA	Université de Tlemcen
	HAMMAD Ahmed	MCA	Université de Franche-Comté, France
Directeur :	LEHSAINI Mohamed	MCA	Université de Tlemcen
Co-directeur :	GUYENNET Hervé	Professeur	Université de Franche-Comté, France

Remerciements

A faire en dernier :-)

Table des matières

Table des figures

Liste des tableaux

Introduction générale

Les progrès technologiques incessants ont permis une évolution perpétuelle dans le domaine des réseaux de capteurs sans fil (RCSF) en raison de leur déploiement dense dans une gamme d'applications très variée du domaine militaire au domaine civil (surveillance environnementale, assistance médicale, contrôle industriel, etc.). Ces applications s'intéressent à de nouveaux petits dispositifs à faible coût et multifonctionnels appelés "capteurs" qui sont capables d'interagir avec leur environnements et ils sont responsables de la collecte des données environnementales et les acheminer vers un point de collecte distant directement ou via une communication multi-sauts. Ces capteurs sont limités en termes de capacité de stockage, de traitement et surtout d'énergie puisqu'ils sont alimentés par des piles qui sont généralement non rechargeables et non remplaçables en raison de l'endroit de déploiement de ces nœuds capteurs. Dans certaines applications les capteurs sont déployés dans des zones hostiles dont le changement de batteries est quasiment impossible et même ils sont menacés par une destruction physique qui peut être accidentelle ou intentionnelle par des ennemis, ce qui les rend inutilisables suite à la panne reproduite.

La consommation d'énergie occupe une place exceptionnelle dans les RCSF puisqu'elle se répercute sur la durée de vie du réseau. Plusieurs travaux de recherche se sont focalisés sur l'efficacité énergétique comme facteur clé dans les protocoles de communication car dans ce type de réseaux, chaque capteur est alimenté par une source d'énergie limitée et généralement irremplaçable. Cette contrainte rend ce dernier victime d'un épuisement d'énergie quand il réalise une communication (transmission, réception) puisque les communications et en particulier les transmissions sont les opérations les plus coûteuses en terme de consommation d'énergie [1]. Par conséquent, les algorithmes conçus pour les RCSF doivent donner plus d'importance à la conservation d'énergie pour permettre une extension de la durée de vie du réseau.

Les RCSF sont soumis à des pannes puisqu'ils sont composés de dispositifs sans fil qui sont souvent peu fiables à cause des changements dans l'environnement. En outre, les capteurs sont alimentés par des batteries dont la durée de vie est limitée et ils peuvent être endommagés accidentellement par des

animaux ou intentionnellement par des êtres humains. Pour faire face à ces pannes, des techniques pour la fiabilité de routage dans les RCSF tels que [2–4] ont été proposés, mais pour qu'elles soient efficaces, elles doivent dépendre d'une topologie de réseau qui assure des chemins alternatifs vers la station de base. Cela exige que le déploiement des RCSF soit planifié pour s'adapter à tout changement de topologie, de telle sorte que lorsque des pannes se produisent les protocoles de routage peuvent toujours continuer à assurer une livraison fiable vers la station de base. Notre contribution est une solution qui permet d'instaurer la tolérance aux pannes lors du déploiement d'un RCSF par l'utilisation de nœuds relais supplémentaires ou le choix des nœuds les plus fiables comme nœuds relais. De ce fait, la tolérance aux pannes est l'un des facteurs les plus importants qui doit être pris en considération afin d'assurer la fiabilité de livraison dans les RCSF et leur fonctionnement sans aucune interruption en cas d'occurrence de pannes. Par ailleurs, l'épuisement d'énergie des nœuds capteurs reste toujours l'une des causes les plus fréquentes et les RCSF sont généralement déployés dans des environnements très hostiles où l'intervention humaine est quasiment impossible ce qui les rend vulnérables et sujets à des pannes. Ainsi l'absence de sécurité physique des capteurs et aussi la fragilité des communications radios provoquent les pannes dans ce type de réseaux. Par conséquent, suite à ces contraintes, le réseau peut éventuellement perdre ses performances puisque la panne d'un seul capteur peut affecter le fonctionnement global du réseau et créer un réseau non connexe ce qui pourrait empêcher l'acheminement de données vers un centre de contrôle distant. Cette anomalie pourra avoir des conséquences négatives dans les applications critiques telles que les applications militaires ou les applications médicales. De ce fait, la tolérance aux pannes est considérée comme un facteur déterminant dans les applications critiques. En outre, il est généralement indispensable que les protocoles conçus pour la tolérance aux pannes tiennent compte des mécanismes de minimisation de la consommation d'énergie dans le but d'avoir un réseau fiable avec une durée de vie maximale.

Dans cette optique, plusieurs travaux de recherche sont engagés dans le développement de nouvelles approches qui permettent de satisfaire les exigences liées à la tolérance aux pannes dans les RCSF. Dans cette thèse, nous proposons deux nouvelles contributions pour la tolérance aux pannes dans les

RCSF qu'on applique sur le protocole de routage LEACH (Low-Energy Adaptive Clustering Hierarchy) [5]. Nous avons choisi d'améliorer les performances de LEACH dans un environnement non-idéal puisque ce dernier est considéré comme l'un des meilleurs protocoles en termes de conservation d'énergie. La première contribution incorpore la tolérance aux pannes afin de rendre le protocole tolérant aux pannes dans un environnement non-idéal. La deuxième contribution implique le modèle Log-Normal (Lognormal Shadowing Model) (LNS) [6] afin d'adapter le protocole LEACH à un environnement réaliste en prenant en compte les fluctuations du signal radio causées par la présence d'obstacles et des interférences ainsi que la distance séparant les nœuds communicants.

Cette thèse s'articule autour de cinq chapitres avec une introduction générale et une conclusion générale.

Dans le premier chapitre, nous présentons un aperçu sur les différents concepts des réseaux de capteurs sans fil et nous citons leurs domaines d'applications ainsi que les contraintes liées à ce type de réseaux. Ensuite, nous abordons le concept de tolérance aux pannes dans les RCSF en commençant par les causes des pannes, les techniques de détection de pannes ainsi que les différentes techniques de tolérance aux pannes.

Dans le deuxième chapitre, nous présentons un état de l'art sur les protocoles de routage tolérants aux pannes proposés dans la littérature et nous détaillons par la suite le protocole de routage LEACH et ses versions améliorées conçues pour la tolérance aux pannes.

Dans le troisième chapitre, nous proposons une solution efficace tolérante aux pannes qui consiste à améliorer le protocole de routage LEACH. Dans cette solution, nous avons intégré une communication multi-sauts entre les clusterheads et la station de base pour minimiser la consommation d'énergie. En outre, un chemin alternatif est ajouté pour remplacer le chemin principal en cas d'éventuelle défaillance d'un des cluster-heads qui le composent. Les résultats de simulation de cette contribution ont montré qu'elle est plus efficace en la comparant avec la version originale de LEACH.

Dans le quatrième chapitre, une nouvelle version du protocole LEACH est donnée. Cette version tient compte de la qualité des liens lors des communications intra-cluster en utilisant le modèle LNS. Ce modèle calcule la pro-

babilité de réception sans erreur d'un paquet de données entre deux nœuds communicants en fonction de la distance qui les sépare. Si cette probabilité est inférieure à un seuil prédéfini, une communication multi-sauts est incorporée pour assurer la fiabilité de transmission de paquets. Cette contribution a montré son efficacité puisqu'elle a permis d'adapter le protocole LEACH à un environnement non-idéal.

Dans le cinquième chapitre, un nouveau protocole de routage hiérarchique tolérant aux pannes est conçu pour les réseaux de capteurs. Ce protocole est adapté à un environnement non idéal qui peut être représenté soit par le modèle lognormal shadowing ou le modèle probabiliste.

Chapitre 1

Les Réseaux de Capteurs Sans Fil (RCSF)

1.1 Introduction

Les avancées récentes dans le domaine de la micro-électro-mécanique et les technologies de communication sans fil ont permis le développement des nœuds de capteurs à faible coût et à faible puissance. Ces capteurs possèdent un ou plusieurs composants de mesure pour collecter différentes grandeurs environnementales telles que la température, l'humidité, la luminosité, etc... Ils sont déployés soigneusement ou aléatoirement dans un champ d'intérêt et communiquent entre eux via un support sans fil formant ensemble un réseau de capteurs sans fil. Ce type de réseaux a subi une attention attractive au cours de cette dernière décennie en raison de sa large variété d'applications dans plusieurs domaines qui ont permis de changer notre façon de vivre en nous permettant d'interagir avec notre environnement. Les RCSF sont souvent caractérisés par leur déploiement dense et à grande échelle avec une limitation de ressources telles que la capacité de stockage, de traitement et d'énergie. Dans ce chapitre, nous donnons une brève présentation des RCSF, leurs caractéristiques et aussi la nécessité d'incorporer la tolérance aux pannes dans ce type de réseaux.

1.2 Un réseau de capteurs sans fil

Un réseau de capteurs sans fil est un ensemble de petits dispositifs appelés "capteurs" qui sont dispersés dans un champ d'intérêt en vue de collecter des informations et les router directement ou via une communication multi-sauts à un nœud puissant appelé "station de base" qui est connecté à une machine via internet ou bien satellite, comme le montre la figure 1.1.

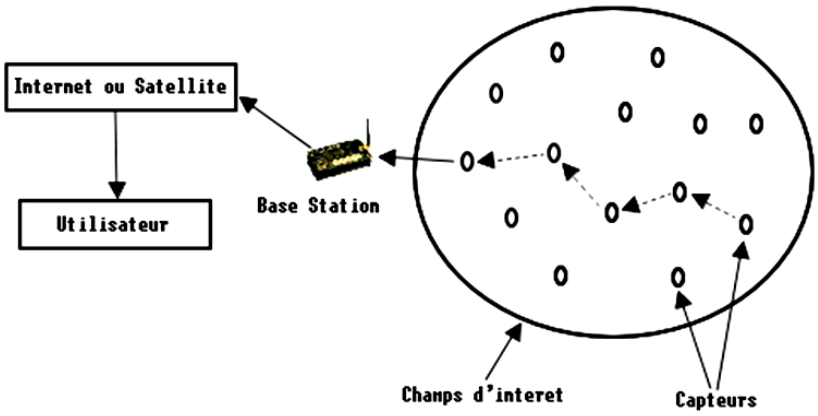

FIGURE 1.1 – Architecture d'un réseau de capteurs sans fil

La portée de transmission des nœuds capteurs dépend de cinq facteurs : la puissance d'émission des paquets de données, la fréquence, la modulation, la localisation et les conditions météorologiques [7]. Elle peut aller de quelques mètres à des centaines de mètres. Par exemple, la portée de transmission de TelosB est de 75m à 100m outdoor et de 20m à 30m indoor [8]. De ce fait, en fonction de déploiement des nœuds capteurs, ils ne seront pas forcément à la portée radio de la station de base. D'où, ils doivent collaborer entre eux pour envoyer les données collectées jusqu'à la station de base via un schéma de routage multi-sauts. Les conditions de déploiement vont alors poser de nouvelles contraintes et de nouveaux défis.

1.2.1 Architecture d'un nœud de capteurs sans fil

Un nœud de capteurs est un dispositif électronique chargé de collecter les informations captées à partir de l'environnement qui l'entoure, les traiter ensuite les transmettre à une destination tout en consommant une certaine énergie [7]. Il est composé d'une unité d'acquisition de données, unité de traitement, unité de transmission, une batterie, et éventuellement d'un système de rechargement de batteries ou un système de localisation. La figure 1.2 résume les différents composants d'un capteur.

- **Unité d'acquisition :** Cette unité est composée de deux unités : des capteurs qui sont capables de mesurer les variations des caractéristiques physiques de leur environnement, et des convertisseurs analogique-

numérique (ADC) [1] ; qui sont chargés de convertir ces variations en signaux numériques afin de pouvoir être traitées par l'unité de traitement.

- **Unité de traitement :** Elle possède deux interfaces ; une pour l'unité d'acquisition et l'autre pour l'unité de transmission. Elle se compose d'une unité de stockage et d'un processeur. Elle traite les informations acquises à partir de l'unité d'acquisition et les envoie à l'unité de transmission.
- **Unité de transmission :** Elle est responsable de toutes les émissions et les réceptions via un support de communication radio qui permet aux capteurs de communiquer entre eux.
- **Batterie :** C'est une source d'énergie par laquelle tous les composants du capteur sont alimentés. Elle correspond généralement à une pile ou une batterie qui s'épuise par le temps. La consommation d'énergie est devenue un facteur critique que doit prendre en compte toutes les applications de capteurs due aux limitations des ressources énergétiques des nœuds. Pour résoudre le problème d'énergie une réalisation récente d'une unité d'alimentation en utilisant des panneaux solaires [9,10]. Cependant, ce problème persiste puisqu'on n'a pas toujours la possibilité de s'alimenter en énergie solaire. D'où, dans presque tous les travaux de recherche on traite la problématique concernée conjointement avec la consommation d'énergie.

Il existe des capteurs qui sont dotés d'un système de localisation tel que le GPS (Global Positioning System) pour être repérer ou pour repérer les capteurs qui se trouvent dans leur voisinage.

1.2.2 Les caractéristiques liées aux nœuds capteurs

Les capteurs ont des caractéristiques intrinsèques [11], dans ce qui suit, nous citons les plus importantes :

1.2.2.1 L'énergie

L'énergie est considérée comme une ressource précieuse dans les RCSF. Elle représente la contrainte la plus importante dans la majorité des applications

1. ADC : Analog to Digital Converter

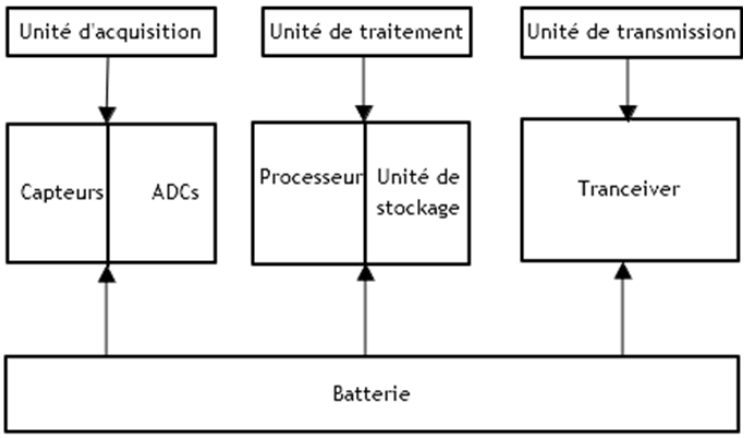

FIGURE 1.2 – Architecture d'un capteur

à base de RCSF puisque chaque nœud est alimenté par une batterie qui n'est généralement ni rechargeable, ni remplaçable. De ce fait, toute application dédiée à fonctionner sur un nœud capteur devrait prendre en considération la contrainte d'énergie pour que ce dernier survive pour une longue durée de vie. D'où pour préserver son énergie, il devrait passer en mode actif que lorsqu'il a de l'information à transmettre ou à recevoir et éviter les transmissions et les réceptions redondantes. Par ailleurs, les communications sont les opérations les plus coûteuses en termes de consommation d'énergie [1].

1.2.2.2 Portée de transmission

La portée de transmission d'un nœud capteur dépend des capacités de rayonnement des antennes et la puissance du signal mis en jeu tel que si la distance entre deux nœuds est assez grande, le risque de perte de données échangées entre eux est plus probable et le coût énergétique sera élevé.

1.2.2.3 Puissance de traitement et de stockage

En raison de coût et de miniaturisation des capteurs, généralement des microcontrôleurs sont choisis comme unité de traitement pour les capteurs [8,12], comme la plateforme Telosb de Crossbow qui est équipée d'un microcontrôleur MSP430 à 8 MHz. La puissance de stockage et de traitement des microcontrôleurs est relativement faible alors que les nœuds dans un réseau sont chargés d'accomplir plusieurs tâches telles que l'agrégation, la compression et même

des fois le calcul cryptographique très complexe dans les applications de sécurité. Pour pallier à cette limitation, les nœuds doivent coopérer entre eux pour atteindre un objectif collectif.

1.3 Les différents facteurs de conception d'un RCSF

La conception des RCSF est influencée par plusieurs facteurs qui doivent être traités par des technologies persistantes et d'une manière appropriée :

1.3.1 La durée de vie du réseau

La vie d'un RCSF dépend de la période de temps durant laquelle le réseau est opérationnel et elle est liée à la vie nodale c'est-à-dire à la vie des nœuds capteurs qui le constituent puisque la quantité dominante d'énergie consommée par un nœud capteur correspond à la détection, la communication et le traitement de données [13]. Plusieurs définitions ont été proposées dans la littérature pour la durée de vie d'un RCSF. Par exemple dans [14–18], les auteurs ont supposé que la durée de vie d'un RCSF représente le temps pendant lequel le premier nœud épuise son énergie complètement, et dans [19,20], cette durée coïncide avec le temps pendant lequel le premier cluster-head (CH) épuise toute son énergie alors que dans [21], c'est la période pendant laquelle tous les capteurs épuisent leur énergie.

1.3.2 La tolérance aux pannes

Les nœuds capteurs sont sujets à des pannes dues à un épuisement d'énergie,à un problème physique ou une interférence. Par conséquent, ces pannes peuvent causer un dysfonctionnement du réseau et entraver ce dernier à effectuer sa mission dans des conditions favorables. D'où il faudrait instaurer des mécanismes et des protocoles qui permettent de garantir le bon fonctionnement du réseau et assurer la continuité de service quand un ou plusieurs capteurs cessent de fonctionner.

1.3.3 Topologie du réseau

La forte densité des RCSF dans les zones à surveiller nécessite une maintenance continue de la topologie par les nœuds capteurs qui doivent être capables d'adapter leur fonctionnement. Cette maintenance consiste généralement en trois phases : le déploiement (d'une manière aléatoire ou prédéfinie), le post-déploiement (les capteurs peuvent se déplacer ou cessent de fonctionner) et le redéploiement (l'ajout de nouveaux capteurs peut changer la topologie du réseau).

1.3.4 La consommation d'énergie

La limitation des ressources énergétiques rend ce genre de réseaux contraint en termes d'énergie puisque le rechargement ou bien le remplacement de la batterie est souvent impossible. C'est pour cette raison que l'économie d'énergie est la problématique majeure dans de nombreuses applications. Des mesures expérimentales ont montré que, la transmission des données est l'opération qui consomme plus d'énergie alors que les calculs consomment très peu d'énergie [1].

1.3.5 La sécurité

Les RCSF peuvent être déployés dans des endroits critiques où l'absence de la sécurité fait appel à des attaques qui peuvent perturber leur fonctionnement et même exploiter des informations importantes collectées par les capteurs de ces réseaux ou injecter de fausses informations . Dans ce cas de figure, la sécurité est l'une des contraintes essentielles surtout dans les applications critiques telles que les applications militaires ou les applications médicales.

1.4 Domaines d'application des RCSF

L'immense variété des domaines d'applications des RCSF a fait l'objet de plusieurs recherches et de développement universitaire ou industriel. Parmi ces domaines qui ont permis aux RCSF de s'avérer très utiles, on peut citer ; le domaine militaire, le domaine médical, le domaine environnemental, etc.

1.4.1 Application militaire

Les applications militaires ont fortement besoin de ce type de réseaux pour permettre la détection et l'emplacement des ennemis ainsi que la surveillance des zones hostiles. Plusieurs projets ont été développés pour protéger des endroits contre les attaques, la surveillance des zones hostiles, l'avertissement aux attaques biologiques tels que DSN (Distributed Sensor Network) [13] développé par la DARPA (Défence Advanced Research Projects Agency), JBREWS (Joint Biological Remote Early Warning System) [22, 23], etc. La figure 1.3 présente un exemple de l'application des RCSF dans le domaine militaire.

FIGURE 1.3 – Application des RCSF dans le domaine militaire

1.4.2 Application à la surveillance

La surveillance par des capteurs a connu un gain significatif en termes de sécurité et de financement. Dans ce type d'applications, les capteurs peuvent être placés dans des endroits dangereux qui ne sont pas accessibles par des êtres humains, et en cas d'intrusion dans une zone de surveillance, ils remontent immédiatement des alertes au centre de contrôle. Par exemple dans les maisons du futur dites "les maisons intelligentes", il y aurait plusieurs types de capteurs placés à des endroits différents. Ces derniers permettent le contrôle de l'habitat à distance et remontent l'information au propriétaire quand un événement pertinent survient.

1.4.3 Application environnementale

La possibilité des réseaux de capteurs de contrôler les paramètres environnementaux a donné naissance à plusieurs applications à l'instar des applications dans le domaine de l'agriculture, la surveillance de l'environnement, les feux de forêts, etc. Par exemple dans le domaine de l'agriculture les capteurs sont implantés dans le sol et mesurent périodiquement l'humidité. Si ces derniers détectent qu'un secteur est devenu sec une alerte sera remontée au centre de contrôle pour arroser le secteur concerné. Cette application permet d'une part d'augmenter la production agricole et d'autre part économiser l'eau nécessaire à l'arrosage surtout dans les pays qui souffrent de la sécheresse. En outre, dans la surveillance environnementale les capteurs sont chargés de surveiller le niveau de pollution dans l'air [23, 24].

FIGURE 1.4 – Application des RCSF dans la surveillance de l'environnement

1.4.4 Application médicale

Dans le domaine de la médecine, un RCSF est capable de surveiller les données physiologiques de l'être humain par des micro-capteurs qui peuvent être avalé ou bien implanter sous la peau. Les capteurs peuvent capturer les signes vitaux d'un patient en temps réel et les transmettre immédiatement vers un support électronique du médecin. Dans [25, 26], des projets de la prise en charge des personnes âgées sont décrits pour leurs assurer une surveillance continue et leurs promouvoir une certaine autonomie.

1.4.5 Application domotique

Le développement technologique a permis l'embarquement des capteurs dans des appareils utilisés quotidiennement dans une maison [27] tels que, les respirateurs, les réfrigérateurs, les machines à laver, etc. Ces capteurs peuvent communiquer entre eux ou avec un autre réseau via internet pour permettre aux utilisateurs de surveiller ces appareils domestiques localement ou à distance.

L'ensemble des technologies qui permettent d'automatiser et de faciliter la gestion des immeubles avec les systèmes embarqués, est désigné par le terme "Smart Home" [28–30] et cela dans le but de faciliter le mode de vie des utilisateurs et le rend plus écologique avec un confort très élevé.

1.5 Technologies de communication dans les RCSF

La communication dans les RCSF exige des technologies qui prennent en compte des spécificités qui répondent aux exigences de ces réseaux. Dans ce qui suit, on présente un certain nombre de technologies sans fil qui s'adaptent aux RCSF [31] :

1.5.1 Buetooth / IEEE 802.15.4

Bluetooth [32,33]est une technique de communication radio de courte distance, généralement utilisée dans les téléphones mobiles et destinée pour simplifier les connexions entre les appareils électroniques. Le seul inconvénient de cette technologie est sa grande consommation d'énergie. En plus, cette technologie ne pourrait pas connecter un grand nombre d'équipements. D'où, Bluetooth ne pourrait pas être utilisée dans les RCSF denses.

1.5.2 Zigbee

Zig bee [34] est un système de communication sans fil de courte portée destinée pour les applications dans les réseaux personnels sans fil, principalement

adopté dans l'implémentation des RCSF. La technologie Zigbee est caractérisée par sa faible complexité, faible coût, faible consommation d'énergie et faible taux de transmission de données, et aussi une compatibilité avec des dispositifs fixes ou mobiles. La norme IEEE 802.15.4 possède la plus faible demande de consommation d'énergie. C'est la norme idéale pour les équipements qui ont des ressources limitées tels que les RCSF.

1.5.3 Dash7-ISO/IEC 18000-7

DASH7 [35] est une nouvelle technologie de communication qui utilise la norme ISO/IEC 18000-7. Elle est caractérisée par sa faible consommation d'énergie ce qui permet d'augmenter la durée de vie de la batterie. Cette durée peut aller jusqu'au plusieurs années. Elle est caractérisée aussi par sa grande portée comparativement aux autres normes.

1.6 Architecture protocolaire

Elle peut être utilisée par la station de base ou bien par les nœuds capteurs. Elle est constituée de cinq couches : une couche d'application, une couche de transport, une couche réseau, une couche de liaison de données et une couche physique, et de trois plans : un plan de gestion d'énergie, un plan de gestion de mobilité et un plan de gestion des tâches [36]. La figure 1.5 illustre les différentes couches et les différents plans dans la pile protocolaire. Cette pile [7] combine l'énergie et le routage, associe les données avec les protocoles actifs au niveau de la couche réseau et communique via un support sans fil. Les plans de gestion d'énergie, de mobilité et des tâches contrôlent et gèrent la consommation d'énergie, les mouvements et la répartition des tâches d'un capteur. Ces plans aident les nœuds à collaborer et partager les ressources entre eux, et aussi à équilibrer la consommation d'énergie pour prolonger la durée de vie du réseau.

La communication dans les réseaux de capteurs nécessite la mise en place d'un protocole de routage afin de gérer les transmissions de données effectuées par les capteurs pour atteindre la station de base. Cette gestion n'est pas facile car la topologie d'un réseau de capteurs est dynamique : un nœud capteur pourrait devenir inaccessible quand il épuise sa batterie ou détériore

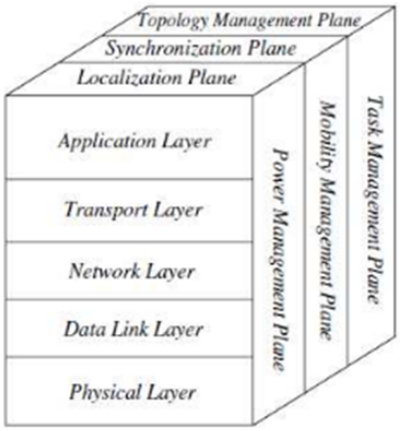

FIGURE 1.5 – Pile protocolaire

ses capacités de communication à cause des conditions environnementales. Les protocoles de routage doivent utiliser des mécanismes permettant d'une part de minimiser la consommation d'énergie et d'autre part garantir la fidélité de routage c'est-à-dire entre tout nœud capteur et la station de base il devrait exister au moins un chemin.

1.7 La tolérance aux pannes dans les RCSF

Après le déploiement des RCSF, un nœud capteur peut avoir une défaillance globale à n'importe quel moment durant son déploiement. Cette défaillance peut être due à un épuisement d'énergie, à une destruction physique accidentelle ou intentionnelle, ou à une interférence. La panne d'un nœud capteur aura éventuellement un impact sur le fonctionnement global du réseau. Pour pallier à cette anomalie, il faut instaurer la tolérance aux pannes qui permet de garantir le fonctionnement du réseau sans interruption même en présence de pannes.

1.7.1 Les pannes

La panne du système se produit lorsque son état devient inactif et fournit un résultat erroné. Elle est la conséquence d'une ou de plusieurs erreurs où une erreur représente un état invalide du système à partir duquel la poursuite de l'exécution est susceptible de conduire à une panne. En outre, une faute

est la première cause de l'erreur qui pourrait provoquer la panne du système. La figure 1.6 montre le séquencement faute, erreur et panne.

FIGURE 1.6 – La trilogie Faute/ Erreur/ Panne

1.7.2 La classification des pannes

Dans [37], une classification des pannes est proposée où la panne peut être due à plusieurs problèmes : selon la durée, la cause ou le comportement. La figure 1.7 résume la classification des pannes.

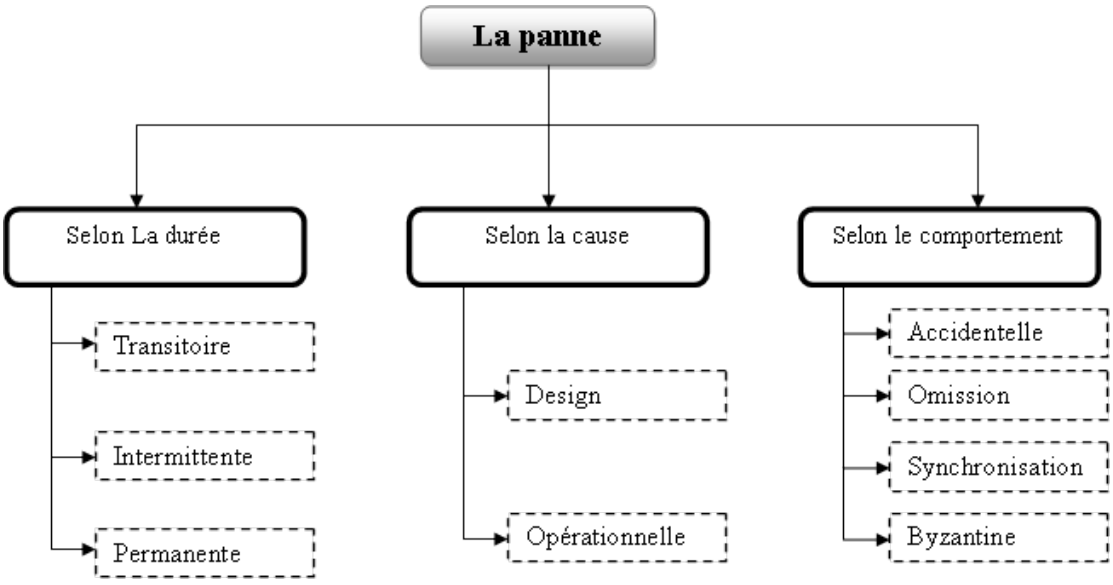

FIGURE 1.7 – Classification des pannes

1.7.2.1 Selon la durée

Dans cette classe, on distingue trois types de pannes :

- La panne transitoire : elle peut être due à un impact temporaire et elle peut disparaître sans aucune intervention.

