République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A/Mira de Béjaia
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de fin de cycle en vue de l'obtention du diplôme de master Recherche en informatique

Option
Réseaux et Systèmes Distribués

Thème

Proposition d'un protocole de routage hiérarchique tolérant aux pannes dans les réseaux de capteurs sans fil

Présenté par :$\mathcal{M}^{\text{lle}}$: ACHOURI Sara
& $\mathcal{M}^{\text{lle}}$: MADI Karima

Soutenu le 02 Juillet 2017 devant le jury composé de :

Président	**Dr BELKHIRI Louiza**	**Maître de conf. A**	**U. A/Mira Béjaia.**
Rapporteur	**Dr REBOUH Nadjette**	**Maître de conf. A**	**U. A/Mira Béjaia.**
Examinatrice	**Dr OUYAHIA Samira**	**Maître de conf. B**	**U. A/Mira Béjaia.**
Examinatrice	**Dr ZIDANI Farroudja**	**Maître de conf. A**	**U. A/Mira Béjaia.**

Promotion 2017

⁂ Remerciements ⁂

Au terme de ce modeste travail, nous tenons à remercier, le bon dieu de nous avoir donné courage, volonté, patience et surtout santé pour le réaliser.

Notre profonde gratitude va à notre promotrice $\mathcal{M}^{me}$ REBOUH Nadjette et $\mathcal{M}^{me}$ OUYAHIA Samira, pour l'honneur qu'elles nous ont fait en nous encadrant, pour leurs précieux conseils, orientations et la confiance placés en nous, dont nous garderons les souvenirs de leurs qualités profondément humaines.

Nous adressons nos plus vifs remerciements aux honorables membres du jury, qui ont bien Accepté de juger ce travail.

Nous remercions, également, toutes les personnes qui ont contribué de près ou de loin à la réalisation de ce mémoire.

Sara et Karima

⁕ *Dédicaces* ⁕

A l'aide de DIEU, le tout puissant, ce travail est achevé, je le dédie à tous ceux qui me sont Très chers.
A ceux que j'ai tant aimée avec beaucoup d'affection, sincèrement je suis très fière de les avoir comme parents et que tous les mots qui puissent exister sur terre ne peuvent exprimer l'amour et le respect que je leurs porte
Ma mère et Mon père
A mon Grand frère Bilal pour grand soutien durant toute ma vie.
A mes très chérs frères : Riyadh, Ala, à qui je souhaite la réussite.
A mes merveilleuses sœurs : Hiloua, Nadjah et l'adorable petite Nina.
A mes oncles, tantes, cousines, cousins.
A mes très chères amies que j'aime : Karima, Hassiba, Kaho, Kanza, Hoho, Sihame, Alim, lynda, etc.
A mes très chères copines de chambre : Sihame, Alim.
A ma camarade Karima et sa famille.
A toute la promotion Recherche 2017.

$\mathcal{M}^{lle}$: ACHOURI Sara

⁂ *Dédicaces* ⁂

A l'aide de DIEU, le tout puissant, ce travail est achevé, je le dédie à tous ceux qui me sont Très chers.
A ceux que j'ai tant aimée avec beaucoup d'affection, sincèrement je suis très fière de les avoir comme parents et que tous les mots qui puissent exister sur terre ne peuvent exprimer l'amour et le respect que je leurs porte
Ma mère et Mon père
A mon Grand frère Karim pour grand soutien durant toute ma vie.
A mes très chérs frères : Kamel, Zahir, à qui je souhaite la réussite.
A mes merveilleuses sœurs : Kahina, Mebrouka.
A mes oncles, tantes, cousines, cousins.
A mes très chères amies que j'aime
A ma camarade Sara et sa famille.
A toute la promotion Recherche 2017.