- La panne intermittente : elle est imprévisible et s'introduit éventuellement.
- La panne permanente : elle persiste jusqu'il y aura une intervention externe pour la traiter.

1.7.2.2 Selon la cause

Dans cette classe, il y a deux types de pannes :

- La panne de design : elle peut se produire à cause d'une mauvaise fabrication d'un composant.
- La panne opérationnelle : elle se produit après le déploiement du réseau (pendant son fonctionnement), elle peut être due à un épuisement d'énergie d'un capteur, une destruction physique quelque soit la cause ou bien à cause des fluctuations de transmission radio.

1.7.2.3 Selon le comportement

Dans cette classe on trouve les types suivants :

- La panne accidentelle : le composant soit cesse de fonctionner ou bien poursuit son fonctionnement mais dans un état invalide.
- La panne d'omission : le composant arrête de fonctionner définitivement.
- La panne de synchronisation : le composant réalise son traitement normalement mais fournit le résultat en retard.
- La panne byzantine : cette panne est arbitraire et imprévisible. Elle peut être due à des attaques malicieuses.

1.7.3 Les sources de pannes dans des applications réelles des RCSF

Les RCSF sont généralement utilisés dans des environnements hostiles et sont donc sujets à des pannes au niveau des différentes couches du système [38]. Par ailleurs, une panne au niveau d'une couche a la possibilité de se propager à des niveaux supérieurs. Par exemple, la panne d'un capteur qui est sur un chemin de routage se répercute sur l'ensemble des nœuds du même chemin

puisque leurs messages ne peuvent pas être transmis jusqu'à ce que le chemin soit rétabli. La panne peut se produire au niveau des nœuds, du réseau ou même au niveau de la station de base.

1.7.3.1 La panne des nœuds

Un nœud est composé de plusieurs composants matériels et logiciels qui peuvent produire des dysfonctionnements à cause d'un épuisement de la batterie, une destruction physique, ou même coté logiciel puisqu'un capteur peut fournir des lectures erronées. Par exemple dans [39–41], des expériences ont été menées pour tester la robustesse des capteurs quand ils sont en contact direct avec de l'eau. Les résultats ont montré que les capteurs sont devenus défaillants à cause des courts-circuits. Dans [42], les capteurs ont été dispersés dans un champ de pommes de terre et durant leur déploiement les chercheurs ont découvert que de temps en temps des signaux erronés sont envoyés à cause de la fragilité des antennes. En outre, si le niveau de la batterie d'un nœud devient faible alors ses composants ne peuvent plus fonctionner correctement.

1.7.3.2 La perturbation des réseaux

Le routage est l'un des aspects fondamentaux dans les RCSF. Il est essentiel de transmettre, recevoir les données, distribuer des mises à jour logicielles et de coordonner entre les nœuds. En outre, il pourrait y avoir des applications de routage spécifiques, par exemple suivre les objets en mouvements car une défaillance dans la couche de routage peut conduire à des messages corrompus ou à des retards de transmission de données inacceptables. Dans les RCSF, les liens de communication entre les nœuds sont très volatiles à cause des interférences radio ou la présence d'obstacles. Par exemple, dans [43] le taux des messsages reçus est seulement 58%, dans [44] l'instabilité des liens entre les nœuds conduit à des changements constants dans les chemins de routage, et dans [45], une autre source de défaillance des liens est la collision des messages. Dans [43], les auteurs ont observé un risque de collision entre les messages des nœuds qui sont à proximité en raison d'un changement et d'un chevauchement de phase.

1.7.3.3 La panne de la station de base

A un niveau supérieur du réseau, un dispositif (station de base) qui recueille toutes les données générées dans le réseau est également sujet à des pannes de ses composants. Lorsque ce dispositif échoue une défaillance massive du réseau se produit puisque les données collectées par les nœuds capteurs ne sont pas accessibles sauf si des mesures de tolérance aux pannes sont présentes.

La station de base peut être déployée dans des zones où aucune alimentation permanente n'est présente. Dans certaines applications les batteries sont dotées de cellules solaires pour être alimentées [39, 42, 46] alors que dans la plupart des applications telles que l'expédition glaciaire rapportée dans [39], cette technique traditionnelle s'est avérée inefficace. Bien que cela ait fonctionné parfaitement dans d'autres applications, dans cet environnement glaciaire la station de base a subi une panne de courant en raison de la neige couvrant les cellules solaires pendant plusieurs jours.

1.7.4 La détection des pannes

Le but de la détection de pannes est de vérifier que les services fournis fonctionnent correctement. C'est la première phase de gestion de pannes où une défaillance inattendue doit être identifiée correctement avant de générer des dommages du réseau. Les approches de détection de pannes existantes dans les RCSF sont classées en : approche centralisée et approche distribuée [47].

1.7.4.1 Approche centralisée

Dans cette approche, les nœuds capteurs principaux identifient les nœuds défaillants ou mal conduits dans les RCSFs. Ce nœud principal peut être une station de base ou un contrôleur central ayant des ressources illimitées en termes d'énergie et de capacité à exécuter plus de mécanismes de gestion de pannes. On suppose que la durée de vie du réseau peut être prolongée si la gestion complexe et la transmission de données peuvent être attribuées aux nœuds principaux.

Par ailleurs, le nœud central adopte un modèle de détection de pannes pour récupérer l'état de performance du réseau et l'état des autres nœuds

par l'envoi des requêtes périodiquement. Cette opération est effectuée afin d'identifier et localiser les nœuds défaillants. Par exemple, Sympathy [48] est un outil de débogage et de détection de pannes dans les RCSF. Il implique des métriques qui permettent la détection efficace de pannes, et comprend un algorithme qui localise les sources de défaillance afin de réduire l'ensemble des notifications de défaillance et indiquer à l'utilisateur un petit nombre de causes probables. Tandis que Staddon et al. [49] a proposé un algorithme qui détecte et notifie les nœuds défaillants à la station de base. Chaque nœud envoie sa partie d'information de topologie du réseau (la liste des nœuds voisins) à la station de base. Par conséquent, la station de base peut construire la topologie du réseau en intégrant chaque partie d'information de topologie du réseau intégré dans les messages de mise à jour des routes. Une fois que la station de base connaît la topologie de tout le réseau, les nœuds défaillants peuvent être localisés efficacement en utilisant une stratégie simple "diviser-et-conquérir".

1.7.4.2 Approche distribuée

Dans cette approche, le concept de prise de décision locale est introduit c'est-à-dire la responsabilité de gestion des pannes est distribuée uniformément dans le réseau. Le but est de permettre à chaque nœud d'avoir certains niveaux de prise de décision avant de communiquer avec le nœud central et que le centre de contrôle ne doit pas être informé, sauf si une erreur est survenue dans le réseau. Des exemples de tel développement sont : l'auto-détection de pannes d'un nœud et l'auto-correction de ses composants physiques (batterie, capteur, antenne) quand ils présentent une anomalie [50, 51], détection de panne en coordonnant avec les voisins [52–55], et l'utilisation de la technique WATCHDOG [56] pour détecter tout mauvais comportement d'un voisin. L'auto-détection de panne d'un nœud dans [50] consiste à analyser les sorties binaires de ses capteurs et les comparer à celles obtenues lors de l'occurrence d'une panne prédéfinie. La détection de pannes via une coordination des voisins est un autre exemple de gestion distribuée de pannes dans lequel les nœuds se coordonnent avec leurs voisins pour détecter et identifier la panne avant de consulter le nœud central. Par exemple dans [57], un nœud capteur peut exécuter un algorithme de diagnostic localisé dans différentes étapes et les nœuds défaillants peuvent être identifiés en comparant les lectures de cap-

teur avec les lectures des voisins médians. Dans ce contexte, Ding et al. [54] ont développé un algorithme pour identifier le nœud défaillant dont les lectures de ses capteurs ont une grande différence avec celles des voisins. Dans cet algorithme, il est supposé que chaque nœud connaît son emplacement physique en utilisant un GPS. Tandis que dans [55], Chen et al. ont proposé un nouvel algorithme de détection de pannes distribué (DFD) qui n'impose pas la connaissance de la position physique des nœuds. Cet algorithme peut identifier les nœuds défaillants même lorsque la moitié des voisins sont défectueux. Il existe aussi l'approche de clustering [58] qui est devenue une technique émergente pour construire des applications évolutives et efficaces en termes de conservation d'énergie dans les RCSFs. Dans [59], Tai et al. décrivent une solution de détection de pannes efficace en utilisant une hiérarchie de communication basée sur des clusters pour traiter simultanément le passage à l'échelle et la précision. Dans cette approche, l'ensemble du réseau est divisé en différents groupes appelés clusters et chaque cluster est constitué d'un cluster-head CH (chef de groupe). Chaque CH est chargé de détecter les nœuds défaillants en échangeant des messages d'une manière continue avec les 1-voisins (les voisins à un saut). En analysant les informations collectées, le CH identifie finalement les nœuds défaillants selon une règle de détection de panne prédéfinie ainsi, cette information de défaillance sera diffusée à l'ensemble des clusters.

1.7.5 Diagnostic des pannes

Le diagnostic des pannes est une étape dans laquelle les causes de panne détectées sont correctement identifiées et distinguées des autres alarmes non pertinentes ou parasites [60]. La précision et l'exactitude des pannes détectées ont été déjà presque examinées et réalisées dans la phase de détection de pannes comme dans [52, 59, 61, 62]. Cependant, la plupart des approches existantes portent sur les modèles de pannes dans lesquels seulement le dysfonctionnement des composants matériels des nœuds est pris en considération. Dans [50, 55], les auteurs supposent que le système logiciel est déjà tolérant aux pannes et ils se concentrent sur les pannes des composants matériels des nœuds. Dans [50], Koushnafar et al. considèrent que la défaillance des nœuds est due aux conditions environnementales. Dans ce travail ils ont supposé que les nœuds défaillants envoient des valeurs incohérentes et arbitraires à

d'autres nœuds lors de la phase de transmission de données. Dans [54], les comportements anormaux des nœuds sont modélisés par des nombres réels au lieu du modèle de décision 0/1. En conséquence, cet algorithme est assez générique puisque les seuils et le nombre réel d'événements sont spécifiés par les exigences de tolérance aux pannes provenant de diverses applications.

1.7.6 Tolérance aux pannes

Dans les RCSF, plusieurs pannes peuvent être détectées due aux contraintes liées à ce type de réseaux tel que la limitation des ressources énergétiques, le déploiement dans des environnements hostiles et l'infiabilité des liens de communication [38]. En cas de présence de pannes, une tolérance aux pannes doit être incorporée immédiatement pour assurer le bon fonctionnement du réseau. Pour ce faire, certaines étapes sont exécutées dans cet ordre : la détection d'erreur, l'isolement de la panne, l'identification de la panne, et le traitement de la panne.

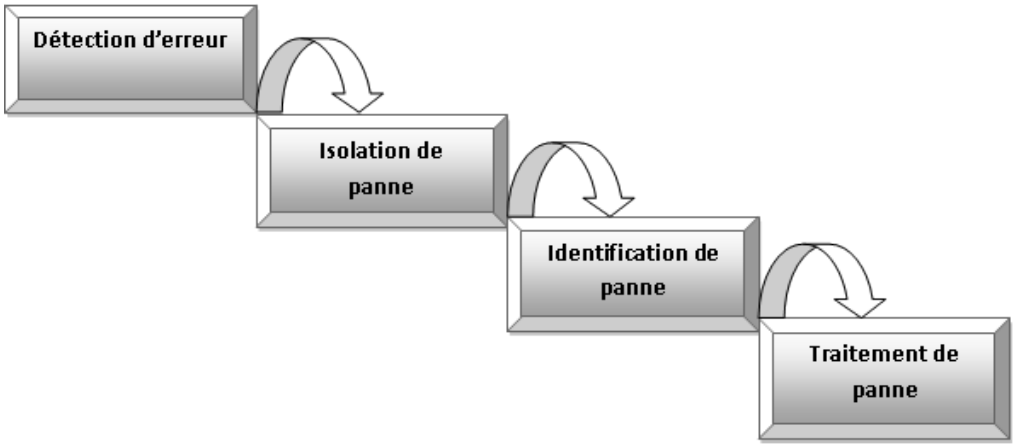

FIGURE 1.8 – Procédure de la tolérance aux pannes

1.7.6.1 Détection d'erreur

Dans cette phase, un événement inattendu se produit suite à des changements subis dans le réseau qui perturbent son fonctionnement malgré l'utilisation des mécanismes préventifs de pannes dans certains systèmes. Dans

ce cas de figure, une technique de détection d'erreur doit être mise en place immédiatement pour éviter la perte de données. Dans les RCSF, la détection d'erreur dépend des applications et de type de pannes.

1.7.6.2 Isolation de panne

Dans cette phase, une limitation des effets de la panne sur une zone particulière doit être établie pour protéger les autres zones et empêcher la propagation de cette panne dans tout le réseau.

1.7.6.3 Identification de panne

Cette phase identifie le composant qui est en panne et annonce sa panne à tous ses voisins pour qu'ils prennent ses précautions contre cette panne et donc, éviter une énorme perte de données. Dans le cas où ce nœud est impliqué dans le routage, il sera évité par les voisins qui ont de l'information à transmettre.

1.7.6.4 Traitement de panne

C'est la phase pendant laquelle une réparation du composant défaillant est accomplie. Cette opération dépend du type de la panne telle que certaines pannes peuvent être traitées immédiatement par une retransmission des données corrompues ou par évitement du nœud dont le composant est défaillant si ce dernier est impliqué dans une opération de routage de données ou bien le remplacer par un autre composant fonctionnel dans le cas où le système contient des composants redondants.

1.8 Les techniques de tolérance aux pannes dans les RCSFs

Plusieurs techniques et approches tolérantes aux pannes ont été proposées pour assurer la fiabilité du réseau en évitant la panne d'un nœud capteur ou traitant immédiatement la panne en cas de détection de défaillance de ce dernier, parmi les solutions existantes, nous citons :

1.8.1 Algorithme préventif

Dans ce type d'algorithmes, des techniques tolérantes aux pannes sont incorporées dans le but d'éviter tout type de pannes, par exemple la minimisation de la consommation d'énergie évite l'épuisement d'énergie d'un nœud capteur et donc prolonger la durée de vie du réseau.

1.8.2 Algorithme curatif

Dans cet algorithme, des techniques tolérantes aux pannes sont implémentées et se déclenchent lors de l'apparition des pannes, par exemple la proposition de deux chefs de groupe dans un cluster tel que la défaillance du chef principal provoque la mise en place du deuxième chef.

1.8.3 La qualité de lien

Pendant le fonctionnement du réseau le lien entre deux capteurs communicants peut être défaillant à cause des fluctuations radio. Pour cela des modèles de vérification de la qualité des liens sont proposés avec des solutions tolérantes aux pannes comme par exemple la proposition d'un chemin alternatif.

1.8.4 Le routage multi-chemins

Cette solution propose d'établir plusieurs chemins depuis chaque capteur vers la destination tel que la détection de panne dans le premier chemin provoque la mise en oeuvre de l'un des chemins alternatifs. Deux mécanismes sont proposés pour établir de chemins multiples :

1.8.4.1 Multi-chemins disjoints (Disjoint multipath)

Ce mécanisme [63] construit un nombre de chemins alternatifs qui ont des nœuds et des liens disjoints avec le chemin principal et avec les autres chemins alternatifs. D'où, une panne dans un ou tous les nœuds et/ou un ou tous les liens du chemin principal n'affecte pas les autres chemins alternatifs.

1.8.4.2 Multi-chemins tressés (Braided multipath)

Cette technique [64] construit un chemin alternatif pour chaque nœud dans le chemin principal qui n'inclut pas ce nœud, quand tous ou la plupart des nœuds sur le chemin principal tombent en panne, la découverte d'une nouvelle route est nécessaire, qui introduit une charge supplémentaire.

1.8.4.3 Multi-chemins maillés (Meshed multipath)

Comme la technique de Gradient de diffusion (GRAB) [65] qui crée un maillage de transmission du nœud source vers la station de base en se basant sur le "coût" de livraison de paquets au niveau de chaque nœud. Les nœuds qui se situent loin de la station de base ont le plus grand coût de transmission de données. Les paquets de données ne sont propagés que sur le chemin de transmission à faible coût vers la station de base.

1.8.4.4 Allocation du canal

Cette solution est implémentée au niveau de la couche MAC et permet d'effectuer une allocation du canal de transmission afin d'éviter les interférences entre les nœuds voisins et les collisions durant la transmission de données.

1.8.5 Retransmission

Cette méthode de tolérance aux pannes [66, 67] propose une transmission d'un paquet de données vers la destination en utilisant un nombre minimum de sauts. Après un temps prédéfini (timeout), si l'émetteur ne reçoit pas un accusé de réception de la part de destinataire, il considère que le paquet a été perdu et donc une retransmission de paquet doit être établie, comme exemple le protocole Direct Diffusion [68].

1.8.6 Réplication

C'est un autre mécanisme de tolérance aux pannes qui introduit la notion de redondance dans la livraison des paquets [66, 67]. Le principe de ce mécanisme est de transmettre de multiples copies du même paquet à travers différents chemins pour assurer la réception d'au moins une copie d'un paquet.

Le mécanisme "erasure coding" [69] et le protocole ReInForm (Reliable Information Forwarding) [70] utilisent ce mode de transmission pour la tolérance aux pannes dans les réseaux. Il existe deux types de réplication : réplication active et réplication passive.

1.8.6.1 Réplication active

Le principe est de disperser les nœuds d'une manière volontaire afin de garantir le bon fonctionnement du réseau tel que si un nœud tombe en panne, les autres qui se situent dans son voisinage peuvent tolérer cette panne en envoyant les données vers la station de base.

Redondance de chemins de routage : Les protocoles de routage doivent prendre en compte que les nœuds proches de la station de base sont plus utilisés dans le processus de transmission de données par rapport à ceux qui sont lointains et donc leurs batteries risquent d'être épuisées rapidement. Pour qu'un réseau soit tolérant aux pannes les nœuds doivent être k-connectés ce qui veut dire que chaque nœud doit avoir au moins k chemins avec le reste du réseau [71]. La figure 1.9 montre un réseau 2-connecté c'est-à-dire un réseau dans lequel entre tout nœud et la station de base il existe au moins deux chemins.

Dans [72], Cardei et al. ont proposé une topologie tolérante aux pannes pour les réseaux hétérogènes tels qu'ils ont différencié deux types de nœuds : les nœuds simples et les nœuds passerelles. Les nœuds simples sont des nœuds moins coûteux mais limités en ressources. Ils sont dispersés en grands nombres dans le réseau et ils sont chargés de collecter les données ambiantes. Les nœuds passerelles sont moins nombreux et ils sont caractérisés par leurs portée de transmission étendue. Ils sont chargés de récupérer les données collectées et les transmettre à la station de base.

Redondance de données collectées Dans cette technique, plusieurs nœuds sont déployés dans une zone de captage afin d'assurer une collection de données fiable puisque les valeurs ambiantes capturées sont censées être similaires. Ces données capturées sont ensuite envoyées à un autre nœud qui est chargé de l'agrégation des données reçues et les transmettre à la station de

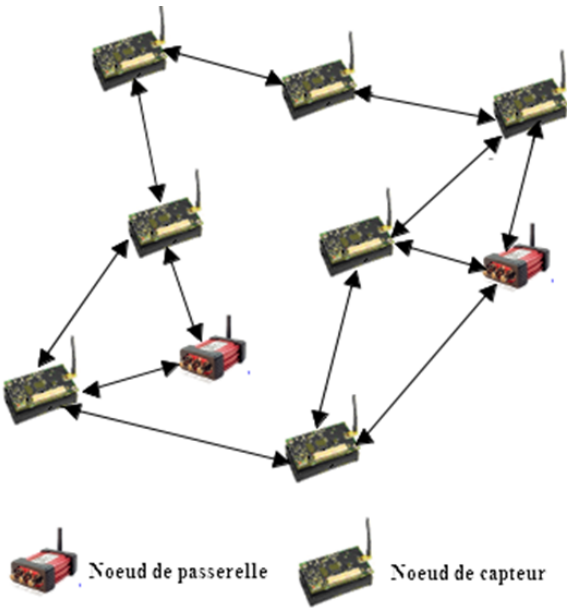

FIGURE 1.9 – Exemple d'un réseau hétérogène 2-connecté

base. Dans ce cas, la défaillance de quelques nœuds ne va pas trop influencer sur la précision des informations collectées tant qu'il reste encore des nœuds opérationnels dans la zone de captage.

1.8.6.2 Réplication passive

Plusieurs nœuds sont déployés pour assurer le bon fonctionnement du réseau, mais seulement le nœud principal est chargé de la réception et le traitement des données [73]. Les données capturées sont envoyées au nœud principal et aux nœuds de secours en même temps mais tant que le nœud principal est opérationnel, les nœuds de secours restent inactifs. En cas de défaillance du nœud principal, un des nœuds de secours sera choisi pour prendre le relais sans perte d'informations. La réplication est généralement considérée comme une technique optimale pour les RCSF. Cette technique ne consomme pas beaucoup d'énergie puisque les nœuds de secours restent inactifs tant qu'aucune panne n'est détectée.

1.9 Conclusion

Dans ce chapitre, nous avons développé la notion de réseaux de capteurs sans fil en présentant quelques applications conçues pour ce type de réseaux, ainsi nous avons donné certaines caractéristiques et quelques concepts nécessaires à la compréhension des RCSFs.

Parmi les concepts liés au RCSF, nous nous sommes intéressés à la tolérance aux pannes dans les réseaux de capteurs sans fil puisque la plupart des applications conçues sont déployées dans des environnements hostiles où les nœuds de capteurs sont vulnérables à des dommages physiques ou tout simplement à un épuisement d'énergie. En effet, il est connu que la consommation d'énergie est un critère de performance capital pour les RCSFs, et le remplacement des nœuds de capteurs en pannes est souvent impossible. De ce fait, la tolérance aux pannes doit être sérieusement considérée pour assurer la fiabilité du réseau ainsi garantir l'extension de sa durée de vie.

Dans le chapitre qui suit, nous allons présenter un panorama des protocoles tolérants aux pannes proposés dans la littérature.

Chapitre 2

Etat de l'art de la tolérance aux pannes dans les RCSF

2.1 Introduction

L'émergence du paradigme des RCSF a permis l'apparition de plusieurs recherches sur ses différents aspects [74] dans des domaines différents suite au faible coût et la multifonction des nœuds capteurs qui composent ce type de réseaux.

Le routage dans les RCSF est le processus qui consiste à faire circuler les données captées du nœud source à la station de base [75]. Les protocoles de routage ont comme but d'assurer la fiabilité et l'efficacité énergétique du réseau et donc d'être résistant aux pannes qui peuvent se produire durant le fonctionnement du réseau.

Dans les RCSFs les pannes sont généralement inévitables à cause de la limitation d'énergie des nœuds capteurs, du déploiement dans des environnements hostiles ainsi que l'infiabilité des liens de communication sans fil. L'occurrence de ces pannes peut empêcher le réseau d'accomplir ses tâches sans interruption. Dans ce cas, il est nécessaire d'instaurer des mécanismes de tolérance aux pannes afin d'assurer la fiabilité de routage dans le réseau même en présence de pannes. Les protocoles de routage sont capables de maintenir et d'assurer la fiabilité de la route de communication sous ces conditions. Dans ce chapitre, nous allons présenter une étude sur les protocoles de routage tolérants aux pannes conçus pour les RCSF.

2.2 Classification des protocoles de routage

L'architecture du réseau peut jouer un rôle primordial dans le fonctionnement des protocoles de routage dans les RCSF [76]. Ces protocoles peuvent

être classifiés selon la structure du réseau en : protocoles de routage plats, hiérarchiques, ou location-based.

2.2.1 Les protocoles de routage plats

Dans ce type de protocoles, tous les nœuds jouent le même rôle pour accomplir les mêmes tâches et les communications sont effectuées saut par saut jusqu'à ce que l'information atteigne la station de base comme le montre la figure 2.1. Ce genre de protocoles de routage est efficace surtout pour les réseaux contenant un petit nombre de nœuds tels que SPIN (Sensor Protocols for Information via Negotiation) [77, 78], Direct Diffusion [68], ACQUIRE [79], MCFA (Minimum Cost Forwarding Algorithm) [80], Rumor [81], GBR (Gradient-Based Routing) [82].

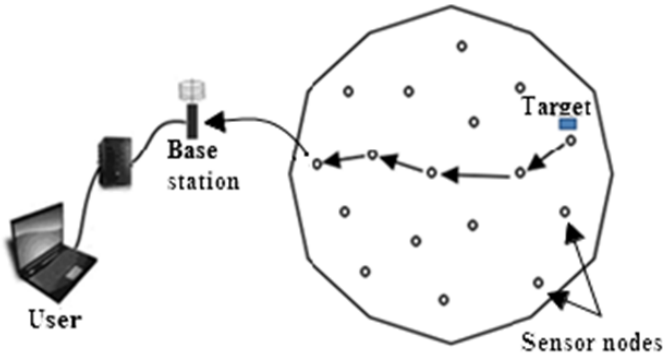

FIGURE 2.1 – Schéma de routage dans les protocoles plats

2.2.2 Les protocoles de routage hiérarchiques

Dans les protocoles de routage hiérarchiques, le réseau est divisé en clusters (groupes) comme s'est montré dans la figure 2.2. Chaque cluster est constitué d'un certain nombre de membres (CMs) qui effectuent seulement la tâche de détection de données à partir de leur environnement là où ils sont déployés et d'un cluster-head CH (chef de groupe) qui est responsable de collecter et agréger les données reçues de ces membres et envoyer les données agrégées à la station de base. En général, le nœud capteur élu comme cluster-head est celui qui possède l'énergie résiduelle la plus élevée. Parmi ces protocoles, nous citons [5], PEGASIS (Power-Efficient Gathering in Sensor Information

Systems) [83], TEEN [84] and APTEEN (Threshold-sensitive Energy Efficient Protocols) [85], HPAR (Hierarchical Power-aware Routing) [86], VGA (Virtual Grid Architecture routing) [87].

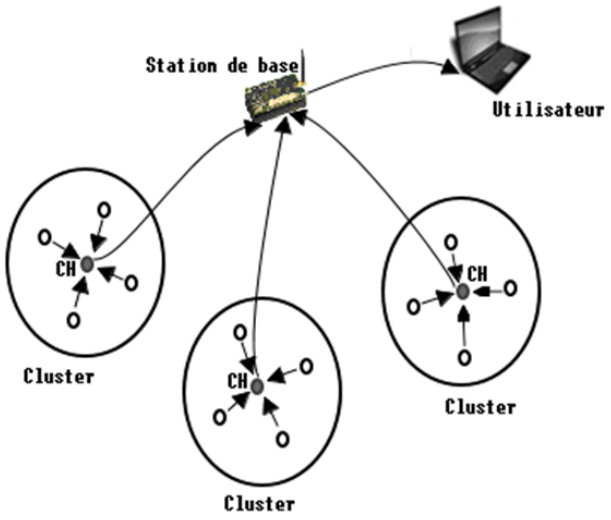

FIGURE 2.2 – Schéma de routage dans les protocoles hiérarchiques

2.2.3 Les protocoles basés sur la localisation (location-based)

Dans ce type de protocoles de routage, les nœuds sont traités en tenant compte de leurs emplacements dans le réseau. Les coordonnées relatives des nœuds voisins peuvent être obtenues en échangeant des informations entre eux et la distance entre les nœuds voisins est estimée en fonction de la puissance du signal des messages échangés. Alternativement, la position des nœuds peut être obtenue directement en communicant avec un satellite en utilisant le GPS. Dans ce cas de figure, il est supposé que les nœuds sont équipés d'un petit récepteur GPS. Certains protocoles basés sur la localisation exigent que les nœuds qui n'ont pas d'activités puissent être mis en veille dans le but de minimiser la consommation d'énergie dans le réseau. Ainsi, plus de nœuds sont en veille plus la consommation d'énergie est réduite. Nous citons quelques protocoles basés sur la localisation tels que Geographic Adaptive Fidelity (GAF) [88], GEAR (Geographic and Energy Aware Routing) [89], GOAFR (The Greedy Other Adaptive Face Routing) [90], SPAN [91].