$\mathcal{M}^{lle}$ ***: MADI karima***

Table des matières

Table des matières i

Table des figures iv

Liste des tableaux vi

Liste des abréviations vii

Introduction générale 1

1 Généralités sur les réseaux de capteurs sans fil 3

1.1 Introduction . . . 3
1.2 Réseaux de capteurs sans fil . . . 3
1.3 Qu'est-ce qu'un noeud capteur ? . . . 4
1.4 Composants d'un capteur . . . 4
1.4.1 Unité de captage . . . 5
1.4.2 Unité de traitement . . . 5
1.4.3 Unité de transmission . . . 5
1.4.4 Unité de contrôle d'énergie . . . 5
1.4.5 Architecture de communication d'un RCSF . . . 6
1.5 Pile protocolaire d'un RCSF . . . 7
1.5.1 Couches de la pile protocolaire . . . 8
1.6 Facteurs de conception des RCSFs . . . 10
1.6.1 Passage à l'échelle(scalabilité) . . . 10
1.6.2 Coût de production . . . 11

1.6.3 Sécurité limitée . . . 11
1.6.4 Système d'exploitation . . . 11
1.6.5 Environnement . . . 11
1.6.6 Moyen de communication . . . 11
1.6.7 Faible consommation . . . 12
1.6.8 Topologie du réseau . . . 12
1.6.9 Tolérance aux pannes . . . 13
1.7 Domaines d'application des RCSFs . . . 13
1.7.1 Applications militaires . . . 13
1.7.2 Applications environnementales . . . 14
1.7.3 Applications industrielles . . . 14
1.7.4 Applications de transport . . . 15
1.7.5 Applications domestiques . . . 15
1.7.6 Applications liées à la sécurité . . . 15
1.7.7 Applications médicales . . . 15
1.8 Conclusion . . . 16

2 Tolérance aux pannes dans les RCSFs 18
2.1 Introduction . . . 18
2.2 Sûreté de fonctionnement . . . 19
2.2.1 Entraves à la sûreté de fonctionnement . . . 20
2.2.2 Attributs de la sûreté de fonctionnement . . . 21
2.2.3 Moyens d'assurer la Sûreté de fonctionnement . . . 23
2.3 Tolérance aux pannes . . . 24
2.3.1 Détection d'erreur . . . 24
2.3.2 Rétablissement du système . . . 25
2.4 Tolérance aux pannes dans les RCSFs . . . 26
2.4.1 Source des pannes dans les RCSFs . . . 26
2.4.2 Classification des solutions de tolérance aux panne dans les RCSFs . . . 28
2.5 Conclusion . . . 31

3 Protocoles de routage tolérants aux pannes dans les RCSFs 32
3.1 Introduction . . . 32
3.2 Protocoles de routage tolérants aux pannes . . . 32
3.2.1 Protocole RERP . . . 33
3.2.2 Protocole ENFAT-AODV . . . 33
3.2.3 Protocole Directed Diffusion (DD) . . . 33
3.2.4 Protocole FaT2D . . . 34
3.2.5 Protocole EAR . . . 34
3.3 Protocoles hiérarchiques . . . 34
3.3.1 Protocole CPEQ (Cluster-based PEQ) . . . 35
3.3.2 KAT Mobility . . . 42
3.3.3 Protocole FTMRS . . . 43
3.3.4 Comparaison des protocoles présentés . . . 46
3.4 Conclusion . . . 48

4 Proposition d'un protocole de routage hiérarchique tolérant aux pannes 49
4.1 Introduction . . . 49
4.2 Protocole de routage hiérarchique tolérant aux pannes . . . 50
4.2.1 Principe de fonctionnement . . . 50
4.2.2 Phase d'exécution . . . 50
4.2.3 Etude critique du protocole proposé . . . 63
4.3 Conclusion . . . 64

Conclusion et perspectives 65

Bibliographie 67

Table des figures

1.1 Noeud capteur [28]. 4
1.2 Architecture d'un noeud capteur [2]. 6
1.3 Architecture de communication d'un RCSF [28]. 7
1.4 Pile protocolaire d'un RCSF [1]. 10
1.5 Domaines d'applications [21]. 16

2.1 Arbre de la sûreté de fonctionnement [24]. 19
2.2 Propagation d'une erreur [23]. 20
2.3 La chaine fondamentale des entraves [23]. 21
2.4 Définition de MTBF [25] 22
2.5 Relation entre MTTF, MTTR et MTBF [25] 22

3.1 Envoi du message de notification [10] 36
3.2 Transférer la souscription au noeud source [10] 37
3.3 Région avec noeuds détruits [10] 38
3.4 Recouvrement de panne [10] 38
3.5 Sélection du cluster-head [11] 39
3.6 Cofiguration d'un cluster [11] 40
3.7 Transmission des données vers la station de base [11]. 41
3.8 Fonctionnement de KAT-Mobility [22] 42