2.3 Les causes des pannes

Les RCSF sont souvent déployés dans des environnements hostiles où ils sont sujets à des défaillances due à plusieurs causes telles que les impacts environnementaux, défaillance matérielle et aussi des bugs logiciels [92]. Ces défaillances peuvent causer des taux de perte très élevés de données, des transmissions avec latence ou même une déconnexion totale du réseau. Par conséquent, cela peut réduire considérablement la durée de vie du réseau et rendre aussi l'infrastructure du réseau inutilisable [93]. En outre, les données collectées par les nœuds capteurs ne peuvent pas être transmises correctement à la station de base à cause de l'existence de défaillance. En outre, les nœuds capteurs doivent transmettre leurs données captées et surmonter les défaillances.

Dans des conditions défavorables, les RCSF doivent être déployés de sorte qu'ils soient en mesure d'identifier les nœuds de capteurs en panne et essayer de les couvrir pour assurer la disponibilité du réseau et être en mesure de garantir une communication des données fiable à la station de base. Ces défis ont conduit à la conception des protocoles de routage tolérants aux pannes pour les RCSF afin d'assurer la fiabilité de transmission de données à la station de base et aussi de garantir le bon fonctionnement du réseau même dans la présence de pannes [94]. Par ailleurs, la panne peut concerner un nœud capteur et/ou un lien. La figure 2.3 résume les différents types de pannes qui peuvent survenir dans les RCSF.

2.4 Les protocoles de routage tolérants aux pannes

Les protocoles de routage proposés pour les RCSF peuvent être classés en trois groupes. Cette classification dépend de la méthode utilisée pour trouver le bon chemin [76, 95]. Le routage proactif dans lequel tous les chemins sont construits et maintenus à l'avance ainsi, ils sont stockés dans une table de routage par contre dans le routage réactif tous les chemins sont construits à la demande et le routage hybride combine les deux techniques. La tolérance aux pannes peut être réalisée en appliquant les protocoles de routage au niveau de la couche réseau dans le cas où certains nœuds présentent une défaillance.

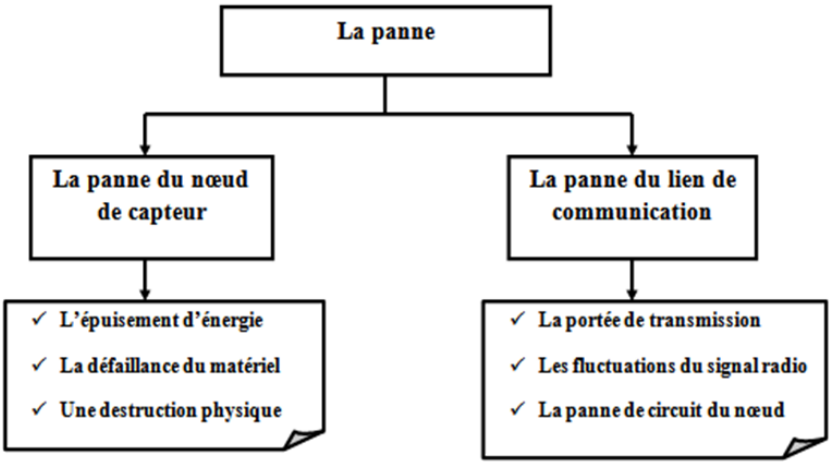

FIGURE 2.3 – Les causes des pannes

Dans ce qui suit, nous distinguons deux architectures de protocoles de routage : architecture plate, architecture hiérarchique et nous présentons quelques protocoles de routage tolérants aux pannes pour chaque catégorie ainsi que leurs fonctionnalités. La figure 2.4 récapitule les protocoles de routage tolérants aux pannes dans les RCSF.

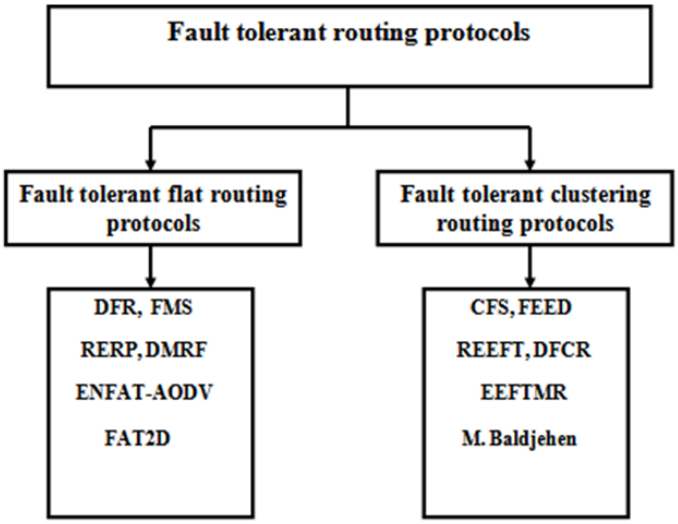

FIGURE 2.4 – Les protocoles de routage tolérants aux pannes dans les RCSF

2.4.1 Les protocoles de routage plats tolérants aux pannes

Dans cette catégorie, les nœuds capteurs communiquent via un routage multi-sauts jusqu'à ce qu'ils atteignent leurs destinations. Ils jouent tous le même rôle et collaborent entre eux pour accomplir la tâche de détection. Par ailleurs, la panne d'un nœud dans cette catégorie est généralement tolérée par la technique de multi-chemins. Dans ce qui suit, nous présentons les fonctionnalités de certains protocoles.

2.4.1.1 Dynamic Fault-tolerant Routing Protocol for prolonging the lifetime of WSN

L'objectif de ce protocole [96] est de maintenir la connectivité du réseau en cas d'épuisement de l'énergie d'un nœud dans le but d'assurer la fiabilité de livraison de données à la station de base tout en prolongeant la durée de vie du réseau.

Dans ce protocole, quand un nœud capteur est sur le point d'épuiser son énergie, il doit trouver un chemin alternatif adéquat vers la station de base en établissant une nouvelle connexion avec ses nœuds voisins. Le chemin alternatif augmente la fiabilité de transmission de données entre les nœuds sources et la station de base. Ce protocole est exécuté en trois phases :

L'implémentation des niveaux et établissement de chemin : Chaque nœud capteur est caractérisé par son identifiant (N_j), son niveau (HC_j), son nœud parent (P_j) et une liste (A_j) pour stocker les paquets de données. La station de base est initialisée avec $HC = 0$, $P = BS$, tandis que les autres nœuds capteurs sont initialisés avec $HC_j = \infty$, $P_j = 1$.

Une fois les nœuds déployés, la station de base diffuse un message d'avertissement (ADVT) avec (N_j, HC_j) pour découvrir les nœuds qui sont au niveau 1. Les nœuds qui reçoivent ce message d'avertissement, considèrent la station de base comme nœud parent. Par ailleurs, lorsqu'un nœud reçoit un message ADVT de la part d'un autre nœud avec son $(HC = N)$, ce dernier augmente son HC à $(N + 1)$. Ainsi, le protocole établit un chemin de chaque nœud capteur vers la station de base.

Transmission de données : Dans cette phase, lorsqu'un événement est détecté par un nœud capteur, ce dernier garde une copie de ce paquet de données avant de le transmettre à son nœud parent. Lorsque le nœud parent le reçoit, il transmet un accusé de réception à l'émetteur. En suite en recevant cet accusé, ce dernier supprime le paquet de données, ainsi ce processus se poursuit jusqu'à ce que l'information atteigne la station de base. Pour assurer la fiabilité du réseau et aucune perte d'information, un temps (timeout) est attribué à chaque paquet de données.

Rétablissement de chemin : Lorsque l'énergie restante d'un nœud parent est inférieure à un seuil prédéfini, ce dernier transmet un message de notification à tous ses nœuds voisins en leur demandant de trouver un autre parent en vue de maintenir la connectivité du réseau et garantir la fiabilité du réseau. Donc, les nœuds fils correspondants transmettent un message HELLO pour trouver des nouveaux parents.

2.4.1.2 Fault-Tolerant Multilevel Routing Protocol (FMS)

Dans [97], Ajay et al. proposent un protocole de routage multi-niveaux tolérant aux pannes avec un ordonnancement du sommeil pour les RCSF appelé FMS. Le but de ce protocole est de maintenir la connectivité du réseau même si un nœud capteur a épuisé son énergie. FMS est capable d'assurer la fiabilité de livraison de données pour les applications orienté-événement. Il est conçu pour les RCSF denses dont les nœuds capteurs sont déployés aléatoirement et chaque nœud possède son propre identifiant (ID_r) ainsi que la communication entre les nœuds voisins est bidirectionnelle. En outre, le protocole propose un ordonnancement de sommeil aléatoire afin de conserver l'énergie tel que la mise en veille d'un nœud capteur ne prévient pas ce dernier de détecter des grandeurs dans son voisinage puisque l'unité d'acquisition sera toujours allumée et la radio sera en mode éteint. Le fonctionnement du protocole FMS s'effectue en deux phases. La première phase est identique à celle du protocole cité au dessus [96] et la deuxième phase consiste à effectuer le processus d'ordonnancement de sommeil périodiquement et la transmission de données. Au cours de cette deuxième phase, un ensemble de nœuds capteurs est sélectionné aléatoirement et mis en mode veille tandis que l'autre ensemble de

nœuds capteurs est mis en mode actif. Cette opération est exécutée périodiquement et durant chaque période, seulement les nœuds capteurs actifs sont responsables de la transmission de données. Si l'énergie résiduelle d'un nœud actif est inférieure à un seuil prédéfini, ce dernier diffuse un message de notification à tous ses nœuds fils qui vont chercher un autre nœud parent qui a plus d'énergie. Donc, les chemins alternatifs sont établis et la connectivité du réseau est maintenue.

2.4.1.3 An adaptive fault-tolerant Routing Protocol with Error Reporting scheme for WSN (RERP)

RERP [98] est un protocole de routage tolérant aux pannes dans lequel il est supposé que chaque nœud capteur possède au moins deux chemins alternatifs vers la station de base. Dans RERP, la possibilité d'un nœud de tolérer une panne qui peut être reproduite, dépend du nombre des nœuds voisins actifs tel que si un nœud a N voisins, il pourra tolérer (N-1) pannes. RERP s'exécute en deux phases principales :

L'établissement des routes : Cette phase se déroule en cinq phases :

a) **La phase d'avertissement :** Dans cette phase, la station de base diffuse un message d'avertissement à tous ses 1-voisins pour confirmer si ces derniers sont capables de recevoir les paquets de données de sa part et les stocker dans sa table de routage.

b) **La phase d'initialisation :** Dans cette phase, les nœuds qui n'ont pas encore un chemin vers la station de base diffusent un message (RREQ) pour le demander. Chaque nœud qui reçoit ce message et possède déjà une route vers la station de base diffuse un message pour répondre à la requête reçue.

c) **La phase de sélection de route :** Dans cette phase, une table de routage sera construite et elle est utilisée pour stocker et maintenir les routes. La sélection des routes est basée sur l'énergie résiduelle de chaque nœud.

d) **La phase de transmission de données :** Lorsqu'un nœud détecte un événement dans son voisinage, il génère un paquet de données et le transmet à la station de base via un mode multi-sauts.

e) **Construction de routes alternatives :** Quand un nœud demande une route vers la station de base, plusieurs réponses peuvent être reçues. Dans ce cas en recevant les réponses, une route sera stockée dans la table de routage principale si le nœud ne possède pas une route vers la station de base sinon elle sera stockée dans la table de routage alternative qui est constituée de deux champs alternatifs : l'identifiant du nœud et son énergie résiduelle.

Rapport d'erreur Ce protocole utilise les messages d'erreurs suivants :

a) **Message d'échec de lien :** Ce message est généré dans deux cas : dans le cas où un message RTS est envoyé mais aucune réponse CTS n'est reçue après un certain nombre de tentatives, ou un paquet de données est envoyé mais aucun accusé de réception n'est reçu et le nombre de tentatives maximal est dépassé.

b) **La sélection du chemin alternatif :** Chaque nœud possède une table de routage alternative dont tous les chemins alternatifs vers la station de base sont stockés. Si la transmission de données a échoué, le nœud choisit un chemin parmi les chemins existants dans la table de routage.

c) **Message de batterie critique :** Quand l'énergie résiduelle d'un nœud est inférieure à un seuil prédéfini, un message de batterie critique est généré et est envoyé à l'émetteur du paquet de données qui va à son tour le diffuser à ses voisins. Puis, chaque nœud qui reçoit ce message enlève le nœud défaillant de sa table de routage.

d) **Message de destination introuvable :** Ce message est généré quand un paquet de données est perdu avant d'être reçu par le nœud destinataire due au non disponibilité d'une route vers la destination.

e) **Message de question/réponse :** Ce message est utilisé par un nœud pour vérifier si la destination est dans sa portée ou pas.

2.4.1.4 A dynamical jumping real-time fault-tolerant routing protocol (DMRF)

Le protocole DMRF [99] effectue deux modes de transmission de données : le mode saut par saut et le mode "jumping". Dans ce protocole, chaque nœud

utilise le temps de transmission restant pour transmettre le paquet de données vers la station de base et l'état de l'ensemble des nœuds candidats (FCS) pour choisir le prochain saut. En cas de défaillance d'un nœud, congestion du réseau ou bien lorsqu'une région est vide le mode de transmission basculera vers le mode "jumping" en vue de réduire le délai de transmission et de garantir la transmission de paquet de données vers la station de base dans le temps spécifié. Ces caractéristiques ont permis au protocole DMRF d'être appliqué dans des applications temps réel.

Dans DMRF, le processus de transmission se déroule en quatre phases :

a) **Phase d'initialisation :** Dans cette phase, le protocole initialise la liste des nœuds voisins, la liste de l'état qui contient des informations sur la défaillance des nœuds, la congestion du réseau ou la région vide, l'ensemble des candidats de transmission (FCS), la table de probabilité du mode "jumping", et le chemin de transmission initial.

b) **Phase de transmission de données :** DMRF détecte les nœuds défaillants, la congestion du réseau ou les régions vides, et le temps restant pour transmettre le paquet de données à la station de base pour vérifier si le paquet de données doit être transmis en mode "jumping". Si aucune des conditions citées dessus ne s'est produite, DMRF sélectionne dynamiquement un candidat de "FCS" basé sur le taux de transmission de paquet de données. En outre, si un nœud est défaillant, une congestion du réseau se produit ou une région est vide, sont détectés ou le temps de transmission de paquet est inférieur au seuil de "jumping", alors le mode de transmission "jumping" doit être lancé.

c) **Phase de transmission "jumping" :** Dans cette phase, chaque nœud met à jour dynamiquement son ensemble de candidats "FCS" en visant d'autres nœuds relais. Le mode de transmission "jumping" peut éviter les nœuds défaillants, la congestion du réseau et la région vide mais il ne peut pas garantir le succès de transmission. Par conséquent, une phase d'ajustement de probabilité doit être effectuée après chaque transmission en mode "jumping".

d) **Phase d'ajustement de probabilité de "jumping" :** Cette phase consiste à ajuster la probabilité de "jumping" selon le résultat de transmission en mode "jumping" et cette information sera ensuite renvoyée

en amont. Lorsque le paquet de données est envoyé à la station de base avec succès, on considére que le processus de transmission est fini. En outre, si la transmission de données échoue la probabilité de "jumping" est ajustée par le mécanisme de "feedback" qui permet non seulement d'éviter les nœuds défaillants, la congestion de réseau et la région vide mais aussi d'améliorer la vitesse de transmission.

2.4.1.5 ENhanced FAult-Tolerant AODV routing protocol (ENFAT-AODV)

ENFAT-AODV [100] est un protocole de routage multi-sauts tolérant aux pannes destiné aux RCSF tel qu'il est capable d'établir rapidement des chemins efficaces entre les nœuds communicants. En outre, ce protocole associe à chaque chemin principal de livraison de données un chemin alternatif. De ce fait, en cas d'échec de transmission de données sur le chemin principal, le chemin alternatif sera utilisé par l'établissement de nouveaux liens fiables au lieu des liens perdus. La sélection des chemins est basée sur le nombre de sauts tel qu'en cas d'existence de deux chemins vers la destination le plus court chemin sera choisi comme chemin principal et l'autre comme chemin alternatif. Les messages de demande de route (RREQ) et de réponse (REP) sont les mêmes que le protocole AODV [101].

Dans le protocole ENFAT-AODV certains champs sont ajoutés dans le message de contrôle tels que "BACKUP", "UPDATE", "DistanceToDest". Par ailleurs, en vue de réduire la complexité d'implémentation, certains éléments ont été éliminés de la version originale du AODV tels que First, Hello, RERR et RREP-ACK due à l'inutilité de ces éléments. Les principales opérations du protocole ENFAT-AODV sont :

a) **La découverte du chemin principal :** En cas de nécessité d'un chemin principal pour la livraison de paquet de données vers la station de base, le nœud source doit effectuer le processus de découverte du chemin principal en diffusant le message de demande de route principale (main RREQ) pour atteindre le nœud destinataire. Quand les nœuds intermédiaires reçoivent ce message, ils créent une route inverse vers le nœud source. Si ce message est reçu pour la première fois par un nœud qui n'est pas le nœud destinataire, ce dernier le diffuse à tous ses

voisins. En outre, si c'est le nœud destinataire ou s'il possède une route principale vers la destination, il génère une réponse de route principale (main RREP). Ensuite, le message (Main RREP) est transmis saut par saut au nœud source et en ce moment tous les nœuds intermédiaires créent une route vers la destination. Quand le nœud source reçoit ce message, il enregistre la route dans sa table de routage principale.

b) **La construction de route alternative :** Durant le processus de réponse de route principale (main RREP), les nœuds qui appartiennent au chemin principal, créent une route alternative vers le nœud destinataire en diffusant un message de demande de route alternative "backup RREQ". Ensuite l'émetteur attend une réponse de route alternative "backup RREP" de la destination ou bien des nœuds intermédiaires qui n'appartiennent pas à la route alternative.

c) **L'entretien des routes :** Durant la phase de transmission de données, si le chemin principal a des liens brisés ou bien la destination du paquet transmis n'est pas active sur la route principale, le nœud utilise immédiatement sa route alternative pour transmettre le prochain paquet de données sans interrompre la transmission de paquet de données. Par suite, le nœud sur le nouveau chemin principal et qui ne possède pas une route alternative effectue un processus de découverte de route alternative "Backup route discovery" pour trouver une nouvelle route alternative.

En résumé on pourra dire que le protocole ENFAT-AODV assure la fiabilité de routage et la disponibilité de routes vers les nœuds destinataires comparativement à la version originale d'AODV.

2.4.1.6 Fault-Tolerant Directed Diffusion for wireless sensor networks (FaT2D)

FaT2D est un protocole [102] tolérant aux pannes basé sur le protocole "Directed Diffusion" [68]. Il permet de garantir une tolérance aux pannes contre les nœuds défaillants en utilisant le mécanisme multi-chemins, l'exploration périodique et la technique de renforcement positif/négatif. En outre, FaT2D définit une nouvelle technique qui permet la détection rapide de pannes avec

une récupération rapide du chemin malgré la défaillance des nœuds et le changement de topologie et il s'exécute selon les phases suivantes :

a) **Détection de pannes :** Un délai de détection de pannes nommé Tfd a été introduit en vue de réduire le délai de recouvrement de panne et par conséquent accélérer la détection de défaillance d'un nœud et la réparation locale du chemin. Si le temps Tfd expire, le protocole FaT2D transmet immédiatement un nouveau message appelé "ExploreRequest" pour notifier la détection de pannes et demander une nouvelle exploration pour trouver un chemin fiable qui remplace celui qui est défaillant. Ainsi, chaque nœud dans le chemin défectueux élimine le gradient correspondant pour remédier aux défaillances.

b) **Recouvrement rapide du chemin :** Quand le Tfd expire, cela notifie la défaillance d'un nœud. De ce fait FaT2D lance le processus pour réparer le chemin défectueux en transmettant un message de demande d'exploration spéciale nommé "exploreRequest" qui contient des informations sur le chemin défectueux. Le message "ExploreRequest" sera envoyé afin d'atteindre la source principale des informations en rapport avec la route défectueuse sans invoquer des boucles de transmission ou bien la recherche des nœuds inappropriés. Lorsque le nœud source reçoit la demande d'exploration de paquet, il arrête de le transmettre et il commence une exploration par inondation comme dans le protocole "Directed Diffusion". Ce mécanisme génère une exploration rapide pour trouver une nouvelle route fiable avec les mêmes règles du protocole "Directed Diffusion".

c) **Elimination de pannes :** Pour chaque nœud intermédiaire qui reçoit le message "ExploreRequest", le protocole FaT2D vérifie si ce nœud appartient au chemin défectueux ou non. Si ce dernier appartient à ce chemin, il va renforcer négativement son gradient. En outre, chaque nœud exécute un renforcement négatif local à tous ses voisins en amont afin de supprimer le chemin défectueux et arrêter l'envoi des données sur ce chemin.

2.4.2 Les protocoles de routage hiérarchiques tolérants aux pannes

Plusieurs protocoles de routage hiérarchiques tolérants aux pannes ont été proposés pour garantir une tolérance aux pannes dans les RCSF. Dans cette catégorie de protocoles de routage, il est généralement considéré que le chef de groupe CH (cluster-head) est sujet à des pannes dues à plusieurs tâches et cette panne est couverte par le vice-CH qui va prendre sa place. Ainsi, si le CH tombe en panne le cluster devient inutile et donc le réseau perd ses fonctionnalités. Dans ce qui suit, nous discutons de quelques protocoles :

2.4.2.1 Cluster-based Fault-tolerant Scheme (CFS)

CFS [103] est un protocole de routage tolérant aux pannes qui a comme but de tolérer les pannes des liens afin de garantir un routage fiable de données. CFS est exécuté en trois phases :

a) **La formation de clusters :** Chaque cluster possède deux CHs : le CH principal (CH_p) et son vice-CH (CH_v). L'élection de ces CHs est basée sur le poids du nœud qui est une combinaison entre la 2-densité du nœud et son énergie résiduelle. Puisque le CH est responsable de plusieurs tâches, le protocole est exécuté en périodes (rounds) pendant lesquelles le nœud ayant le plus grand poids dans son 2-voisinage est élu comme CH_p et le deuxième comme CH_v. Après, le CH_p diffuse un message d'avertissement pour construire son cluster. Chaque nœud qui n'est pas un CH et n'est pas un membre d'un autre cluster, transmet un message REQ-JOIN pour joindre son CH_p qui a envoyé le message.

b) **L'établissement des routes :** Tous les CHs établissent un chemin CH-à-CH envers la station de base pour la transmission de données et créent un temps pour la communication intra-cluster pour éviter les interférences. Lorsqu'un événement est détecté, le membre concerné envoie cette information au CH_p et CH_v en même temps. Si CH_p ne relaye pas le message dans un timeout il sera considéré comme défaillant et le CH_v le transmettra.

c) **Transmission de données :** Dans cette phase, les nœuds commencent à transmettre les données collectées à leur CH_p correspondants. Après

la radio de chaque membre est éteinte jusqu'à l'arrivée de son temps de transmission. Chaque CH agrège les données reçues de ses membres et les envoie vers la station de base.

2.4.2.2 Fault-Tolerant Energy-Efficient Distributed Clustering for WSN (FEED)

Dans le protocole FEED [104], le réseau est divisé en un ensemble de clusters. Chaque cluster contient un chef de groupe (CH), un pivot de CH (PCH) qui a des capacités supplémentaires par rapport à un CH, et d'un nœud superviseur (SN) qui peut remplacer son CH ou son PCH correspondant lorsque l'un d'eux tombe en panne. L'élection du CH est basée sur quelques facteurs tels que la densité, la centralité, l'énergie restante et la distance entre les nœuds. FEED se déroule en quatre phases :

a) **La première phase :** Les nœuds échangent un message entre eux et chacun d'eux calcule la densité et la centralité. Dans ce protocole proposé, une nouvelle méthode de calcule de centralité est introduite. Ensuite, chaque nœud calcule son premier score en fonction de son énergie, densité et centralité.

b) **La deuxième phase :** Chaque nœud qui a le plus grand poids (énergie, densité et centralité) parmi ses voisins, se considère comme volontaire.

c) **La troisième phase :** Dans cette phase, chaque nœud ajoute le facteur distance au premier score calculé dans la phase précédente, et le volontaire avec le deuxième meilleur score est élu adjoint.

d) **La dernière phase :** Les nœuds volontaires calculent leur score final et selon ces scores calculés, ils s'affirment comme des nœuds CH, PCH ou SN. Après cela chaque nœud dont le statut est différent de CH, PCH et SN, rejoint le cluster le plus proche.

2.4.2.3 Reliable energy efficient fault tolerant clustering for WSN (REEFT)

Le protocole REEFT [105] permet :

- d'économiser la consommation d'énergie en construisant des clusters statiques avec des CHs fiables,

- de prolonger la durée de vie du réseau en distribuant les CHs dans la zone d'intérêt et en générant des clusters équilibrés en taille,
- d'assurer la tolérance aux pannes au niveau des CHs défaillants.

REEFT s'effectue en trois phases :

a) **La phase de génération de clusters :** Dans cette phase, le réseau est organisé en un certain nombre de clusters. La station de base est responsable de l'initialisation de tous les nœuds dans le réseau, et exécute l'algorithme de groupement hiérarchique. Ensuite les résultats de ces opérations sont envoyés à tous les nœuds dans le réseau. Enfin, les nœuds s'auto-organisent et établissent des liens de communication entre eux dans chaque cluster.

b) **La phase d'élection de CH :** Les CHs sont élus selon leur énergie résiduelle, leur voisinage et la qualité des liens de communication pour assurer la fiabilité du canal radio. La qualité du lien est évaluée en fonction des messages HELLO et des paquets d'accusé de réception reçus. Les nœuds qui se trouvent au centre du cluster, ont plus d'avantage pour devenir des CHs.

c) **La phase d'agrégation de données :** Chaque CH crée un trafic TDMA et distribue des slots de temps à tous ses membres afin d'éviter les collisions. Ensuite, chaque nœud membre transmet les données détectées à son CH correspondant. Á la fin de chaque période (round), chaque CH agrège les données reçues de ses membres et les envoie à la station de base. En outre, en cas de défaillance d'un CH, le nœud avec la plus forte densité devient le nouveau CH.

2.4.2.4 Energy-efficient fault-tolerant clustering and routing algorithms for WSN (DFCR)

DFCR [106] est un protocole qui prend en considération la conservation d'énergie et la tolérance aux pannes qui sont les deux enjeux majeurs dans le déploiement des RCSFs. Au début de cet algorithme, la station de base diffuse un message "HELLO" pour que tous les CHs peuvent calculer la distance à la station de base en fonction de RSSI (Received Signal Strength Indicator) du message reçu. Puis la station de base diffuse un message de "HopPacket"

qui indique le nombre de sauts du CH à la station de base. Après cela, chaque CH envoie le paquet à tous ses CHs voisins. En recevant ce paquet, chaque CH compare la valeur du compteur avec la valeur de son propre compteur. Si cette valeur reçue est inférieure à celle stockée le CH incrémente son compteur de 1 et le retransmet, sinon, il ignore le paquet. Ensuite, la phase de mise en place sera lancée où chaque CH diffuse un message "HELLO" dans sa portée de communication. Le nœud qui reçoit au moins un message, est considéré comme couvert. Par ailleurs, il diffuse un message "Help" et chaque nœud voisin qui reçoit ce message, envoie une réponse pour former son chemin alternatif. En outre, il peut exister des nœuds qui ne sont pas couverts par un CH en raison de déploiement aléatoire ou bien la défaillance brutale de CHs. Dans ce cas, ces nœuds sont affectés à un autre CH via une communication multi-sauts utilisant les nœuds couverts comme nœuds relais. Dans la deuxième phase, les CHs agrègent les données reçues de leurs membres et sélectionnent le prochain nœud relais pour atteindre la station de base. Cette sélection dépend de la distance et le nombre de sauts calculés précédemment pour minimiser la consommation d'énergie.

2.4.2.5 Energy-Efficient Fault-Tolerant Multipath routing scheme for wireless sensor networks (EEFTMR)

EEFTMR [107] est un protocole basé sur le routage multi-chemins tel que le plus court chemin est considéré comme le chemin principal pour assurer un routage de données efficace en termes d'énergie et deux autres chemins alternatifs en cas de défaillance du chemin principal et pour gérer la surcharge du trafic sur le chemin principal.

Dans EEFTMR, les nœuds sont arrangés en petits clusters dont chaque membre a plus d'un chemin pour communiquer avec son CH correspondant tel que chaque membre envoie les données captées à d'autres membres du même cluster à travers trois routes alternatives. Le chemin le plus court est considéré comme le chemin principal pour une livraison de données rapide vers le CH et si ce chemin échoue, le prochain plus court chemin alternatif est utilisé pour couvrir la défaillance du chemin principal et assurer la fiabilité de transmission de données. Dans ce protocole, les CHs et la station de base communiquent également avec de multiples chemins alternatifs ; le plus court

chemin est principalement utilisé pour la transmission de données et les deux autres chemins alternatifs sont utilisés pour rendre le réseau tolérant aux pannes. Pour la détection de pannes, les auteurs considèrent que si un nœud n'a reçu aucune donnée pour une longue durée alors ce dernier envoie un message "Health" à tous ses voisins et attend une réponse. Si ce nœud reçoit une réponse de la part de tous ses nœuds voisins, il considère qu'une erreur s'est produite lors de la transmission précédente, sinon il considère que son circuit de réception est en panne. Par ailleurs, si aucun de ses voisins n'a transmis une réponse, il considère que son circuit émetteur est en panne. Cette information est ensuite transmise à tous les voisins et la défaillance du circuit d'un nœud est détectée par le nœud lui-même en comparant ses données captées avec celles reçues. Si la donnée captée est inférieure à un seuil signifie que le circuit de ce nœud est en bon état, sinon il est considéré en état de défaillance.

2.4.2.6 A Multi-Hop, Multi-Path Fault-Tolerant Hierarchical Routing Protocol for WSN

Dans ce protocole [108] trois types de nœuds sont impliqués : membre du cluster (CM), cluster-head (CH), chef de zone de chevauchement (OAH). Le protocole est exécuté périodiquement et chaque période est constituée d'une phase de configuration et de la phase régulière.

La phase de configuration : Cette phase comprend trois étapes :

1. **L'identification des CHs :** Cette opération est similaire au protocole populaire LEACH [109] tel que chaque CH génère un nombre aléatoire entre 0 et 1, et si ce nombre est inférieur à un seuil prédéfini, le nœud se considère comme CH pour la période courante.
2. **Identification des clusters :** Cette phase est similaire à LEACH, la seule différence est qu'un membre peut appartenir à plus d'un cluster tel que, après la sélection des CHs, chaque CH diffuse un message d'annonce pour informer son nouveau rôle. Ensuite selon la puissance du signal RSSI du message reçu, chaque nœud membre décide à quel cluster il va appartenir. Chaque nœud peut appartenir à d'autres clusters et informe le CH correspondant qu'il sera membre de son cluster.

3. **Identification des chefs de zone de chevauchement :** Chaque nœud qui appartient à plus d'un cluster est considéré comme candidat au status (OAH). Il devrait alors informer son CH correspondant et une fois qu'il est élu, il deviendra un (OAH). Un CH peut avoir un OAH commun avec chacun des clusters voisins. Un OAH assure la communication inter-cluster entre chaque paire de clusters auxquels il appartient.

La phase régulière : Dans cette phase, chaque CH agrège les données reçues de tous ses membres. Puis, il les transmet à chaque OAH appartenant à son cluster en un seul saut en utilisant la méthode TDMA. Après, ce dernier envoie ces données à ses CHs associés. Ce processus de transmission de données se poursuit en un routage multi-chemins jusqu'à ce qu'il atteigne la station de base, tel que si un chemin devient défaillant, les données ne peuvent pas être perdues car elles sont transmises via plusieurs chemins. Après l'expiration de la période, le réseau déclenche une nouvelle période pour ne pas épuiser rapidement la batterie des CHs.

2.5 Comparaison entre les protocoles de routage

Le tableau 2.1 présente une comparaison entre tous les protocoles cités dans ce chapitre en tenant compte de divers paramètres qui sont sélectionnés selon des applications dans lesquelles les réseaux de capteurs peuvent être appliqués. Ces paramètres sont : l'architecture de routage, la transmission de données, la stratégie de déploiement, l'efficacité énergétique, la tolérance aux pannes, la fiabilité et les techniques utilisées pour tolérer les pannes.

La plupart des protocoles existants utilisent le mode de communication multi-sauts, et comme nous le voyons, les protocoles basés sur une architecture hiérarchique ont une efficacité énergétique élevée par rapport à ceux basés sur une architecture plate. Dans les protocoles de routage hiérarchiques les nœuds communiquent avec leur CHs correspondants et les CHs communiquent avec la station de base pour transmettre leurs données agrégées. Les CHs peuvent être élus suivant certains paramètres dans le but d'économiser la consommation d'énergie des nœuds. Également, tous les protocoles ont utilisé un déploiement

aléatoire des nœuds. La diffusion aléatoire est nécessaire en raison du réseau requis à grande échelle ou de l'inaccessibilité de la région de déploiement. Ainsi, la tolérance aux pannes devrait être instaurée pour assurer la fiabilité de livraison de données à la station de base. Par ailleurs, si la défaillance d'un nœud s'est produite, les protocoles impliquent des techniques différentes telles que : multi-chemins, le chemin alternatif et le vice-CH, etc... pour garantir la fiabilité de livraison de données.

TABLE 2.1 – Récapitulatif sur les protocoles tolérants aux pannes

Protocoles	Architecture	Transmission de données	Stratégie de déploiement	Efficacité énergétique	Technique Utilisée
Multi-level	Plate	Multi-sauts	Aléatoire	Moyenne	Chemin alternatif
FMS	Plate	Multi-sauts	Aléatoire	Elevée	Chemin alternatif
RERP	Plate	Multi-sauts	Aléatoire	Faible	Chemin alternatif
DMRF	Plate	Multi-sauts & Jumping Mode	Aléatoire	Moyenne	Transmission Jumping
ENFAT-AODV	Plate	Multi-sauts	Aléatoire	Faible	Chemin alternatif
FAT2D	Plate	Multi-sauts	Aléatoire	Moyenne	Multi-chemins
CFS	Hiérarchique	Multi-sauts	Aléatoire	Elevée	Vice-CH
FEED	Hiérarchique	Un seul saut	Aléatoire	Elevée	Nouveau CH
REEFT	Hiérarchique	Un seul saut	Aléatoire	Très Elevée	Vice-CH
DFCR	Hiérarchique	Multi-sauts	Aléatoire	Très Elevée	Nouveau CH
EEFTMR	Hiérarchique	Multi-sauts	Aléatoire	Elevée	Multi-chemins
Beldjehem	Hiérarchique	Multi-sauts	Aléatoire	Elevée	Multi-chemins

2.6 Le protocole de routage hiérarchique LEACH et ses descendants

Plusieurs protocoles de routage hiérarchiques ont été proposés dans la littérature comme le protocole LEACH [5, 109] qui est le protocole de routage le plus connu en termes de minimisation de consommation d'énergie. En outre, plusieurs approches ont été développées pour améliorer LEACH et réduire ses

limites.

LEACH est un protocole hiérarchique distribué qui utilise la rotation aléatoire des CHs pour répartir la consommation d'énergie entre les nœuds du réseau. Les objectifs principaux de LEACH sont :

- Extension de la durée de vie du réseau,
- Réduire la consommation d'énergie de chaque nœud dans le réseau,
- Utilisation de l'agrégation de données pour réduire le nombre de messages de communication.

L'idée de base du protocole LEACH est que tous les nœuds élisent eux-mêmes les CHs. Les nœuds qui ne sont pas des CHs rejoignent le cluster dont le CH est le plus proche comme le montre la figure 2.5. Après la formation des clusters, les nœuds membres envoient les données captées à leur CH correspondant qui va agréger les données reçues et les transmettre directement à la station de base. L'élection du CH est effectuée une fois à chaque période (round), et les nœuds qui ont été sélectionnés comme CHs ne peuvent pas devenir des CHs une autre fois dans les prochaines périodes pour ne pas épuiser leurs batteries rapidement. En outre, le protocole LEACH assure que chaque nœud dans le réseau possède une probabilité pour être choisi comme CH, ainsi la consommation d'énergie est répartie uniformément entre les nœuds. Par conséquent, LEACH prolonge la durée de vie du réseau par rapport aux autres protocoles.

Le protocole LEACH est exécuté en périodes dont chaque période est constituée d'une phase de mise en place et une phase de transfert de données. Dans la première phase, chaque nœud décide de devenir un CH ou non en générant un nombre aléatoire ente 0 et 1. Si le nombre généré est inférieur au seuil alors ce dernier devient un CH dans la période courante. Chaque nœud calcule le seuil selon l'équation 2.1.

$$T(i) = \begin{cases} \frac{p}{1-p*(r \ mod \ \frac{1}{p})} & \text{if } i \in G \\ 0 & \text{otherwise} \end{cases} \tag{2.1}$$

Où P est le pourcentage des nœuds qui sont des CHs, r est le numéro de la période courante, G est l'ensemble des nœuds qui n'ont pas été sélectionné

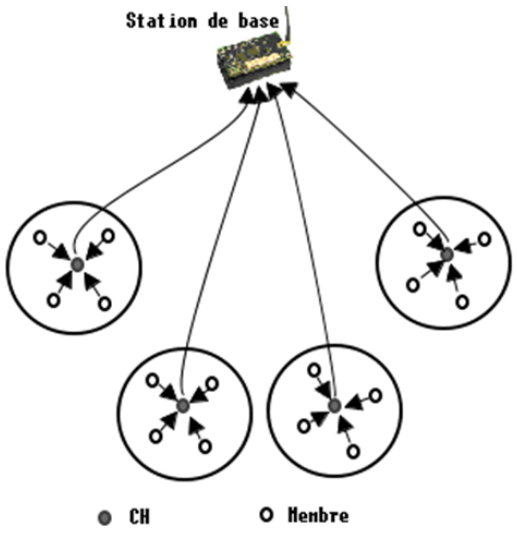

FIGURE 2.5 – Le protocole LEACH

comme CH dans les (1/p) périodes précédentes. En utilisant cette fonction de calcul du seuil, tous les nœuds concourent pour être CH dans un ordre aléatoire. Pendant cette phase, les nœuds qui sont élus comme CHs, diffusent un message de notification dans leur voisinage. Chaque non-CH peut recevoir plusieurs messages de notification mais il rejoint le cluster-head le plus proche afin de minimiser la consommation d'énergie requise pour transmettre les paquets de données.

Après la formation des clusters, un ordonnanceur TDMA (Time Division Multiple Access) est exécuté par chaque CH pour attribuer des time-slots aux nœuds membres. Cette technique de gestion de trafic permet à chaque nœud membre de n'envoyer les données collectées que dans son time-slot afin d'éviter les interférences lors des communications intra-cluster. Puis, la phase de transfert de données sera déclenchée. Durant cette phase, chaque nœud membre transmet ses données captées au CH correspondant durant son time-slot.

Quand les CHs reçoivent tous les données de leurs membres du cluster, ils agrègent les données en un seul paquet et envoient les paquets agrégés à la station de base directement. Cependant, pour éviter les interférences lors des communications CH-à-BS, chaque CH choisit un code CDMA (Code Division Multiple Access) différent des autres CHs.

Dans cette version améliorée de LEACH [110], les auteurs proposent deux

versions de LEACH pour en faire un protocole tolérant aux pannes. Dans la première version nommée FT1-LEACH, chaque cluster contient deux CHs : CH primaire (CH_p) et CH secondaire (CH_s). Les nœuds membres de chaque cluster transmettent leurs paquets de données au (CH_p) et (CH_s) à la fois et seulement le (CH_p) est responsable de transmettre les données à la station de base dans un intervalle de temps limité (timeout). Après l'expiration du timeout si cette tâche n'est pas accomplie le (CH_s) considère que le (CH_p) est en panne et envoie les données collectées à la station de base.

Dans la deuxième version appelée FT2-LEACH, les auteurs proposent d'utiliser la technique de checkpoint qui est capable de tolérer la défaillance dans tout le réseau. Dans cette approche, il est supposé que la station de base est responsable du stockage des informations disponibles sur chaque cluster (CH et ses membres) et si pendant une période la station de base ne reçoit aucun message de la part d'un CH, il est considèré comme nœud défaillant et l'élection du nouveau CH est faite parmi les membres du cluster dont le CH est défaillant.

Dans cette version améliorée de LEACH [111], il est proposé que chaque nœud membre dans un cluster est couvert par deux CHs ; le CH principal et son adjoint qui prend le rôle du CH principal en cas de défaillance de ce dernier. La sélection des CHs est basée sur trois critères : la distance minimale, l'énergie résiduelle maximale, l'énergie minimale. Chaque non-CH rejoint son CH correspondant selon la puissance du signal RSSI tel que la plus grande puissance du signal du message reçu signifie la plus courte distance et donc la transmission de données ne sera pas coûteuse en termes de consommation d'énergie.

Dans [112], un nouvel algorithme de tolérance aux pannes est proposé pour le protocole LEACH afin de déterminer la défaillance des CHs dans un temps très réduit après le début de chaque période (round). Donc pour détecter la défaillance du CH, ce dernier envoie un petit message "HELLO" à tous les nœuds qui sont prêts à recevoir ce message et si aucune transmission n'est reçue, les nœuds peuvent annoncer que le CH est défaillant. Après la défaillance du CH, un modèle de recouvrement de panne choisit un nouveau CH selon la position des nœuds.

Dans cette nouvelle version de LEACH [113], chaque cluster contient un

CH qui est responsable de l'envoi des données reçues de ses membres du cluster à la station de base et un vice-CH qui deviendra un CH en cas de défaillance du CH. Les membres du cluster collectent les données à partir de l'environnement et les envoient au CH correspondant. Cependant, dans la version originale de LEACH, le CH est responsable de la collecte des données reçues de ses membres et les envoie vers la station de base qui peut être située loin de celui-ci. Par conséquent le CH va épuiser son énergie rapidement à cause des opérations coûteuses en termes d'énergie telles que la réception, l'émission et l'overhearing. Pour éviter la défaillance des clusters le protocole V-LEACH implique un CH secondaire (vice-CH) dans chaque cluster qui va prendre le rôle du CH primaire en cas de défaillance de ce dernier.

Dans [114], Min et Zaw proposent une version améliorée de LEACH pour obtenir une tolérance aux pannes efficace. Ils ont proposé une nouvelle phase en plus de celle définie dans la version originale de LEACH appelée la phase de détection de pannes dans laquelle, quand la défaillance du CH est détectée la phase de recouvrement de panne est déclenchée. En plus, si la défaillance d'un CH est identifiée tous les membres du cluster sont informés du CH défaillant et pour l'opération de recouvrement de panne de CH, la station de base choisit un nouveau CH en se basant sur l'énergie résiduelle des membres pour remplacer le CH en panne.

Dans cette version [115], les auteurs proposent deux mécanismes de recouvrement de panne du CH. Le premier consiste à remplacer le CH défaillant par le nœud qui a plus d'énergie dans le cluster correspondant alors que le deuxième mécanisme désigne deux CHs dans chaque cluster à l'aide des jetons pour éviter l'effet de redondance. Il est supposé que tous les membres du cluster envoient les données détectées aux CH_1 et CH_2 en même temps tel que le CH_1 soit responsable de la collecte d'informations reçues de ses membres et les envoie à la station de base et le CH_2 reçoit les données seulement sans les envoyer. Si à un moment, CH_1 devient défaillant alors CH_2 sera le nouveau CH. Toutefois, si CH_1 et CH_2 cessent de fonctionner simultanément, le processus entier commence la phase de notification.

2.7 Conclusion

L'un des principaux défis dans la conception des protocoles de routage pour les RCSFs est de garantir la livraison de données à la station de base. En outre, ces protocoles doivent également minimiser la consommation d'énergie à cause des ressources énergétiques limitées des nœuds capteurs. L'objectif ultime de la conception du protocole de routage est de garantir la livraison de données à la station de base malgré la défaillance de certains nœuds et de maintenir le fonctionnement des nœuds aussi longtemps que possible, ce qui prolonge la durée de vie du réseau. Dans ce chapitre, nous avons présenté une étude sur les protocoles de routage tolérants aux pannes conçus pour les RCSFs.

Divers paramètres sont sélectionnés pour évaluer les performances de ces protocoles tels que l'architecture de routage, la tolérance aux pannes, la fiabilité, etc.. pour comparer les protocoles cités. Ces paramètres sont sélectionnés selon les applications et l'environnement dans lequel le RCSF est exploité. Ensuite nous avons présenté une étude sur le protocole de routage LEACH et ses versions améliorées tolérantes aux pannes. Ainsi la conception des protocoles de routage tolérants aux pannes pour les RCSFs doit tolérer la défaillance des nœuds et assurer une livraison fiable de données à la station de base dans des environnements réalistes.

Dans le chapitre suivant, nous allons présenter une nouvelle version de LEACH tolérante aux pannes en tenant compte de la consommation d'énergie.

Chapitre 3

Une nouvelle version tolérante aux pannes du protocole LEACH pour les RCSF

3.1 Introduction

Un RCSF est un ensemble de nœuds capteurs qui détectent les phénomènes physiques à partir de l'environnement où ils sont déployés. Chaque nœud traite les données détectées et les envoie à la station de base selon une communication sans fil. Ces nœuds sont déployés de façon aléatoire dans des environnements hostiles et souvent inaccessibles pour l'être humain dans le but de surveiller et de contrôler un phénomène particulier [116]. En effet, certains événements tels que l'épuisement des batteries des nœuds puisque ces dernières ne peuvent pas être rechargées ou remplacées à cause des environnements hostiles, des dommages physiques des nœuds, de panne des liens de communication, etc.. qui peuvent se produire pendant le fonctionnement d'un RCSF et l'empêcher de fonctionner correctement [110, 117]. Donc, les RCSFs doivent avoir une durée de vie prolongée pour accomplir leurs tâches exigées correctement. Par conséquent, la défaillance de certains nœuds peut perturber leur fonctionnement et peut rendre d'autres nœuds inaccessibles et les données peuvent être perdues et donc ne pouvaient pas atteindre la destination. Ainsi, les liens de communication entre les nœuds seront perturbés et dans ce cas, il s'avère nécessaire d'établir un système tolérant aux pannes qui assure la fiabilité du routage même en cas de défaillance dans le réseau.

Dans les RCSFs, la consommation d'énergie est considérée comme une contrainte majeure [118] qui doit être prise en considération. Plusieurs protocoles efficaces en termes de consommation d'énergie ont été proposés pour résoudre ce problème comme le protocole LEACH. Ces protocoles visent à

prolonger la durée de vie des réseaux selon plusieurs procédés. Par exemple dans LEACH, on assiste à un changement de la distribution des clusters après chaque période ceci dans le but d'équilibrer la consommation d'énergie entre les nœuds dans le réseau. Par ailleurs, ces protocoles supposent que les nœuds soient déployés dans un environnement idéal c'est-à-dire les nœuds ne sont pas soumis à des pannes et les liens radio sont toujours fiables. Dans cette optique, plusieurs protocoles ont été proposés pour surmonter les conséquences des pannes dans le protocole LEACH, parmi ces travaux notre contribution, qui est constituée de deux propositions :

- Créer des chemins CH-à-CH pour minimiser la consommation d'énergie.
- Créer un chemin alternatif CH-à-CH en plus de chemin principal pour assurer une tolérance aux pannes dans le réseau lorsque certains CHs tombent en panne.

3.2 Motivations

Dans les RCSF, les protocoles de routage ont été conçus pour équilibrer la consommation d'énergie et prolonger la durée de vie des réseaux. Cependant, l'occurrence des pannes peut dégrader leurs performances. Á cet effet, nous avons proposé une amélioration du protocole LEACH. Sa version originale a donné de bons résultats en termes de conservation d'énergie même s'il utilise des communications directes avec la station de base indépendamment de l'emplacement des CHs. Par ailleurs, l'utilisation des communications multi-sauts pourraient améliorer la conservation d'énergie par rapport aux communications en un seul saut avec la station de base [119]. En outre, la consommation d'énergie des communications sans fil est directement liée à la distance qui sépare les nœuds communicants et au facteur d'atténuation du signal qui caractérise l'environnement. En plus, une communication à un seul saut est coûteuse en termes de consommation d'énergie. Par conséquent, la plupart des algorithmes de routage utilise une communication multi-sauts puisqu'il est plus efficace.

Dans le protocole LEACH, il est supposé que le déploiement des nœuds est dans un environnement idéal c'est-à-dire qu'ils ne subissent aucune défaillance jusqu'à l'épuisement de leurs batteries. De ce fait, dans le but d'améliorer les

performances de LEACH, nous avons proposé deux contributions. La première vise à étendre la durée de vie du réseau en utilisant des communications multi-sauts, et la seconde vise à rendre LEACH tolérant aux pannes dans un environnement non-idéal.

3.3 Contribution 1

Cette contribution se déroule en deux phases [120] :

3.3.1 La première phase (setup phase)

Au début de cette phase, la station de base diffuse un message "HELLO" à tous les nœuds du réseau. Chaque nœud qui reçoit ce message peut connaître sa position par rapport à la station de base c'est-à-dire s'il est proche ou loin de la station de base selon la force du signal du message reçu (RSSI). Puis, le processus de sélection des CHs est déclenché.

Lors de la formation des clusters, on distingue deux types de CHs : les CHs qui sont proches de la station de base dont le statut est CH_{Sup} et les CHs qui sont loins de la station de base dont le statut est CH_{Inf}. Chaque CH qui a pour statut CH_{Sup} diffuse un message "HELLO" et chaque CH de type CH_{Inf} qui reçoit ce message, calcule la nouvelle force de signal (RSSI) du message reçu pour choisir son nœud relais parmi les CHs CH_{Sup}. En outre, nous impliquons un autre paramètre appelé "crédibilité" pour sélectionner le nœud relais. Par conséquent, la sélection des CHs de CH_{Sup} en tant que nœuds relais par les CHs de type CH_{Inf} repose sur deux paramètres :

— La puissance du signal RSSI reçue de chaque message envoyé par le CH CH_{Sup}.

— La crédibilité (cred) où "cred" est un nombre aléatoire compris entre 0 et 1 ($0 < cred < 1$).

3.3.2 La deuxième phase (steady phase)

Dans cette phase, Chaque CH de type CH_{Inf} crée une liste pour garder tous les messages HELLO reçus par les CHs qui sont proches à la station de

base. Puis, il choisit le nœud relais parmi tous les CHs de type CH_{Sup} selon les deux paramètres mentionnés ci-dessus.

3.4 Contribution 2

La communication multi-sauts minimise la consommation d'énergie mais elle est sujet à des pannes tel que quand un nœud relais (CH : CH_{Sup}) cesse de fonctionner alors le chemin auquel ce nœud appartient pourrait être endommagé. Il en résulte par la suite une dégradation des performances du réseau puisque toutes les informations captées par les nœuds membres seront perdues ainsi que l'énergie consommée sera gaspillée. Pour éviter ces nœuds défaillants et aussi la perte des données qui peut être considérable, un chemin alternatif est établi pour assurer la fiabilité de la transmission de données et garantir la bonne réception au niveau de la station de base. Par conséquent, lorsqu'un CH remarque que son premier nœud relais est devenu défaillant, alors il sélectionne un autre nœud relais qui fait partie de son chemin alternatif et qui est sûrement actif. Ce processus offre une tolérance aux pannes et aussi une disponibilité du système durant toute la durée de vie du réseau. La figure 3.1 illustre notre approche proposée avec les deux contributions citées ci-dessus.

3.5 Avantages et inconvénients de la version améliorée de LEACH

Notre approche proposée vise à améliorer les performances du protocole LEACH dans un environnement non-idéal. Cette approche permet les avantages suivants :

- Minimise la consommation d'énergie,
- En présence de panne, le protocole est résistant aux défaillances,
- Le taux de perte de paquets est presque négligeable,
- Assure la disponibilité du réseau.

Cependant cette approche présente quelques inconvénients qui n'ont pas une grande influence sur la bonne conduite des réseaux tels que :

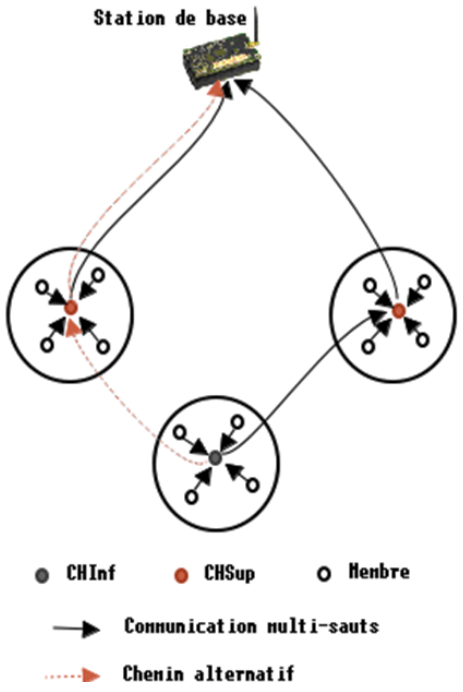

FIGURE 3.1 – Le protocole LEACH modifié

- Plus de messages de notification échangés,
- L'overhead est élevé.

3.6 Simulation et évaluation

Nous avons effectué plusieurs simulations pour illustrer les performances de nos contributions à l'aide du simulateur TOSSIM [121], et nous les avons comparés avec la version originale de LEACH en termes de consommation d'énergie et de taux de paquets reçus avec succès à la station de base. Pour cela, nous avons utilisé un réseau qui contient respectivement 50, 100, 150 et 200 nœuds fixes, qui sont déployés de manière aléatoire sur une surface carrée 100m*100m et l'énergie initiale est égale à 2 joules pour chaque nœud à l'exception de la station de base. Les simulations ont été réalisées dans 600 secondes. Le tableau 3.1 résume les paramètres de simulation.

Dans ce contexte, nous avons calculé la consommation d'énergie selon le modèle d'énergie de Shnayder et al. [122]. Dans ce modèle, la consommation d'énergie de la transmission et la réception d'un seul bit en utilisant le capteur

TABLE 3.1 – Les paramètres de simulation

Paramètre	Valeur
Zone de déploiement	100m x 100m
Temps de simulation	500 sec
Taille du réseau	50, 100, 150, 200
Taille du paquet	29 bytes
Energie initiale du nœud	2J

MICA2 est respectivement 4.602 μJ et 2.34 μJ. Nous avons également utilisé un modèle de pannes c'est-à-dire qu'il y a une probabilité qu'un CH puisse cesser de fonctionner.

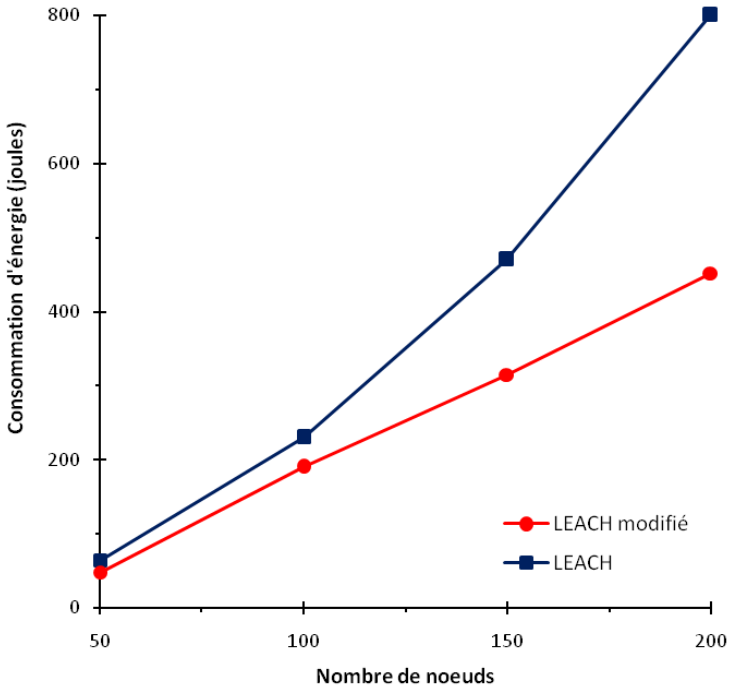

FIGURE 3.2 – Variation de la consommation d'énergie avec le nombre de nœuds

La figure 3.2 montre que la consommation d'énergie dans notre approche proposée est inférieure à celle de la version originale de LEACH. En effet, dans notre approche, nous avons supposé que lorsque la station de base est assez loin du CH qui veut envoyer des informations, ce dernier pouvait impliquer un autre CH comme nœud relais proche à la station de base. Cependant, dans

la version originale de LEACH, les CHs transmettent directement les données agrégées à la station de base quelle que soit la distance qui les sépare de la station de base. En outre, il est prouvé que l'utilisation d'un routage multi-sauts consomme moins d'énergie par rapport à une communication directe i.e communication utilisant un seul saut [1].