4.1 Les étapes d'élection de CH1 et CH2 52
4.2 Organigramme de l'élection de deux CH 53
4.3 Composition d'un cluster 55
4.4 Etablissement des routes 56

4.5 Processeus de transmissuin de donnéesvers le CH 58
4.6 Processeus de transmission de données vers le CH actif 59
4.7 Processeus de transmission de données vers la SB 60
4.8 Organigramme de transmission des données 61
4.9 Organigramme de détection de pannes et de recouvrement 63

Liste des tableaux

3.1 Comparaison entre les protocoles 47

Liste des abréviations

ACK Acknowedgment
AGR-NTF Aggregator Notification
AODV Ad-Hoc On-Demnde DistanceVector
CTS Clear To Send
CEPQ Cluster-based PEQ
DD Directed diffusion
EAR Energy Aware Routing Protocol for Wireless Sensor Networks in ReporT
ENFAT-AODV Enhanced Fault-Tolerance Mechanism of AODV
FAT2D Fault Tolerant Directed Diffusion Protocol for Wireless Sensor Networks
FTMRS Fault-Tolerant Multipath Routing Scheme For Energy Efficient Wireless Sensor Networks
KAT-mobility K-means And TSP-based mobility
LEACH LOW-Energy Adaptive Clustering Hierarchy
MTBF Mean Time Between Failure
MTTF Mean Time To Failure
MTTR Mean Time To Repair
PEQ Periodic, Event-driven, Query-based
RCSF Réseau de Capteurs Sans Fil
RERP Routing with Error Reporting Protocol
RREP Route REPly
RREQ Route REQuest
RTS Request To Send
SB Station de base
SETAGR Set aggregator

TFD Timing Failure Detection
TTL Time To live

Introduction générale

Durant ces dernières années, les domaines de l'électronique, la mécanique et les technologies de communication sans fil ont été marqués par un développement très rapide. Ce développement a permis la production à un coût raisonnable de petits dispositifs communicants équipés d'outils appelés capteurs. De nos jours l'émergence des réseaux de capteurs sans fil (RCSF) représente une thématique de recherche prometteuse aussi bien sur le plan académique qu'industriel.

Un RCSF est constitué des noeuds capteurs autonomes, dotés de capacités de captage de grandeurs de phénomènes physiques environnementaux (température, pression, humidité, vibrations etc.) et capables de communiquer entre eux au moyen d'un support de communication sans fil. Ensemble, ces capteurs forment un réseau capable de superviser une région ou un phénomène d'intérêt, de fournir les informations utiles collectées à une station de base ou sink, qui à son tour, les transmet vers un centre de contrôle ou usagers finaux.

Dans les réseaux sans fil, on donne plus de l'importance à l'acheminement de l'information qui est assuré par des algorithmes de routage. De ce fait, il est judicieux de concevoir des protocoles de routage qui doivent prendre en considération les changements de la topologie du réseau, ainsi que d'autres caractéristiques comme la bande passante, le nombre de liens, la limitation d'énergie, etc. En outre, les capteurs sont des dispositifs fragiles sujets à des pannes multiples et dans certains cas il y aurait des capteurs défaillants qui sont impliqués dans l'acheminement des données à la station de base. Il résulte à cet effet que les données ne peuvent arriver correctement à cette dernière. Pour remédier à cette anomalie, plusieurs protocoles de routage

tolérants aux pannes ont été proposés dans la litérature. L'objectif de ce mémoire est de créer un protocole de routage hiérarchique éfficace qui tolére les pannes et assure la livraison des données vers la station de base et prolongé la duré de vie de réseau.

Ce manuscrit est organisé en quatre chapitres, et chaque chapitre est détaillé comme suit :

Dans le premier chapitre, nous allons donner un bref aperçu sur les réseaux de capteurs sns fil seront données, indiquant leurs caractéristiques, leur domaine d'application ainsi que les facteurs influençant sur leur conception. Au cours du deuxième chapitre, nous aborderons le concept de tolérance aux pannes en introduisant des généralités, des définitions et les mécanismes utilisés.