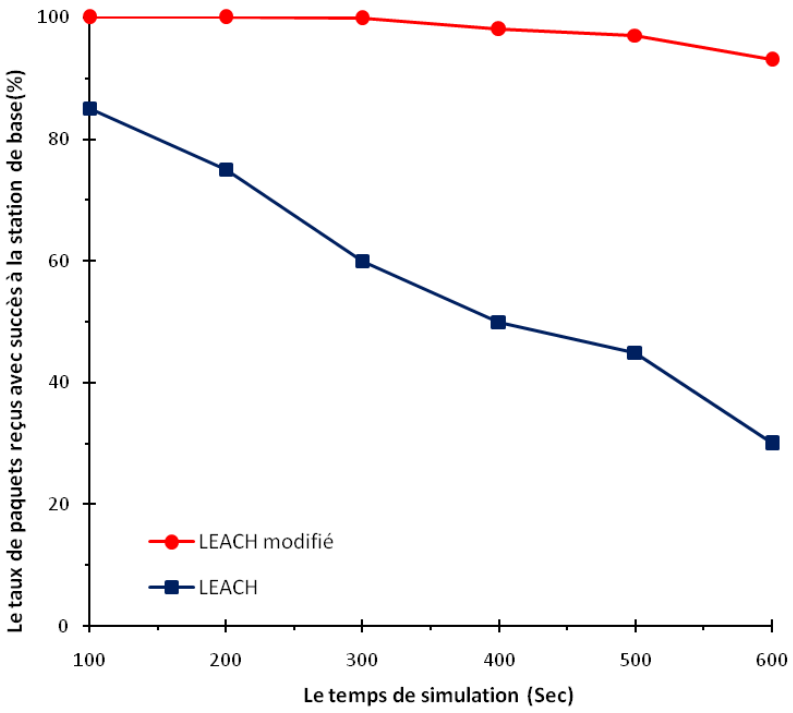

FIGURE 3.3 – Le taux de paquets reçus avec succès en fonction du temps

La figure 3.3 montre que le taux de paquets reçus avec succès par la station de base dans LEACH modifié est plus élevé que dans la version originale de LEACH. Dans LEACH, quand un CH tombe en panne, ceci affecte son propre cluster et les données reçues de ses membres ne peuvent pas atteindre la station de base et par suite le cluster devient inutile alors que dans notre contribution si un CH cesse de fonctionner, il ne sera pas utilisé comme nœud relais et le CH peut utiliser un autre nœud relais dans le chemin alternatif.

3.7 Conclusion

Dans ce chapitre, nous avons proposé une version améliorée de LEACH pour améliorer sa version originale en utilisant un routage multi-sauts et permettre une tolérance aux pannes dans les RCSF. L'utilisation de LEACH en utilisant un routage multi-sauts augmente considérablement la quantité d'informations reçues par la station de base durant toute la durée de vie du réseau. En outre, nous avons proposé une autre version améliorée de LEACH qui rend le protocole tolérant aux pannes. Dans ce contexte, les résultats de simulation ont montré que notre contribution a abouti avec succès à un comportement efficace en termes de consommation d'énergie et de taux de paquets reçus par la station de base.

Dans le chapitre suivant, nous allons présenter une autre version améliorée du protocole LEACH en utilisant le modèle LogNormal Shadowing Model (LNS) [6] qui implique la qualité du lien pour calculer la probabilité de réception sans erreur entre les nœuds communicants.

Chapitre 4

Une nouvelle version de LEACH pour un environnement non-idéal

4.1 Introduction

Un RCSF est un ensemble de nœuds qui sont déployés dans une zone d'intérêt dans le but de communiquer, contrôler et détecter l'environnement proche avec la capacité de calculer, envoyer et recevoir les données détectées. Récemment, plusieurs chercheurs ont consacré beaucoup d'études dans plusieurs domaines comme la surveillance de l'environnement, le contrôle industriel, le transport et le domaine médical. Dans ces applications, assurer la fiabilité du réseau est nécessaire pour une collecte fiable de données c'est-à-dire sans perte d'informations. En outre, assurer une longue durée de vie du réseau est un grand défi pour les RCSF, ainsi que la mise en point de la conception des protocoles de routage [123].

Le processus de routage est une opération fondamentale dans les RCSFs. Il consiste à transmettre un message d'un nœud source vers la station de base qui est éloignée selon différentes techniques de routage : hiérarchique, basé sur la localisation (location-based) et centré sur les données (data-centric) [95]. En outre, la conception de la plupart des protocoles de routage était basée sur une couche physique idéale modélisée par le graphe du disque unitaire [124]. Cependant, bien que ce modèle soit couramment utilisé, il ne peut pas être considéré comme un modèle réaliste car il suppose que les messages envoyés sont toujours reçus sans erreur si la distance entre l'émetteur et le récepteur est inférieure ou égale à la portée de transmission de l'émetteur [125]. Cette hypothèse ne tient pas compte des fluctuations aléatoires du signal radio, qui a un impact significatif sur les transmissions à cause des erreurs générées par les fluctuations dans les messages échangés entre les nœuds. Par conséquent, il est intéressant d'étudier le comportement de ces protocoles de routage dans

un environnement réaliste pour illustrer l'effet des fluctuations du signal radio sur les performances de ces protocoles. Parmi toutes les solutions proposées, nous avons choisi de mettre l'accent sur le protocole LEACH [5] car il fournit de bons résultats en utilisant une couche physique idéale et c'est un protocole de routage le plus populaire conçu pour les RCSF.

Dans ce chapitre, nous avons utilisé le modèle "lognormal shadowing" [6] pour un environnement de simulation réaliste et analyser les performances du protocole LEACH par ce modèle. Le modèle considéré prend en compte les fluctuations du signal radio et pourrait donc être plus réaliste que le modèle couramment utilisé celui du disque unitaire. De plus, il calcule la probabilité de réception sans erreur entre les nœuds communicants en fonction de la distance qui les sépare. Ensuite, nous avons proposé un protocole de routage tolérant aux pannes basé sur LEACH appelé FTLR (Fault-Tolerant LEACH-based Routing protocol) [126] pour qu'il s'adapte à un environnement réaliste. Dans notre contribution, nous supposons que si la probabilité de réception sans erreur est inférieure à un certain seuil alors le message sera corrompu. Dans ce cas, pour éviter trop de messages corrompus, nous avons proposé un routage multi-sauts dans le cluster où le nœud membre pourrait impliquer un voisin comme nœud relais pour atteindre son CH correspondant.

4.2 Préliminaires

Avant de présenter notre contribution, nous donnons quelques définitions et notations qui facilitent la compréhension de ce qui suit.

4.2.1 Notations et hypothèses

Un RCSF peut être modélisé par un graphe non orienté $G = (E, V)$ où V représente l'ensemble des nœuds et $E \subseteq V^2$ est un ensemble d'arêtes tel que une arête $e = (u, v)$ appartient à E si et seulement si un nœud u est capable de transmettre des messages à v et vice-versa. Un identifiant est attribué à chaque nœud $u \in V$ $(id(u))$. L'ensemble des voisins d'un nœud u est représenté par $N_1(u)$ comme présenté par l'équation 4.1 et la cardinal de cet ensemble est connu comme le degré de u, noté $\delta(u)$.

$$N_1(u) = \{v \in V : (v \neq u) \wedge (u, v) \in E\} \tag{4.1}$$

Nous considèrons les hypothèses suivantes :

- Chaque nœud a une antenne omnidirectionnelle ainsi qu'une seule transmission d'un nœud peut être reçu par tous les nœuds dans son voisinage.
- Les nœuds sont presque statiques dans un délai raisonnable.
- Un nœud est considéré comme voisin d'un autre nœud si la probabilité de réception des messages entre eux est supérieure à un seuil prédéfini p_0.
- Un message peut être reçu sans erreur, si la distance séparant les nœuds communicants est inférieure ou égale à $R(p_0)$ dans lequel la probabilité de réception avec succès à cette distance est égale à p_0.

4.2.2 Le modèle radio

Dans cette section, nous présentons d'abord le modèle de disque unitaire (UDG : Unit Disk Graph). Supposons un graphe $G = (E, V)$, où tous les nœuds ont la même portée de transmission désigné par R_c. Le modèle de disque unitaire définit l'ensemble E des arêtes selon l'équation 4.2.

$$E = \{(u, v) \in V_2 : (u \neq v) \wedge dist(u, v) \leq R_c\} \tag{4.2}$$

Où $dist(u, v)$ est la distance euclidienne entre u et v. Ce modèle bien qu'il soit couramment utilisé ne peut pas être considéré comme un modèle réaliste car il suppose que les messages sont toujours reçus sans erreur si la distance entre les nœuds communicants est inférieure ou égale au rayon de transmission R_c [125]. Cette hypothèse ne tient pas compte des fluctuations aléatoires du signal radio, qui peut avoir un impact significatif sur les transmissions. Cependant, il est intéressant d'évaluer les performances de ces protocoles de routage dans un environnement réaliste. Pour cela, nous avons impliqué le facteur qualité de lien pour déterminer la probabilité de réception sans erreur entre les nœuds afin de savoir si le message a été reçu correctement ou bien corrompu. Cette probabilité implique plusieurs facteurs tels que la puissance du signal, la distance séparant les nœuds communicants et aussi la présence des obstacles,

etc. Il peut être difficile d'obtenir une évaluation précise de tous ces facteurs, qui sont eux même sujets à des erreurs. Par conséquent, nous supposons que la puissance du signal diminue progressivement en fonction de la distance. De ce fait la probabilité d'une réception sans erreur peut être calculée en fonction de la distance séparant les deux nœuds communicants. Ainsi, nous proposons d'utiliser le modèle "lognormal shadowing" décrit dans [6, 127] pour évaluer cette probabilité selon l'équation (4.3).

$$F(x) = \begin{cases} 1 - \frac{(\frac{x}{R_c})^{2\alpha}}{2}, & si\ 0 < x \leq R_c \\ \frac{(\frac{2R_c - x}{R_c})^{2\alpha}}{2}, & si\ R_c < x \leq 2R_c \\ 0 & \text{Sinon} \end{cases} \tag{4.3}$$

Où α représente le coefficient d'atténuation qui dépend de l'environnement et x est la distance séparant l'émetteur du récepteur. Dans cette formule, nous supposons que la probabilité de réception sans erreur avec une portée de transmission R_c est égale 0.5. La figure 4.1 illustre l'évolution de la probabilité de réception sans erreur en fonction de la distance entre les nœuds communicants avec $R_c = 10$ et $\alpha = 2$.

4.3 Contribution

Comme mentionné dans le chapitre 2, plusieurs travaux ont été proposés pour rendre le protocole LEACH tolérant aux pannes, mais ces travaux ne prennent pas compte de la qualité du lien lors de transmission de données. En outre, il y a des contributions qui impliquent plus d'un CH dans chaque cluster pour assurer la fiabilité de transmission de données comme dans [110, 111, 113], mais ces contributions ne pouvaient pas garantir cet objectif dans un environnement réaliste. Dans ce contexte, nous avons évalué LEACH dans un environnement réaliste représenté par le modèle "lognormal shadowing" pour illustrer ses limites dans de tels environnements. Ensuite, nous avons proposé une version améliorée de LEACH qui implique la qualité du lien dans la sélection des nœuds relais pour rendre le protocole LEACH adaptable à un environnement réaliste.

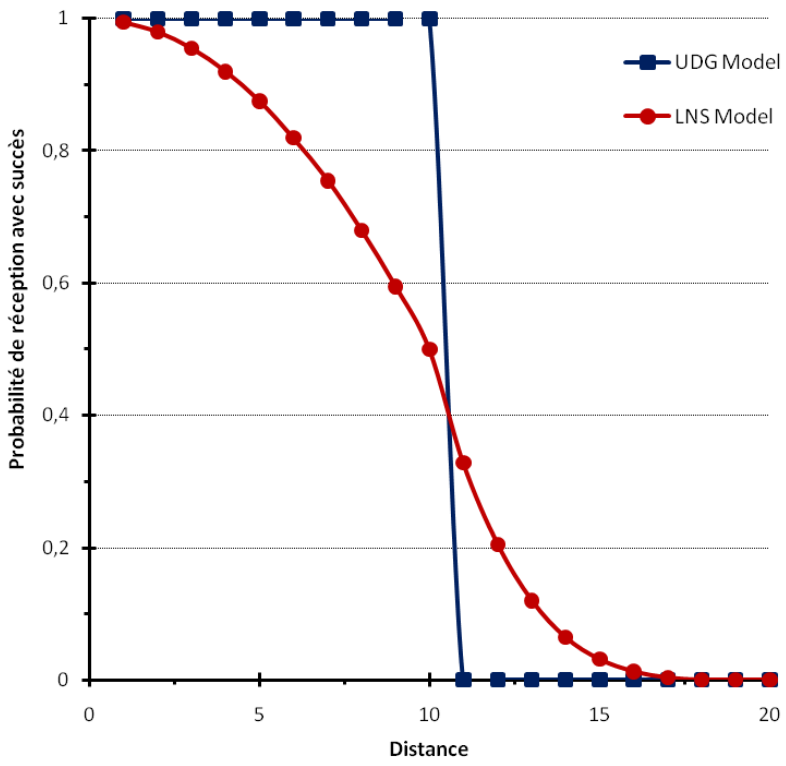

FIGURE 4.1 – Probabilité de réception sans erreur dans le modèle LNS et le modèle UDG

Avant de présenter notre contribution, nous avons évalué d'abord les performances du protocole LEACH par le modèle "lognormal shadowing" pour montrer ses faiblesses en termes de nombre de paquets perdus, le taux de paquets corrompus et la consommation d'énergie.

4.3.1 Evaluation de LEACH dans un environnement réaliste [128]

Dans cette section, nous avons évalué les performances de la version originale de LEACH dans un environnement réaliste en termes de nombre de paquets perdus et le taux de paquets corrompus. Pour cela, nous avons utilisé le simulateur TOSSIM [121]. Ensuite, nous avons analysé les résultats obtenus pour illustrer les faiblesses de la version originale de LEACH dans ce type d'environnements. Nous avons utilisé le modèle "lognormal shadowing" pour représenter un environnement réaliste. Ce modèle implique la qualité du lien

dans la probabilité de réception sans erreur. En outre, nous avons fait varier la probabilité de réception avec succès entre p= 0.6, 0.7 et 0.8 pour différentes tailles de réseau : 20, 40, 60, 80 et 100 nœuds.

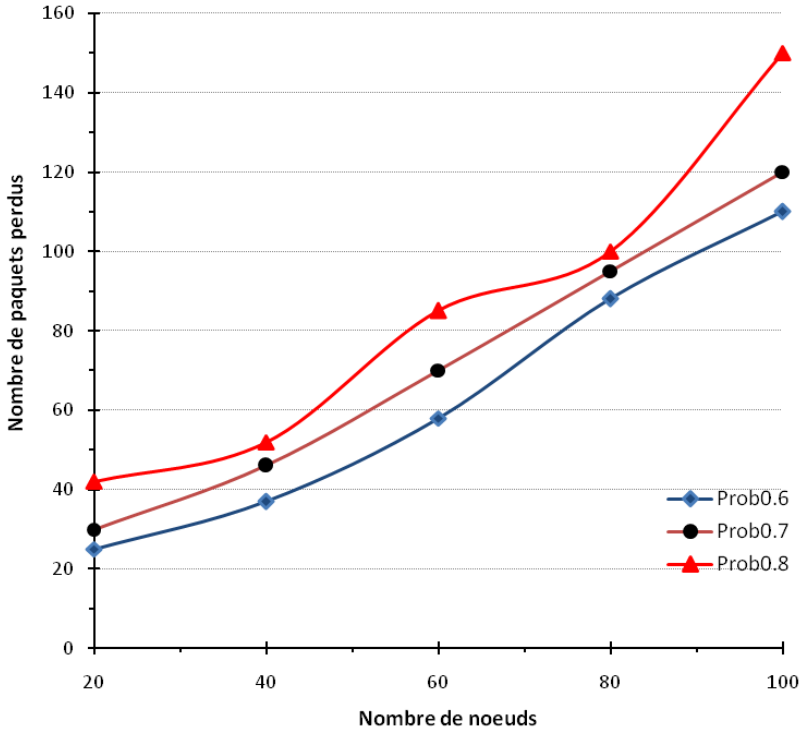

FIGURE 4.2 – Nombre de paquets perdus vs. La taille du réseau

La figure 4.2 montre la variation du nombre de paquets perdus en fonction de la taille du réseau pour différentes valeurs de probabilité de réception sans erreur. Nous observons que le nombre de paquets augmente lorsque la probabilité augmente. Ces résultats obtenus signifient que les performances de LEACH se dégradent dans un environnement réaliste et la version originale de ce protocole n'est pas adaptée pour un environnement non idéal.

La figure 4.3 illustre le taux de perte de paquets en fonction de la taille du réseau avec différentes valeurs de probabilité. Nous remarquons que le taux de paquets corrompus augmente lorsque la probabilité de réception avec succès augmente. Par exemple, dans un réseau qui contient 100 nœuds avec une probabilité égale à 0.8, le taux de paquets perdus devient la moitié de tous les paquets transmis. De ce fait, il est nécessaire de prendre en compte la qualité du lien dans le processus de transmission de données.

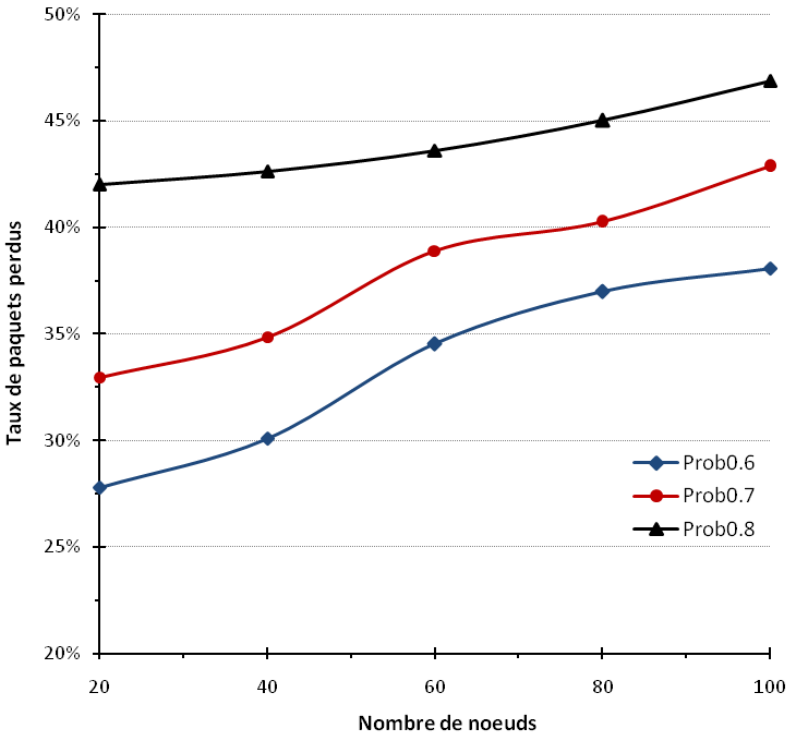

FIGURE 4.3 – Le taux de perte de paquets vs. La taille du réseau

4.3.2 Protocole proposé : le protocole FTLR

Selon les résultats obtenus après une analyse du protocole LEACH, il est démontré qu'il est nécessaire d'améliorer ses performances, afin qu'il soit adapté à un environnement réaliste. Ainsi, nous avons proposé un schéma de routage multi-sauts nommé le protocole FTLR au lieu d'un schéma de routage à un saut pour surmonter les limites de LEACH. Ainsi quand un nœud ne peut pas communiquer correctement avec son CH alors un nœud relais est impliqué pour garantir la bonne réception des paquets de données de la part du CH.

Notre contribution tient compte de la qualité des liens afin d'éviter les liens de communication non fiables. Ainsi quand un nœud membre veut transmettre les données à son CH correspondant, il calcule d'abord la probabilité de réception sans erreur. Si cette probabilité est supérieure à un seuil prédéfini $Thresh_1$ alors le paquet sera reçu sans erreur, sinon une communication multi-sauts sera incorporée pour assurer une livraison fiable de données et en

même temps, minimiser la consommation d'énergie puisqu'une communication multi-sauts consomme moins d'énergie qu'une communication à un saut. Nous avons supposé que si un nœud membre d'un cluster possède un lien de communication fiable avec son CH, il est considéré comme un nœud parfait (perfect node), et une liste de ce type de nœuds sera créée par la suite. En outre, lorsque la probabilité de réception sans erreur est inférieure au seuil prédéfini, le nœud membre du cluster sélectionne le nœud optimal du prochain saut parmi ses voisins pour atteindre son CH. Cette sélection est effectuée selon l'algorithme suivant :

Algorithme de sélection du prochain saut :

- M_i : Identifiant d'un noeud membre i d'un cluster,

- CH_i : Identifiant du cluster-head i,

- $\binom{x_m}{y_m}$: les coordonnées de M_i,

- $\binom{x_c}{y_c}$: les coordonnées de CH_i

Début

- M_i calcule la distance qui le sépare de son CH,

$d = \sqrt[2]{(x_m - x_c)^2 + (y_m - y_c)^2}$

- M_i calcule la probabilité de réception sans erreur,

$Pr(x) = 1 - \frac{(\frac{x}{R_c})^{2\alpha}}{2}$

if (Pr(x) < Threshold) **then**

M_i choisit parmi ses 1-voisins celui qui lui garantit une livraison fiable avec son CH,

repeat

- Choisir v de $N_1(M_i)$

- Calculer les distances : d_1 et d_2

- d_1 : la distance de M_i à v,

- d_2 : la distance de v à CH_i,

$$Pr_1(d_1) = 1 - \frac{(\frac{d_1}{R_c})^{2\alpha}}{2}$$

$$Pr_2(d_2) = 1 - \frac{(\frac{d_2}{R_c})^{2\alpha}}{2}$$

until $((Pr_1 \geq Thresh) and (Pr_2 \geq Thresh))$

end if

Fin

4.4 Les résultats de simulation

Dans nos expériences, nous avons effectué des simulations en nous basant sur le modèle LNS "LogNormal Shadowing" pour évaluer les performances du protocole FTLR en termes de taux de perte de paquets et la consommation d'énergie. Pour cela, nous avons utilisé une topologie du réseau dans laquelle les nœuds sont distribués aléatoirement sur un plan dont les coordonnées sont entre (x=0, y=0) et (x=500, y=500). Nous avons effectué des simulations en utilisant deux seuils distincts : $Thresh_1 = 0.6$ et $Thresh_2 = 0.7$ pour une probabilité de réception sans erreur. Le tableau 4.1 résume les paramètres de simulation utilisés pour ces évaluations.

TABLE 4.1 – Les paramètres de simulation

Parameter	Value
Zone de déploiement	100m x 100m
Temps de simulation	500 sec
Taille du réseau	20, 40, 60, 80, 100
Taille du paquet	29 bytes
Energie initiale du nœud	2J
Seuil	0.6, 0.7
α	2

4.4.1 Le taux de perte de paquets

Nous avons évalué le protocole FTLR et la version originale de LEACH avec le modèle LNS

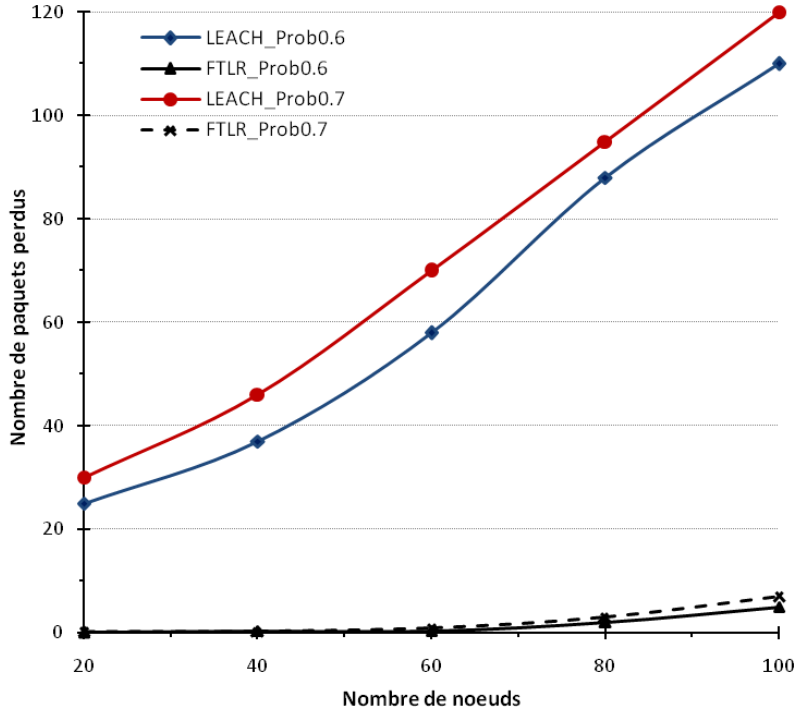

FIGURE 4.4 – Comparaison entre LEACH et FTLR en terme de nombre de paquets perdus

La figure 4.4 montre que le nombre de paquets perdus est presque négligeable dans le protocole FTLR par rapport à LEACH, ce qui signifie que la fiabilité est obtenue avec le protocole FTLR pour différentes valeurs de probabilité $Thresh_1 = 0.6$ et $Thresh_2 = 0.7$.

La figure 4.5 prouve l'efficacité de notre contribution puisque le taux de paquets perdus est presque négligeable. Par conséquent, on pourra dire que la fiabilité requise est atteinte. Par ailleurs, le but de notre contribution est de fournir un compromis suffisant entre garantir la fiabilité de transmission de données et atteindre une tolérance aux pannes des liens de communication. Ainsi, en se basant sur les résultats obtenus, le protocole FTLR peut surpasser la version originale et il peut être appliqué dans un environnement réaliste puisque la fiabilité et la tolérance aux pannes sont garanties.

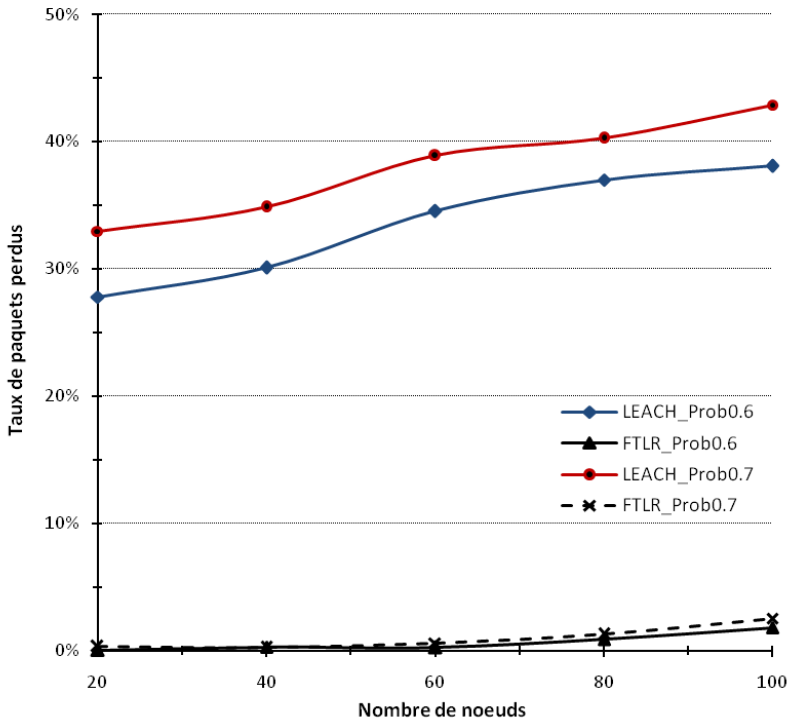

FIGURE 4.5 – Comparaison entre LEACH et FTLR en termes de taux de paquets perdus

4.4.2 La consommation d'énergie

Comme la consommation d'énergie est l'une des préoccupations majeures dans les RCSFs, nous avons évalué et comparé la consommation d'énergie entre les deux protocoles LEACH et FTLR. Nous avons supposé que si la probabilité de réception sans erreur est inférieure à un seuil prédéfini, le nœud membre génère un nombre aléatoire entre 0 et 1, et si ce nombre est supérieur à 0.5 alors il effectue une retransmission de paquets sinon le paquet sera considéré comme un paquet perdu. Dans ce contexte, la consommation d'énergie est calculée selon le modèle d'énergie de [122], qui considère l'énergie consommée pour l'émission et la réception d'un bit en utilisant un capteur de type MICA2 est respectivement 4.602 μJ et 2.34 μJ.

Les figures 4.6 et 4.7 montrent respectivement que le protocole FTLR consomme moins d'énergie par rapport au protocole LEACH puisqu'une communication multi-sauts est efficace en termes de minimisation de consommation d'énergie, par contre la retransmission est définie par sa consom-

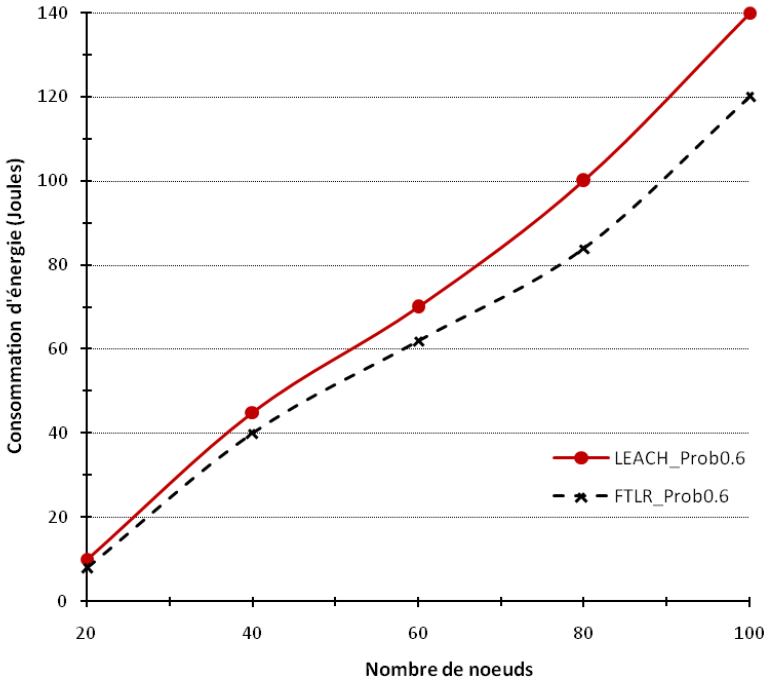

FIGURE 4.6 – Consommation d'énergie dans LEACH et FTLR_Prob0.6

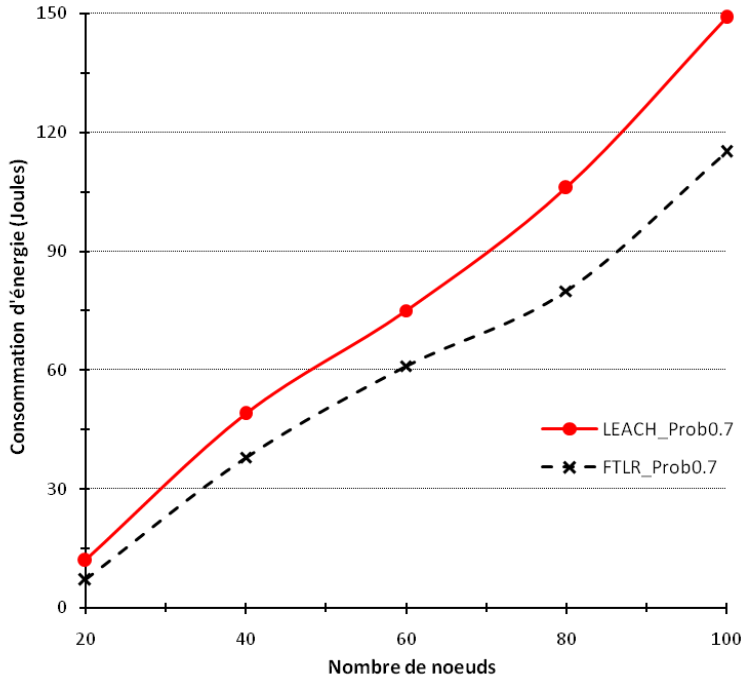

FIGURE 4.7 – Consommation d'énergie dans LEACH et FTLR_Prob0.7

mation importante d'énergie lorsque les paquets de données sont perdus ou contiennent des erreurs.

4.5 Conclusion

Dans ce chapitre, nous avons proposé d'utiliser le modèle LNS pour évaluer les performances de la version originale du protocole LEACH [109] afin d'illustrer son efficacité dans différents environnements. Le modèle LNS prend en compte les fluctuations du signal radio et pourrait donc être considéré comme un modèle réaliste par rapport au modèle UDG. Les résultats obtenus ont montré les faiblesses du protocole LEACH dans un environnement de simulation non idéal tel que le modèle LNS. En outre, nous avons proposé un protocole de routage tolérant aux pannes basé sur le protocole LEACH et qui est adapté à des environnements non idéals. Les résultats de simulation montrent que notre contribution proposée offre de meilleures performances par rapport au protocole LEACH en termes de taux de perte de paquets et de consommation d'énergie.

Dans le chapitre suivant, nous allons présenter un nouveau protocole hiérarchique tolérant aux pannes pour les RCSFs adapté à des environnements réalistes.

Chapitre 5

Conception d'un protocole de routage basé sur la qualité des liens pour les RCSF

5.1 Introduction

La préoccupation majeure concernant les RCSFs est la consommation d'énergie puisque les capteurs sont alimentés par une source énergétique limitée qui est généralement irremplaçable en raison des environnements hostiles dans lesquels ils sont déployés. Ainsi de nombreuses recherches se sont focalisées sur la conception des protocoles de conservation d'énergie comme dans [19, 129, 130]. Dans ce contexte, les protocoles de routage hiérarchiques sont considérés comme des protocoles prometteurs pour minimiser la consommation d'énergie dans les RCSF [5, 95, 131].

Dans les protocoles de routage hiérarchiques, le réseau est divisé en groupes appelés "clusters", où chaque groupe est constitué d'un certain nombre de nœuds membres qui détectent les données à partir de leur environnement et les envoient à leur chef de groupe correspondant appelé "cluster-head" (CH). Le cluster-head est responsable de collecter les données de ses membres, les agréger et les envoyer à la station de base. En raison de ces différentes tâches réalisées par le CH, ce dernier peut épuiser son énergie rapidement. Dans ce contexte, plusieurs chercheurs ont consacré leurs travaux en vue de trouver une solution efficace pour prolonger la durée de vie du CH. En outre, les nœuds de capteurs sont sujets à des défaillances en raison de leur déploiement dans des environnements souvent hostiles, de la limitation de leurs ressources énergétiques et les fluctuations du signal radio. La défaillance d'un nœud peut affecter la durée de vie de l'ensemble du réseau et diminuer sa performance ainsi la défaillance des CHs peut perturber le fonctionnement du réseau de

telle sorte qu'il pourrait être inutile. Dans ce cas de figure, les protocoles de routage hiérarchiques permettent la tolérance aux pannes pour garder le réseau opérationnel. Plusieurs travaux de recherche ont été basés sur une hypothèse idéale concernant le canal sans fil c'est-à-dire le canal radio est considéré toujours fiable. Cette hypothèse ne reflète pas une réalité dans les RCSF. De ce fait, il s'avère nécessaire d'étudier les performances des protocoles conçus pour un environnement idéal dans un environnement non idéal pour voir leur robustesse dans ce type d'environnement.

Dans un environnement réaliste, les fluctuations du signal radio peuvent provoquer la non-fiabilité des liens de communication entre les nœuds et par la suite provoquer la perte de paquets de données. Dans des travaux, les auteurs ont proposé des protocoles dans un environnement dont les liens de communication sont non fiables. Dans ces protocoles, les nœuds relais sont évalués et le nœud avec la plus grande probabilité de livraison fiable de données est considéré comme nœud fiable.

Dans ce chapitre, nous proposons une nouvelle approche optimale pour faire face à la tolérance aux pannes dans les protocoles de routage hiérarchiques conçus pour les RCSF tout en minimisant la consommation d'énergie. Dans cette approche, les CHs sont sélectionnés selon leur énergie résiduelle avec une certaine probabilité. La communication au sein d'un cluster est basée sur deux modèles : (i) le modèle LogNormal Shadowing (LNS) [6], qui calcule la probabilité de réception sans erreur entre chaque couple de nœuds en communication en se basant sur la distance euclidienne et (ii) le modèle probabiliste dans lequel la probabilité de réception est générée aléatoirement. Dans les deux modèles, si la probabilité de réception est supérieure à un seuil prédéfini, le lien de communication sera considéré comme un lien fiable entre le membre et son CH correspondant et dans ce cas une communication directe sera établie entre eux, sinon une communication multi-sauts est incorporée. Dans ce deuxième cas, les nœuds qui ont des liens fiables avec leur CHs sont utilisés comme des nœuds relais. En outre, la communication entre les CHs et la station de base utilise le modèle LNS et le modèle probabiliste. Si la probabilité de réception de paquets de données est supérieure à un seuil, une communication directe est effectuée autrement, une communication multi-sauts est établie et les CHs avec une probabilité élevée sont sélectionnés comme des

nœuds relais. Cette approche proposée prend en considération la défaillance des CHs en permettant à chaque CH de sélectionner son adjoint (vice-CH) selon son énergie résiduelle et la distance qui les séparent. Si un CH cesse de fonctionner, son CH adjoint deviendra le nouveau CH et la même procédure de contrôle de qualité des liens entre les membres et le nouveau CH et aussi entre le nouveau CH et la station de base est effectuée en se basant sur les deux modèles (LNS, probabiliste).

5.2 Préliminaires et hypothèses

5.2.1 Hypothèses

Nous considérons un RCSF constitué de N nœuds homogènes répartis aléatoirement sur une région pour surveiller un environnement. Nous supposons que chaque nœud possède une information locale telle que l'énergie résiduelle et la distance qui le sépare de son CH correspondant. Nous considérons que chaque nœud dans le réseau a une énergie initiale qui est égale à 2 joules et le processus de collecte de données est divisé en périodes comme dans le protocole LEACH [5] où à chaque période, le CH agrège les données reçues de ses membres via une communication multi-sauts pour éviter la redondance des données et minimiser le nombre de paquets de données transmis. Ensuite, le CH envoie les données agrégées à la station de base en impliquant d'autres CHs comme nœuds relais ou via une communication directe selon la qualité des liens.

5.2.2 Les causes de l'irrégularité de la radio

L'irrégularité de la radio est un phénomène non négligeable dans les communications sans fil. Elle provoque des interférences et des liens asymétriques dans les couches supérieures. Par conséquent, elle pourrait directement ou indirectement affecter les performances de ces couches en particulier la couche réseau.

L'irrégularité de la radio est causée par deux types de facteurs : les dispositifs et les médiums de propagation [132]. Les caractéristiques du dispositif impliquent le type d'antennes (directionnelle ou omnidirectionnelle), la puis-

sance d'émission, les gains de l'antenne (au niveau de l'émetteur et du récepteur), la sensibilité du récepteur et le rapport signal-sur-bruit (SNR [1]). Les propriétés du médium comprennent le type de support, le bruit et certains d'autres facteurs environnementaux, comme la température et les obstacles dans les médiums de propagation.

En général, l'irrégularité de la radio est causée par l'anisotropie des propriétés du milieu de propagation et l' hétérogénéité des propriétés des dispositifs. Parmi tous ces facteurs, on trouve les pertes de chemins non isotropes et les différences dans la puissance du signal d'émission.

5.2.3 Les modèles radio

La plupart des protocoles de routage dans les RCSF sont basés sur le modèle UDG où la communication entre deux nœuds dépend de la distance qui les sépare. Si la distance est inférieure à la portée de transmission, les messages échangés entre les nœuds sont reçus sans erreur. Toutefois, la propagation du signal radio pourrait être affectée par plusieurs facteurs qui contribuent à la dégradation de sa qualité. En plus, les effets de ces facteurs sont encore plus significatifs sur la propagation du signal radio qui a une faible puissance. Par ailleurs, les liens radio dans les RCSF sont souvent imprévisibles [133]. La qualité de ces liens varie dans le temps [134,135] et dans l'espace [132,136–138] et la connectivité est généralement asymétrique [132, 139, 140].

Dans ce contexte, on distingue trois modèles de propagation illustrant l'irrégularité de la radio :

5.2.3.1 Le modèle radio isotrope

Dans le modèle radio isotrope, la puissance du signal reçu est généralement représentée par l'équation 5.1.

$$ReceivedSignalStrength = SendingPower - PathLoss + Fading \quad (5.1)$$

La puissance d'émission (Sending Power) d'un nœud est déterminée par l'état de la batterie et le type d'émetteur, d'amplificateur et d'antenne. La

1. SNR : Signal-Noise Ratio

perte de chemin (Path Loss) décrit la perte d'énergie du signal lorsqu'il est transmis au récepteur. Plusieurs modèles sont utilisés pour estimer la perte de chemin, tels que le modèle de propagation dans l'espace libre (the freespace propagation model), le modèle de propagation à deux rayons (the two-ray model) et le modèle Hata [141]. Ces modèles sont dits isotropes puisque dans ces modèles l'atténuation du signal est la même dans toutes les directions.

5.2.3.2 Le modèle de l'irrégularité de la radio

Le modèle de l'irrégularité de la radio est une extension du modèle radio isotrope. Il améliore le modèle radio isotrope par approximation de trois propriétés principales du signal radio : la non-isotropie, la variaton continue et l'hétérogénéité.

Le modèle de l'irrégularité de la radio est représenté par le modèle DOI (Degree Of Irregularity) [142] qui est utilisé pour désigner l'irrégularité du motif de la radio. La figure illustre la variation de la propagation de la radio en fonction du coefficient DOI. Par exemple, quand DOI est nul le modèle généré correspond au modèle du disque unitaire. On pourra dire que ce modèle correspond bien à un modèle probabiliste.

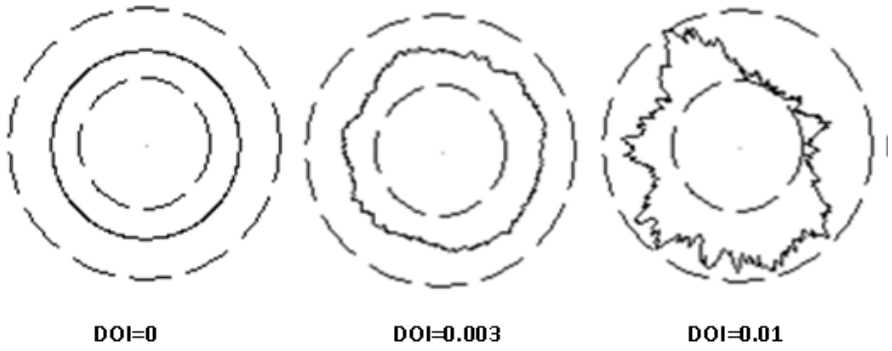

FIGURE 5.1 – Le modèle de propagation DOI

5.2.3.3 Le modèle LogNormal Shadowing

Dans ce modèle, la qualité du lien entre deux nœuds communicants est estimée en fonction de la distance qui les sépare et le coefficient d'atténuation de l'environnement (α). L'équation 5.2 explicite le calcul de la probabilité

d'une réception sans erreur.

$$F(x) = \begin{cases} 1 - \frac{(\frac{x}{R_c})^{2\alpha}}{2}, & si\ 0 < x \leq R_c \\ \frac{(\frac{2R_c - x}{R_c})^{2\alpha}}{2}, & si\ R_c < x \leq 2R_c \\ 0 & \text{Sinon} \end{cases} \quad (5.2)$$

Où α représente le facteur d'atténuation qui dépend de l'environnement. Sa valeur varie entre 2 et 4. Par exemple dans un environnement fortement perturbé sa valeur est de l'ordre de 4. x est la distance séparant les deux nœuds communicants et R_c est la portée de transmission d'un nœud dans un environnement idéal.

Dans ce contexte, nous proposons un protocole de routage tolérant aux pannes qui repose sur l'estimation de la qualité des liens pour surmonter la non-fiabilité des liens à faible puissance. L'estimation de la qualité de lien est calculée selon le modèle LogNormal Shadowing [6]. Dans ce modèle, la probabilité d'une réception sans erreur est calculée en fonction de la distance euclidienne séparant les deux nœuds communicants. L'équation (1) illustre le calcul de cette probabilité :

5.2.4 Le modèle de panne

Dans les RCSF, il existe plusieurs causes de défaillances. Ces défaillances peuvent affecter les nœuds ou les liens de communication sans fil. La défaillance des nœuds peut être due à un épuisement d'énergie, une destruction physique par un ennemi ou bien le mauvais fonctionnement des composants matériels en raison de leur déploiement dans des environnements hostiles et la défaillance des liens sans fil peut être due par un obstacle externe ou des fluctuations des signaux radio. Ces défaillances peuvent affecter l'ensemble du réseau et provoquer le changement de topologie du réseau.

5.3 Contribution

Dans cette contribution, nous traitons la défaillance des CHs et nous testons aussi la fiabilité des liens de communication entre chaque deux nœuds en

se basant sur le modèle LNS qui calcule la probabilité de réception sans erreur en fonction de la distance euclidienne, et sur le modèle probabiliste dans lequel la probabilité de réception est générée aléatoirement avec l'irrégularité de la propagation du signal radio [143].

Avant de présenter notre protocole de routage tolérant aux pannes, nous discutons d'abord le protocole LEACH qui est considéré parmi les meilleurs protocoles de routage hiérarchiques en termes d'efficacité énergétique. Le fonctionnement du protocole LEACH est divisé en périodes où chaque période est constituée de deux phases (setup phase, steady phase). Dans la première phase, l'élection des CHs et la formation des clusters sont effectuées et dans la deuxième phase, le processus de transmission de données sera lancé tel que les membres envoient les données captées à leur CH correspondant qui va les agréger et les envoyer directement à la station de base. Dans ce qui suit, nous avons évalué tout d'abord le protocole LEACH dans un environnement non idéal en considérant la défaillance des CHs (LEACH-1). Ensuite, nous l'avons évalué dans un environnement réaliste en impliquant la qualité des liens selon le modèle LNS en considérant également la défaillance des CHs (LEACH-2).

5.3.1 Evaluation de LEACH

Dans cette section, nous évaluons les performances de la version originale du protocole LEACH dans deux scénarios. Dans le premier scénario, nous considérons un réseau avec une certaine probabilité de panne des CHs, tels que le nombre de CHs qui peut tomber en panne varie entre 1 et $(K/2)$ où K représente le nombre de CHs. Dans le deuxième scénario, nous évaluons les performances de LEACH dans un environnement réaliste avec une certaine probabilité de défaillance des CHs. Ces évaluations concernent le nombre de paquets perdus et le taux de perte de paquets. L'évaluation de LEACH est effectuée selon le modèle LNS avec une probabilité de réception sans erreur de l'ordre 0.6 et un réseau de taille N= 50, 100, 150, 200 nœuds et dans un temps de simulation T= 500 secondes.

La figure 5.2 montre que les performances du protocole LEACH se dégradent dans un environnement non-idéal. Ceci est une preuve que la panne des CHs a un impact négatif sur les performances de LEACH (LEACH-1). En plus, si on tient compte de la qualité des liens, on remarque que ses perfor-

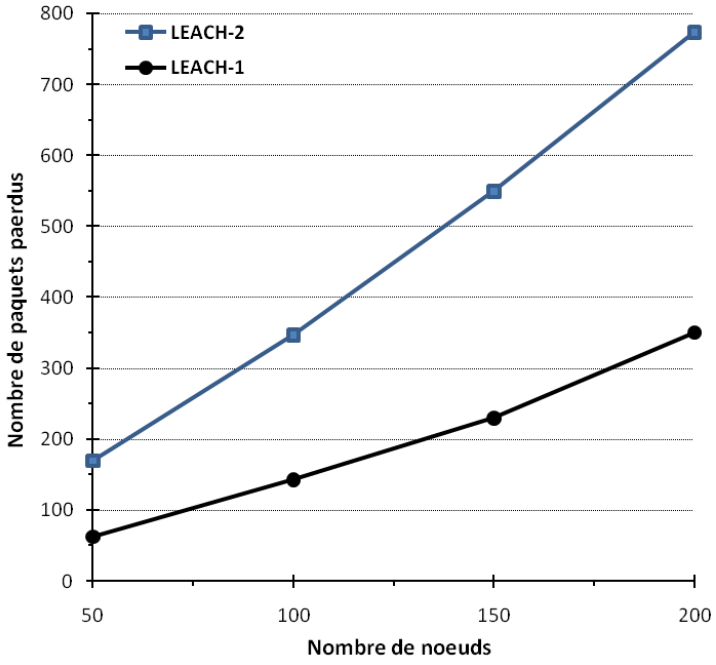

FIGURE 5.2 – Nombre de paquets perdus vs la taille du réseau

mances se dégradent un peu plus (LEACH-2).

La figure 5.3 montre que le taux de perte de paquets varie proportionnellement avec la taille du réseau c'est-à-dire le taux de perte de paquets augmente lorsque le nombre de nœuds augmente. Dans LEACH-2, le taux de perte de paquets est très élevé. En effet, plus de la moitié des paquets transmis sont corrompus ce qui signifie que le protocole LEACH n'est pas adaptable à un environnement non-idéal.

5.3.2 Protocole de routage basé sur la qualité des liens

Les résultats obtenus ci-dessus prouvent que le protocole LEACH diminue grandement ses performances dans un environnement non-idéal. Pour faire face à ce problème dans les RCSF, nous avons proposé un nouvel algorithme qui prend en considération la défaillance des CHs et la fiabilité des liens de communication. Avant de présenter notre algorithme, nous décrivons d'abord certaines terminologies :

— N : le nombre de nœuds dans le réseau $(S_1, S_2, ..., S_n)$.

— K : le nombre de CHs $(CH_1, CH_2, ..., CH_k)$ où $k < N$.

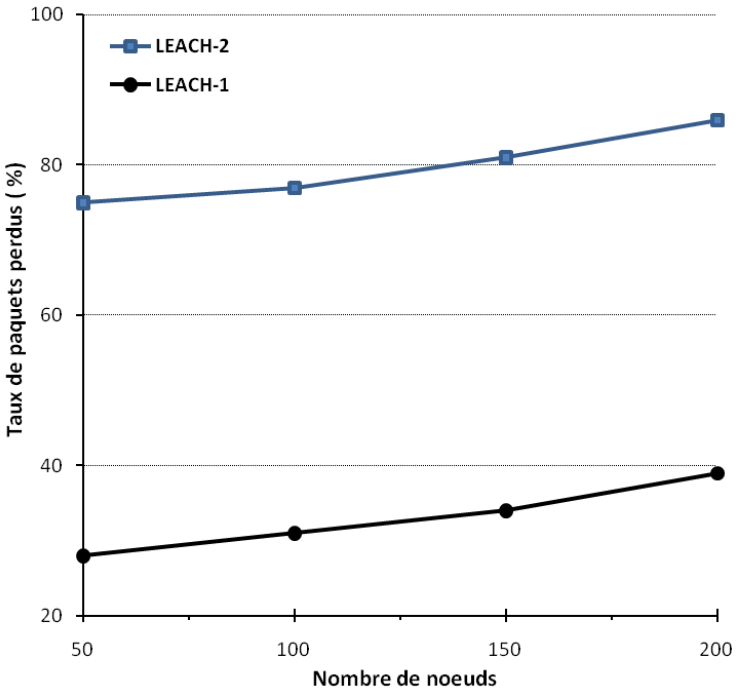

FIGURE 5.3 – Taux de perte de paquets vs la taille du réseau

— $E_{residual}$: l'énergie résiduelle de chaque nœud.

— $d(S_i, S_j)$: la distance entre S_i et S_j.

— $Mem(CH_i)$ est la liste des membres qui ont des liens fiables avec leur CH_i.

— $CH_r(CH)$ est la liste des CHs et des vice-CHs qui ont des liens fiables avec la station de base.

— $Mev(CH_i)$ est une liste des membres qui ont des liens fiables avec leur vice-CH.

5.3.2.1 L'algorithme proposé

Au début, la station de base diffuse un message "HELLO" pour informer tous les nœuds dans le réseau que la première période (round) a été déclenchée. Après, la sélection des CHs est effectuée en se basant sur deux métriques :

— L'énergie résiduelle de chaque nœud.

— Un nombre aléatoire compris entre 0 et 1.

Chaque nœud génère un nombre aléatoire entre 0 et1, si ce nombre est inférieur à un seuil et l'énergie résiduelle est élevée comparativement avec ses nœuds voisins alors le nœud sera élu comme CH pour la période courante. Aussi le nœud élu comme CH dans les périodes précédentes ne doit pas être réélu et cela dans le but de prolonger la durée de vie du réseau aussi longtemps que possible et d'équilibrer la consommation d'énergie du réseau. Ensuite, le processus de formation des clusters sera lancé tel que chaque CH diffuse un message "HELLO" pour former son cluster. Chaque nœud non-CH qui reçoit ce message et n'appartient pas à un autre cluster, répond par un massege "JOIN-REQUEST" pour informer le CH qu'il est membre de son cluster. Après un vice-CH est élu parmi les nœuds membres en se basant sur son énergie résiduelle et la distance qui le sépare de son CH. Durant le déploiement, le vice-CH agit en tant que membre et si à un moment le CH principal cesse de fonctionner alors ce dernier devient le nouveau CH et diffuse cette information à tous les nœuds membres du cluster.

Communication basée sur le modèle Lognormal shadowing : On distingue deux types de communications : intra-cluster et inter-cluster :

Communication intra-cluster : Au début, chaque nœud membre vérifie la qualité du lien de communication avec son CH correspondant en se basant sur le modèle "LogNormal Shadowing" qui calcule la probabilité de réception sans erreur d'un paquet de données. Si cette probabilité est supérieure à un seuil prédéfini alors le nœud membre envoie ses données captées directement à son CH, sinon il utilise un nœud relais comme nœud intermédiaire pour atteindre son CH. Ce nœud relais est sélectionné selon la distance c'est-à-dire celui qui est le plus proche est sélectionné comme nœud relais. On suppose qu'à un moment donné, le CH principal cesse de fonctionner à cause d'un épuisement d'énergie ou des dommages physiques. Cette panne est détectée par le vice-CH lorsqu'il ne reçoit aucun message de contrôle, il considère que le CH est en panne est dans ce cas le vice-CH va prendre son rôle et informe tous les membres du cluster de son nouveau statut. Durant la transmission de données, chaque membre vérifie la qualité du lien de communication avant d'envoyer ses données au vice-CH. Dans ce qui suit, nous

allons présenter l'algorithme de communication.

Algorithme1 : Communication intra-cluster
Début

- $d_h(M_i, CH)$ est la distance euclidienne entre le nœud membre et son CH,
- $d_v(M_i, CH_{vice})$ est la distance euclidienne entre le nœud membre et son vice-CH,
- $\binom{x_c}{y_c}$: les coordonnées du CH,
- $\binom{x_v}{y_v}$: les coordonnées du vice-CH,
- $\binom{x_i}{y_i}$: les coordonnées de M_i (nœud membre),

$Mem(M_i) = \emptyset$

while Actif(CH) **do**

- $M_i\binom{x_i}{y_i}$ calcule la distance qui le sépare de son $CH\binom{x_c}{y_c}$:

$$d = \sqrt[2]{(x_i - x_c)^2 + (y_i - y_c)^2}$$

- M_i calcule la probabilité de réception sans erreur,

$$Pr(d) = 1 - \frac{(\frac{d}{R_c})^{2\alpha}}{2}$$

if (Pr(d) $\geqslant$ Seuil) **then**

- M_i envoie ses données directement au CH correspondant,

$$Mem(CH_i) = Mem(CH_i) \cup \{M_i\}$$

else

- M_i sélectionne un nœud relais ($Mj \in Mem(CH_i)$) avec une distance minimale,

- M_i Transmet les données collectées au M_j,

end if

end while

if Actif(CH)=False **then**

- Quand le CH principal cesse de fonctionner, le vice-CH va prendre son rôle,

- $M_i\binom{x_i}{y_i}$ calcule la distance qui le sépare de son $vice-CH\binom{x_v}{y_v}$:

$d_v = \sqrt[2]{(x_i - x_v)^2 + (y_i - y_v)^2}$

- M_i calcule la probabilité de réception sans erreur,

$Pr(d_v) = 1 - \frac{(\frac{d_v}{R_c})^{2\alpha}}{2}$

if $(Pr(d_v) \geqslant Seuil)$ **then**

- M_i envoie ses données directement au CH correspondant,

$Mem(CH_i) = Mem(CH_i) \cup \{M_i\}$

else

- M_i sélectionne un nœud relais $(Mj \in Mem(CH_i))$ avec une distance minimale,

- M_i transmet les données collectées au M_j,

end if

end if

Fin

Communication inter-cluster : Chaque CH est responsable de l'agrégation des données collectées par ses membres. Il calcule la probabilité de réception sans erreur de données par la station de base en fonction de la qualité du lien de communication qui le lie avec cette dernière. Si cette probabilité est supérieure à un seuil prédéfini une communication directe est effectuée avec la station de base, sinon le CH qui veut envoyer, choisit le CH voisin le plus proche comme nœud relais pour atteindre la station de base. Par ailleurs, la panne du CH principal peut affecter le fonctionnement du cluster ainsi que le réseau en entier, pour cela le vice-CH doit prendre son rôle immédiatement pour ne pas perdre les performances du protocole proposé. Cette opération est effectuée selon l'algorithme suivant :

Algorithme2 : Communication inter-cluster
Début

- $dd(CH, BS)$ est la distance euclidienne entre le CH et la station de

base BS,

- $dd_v(CH_v, BS)$ est la distance euclidienne entre le nouveau CH et la station de base,

- $\binom{x_c}{y_c}$: les coordonnées du CH,
- $\binom{x_v}{y_v}$: les coordonnées du vice-CH,
- $\binom{x_b}{y_b}$: les coordonnées de la station de base BS,

$CH_r(CH) = \emptyset$

while Actif(CH) **do**

- $CH_i\binom{x_c}{y_c}$ calcule la distance qui le sépare de la station de base $BS\binom{x_b}{y_b}$:

$dd = \sqrt[2]{(x_b - x_c)^2 + (y_b - y_c)^2}$

- CH_i calcule la probabilité de réception sans erreur $Pr_1(dd)$,

$Pr_1(dd) = 1 - \frac{(\frac{dd}{R_c})^{2\alpha}}{2}$

if $(Pr_1(dd) \geqslant Seuil)$ **then**

- CH_i envoie ses données directement à la station de base,

$CH_r(CH) = CH_r(CH) \cup \{CH_i\}$

else

- CH_i sélectionne un nœud relais ($CH_j \in CH_r(CH)$) ayant une distance minimale vers la station de base,

- CH_i transmet les données collectées au CH_j,

end if

end while

if Actif(CH)=False **then**

- $CH_{vice}\binom{x_v}{y_v}$ calcule la distance qui le sépare de la station de base $BS\binom{x_b}{y_b}$:

$dd_v = \sqrt[2]{(x_b - x_v)^2 + (y_b - y_v)^2}$

- CH_{vice} calcule la probabilité de réception sans erreur $(Pr_2(dd_v))$,

$Pr(dd_v) = 1 - \frac{(\frac{dd_v}{R_c})^{2\alpha}}{2}$

if $(Pr(dd_v) \geqslant Seuil)$ **then**

- CH_{vice} envoie les données agrégées directement à la station de base,

$CH_r(CH) = CH_r(CH) \cup \{CH_{vice}\}$

else

- CH_{vice} sélectionne un nœud relais ($CH_j \in CH_r(CH)$) ayant une distance minimale vers la station de base,

- CH_{vice} transmet les données collectées au CH_j,

end if

end if

Fin

5.3.3 Evaluation des performances

Nous avons effectué plusieurs simulations en nous basant sur le modèle "LogNormal Shadowing" et le modèle probabiliste afin d'évaluer notre protocole proposé en termes du nombre de communications, le taux de perte de paquets et la consommation d'énergie. Pour ce faire, nous avons considéré un réseau composé de 100 nœuds fixes et dispersés aléatoirement sur une superficie de 100m x 100m. Nous avons effectué plusieurs simulations avec une variation du nombre de périodes et nous avons fixé un seuil ($L = 0.6$) pour la probabilité de réception sans erreur basée sur le modèle LNS et la valeur du coefficient d'atténuation α est compris entre 2 et 4 tout dépend de l'environnement et un seuil ($P = 0.5$) pour le modèle probabiliste. Le tableau 5.1 résume les paramètres de simulation.

Nous avons réalisé 10 simulations pour chaque scénario en variant le nombre de périodes de 5, 10, 15,.., 35 périodes. Puis, nous calculons la moyenne pour cerner l'erreur de simulation.

La figure 5.4 illustre l'évolution du nombre de communications en fonction du nombre de périodes. Le nombre de communications inclut le nombre de messages échangés pour la formation et l'organisation des clusters, le nombre

TABLE 5.1 – Les paramètres de simulation

Parameter	Value
Zone de déploiement	100m x 100m
Temps de simulation	5, 10, .., 35 (rounds)
Nombre de nœuds	100
Taille du paquet	29 bytes
Energie initiale du nœud	2J
Seuil P	0.6
Seuil L	0.5

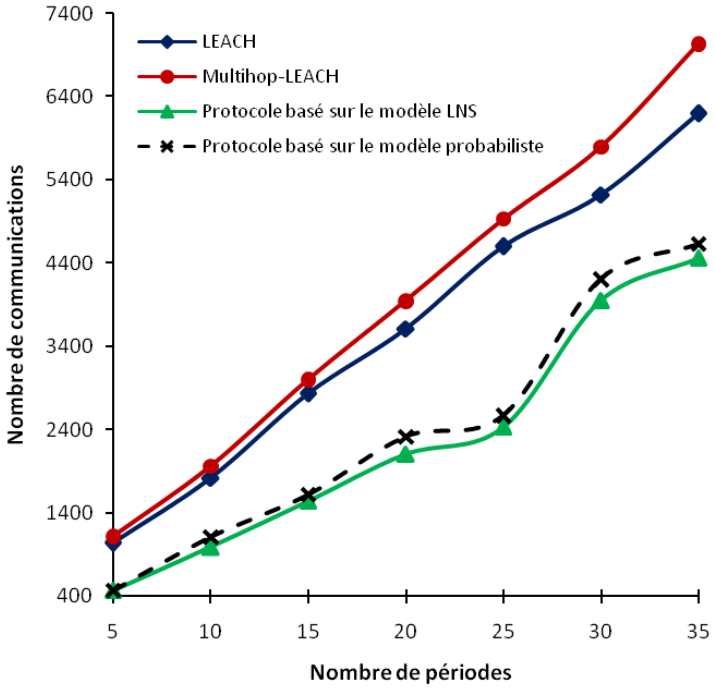

FIGURE 5.4 – Nombre de communications vs. nombre de périodes

de transmissions de données détectées aux cluster-heads et le nombre de transmissions de données entre les clusterheads et la station de base, etc. On peut voir que le surcoût de communications dans LEACH et multihop-LEACH est élevé par rapport au nouveau protocole proposé. En effet, dans ce dernier le paquet de données n'est envoyé que si un événement est détecté et le membre joue le rôle d'un nœud relais, avant qu'il envoie ses données collectées au CH

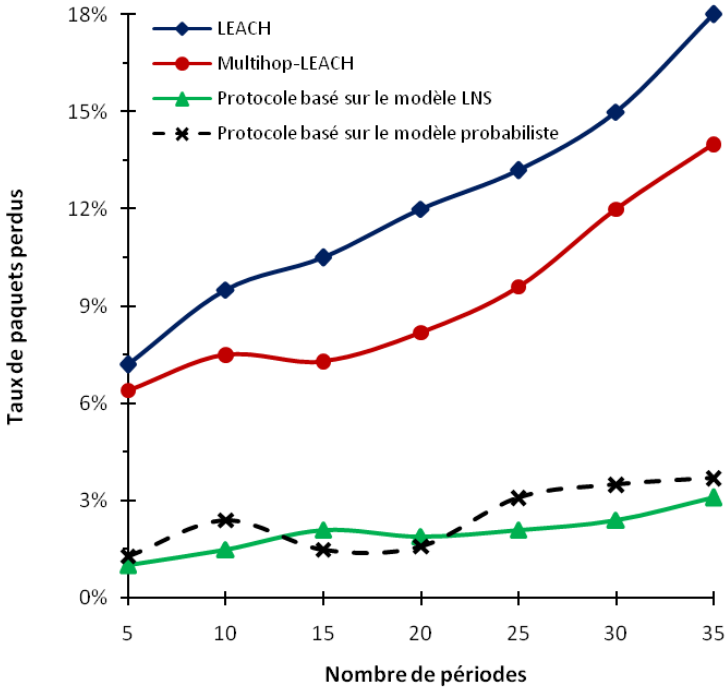

FIGURE 5.5 – Taux de perte de paquets vs. nombre de périodes

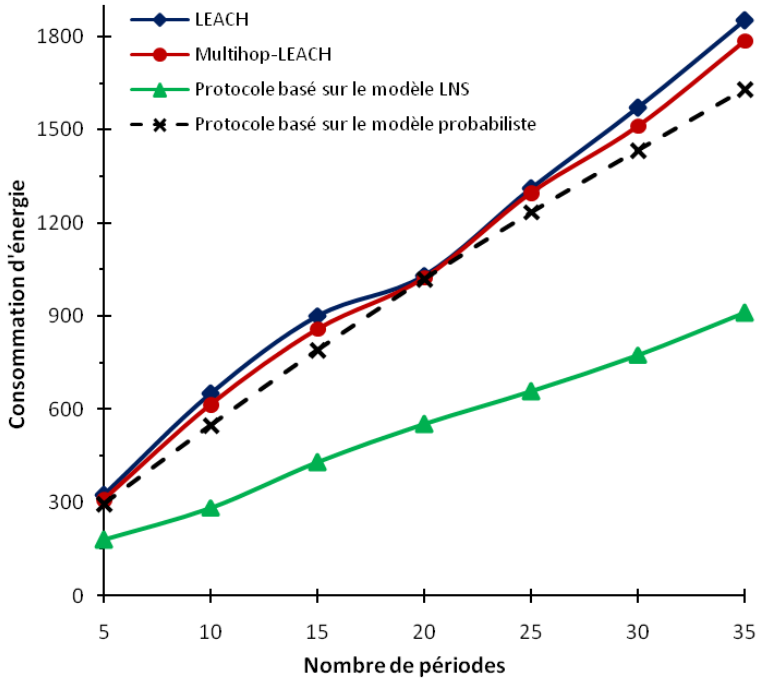

FIGURE 5.6 – Consommation d'énergie vs. nombre de périodes

il attendra un laps de temps, s'il y a un paquet transmis par son voisin. De ce fait, un seul paquet de données sera envoyé au CH et par conséquent le nombre de communications redondantes sera minimisé. Ce procédé est appliqué même dans les communications entre les CHs et la station de base.

La figure 5.5 présente le taux de perte de paquets en fonction du nombre de périodes. Ce qui montre l'efficacité de notre protocole proposé dans un environnement non-idéal. En outre, cette figure confirme que le protocole LEACH et multihop-LEACH perdent leurs performances dans un environnement non-idéal. Ces deux protocoles ont été évalués par le modèle LNS. Le taux de perte de paquets est élevé à cause de la non-fiabilité des liens de communications par contre dans notre algorithme la non-fiabilité des liens est traitée par une communication multi-sauts pour assurer la bonne réception des paquets de données dans les deux modèles : le modèle LNS et le modèle probabiliste.

La figure 5.6 montre que l'énergie consommée dans le protocole LEACH et multihop-LEACH est élevée par rapport au nouveau protocole proposé. L'énergie consommée inclut la formation des clusters, la communication entre les nœuds membres et leurs CHs correspondants, ainsi entre les CHs et la station de base et aussi elle concerne la réception de paquets de données, l'agrégation de données, etc. Dans notre nouveau protocole, la communication intra-cluster est soit à multi-sauts ou directe tout dépend de la fiabilité des liens. Par contre dans LEACH et multihop-LEACH la communication est directe. De même, la communication inter-cluster est établie directement avec la station de base dans LEACH et elle est à multi-sauts dans multihop-LEACH, alors que dans notre protocole proposé la communication est établie à multi-sauts si le lien de communication entre le CH et la station de base n'est pas fiable.

5.4 Conclusion

La conservation d'énergie et la tolérance aux pannes sont deux enjeux majeurs dans les réseaux de capteurs sans fil (RCSF) puisque les nœuds capteurs sont limités en termes de ressources énergétiques et sont sujets à des défaillances dans de nombreuses applications. Dans ce chapitre, nous avons proposé un protocole de routage hiérarchique tolérant aux pannes basé sur le

modèle LogNormal Shadowing. Il prend en considération les fluctuations du signal radio en vue d'assurer une livraison fiable dans un environnement réaliste où les liens peuvent être fiables ou bien non fiables tout dépend du degré d'atténuation dans l'environnement considéré. Le protocole proposé a été évalué par le modèle probabiliste tel que la probabilité de réception sans erreur d'un paquet de données est calculée aléatoirement. Les résultats de simulation ont montré que notre protocole peut s'adapter à un environnement réaliste puisqu'il assure la réception des paquets de données malgré la non fiabilité des liens et aussi, il consomme moins d'énergie par rapport aux protocoles LEACH et multihop-LEACH en minimisant le nombre de communications redondantes.

Conclusion générale et Perspectives

Les réseaux de capteurs sans fil ont connu un grand essor au cours de ces dernières années. Toutefois, la conception des applications liées aux RCSFs doit faire face à certaines difficultés en raison de leurs capacités limitées et leurs ressources énergétiques très réduites qui constituent généralement un souci majeur au déploiement des réseaux de capteurs. L'objectif principal de cette thèse était d'appliquer le paradigme de tolérance aux pannes dans les RCSF pour assurer la fiabilité du routage et garantir le fonctionnement des réseaux sans aucune interruption même en cas de présence de défaillances. Ces défaillances peuvent être due à des pannes matérielles à cause des environnements hostiles dans lesquels ils sont déployés ou tout simplement à un épuisement d'énergie puisque les nœuds capteurs sont alimentés par des piles non rechargeables. Les travaux de recherche réalisés dans cette thèse sont résumés dans ce qui suit :

Dans le premier chapitre, nous avons introduit la notion des RCSFs et présenté les différents défis liés à la conception de ce type de réseaux en donnant un aperçu sur les dispositifs miniaturisés qui constituent ces réseaux. Enfin, nous avons abordé la tolérance aux pannes en détaillant les différentes causes de pannes, les techniques de détection de pannes ainsi que les différentes techniques proposées pour une tolérance aux pannes efficace.

Dans le deuxième chapitre, un état de l'art détaillé est présenté sur les protocoles de routage tolérants aux pannes existants dans la littérature pour les architectures de réseau plates et hiérarchiques. Puis, nous avons donné une étude comparative entre ces différents protocoles en se basant sur divers paramètres qui sont sélectionnés selon des applications dans lesquelles les réseaux de capteurs peuvent être appliqués tels que la consommation d'énergie, la fiabilité du réseau, la tolérance aux pannes, etc. Dans la deuxième partie de ce chapitre, une description détaillée du protocole de routage LEACH est donnée avec un panorama des versions améliorées tolérantes aux pannes du protocole LEACH.

Dans le troisième chapitre, nous avons présenté notre première contribution qui a visé deux performances distinctes : la consommation d'énergie et la tolérance aux pannes. En effet, il est bien connu que le protocole LEACH souffre de quelques limitations malgré son efficacité énergétique. Dans cette optique, notre contribution vise à minimiser la consommation d'énergie en utilisant une communication multi-sauts au lieu d'une communication directe entre les CHs et la station de base. Puisque la consommation d'énergie pour la transmission de données dépend de la distance séparant les nœuds communicants, on a supposé que les CHs proches de la station de base sont utilisés comme nœuds relais entre les CHs lointains et la station de base. Après, un chemin alternatif est proposé pour tolérer la défaillance d'un ou plusieurs CHs tel que chaque CH possède deux chemins vers la station de base, l'un qui est principal et l'autre alternatif pour assurer une tolérance aux pannes efficace même en cas d'existence de pannes.

Dans le quatrième chapitre, nous avons présenté notre deuxième contribution qui propose une approche robuste appelée FTLR (Fault-Tolerant LEACH-based Routing protocol). Cette approche est une version améliorée du protocole LEACH dans laquelle nous avons mis l'accent sur la qualité des liens pour les communications intra-cluster en nous basant sur le modèle "LogNormal Shadowing" (LNS). Puisque la plupart des protocoles de routage conçus pour les RCSFs utilisent le modèle de disque unitaire qui ne prend pas en compte les fluctuations du signal radio vu qu'il considère que si la distance séparant les nœuds communicants est inférieure ou égale à la portée de transmission alors le message sera reçu sans erreur. Cependant, les fluctuations du signal ont un impact négatif sur la qualité de transmission. À cet effet, ces protocoles doivent être modifiés pour être adaptés à des environnements réalistes. Parmi les modèles qui représentent les environnements réalistes on trouve le modèle Lognormal Shadowing et le modèle probabiliste. Dans le modèle LNS, la probabilité de réception sans erreur d'un paquet de données est calculée en fonction de la distance euclidienne séparant les nœuds communicants. En se basant sur ce modèle, nous avons focalisé notre étude particulièrement sur les performances du protocole LEACH dans un environnement réaliste mais malheureusement les résultats de simulation ont montré que les performances du protocole LEACH sont dégradées en cas de présence des fluctuations radio.

Ainsi, pour améliorer les performances de LEACH dans un tel environnement, nous avons supposé qu'avant chaque émission d'un paquet de données, le nœud vérifie d'abord la qualité du lien. Si cette qualité du lien est bonne on pourra dire que la livraison fiable est garantie et par conséquent le nœud membre transmet ses données collectées directement à son CH correspondant, sinon il incorpore un autre nœud membre comme nœud relais. Les résultats de simulation prouvent que notre contribution a amélioré les performances de LEACH en termes de taux de paquets perdus et de consommation d'énergie.

Dans le cinquième chapitre, nous avons proposé un protocole de routage tolérant aux pannes qui est efficace dans un environnement non idéal en termes de perte de paquets et de consommation d'énergie. Ce protocole prend en considération la qualité du lien avant l'envoi de données pour assurer une livraison fiable.

Dans cette thèse nous avons traité les problèmes liés à la fiabilité de livraison dans les RCSF et la nécessité d'instaurer la tolérance aux pannes dans la conception des applications pour les RCSFs ce qui a envisagé plusieurs perspectives.

Puisque la plupart des protocoles existants reposent sur une couche physique basée sur le modèle du disque unitaire, l'évaluation de ces protocoles dans une couche réaliste pourrait être intéressante. Nos futurs travaux comprennent l'analyse d'autres protocoles dans un environnement réaliste. En plus, l'utilisation d'autres modèles de vérification de la qualité des liens de communication tels que les modèles standards de "fading" : "Rayleigh and Rice fading" [144,145] qui assure la fiabilité des liens de communications sans fil. Puis on compare l'efficacité de ces protocoles par rapport aux différents modèles réalistes. En outre, malgré l'efficacité de l'aspect mobile qui permet le développement dans le domaine des RCSFs, plusieurs travaux de recherche ne prennent pas en considération cet aspect. De ce fait, il est important d'étendre nos travaux proposés vers la mobilité pour détecter le nœud défaillant dans un temps très réduit et corriger la défaillance détectée.

Bibliographie personnelle

Conférences internationales

1. Chifaa Tabet Hellel, Mohamed Lehsaini, Hervé Guyennet, "A Version of LEACH Adapted to the Lognormal Shadowing Model", International Conference on Modeling Approaches and Algorithms for Advanced Computer Applications (CIIA'2015), pp 465-475, vol 456. Springer International Publishing, 2015, Saida, Algeria.
2. Chifaa Tabet Hellel, Mohamed Lehsaini, Hervé Guyennet, "Fault-Tolerance in LEACH Protocol (MC-LEACH)", In the proceeding of International Conference on advanced Networking, Distributed Systems and Applications (INDS), pp.112-115, June 2014, Bejaia, Algeria.
3. Chifaa Tabet Hellel, Mohamed Lehsaini, "Fault-tolerant Multi-hop LEACH Protocol (FM-LEACH)", In the proceeding of International Conference on Artificial Intelligence and Information Technology (ICAIIT), March 2014, Ouargla, Algeria.
4. Mohamed Lehsaini, Mohammed Feham, Chifaa Tabet Hellel, "Improvement of Scalar Multiplication Time for Elliptic Curve Cryptosystems",In the proceeding of the 11^{th} IEEE International Symposium on Programming and Systems (ISPS'2013), pp 53-57, April 2013, Algiers, Algeria.
5. Mohamed Lehsaini, Chifaa Tabet Hellel, "A Novel Cluster-based Fault-tolerant Scheme for Wireless Sensor Networks", In the proceeding of the 24^{th} IEEE International Conference on Microelectronics (ICM), pp 1-4, 2012. Algiers, Algeria.

Conférences nationales

1. Chifaa Tabet Hellel, Mohamed Lehsaini, Hervé Guyennet, "Fault-tolerant Routing Protocols for Wireless Sensor Networks : A Survey", In the proceeding of National Conference on Technology of Information and Telecommunications (CNTIT'2013), 2013, Tlemcen, Algeria.

Revues Internationales

1. Chifaa Tabet Hellel, Mohamed Lehsaini, Hervé Guyennet, "An Enhanced Fault-tolerant Version of LEACH for Wireless Sensor Networks". International Journal of Advancements in Computing Technology (IJACT), vol. 6, no. 6, p.50-57, 2014.
2. C. Tabet Hellel, M. Lehsaini, and H. Guyennet, "Fault-tolerant LEACH-based routing protocol for wireless sensor networks," International Journal of Computer Networks and Communications (IJCNC), vol. 7, no. 3, pp. 117-129, 2015.
3. Chifaa Tabet Hellel, Mohamed Lehsaini, Hervé Guyennet, "Fault-tolerant Routing Protocols for Wireless Sensor Networks : A Survey". International Journal of Information and Communication Technology (IJICT). Soumis.
4. Chifaa Tabet Hellel, Mohamed Lehsaini, Hervé Guyennet, "Design of a routing protocol based on link quality for WSN", journal of Wireless Networks. Soumis.

Bibliographie

[1] V. Raghunathan, C. Schurgers, P. Sung, and M. Srivastava, "Energy-aware wireless microsensor networks," *Signal Processing Magazine, IEEE*, vol. 19, no. 2, pp. 40–50, March 2002.

[2] A. Boukerche, R. W. N. Pazzi, and R. B. Araujo, "Fault-tolerant wireless sensor network routing protocols for the supervision of context-aware physical environments," *Journal of Parallel and Distributed Computing*, vol. 66, no. 4, pp. 586–599, 2006.

[3] Y. Zeng, C. Sreenan, L. Sitanayah, N. Xiong, J. Park, and G. Zheng, "An emergency-adaptive routing scheme for wireless sensor networks for building fire hazard monitoring," *Journal of Sensors*, vol. 11, no. 3, pp. 2899–2919, 2011.

[4] O. Chipara, Z. He, G. Xing, Q. Chen, X. Wang, C. Lu, J. Stankovic, and T. Abdelzaher, "Real-time power-aware routing in wireless sensor networks," in *Proceedings of the* 14^{th} *IEEE Workshop Quality of Service (IWQoS'06)*, 2006, pp. 83–92.

[5] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proceedings of the* 33^{rd} *Annual Hawaii International Conference on System Sciences*, January 2000, pp. 1–10.

[6] T. S. Rappaport, *Wireless Communications : Principles and Practice*. Prentice Hall, 2002.

[7] C. Boano, J. Brown, Z. He, U. Roedig, and T. Voigt, "Low-Power radio communication in industrial outdoor deployments : The impact of weather conditions and ATEX-Compliance," in *Sensor Applications, Experimentation, and Logistics*, ser. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, N. Komninos, Ed. Springer Berlin Heidelberg, 2010, vol. 29, pp. 159–176.

[8] C. Mettu. (2011) Telosb datasheet @ONLINE. [Online]. Available : https://fr.scribd.com/doc/68138250/Telosb-Datasheet-t

[9] K. Lin, J. Yu, J. Hsu, S. Zahedi, D. Lee, J. Friedman, A. Kansal, V. Raghunathan, and M. Srivastava, "Heliomote : Enabling long-lived sensor networks through solar energy harvesting," in *Proceedings of the* 3^{rd} *International Conference on Embedded Networked Sensor Systems (SenSys'05)*. ACM, 2005, pp. 309–309.

[10] T. Voigt, H. Ritter, and J. Schiller, "Utilizing solar power in wireless sensor networks," in *Proceedings of the* 28^{th} *Annual IEEE International Conference on Local Computer Networks (LCN'03)*, October 2003, pp. 416–422.

[11] S. Harchi, "Un protocole de session dans les réseaux de capteurs sans fil," Ph.D. dissertation, Université de Lorraine, 2013.

[12] B. Malli. (2011, May) Micaz datasheet @ONLINE. [Online]. Available : https://fr.scribd.com/doc/56641260/Micaz-Datasheet

[13] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks : a survey," *Computer Networks*, vol. 38, no. 4, pp. 393–422, 2002.

[14] K. Holger and A. Willig, *Protocols and Architectures for Wireless Sensor Networks*. Wiley Online Library, 2005.

[15] C. Jae-Hwan and L. Tassiulas, "Energy conserving routing in wireless ad-hoc networks," in *Proceedings of the* 19^{th} *Annual Joint Conference of the IEEE Computer and Communications Societies*, vol. 1, 2000, pp. 22–31.

[16] A. Giridhar and P. R. Kumar, "Maximizing the functional lifetime of sensor networks," in *Proceedings of* 4^{th} *International Symposium on Information Processing in Sensor Networks (IPSN'2005)*, April 2005, pp. 5–12.

[17] V. Mhatre, C. Rosenberg, D. Kofman, R. Mazumdar, and N. Shroff, "A minimum cost heterogeneous sensor network with a lifetime constraint," *IEEE Transactions on Mobile Computing*, vol. 4, no. 1, pp. 4–15, January 2005.

[18] W. Wang, V. Srinivasan, and K. C. Chua, "Using mobile relays to prolong the lifetime of wireless sensor networks," in *Proceedings of the* 11^{th}

Annual International Conference on Mobile Computing and Networking. ACM, 2005, pp. 270–283.

[19] C. F. Chiasserini, I. Chlamtac, P. Monti, and A. Nucci, "Energy-efficient design of wireless ad hoc networks," in *Proceedings of the* 2^{nd} *International IFIP-TC6 Networking Conference on Networking Technologies, Services, and Protocols ; Performance of Computer and Communication Networks ; and Mobile and Wireless Communications*. Springer-Verlag, 2002, pp. 376–386.

[20] S. Soro and W. B. Heinzelman, "Prolonging the lifetime of wireless sensor networks via unequal clustering," in *Proceedings of the* 19^{th} *IEEE International on Parallel and Distributed Processing Symposium.*, April 2005, pp. 8 pp.–.

[21] D. Tian and N. D. Georganas, "A coverage-preserving node scheduling scheme for large wireless sensor networks," in *Proceedings of the* 1^{st} *ACM International Workshop on Wireless Sensor Networks and Applications*. ACM, 2002, pp. 32–41.

[22] C. Chee-Yee and S. Kumar, "Sensor networks : evolution, opportunities, and challenges," *Proceedings of the IEEE*, vol. 91, no. 8, pp. 1247–1256, August 2003.

[23] M. J. Brown, "Users guide developed for the JBREWS project," Los Alamos National Laboratory of California University, Tech. Rep., 1999.

[24] G. Werner-Allen, K. Lorincz, M. Ruiz, O. Marcillo, J. Johnson, J. Lees, and M. Welsh, "Deploying a wireless sensor network on an active volcano," *Internet Computing, IEEE*, vol. 10, no. 2, pp. 18–25, March 2006.

[25] R. Steele, A. Lo, C. Secombe, and Y. K. Wong, "Elderly persons' perception and acceptance of using wireless sensor networks to assist healthcare," *International Journal of Medical Informatics*, vol. 78, no. 12, pp. 788 – 801, 2009.

[26] M. Mana, "Adaptation et intégration de la sécurité biométrique aux réseaux de capteurs corporels sans fil," Ph.D. dissertation, Université de Tlemcen, 2011.

[27] E. Petriu, N. D. Georganas, D. Petriu, D. Makrakis, and V. Groza, "Sensor-based information appliances," *Instrumentation Measurement Magazine, IEEE*, vol. 3, no. 4, pp. 31–35, December 2000.

[28] V. Ricquebourg, D. Menga, D. Durand, B. Marhic, L. Delahoche, and C. Loge, "The smart home concept : our immediate future," in *Proceedings of the* 1^{st} *IEEE International Conference on E-Learning in Industrial Electronics*, December 2006, pp. 23–28.

[29] A. M. Tabar, A. Keshavarz, and H. Aghajan, "Smart home care network using sensor fusion and distributed vision-based reasoning," in *Proceedings of the* 4^{th} *ACM International Workshop on Video Surveillance and Sensor Networks*. ACM, 2006, pp. 145–154.

[30] D.-M. Han and J.-H. Lim, "Smart home energy management system using ieee 802.15.4 and zigbee," *IEEE Transactions on Consumer Electronics*, vol. 56, no. 3, pp. 1403–1410, August 2010.

[31] Z. W. Luo, *Service Science and Logistics Informatics : Innovative Perspectives*. IGI GLOBAL Disseminator of Knowledge, 2010.

[32] Y. Zhang and H. Xiao, "Bluetooth-based sensor networks for remotely monitoring the physiological signals of a patient," *IEEE Transactions on Information Technology in Biomedicine*, vol. 13, no. 6, pp. 1040–1048, November 2009.

[33] C. M. Yu and Y. B. Yu, "Reconfigurable algorithm for bluetooth sensor networks," *IEEE Sensors Journal*, vol. 14, no. 10, pp. 3506–3507, October 2014.

[34] R. de Francisco, H. Li, G. Dolmans, and H. de Groot, in *Proceedings of the* 20^{th} *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications,*.

[35] L. Hwakyung, C. Sang-Hwa, L. Yun-Sung, and H. Yoobin, "Performance comparison of DASH7 and ISO/IEC 18000-7 for fast tag collection with an enhanced csma/ca protocol," in *Proceedings of the* 10^{th} *IEEE International Conference on Embedded and Ubiquitous Computing (HPCC_EUC), and High Performance Computing and Communications*, November 2013, pp. 769–776.

[36] H. Hongwei, X. Youzhi, Y. Hairong, S. Mubeen, and Z. Hongke, "An elderly health care system using wireless sensor networks at home," in *Proceedings of the* 3^{th} *International Conference on Sensor Technologies and Applications (SENSORCOMM'09)*, June 2009, pp. 158–163.

[37] Y. Challal, H. Bettahar, and A. Bouabdallah, "Les réseaux de capteurs (WSN : Wireless Sensor Networks)," Université de Technologie de Compiègne, FRANCE, Tech. Rep., 2008.

[38] L. Paradis and Q. Han, "A survey of fault management in wireless sensor networks," *Journal of Netwoks Systems Management*, vol. 15, no. 2, pp. 171–190, june 2007.

[39] K. Martinez, P. Padhy, A. Riddoch, H. Ong, and J. Hart, "Glacial environment monitoring using sensor networks," in *Proceedings of Workshop on Real-World Wireless Sensor Networks (REALWSN'05)*. ACM, June 2005.

[40] J. Tateson, C. Roadknight, A. Gonzalez, T. Khan, S. Fitz, I. Henning, N. Boyd, C. J. Vincent, and I. Marshall, "Real world issues in deploying a wireless sensor network for oceanography," in *Proceedings of Workshop on Real-World Wireless Sensor Networks (REALWSN'05)*. ACM, June 2005.

[41] R. Szewczyk, J. Polastre, A. Mainwaring, and D. Culler, "Lessons from a sensor network expedition," in *Wireless Sensor Networks*. Springer Berlin Heidelberg, 2004, vol. 2920, pp. 307–322.

[42] K. Langendoen, A. Baggio, and O. Visser, "Murphy loves potatoes : experiences from a pilot sensor network deployment in precision agriculture," in *Proceedins of the* 20^{th} *International on Parallel and Distributed Processing Symposium (IPDPS'2006)*, April 2006, pp. 8 pp.–.

[43] R. Szewczyk, A. Mainwaring, J. Polastre, J. Anderson, and D. Culler, "An analysis of a large scale habitat monitoring application," in *Proceedings of the 2Nd International Conference on Embedded Networked Sensor Systems (SenSys'04)*, 2004, pp. 214–226.

[44] T. Schmid, H. Dubois-Ferrière, and M. Vetterli, "Sensorscope : Experiences with a wireless building monitoring sensor network," in

Proceedings of Workshop on Real-World Wireless Sensor Networks (REALWSN'05). ACM, June 2005.

[45] T. John and G. Daan, "Radio wave propagation in potato fields," in *Proceedings of the* 1^{st} *Workshop on Wireless Network Measurements*, 2005.

[46] G. Tolle, J. Polastre, R. Szewczyk, D. Culler, N. Turner, K. Tu, S. Burgess, T. Dawson, P. Buonadonna, D. Gay, and W. Hong, "A macroscope in the redwoods," in *Proceedings of the* 3^{rd} *International Conference on Embedded Networked Sensor Systems (SenSys'05).* ACM, 2005, pp. 51–63.

[47] R. V. Kshirsagar and A. B. Jirapure, "A survey on fault detection and fault tolerance in wireless sensor networks," *IJCA Proceedings on International Conference on Benchmarks in Engineering Science and Technology*, vol. ICBEST, no. 1, pp. 6–9, October 2012.

[48] N. Ramanathan, K. Chang, R. Kapur, L. Girod, E. Kohler, and D. Estrin, "Sympathy for the sensor network debugger," in *Proceedings of the* 3^{rd} *International Conference on Embedded Networked Sensor Systems (SenSys'05).* ACM, 2005, pp. 255–267.

[49] J. Staddon, D. Balfanz, and G. Durfee, "Efficient tracing of failed nodes in sensor networks," in *Proceedings of the* 1^{st} *ACM International Workshop on Wireless Sensor Networks and Applications.* ACM, 2002, pp. 122–130.

[50] F. Koushanfar, M. Potkonjak, and A. Sangiovanni-Vincentell, "Fault tolerance techniques for wireless ad hoc sensor networks," in *Proceedings of IEEE on Sensors*, vol. 2, 2002, pp. 1491–1496.

[51] S. Harte, A. Rahman, and K. Razeeb, "Fault tolerance in sensor networks using self-diagnosing sensor nodes," in *Proceedings of the IEEE International Workshop on Intelligent Environments*, June 2005, pp. 7–12.

[52] C. F. Hsin and M. Liu, "A distributed monitoring mechanism for wireless sensor networks," in *Proceedings of the* 1^{st} *ACM Workshop on Wireless Security (WiSE'02).* ACM, 2002, pp. 57–66.

[53] C. Hsin and M. Liu, "Self-monitoring of wireless sensor networks," *Computer Communications*, vol. 29, no. 4, pp. 462–476, 2006.

[54] M. Ding, C. Dechang, X. Kai, and C. Xiuzhen, "Localized fault-tolerant event boundary detection in sensor networks," in *Proceedings IEEE of the* 24^{th} *Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'2005)*, vol. 2, March 2005, pp. 902–913.

[55] J. Chen, S. Kher, and A. Somani, "Distributed fault detection of wireless sensor networks," in *Proceedings of the 2006 Workshop on Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks*. ACM, 2006, pp. 65–72.

[56] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proceedings of the* 6^{th} *Annual International Conference on Mobile Computing and Networking*. ACM, 2000, pp. 255–265.

[57] A. Sheth, C. Hartung, and R. Han, "A decentralized fault diagnosis system for wireless sensor networks," in *Proceedings IEEE International Conference on Mobile Adhoc and Sensor Systems Conference*, November 2005, pp. 3 pp.–194.

[58] D. Estrin, R. Govindan, J. Heidemann, and S. Kumar, "Next century challenges : Scalable coordination in sensor networks," in *Proceedings of the* 5^{th} *Annual ACM/IEEE International Conference on Mobile Computing and Networking*. ACM, 1999, pp. 263–270.

[59] A. T. Tai, K. S. Tso, and W. H. Sanders, "Cluster-based failure detection service for large-scale ad hoc wireless network applications," in *Proceedings of International Conference on Dependable Systems and Networks*, June 2004, pp. 805–814.

[60] M. Yu, H. Mokhtar, and M. Merabti, "A survey on fault management in wireless sensor networks," in *Proceedings of the 8th Annual PostGraduate Symp. on the Convergence of Telecommunications, Networking and Broadcasting*, June 2007.

[61] X. Luo, D. Ming, and Y. Huang, "On distributed fault-tolerant detection in wireless sensor networks," *IEEE Transactions on Computers,*, vol. 55, no. 1, pp. 58–70, January 2006.

[62] T. Clouqueur, K. Saluja, and P. Ramanathan, "Fault tolerance in collaborative sensor networks for target detection," *IEEE Transactions on Computers*, vol. 53, no. 3, pp. 320–333, March 2004.

[63] S. Li and Z. Wu, "Node-disjoint parallel multi-path routing in wireless sensor networks," in *Proceedings of The* 2^{nd} *IEEE International Conference on Embedded Software and Systems*, December 2005, pp. 6 pp.–.

[64] Y. Yang, C. Zhong, Y. Sun, and J. Yang, "Network coding based reliable disjoint and braided multipath routing for sensor networks," *Journal of Network and Computer Applications*, vol. 33, no. 4, pp. 422–432, 2010.

[65] F. Ye, G. Zhong, S. Lu, and L. Zhang, "GRAdient Broadcast : A robust data delivery protocol for large scale sensor networks," *Wireless Networks*, vol. 11, no. 3, pp. 285–298, May 2005.

[66] F. Wei, L. Zhang, T. Liu, M. E. Haque, X. Lu, and K. Mori, "Autonomous fault tolerance technology of emergency community in wireless sensor network," in *Proceedings of the* 11^{th} *IEEE International Symposium on Autonomous Decentralized Systems (ISADS)*, March 2013, pp. 1–6.

[67] S. Halder, M. Mazumdar, P. Chanak, and I. Banerjee, "FTLBS : fault tolerant load balancing scheme in wireless sensor network," in *Proceedings of the* 2^{th} *International Conference on Advances in Computing and Information Technology (ACITY)*, July 2012, pp. 805–814.

[68] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed Diffusion : a scalable and robust communication paradigm for sensor networks," in *Proceedings of the* 6^{th} *Annual International Conference on Mobile Computing and Networking*. ACM, 2000, pp. 56–67.

[69] A. G. Dimakis, V. Prabhakaran, and K. Ramchandran, "Ubiquitous access to distributed data in large-scale sensor networks through decentralized erasure codes," in *Proceedings of the* 4^{th} *International Symposium on Information Processing in Sensor Networks*, April 2005, pp. 111–117.

[70] B. Deb, S. Bhatnagar, and B. Nath, "ReInForM : reliable information forwarding using multiple paths in sensor networks," in *Proceedings of* 28^{th} *Annual IEEE International Conference on Local Computer Networks*, October 2003, pp. 406–415.

[71] N. Li and J. C. Hou, "FLSS : a fault-tolerant topology control algorithm for wireless networks," in *Proceedings of the* 10^{th} *Annual International Conference on Mobile Computing and Networking.* ACM, 2004, pp. 275–286.

[72] M. Cardei, Y. Shuhui, and W. Jie, "Algorithms for fault-tolerant topology in heterogeneous wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 19, no. 4, pp. 545–558, April 2008.

[73] Y. Shou, "Cryptographie sur les courbes elliptiques et tolérance aux pannes dans les réseaux de capteurs," Ph.D. dissertation, Université de Franche-Comté, France, 2014.

[74] I. F. Akyildiz and C. V. Mehmet, *Wireless Sensor Networks.* Digital version, Wiley Online Library, 2010.

[75] G. M. Shafiullah, A. Gyasi-Agyei, and P. Wolfs, "A survey of energy-efficient and qos-aware routing protocols for wireless sensor networks," in *Novel Algorithms and Techniques In Telecommunications, Automation and Industrial Electronics.* Springer Netherlands, 2008, pp. 352–357.

[76] J. N. Al-Karaki and A. E. Kamal, "Routing techniques in wireless sensor networks : a survey," *Wireless Communications, IEEE*, vol. 11, no. 6, pp. 6–28, December 2004.

[77] W. R. Heinzelman, J. Kulik, and H. Balakrishnan, "Adaptive protocols for information dissemination in wireless sensor networks," in *Proceedings of the* 5^{th} *Annual ACM/IEEE International Conference on Mobile Computing and Networking.* ACM, 1999, pp. 174–185.

[78] J. Kulik, W. Heinzelman, and H. Balakrishnan, "Negotiation-based protocols for disseminating information in wireless sensor networks," *Wireless Networks*, vol. 8, no. 2/3, pp. 169–185, March 2002.

[79] N. Sadagopan, B. Krishnamachari, and A. Helmy, "The ACQUIRE mechanism for efficient querying in sensor networks," in *Proceedings of the IEEE International Workshop on Sensor Network Protocols and Applications (SNPA'03)*, 2003, pp. 149–155.

[80] F. Ye, A. Chen, S. Lu, and L. Zhang, "A scalable solution to minimum cost forwarding in large sensor networks," in *Proceedings of* 10^{th} *Inter-*

national Conference on Computer Communications and Networks, 2001, pp. 304–309.

[81] D. Braginsky and D. Estrin, "Rumor routing algorthim for sensor networks," in *Proceedings of the* 1^{st} *ACM International Workshop on Wireless Sensor Networks and Applications*, 2002, pp. 22–31.

[82] C. Schurgers and M. Srivastava, "Energy efficient routing in wireless sensor networks," in *Proceedings of IEEE Military Communications Conference, Communications for Network-Centric Operations : Creating the Information Force*, vol. 1, 2001, pp. 357–361.

[83] S. Lindsey and C. Raghavendra, "PEGASIS : Power-efficient gathering in sensor information systems," in *Proceedings of IEEE International Aerospace Conference*, vol. 3, 2002, pp. 1125–1130.

[84] A. Manjeshwar and D. P. Agrawal, "TEEN : a routing protocol for enhanced efficiency in wireless sensor networks," in *Proceedings of the* 15^{th} *International Symposium on Parallel and Distributed Processing*, April 2001, pp. 2009–2015.

[85] A. Manjeshwar and D. Agrawal, "APTEEN : a hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks," in *Proceedings of IEEE International Symposium on Parallel and Distributed Processing*, April 2002, pp. 8 pp–.

[86] Q. Li, J. Aslam, and D. Rus, "Hierarchical Power-aware routing in sensor networks," in *Proceedings of the DIMACS Workshop on Pervasive Networking*, 2001.

[87] J. Al-Karaki, R. Ul-Mustafa, and A. Kamal, "Data aggregation in wireless sensor networks-exact and approximate algorithms," in *Proceedins of Workshop on High Performance Switching and Routing*, 2004, pp. 241–245.

[88] Y. Xu, J. Heidemann, and D. Estrin, "Geography-informed energy conservation for ad hoc routing," in *Proceedings of the* 7^{th} *Annual International Conference on Mobile Computing and Networking*. ACM, 2001, pp. 70–84.

[89] Y. Yu, R. Govindan, and D. Estrin, "Geographical and energy aware routing : a recursive data dissemination protocol for wireless sensor networks," UCLA Computer Science Department, Tech. Rep., 2001.

[90] F. Kuhn, R. Wattenhofer, and A. Zollinger, "Worst-Case optimal and Average-case efficient geometric ad hoc routing," in *Proceedings of the 4^{th} ACM International Symposium on Mobile Ad Hoc Networking and Computing*. ACM, 2003, pp. 267–278.

[91] B. Chen, K. Jamieson, H. Balakrishnan, and R. Morris, "SPAN : an energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks," *Wireless Networks*, vol. 8, no. 5, pp. 481–494, Sep 2002.

[92] X. Chen, Y.-A. Kim, B. Wang, W. Wei, Z. J. Shi, and Y. Song, "Fault-tolerant monitor placement for out-of-band wireless sensor network monitoring," *Ad Hoc Networks*, vol. 10, no. 1, pp. 62–74, 2012.

[93] A. Challal, Y.and Ouadjaout, N. Lasla, M. Bagaa, and A. Hadjidj, "Secure and efficient disjoint multipath construction for fault tolerant routing in wireless sensor networks," *Journal of Network and Computer Applications*, vol. 34, no. 4, pp. 1380–1397, 2011.

[94] D. D. Geeta, N. Nalini, and R. C. Biradar, "Fault tolerance in wireless sensor network using hand-off and dynamic power adjustment approach," *Journal of Network and Computer Applications*, vol. 36, no. 4, pp. 1174–1185, 2013.

[95] K. Akkaya and M. Younis, "A survey on routing protocols for wireless sensor networks," *Ad Hoc Networks*, vol. 3, pp. 325–349, 2005.

[96] A. Ajay, N. Tarasia, S. Dash, and S. S. A. Ray, "A dynamic fault tolerant routing protocol for prolonging the lifetime of wireless sensor networks," *International Journal of Computer Science and Information Technologies*, vol. 2, no. 2, pp. 727–734, 2011.

[97] A. Ajay, N. Tarasia, S. Dash, S. Ray, and A. R. Swain, "Fault-tolerant multilevel routing protocol with sleep scheduling (FMS) for wireless sensor networks," *European Journal of Scientific Research*, no. 1, pp. 97–108.

[98] K. Kulothungan, J. A. Arul Jothi, and A. Kannan, "An adaptive fault-tolerant routing protocol with error reporting scheme for wireless sensor networks," *European Journal of Scientific Research*, vol. 60, no. 1, pp. 19–32, 2011.

[99] G. Wu, C. Lin, F. Xia, L. Yao, H. Zhang, and B. Liu, "Dynamical jumping real-time fault-tolerant routing protocol for wireless sensor networks," *Journal of Sensors*, vol. 10, no. 3, pp. 2416–2437, 2010.

[100] Z. Che-Aron, W. Al-Khateeb, and F. Anwar, "The enhanced fault-tolerance mechanism of AODV routing protocol for wireless sensor network," *International Journal of Computer Science and Network Security*, vol. 10, no. 6, pp. 41–50, 2010.

[101] C. Perkins and E. Royer, "Ad-hoc on-demand distance vector routing," in *Proceedings of the* 2^{nd} *IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'99)*, Feb 1999, pp. 90–100.

[102] F. Benhamida and Y. Challal, "FaT2D : fault-tolerant directed diffusion for wireless sensor networks," in *Proceedings of International Conference on Availability, Reliability, and Security (ARES'10)*, February 2010, pp. 112–118.

[103] M. Lehsaini and C. Tabet Hellel, "A novel cluster-based fault-tolerant scheme for wireless sensor networks," in *Proceedings of the* 24^{th} *IEEE International Conference on Microelectronics (ICM'2012)*, December 2012, pp. 1–4.

[104] M. Mehrani, J. Shanbehzadeh, A. Sarrafzadeh, S. Mirabedini, and C. Manford, "FEED : fault-tolerant,energy efficient, distributed clustering for wsn," in *Proceedings of the* 12^{th} *International Conference on Advanced Communication Technology*, vol. 1, February 2010, pp. 580–585.

[105] L. Venkatesan and S. Shanmugavel, "Reliable energy-efficient fault-tolerant clustering for wireless sensor networks," *Asian Journal of Scientific Research*, vol. 7, no. 1, pp. 33–44, 2014.

[106] M. Azharuddin, P. Kuila, and P. K. Jana, "Energy efficient fault tolerant clustering and routing algorithms for wireless sensor networks," *Journal*

of Computers and Electrical Engineering, vol. 41, no. 0, pp. 177–190, 2015.

[107] P. Chanak and I. Banerjee, "Energy-efficient fault-tolerant multipath routing scheme for wireless sensor networks," *The Journal of China Universities of Posts and Telecommunications*, vol. 20, no. 6, pp. 42–61, 2013.

[108] M. Beldjehem, "Towards a multi-hop, multi-path fault-tolerant and load balancing hierarchical routing protocol for wireless sensor network," *The Journal of Wireless Sensor Network*, vol. 5, no. 11, pp. 215–222, 2013.

[109] A. P. Heinzelman, W. B.and Chandrakasan and H. Balakrishnan, "An application specific protocol architecture for wireless microsensor networks," *IEEE Transactions on Wireless Communications*, vol. 1, no. 4, pp. 660–667, 2002.

[110] M. Lehsaini and H. Guyennet, "Improvement of LEACH for fault-tolerance in sensor networks," in *Proceedings of the* 4^{th} *International Conference on Modeling Approaches and Algorithms for Advanced Computer Applications (CIIA'2013)*, May 2013, pp. 175–183.

[111] A. Ahlawat and V. Malik, "An extended vice-cluster selection approach to improve V LEACH protocol in wsn," in *Proceedings of The* 3^{rd} *IEEE International Conference on Advanced Computing and Communication Technologies,*, April 2013, pp. 236–240.

[112] A. Mohammed and M. Shanmukhaswamy, "New algorithm for optimized cluster heads with failure detection and failure recovery to extend coverage of wireless sensor network," *International Journal of Scientific and Research Publications*, vol. 2, no. 11, pp. 1–4, 2012.

[113] M. Bani Yassein, A. Al-zou'bi, Y. Khamayseh, and W. Mardini, "Improvement on LEACH protocol of wireless sensor network (VLEACH)," *International Journal of Digital Content Technology and its Applications*, vol. 3, no. 2, pp. 260–264, 2009.

[114] H. Y. Min and W. Zaw, "Energy-efficient fault-tolerant routing LEACH (EF-LEACH) protocol for wireless sensor networks," in *Proceedings of International Conference on Advances in Engineering and Technology (ICAET'2014)*, March 2014, pp. 36–20.

[115] R. Mitra and A. Biswas, "Incorporating fault tolerance in LEACH protocol for wireless sensor network," *International Journal of Computer Science and Communication Networks (IJCSCN)*, vol. 2, no. 3, pp. 380–384, 2012.

[116] T. Liu, Q. Li, and P. Liang, "An energy-balancing clustering approach for gradient-based routing in wireless sensor networks," *Computer Communications*, vol. 35, no. 17, pp. 2150–2161, 2012.

[117] I. El-Korbi, Y. Ghamri-Doudane, R. Jazi, and L. A. Saidane, "Coverage-connectivity based fault tolerance procedure in wireless sensor networks," in *Proceedings of the* 9^{th} *IEEE International Conference on Wireless Communications and Mobile Computing*, July 2013, pp. 1540–1545.

[118] V. Katiyar, N. Chand, G. Gautam, and A. Kumar, "Improvement in LEACH protocol for large-scale wireless sensor networks," in *Proceeding of IEEE International Conference on Emerging Trends in Electrical and Computer Technology*, March 2011, pp. 1070–1075.

[119] N. Israr and I. Awan, "Multihop clustering algorithm for load balancing in wireless sensor networks," *International Journal of Simulation Systems, Science and Technology*, vol. 8, no. 1, pp. 13–25, 2007.

[120] C. Tabet Hellel, M. Lehsaini, and H. Guyennet, "An enhanced fault-tolerant version of leach for wireless sensor networks," *International Journal of Advancements in Computing Technology (IJACT)*, vol. 6, no. 6, pp. 50–57, 2014.

[121] P. Levis, N. Lee, M. Welsh, and D. Culler, "TOSSIM : accurate and scalable simulation of entire tinyos applications," in *Proceedings of the* 1^{st} *International Conference on Embedded Networked Sensor Systems (SenSys'03)*. ACM, 2003, pp. 126–137.

[122] V. Shnayder, M. Hempstead, B. Chen, G. W. Allen, and M. Welsh, "Simulating the power consumption of large-scale sensor network applications," in *Proceedings of the* 2^{nd} *International Conference on Embedded networked sensor systems (SenSys'04)*, November 2004, pp. 188–200.

[123] W. Guo and W. Zhang, "A survey on intelligent routing protocols in wireless sensor networks," *Journal of Network and Computer Applications*, vol. 38, no. 0, pp. 185–201, 2014.

[124] N. C. Brent, J. C. Charles, and S. J. David, "Unit disk graphs," *Discrete Mathematics*, vol. 86, no. 1-3, pp. 165–177, 1990.

[125] M. Lehsaini, H. Guyennet, and M. Feham, "MPR-based broadcasting in ad hoc and wireless sensor networks with a realistic environment," *International Journal of Computer Science and Network Security*, vol. 7, no. 10, pp. 82–89, 2007.

[126] C. Tabet Hellel, M. Lehsaini, and H. Guyennet, "Fault-tolerant leach-based routing protocol for wireless sensor networks," *International Journal of Computer Networks and Communications (IJCNC)*, vol. 7, no. 3, pp. 117–129, 2015.

[127] J. Kuruvila, A. Nayak, and I. Stojmenovic, "Hop-count optimal position-based packet routing algorithms for ad hoc wireless networks with a realistic physical layer," in *Proceedings of IEEE International Conference on Mobile Ad-hoc and Sensor Systems*, October 2004, pp. 398–405.

[128] C. Tabet Hellel, M. Lehsaini, and H. Guyennet, "A version of leach adapted to the lognormal shadowing model," in *In Proceedings of International Conference on Modeling Approaches and Algorithms for Advanced Computer Applications (CIIA'2015)*, May 2015, pp. 465–475.

[129] C. Alippi, G. Anastasi, C. Galperti, F. Mancini, and M. Roveri, "Adaptive sampling for energy conservation in wireless sensor networks for snow monitoring applications," in *In Proceedings of the IEEE International Conference on Mobile Adhoc and Sensor Systems*, October 2007, pp. 1–6.

[130] K. Arisha, M. Youssef, and M. Younis, "Energy-aware tdma-based mac for sensor networks," in *System-Level Power Optimization for Wireless Multimedia Communication*. Springer US, 2002, pp. 21–40. [Online]. Available : http://dx.doi.org/10.1007/0-306-47720-3_2

[131] A. A. Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks," *Computer Communications*, vol. 30, no. 14âĂŞ15, pp. 2826–2841, 2007.

[132] G. Zhou, T. He, S. Krishnamurthy, and J. A. Stankovic, "Models and solutions for radio irregularity in wireless sensor networks," *ACM Transactions on Sensor Networks*, 2010.

[133] N. Baccour, A. Koubâa, L. Mottola, M. A. Zúñiga, H. Youssef, C. A. Boano, and M. Alves, "Radio link quality estimation in wireless sensor networks : A survey," *ACM Transactions on Sensor Networks*, vol. 8, no. 4, pp. 1–34, September 2012.

[134] A. Cerpa, J. L. Wong, M. Potkonjak, and D. Estrin, "Temporal properties of low power wireless links : Modeling and implications on multihop routing," in *Proceedings of the* 6^{th} *International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'05).* ACM, 2005, pp. 414–425.

[135] K. Srinivasan, P. Dutta, A. Tavakoli, and P. Levis, "An empirical study of low-power wireless," *ACM Transactions on Sensor Networks*, 2010.

[136] J. Zhao and R. Govindan, "Understanding packet delivery performance in dense wireless sensor networks," in *Proceedings of the* 1^{st} *International Conference on Embedded Networked Sensor Systems (SenSys'03).* ACM, 2003, pp. 1–13.

[137] N. Reijers, G. Halkes, and K. Langendoen, "Link layer measurements in sensor networks," in *Proceedings of the* 1^{st} *IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS'04).* ACM, 2004, pp. 24–27.

[138] A. Cerpa, N. Busek, and D. Estrin, "Scale : A tool for simple connectivity assessment in lossy environments," CENS System Laboratory, Tech. Rep., 2003.

[139] A. Cerpa, J. L. Wong, L. Kuang, M. Potkonjak, and D. Estrin, "Statistical model of lossy links in wireless sensor networks," in *Proceedings of the* 4^{th} *IEEE International Symposium on Information Processing in Sensor Networks (IPSN'05)*, 2005, pp. 81–88.

[140] P. Misra, N. Ahmed, and J. Sanjay, "An empirical study of asymmetry in low-power wireless links," *IEEE Communications Magazine*, vol. 50, no. 7, pp. 137–146, July 2012.

[141] P. M. Shankar, *Introduction to Wireless Systems.* New York, NY, USA : John Wiley & Sons, Inc., 2001.

[142] T. He, C. Huang, B. M. Blum, J. A. Stankovic, and T. Abdelzaher, "Range-free localization schemes for large scale sensor networks," in *Proceedings of the* 9^{th} *Annual International Conference on Mobile Computing and Networking (MobiCom'03).* ACM, 2003, pp. 81–95.

[143] G. Zhou, T. He, S. Krishnamurthy, and J. A. Stankovic, "Impact of radio irregularity on wireless sensor networks," in *Proceedings of the* 2^{nd} *ACM International Conference on Mobile Systems, Applications, and Services (MobiSys'04).* ACM, 2004, pp. 125–138.

[144] M. Haenggi, "Analysis and design of diversity schemes for ad hoc wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 1, pp. 19–27, January 2005.

[145] A. Abdi, C. Tepedelenlioglu, M. Kaveh, and G. Giannakis, "On the estimation of the k parameter for the rice fading distribution," *IEEE Communications Letters*, vol. 5, no. 3, pp. 92–94, March 2001.

Résumé : Les réseaux de capteurs sans fil (RCSF) sont enclins à plusieurs pannes dues aux limitations énergétiques des nœuds ainsi que leur déploiement dans des environnements hostiles dans lesquels le remplacement des batteries épuisées ou bien des capteurs détruits est quasi impossible. La panne des nœuds ou des liens de communication peut affecter le bon fonctionnement du réseau ainsi que sa durée de vie et dégrade ses performances. Dans ce contexte, la tolérance aux pannes doit être sérieusement considérée pour le bon fonctionnement du réseau même en cas de présence des défaillances.

Dans cette thèse, nous avons abordé le problème de la tolérance aux pannes dans les RCSF tout en minimisant la consommation d'énergie. Nous avons proposé trois contributions. Deux contributions améliorent le protocole de routage LEACH pour qu'il préserve ses performances dans un environnement non-idéal. La première contribution consiste à améliorer le protocole LEACH pour le rendre tolérant aux pannes dans un environnement non idéal tout en minimisant la consommation dŠénergie, et dans la deuxième contribution, une nouvelle version de LEACH est proposée, appelée FTLR (Fault-Tolerant LEACH-based Routing protocol) qu'il s'adapte à un environnement réaliste basé sur le modèle Log-Normal Shadowing. Dans la troisième contribution, nous avons proposé un nouveau protocole de routage hiérarchique tolérant aux pannes adapté à un environnement réaliste.

Mots clés : Réseaux de capteurs sans fil, tolérance aux pannes, LEACH, modèle Log-Normal Shadowing, modèle probabiliste.

Title of thesis

Abstract : Wireless sensor networks (WSN) are more prone to failures due to energy limitations of the nodes and their deployment in hostile environments in which to replace expired batteries or destroyed sensors is impossible. The failure of nodes or communication links may affect the operation of the network and its lifetime and degrades performance. In this context, fault tolerance must be seriously considered to ensure reliable delivery and smooth operation even in case of presence of network failures.

In this thesis, we are interested to deal with fault-tolerance in WSN taking into account energy constraints. We proposed three contributions. Two contributions are based on the LEACH routing protocol to improve its performance in a non-ideal environment. The first contribution improves the LEACH protocol to make it fault-tolerant in a non-ideal environment while minimizing energy consumption, and in the second contribution, a novel version of LEACH is proposed, called FTLR (Fault-Tolerant LEACH-based Routing protocol) that it adapts to a realistic environment based on the Log-Normal Shadowing model. In the third contribution, we proposed a hierarchical fault-tolerant routing protocol adapted to a realistic environment to ensure reliable communication links based on the model "Log-Normal Shadowing" and the probabilistic model.

Keywords : Wireless sensor network, fault tolerance, LEACH, LogNormal Shadowing model, probabilistic model