Ensuite, nous présentons dans le troisième chapitre Quelque protocole de routage tolérant aux pannes et les différentes solutions appliquées, nous concluons ce chapitre avec une comparaison de ces protocoles selon plusieurs critères

Le dernier chapitre consiste a proposé un nouveau protocole tinée a la description de notre proposition à travers les différant phase qui la constituent avec leurs avantages et leurs inconvénients. Enfin ce travail s'achève par une conclusion générale et quelque perspective.

Chapitre 1

Généralités sur les réseaux de capteurs sans fil

1.1 Introduction

Les réseaux de capteurs sans fil (RCSFs) offrent un nouveau domaine de recherche scientifique et technologique qui présente de grande possibilités pour mieux aider l'homme à interagir avec l'environnement naturel ou artificiel. C'est un type spécial de réseaux ad-hoc sans fil, formés par des petits dispositifs, qui représentent de sévères restrictions d'énergie et de capacité de traitement et de communication appelés nœuds capteur. Ce chapitre introduit des définitions sur les RCSFs, leur architectures et présente une étude sur les différents domaines d'application et les principaux facteurs et contraintes conceptuels des RCSFs.

1.2 Réseaux de capteurs sans fil

Un réseau de capteur sans fil (RCSF) est un type particulier de réseau mobile ad-hoc MANET, utilisant un très grand nombre de capteurs, pour former un réseau sans infrastructure établie. Un capteur analyse son environnement, et propage les données récoltées aux capteurs appartenant à sa zone de couverture, et chaque capteur relaie l'information sur sa propre zone de couverture, par conséquent le réseau se trouve entièrement couvert[15].

1.3 Qu'est-ce qu'un noeud capteur ?

Un capteur est un petit appareil autonome capable d'effectuer des mesures simples sur son environnement immédiat, comme la température, la vibration, la pression, la pollution, l'humidité, le bruit, le mouvement, etc, et il permet aussi de collecter, traiter, transmettre des informations via les ondes radio sur une distance limitée à quelques mètres à une autre entité (capteurs, unité de traitements, etc.). Un capteur est capable de transformer une grandeur physique observée (température, humidité, etc) en une grandeur utilisable (intensité électrique, position d'un flotteur, etc.)[31].

FIGURE 1.1 – Noeud capteur [28].

1.4 Composants d'un capteur

Un nœud capteur contient quatre unités de base : l'unité de captage, l'unité de traitement, l'unité de transmission et l'unité de contrôle d'énergie. Il peut contenir également, suivant son domaine d'application, des modules supplémentaires tels qu'un système de localisation (GPS) ou bien un système générateur d'énergie (cellule solaire).
On peut même trouver des micro-capteurs, un peu plus volumineux, dotés d'un système mobilisateur chargé de déplacer le micro-capteur en cas de nécessité.

1.4.1 Unité de captage

L'unité de captage est composée d'un ou plusieurs capteurs qui effectuent des mesures numériques sur les paramètres environnementaux et d'un convertisseur Analogique/Numérique (CAN) qui convertit l'information relevée et la transmettre à l'unité de traitement [21].

1.4.2 Unité de traitement

L'unité de traitement est composée de deux interfaces : une interface pour l'unité de captage et une interface pour l'unité de transmission. Elle est dotée également d'un processeur et d'un système d'exploitation spécifique, elle acquiert les informations en provenance de l'unité de capture et les envoie à l'unité de transmission[2].

1.4.3 Unité de transmission

Cette unité est responsable de toutes les émissions et les réceptions de données via un support de communication radio [2].

1.4.4 Unité de contrôle d'énergie

L'unité source d'énergie d'un capteur peut être une pile ou une batterie qui fournit à toutes les autres unités, l'énergie nécessaire pour faire ses tâches. Cependant, et en conséquence de sa taille réduite, la ressource énergétique dont il dispose est limitée et est généralement irremplaçable. Des techniques alternatives d'alimentation (comme solaire, vibration, etc.) ont été proposées dans la littérature. Ces techniques supposent que les nœuds capteurs sont équipés de dispositifs qui permettront de collecter l'énergie de leur environnement.
Toutefois, ces techniques ne garantissent pas une alimentation en continu des nœuds capteurs et restent très dépendantes de nombreux facteurs environnemen-

taux mais peuvent être utilisées en complément à toutes les solutions des RCSFs qui économisent de l'énergie [17].

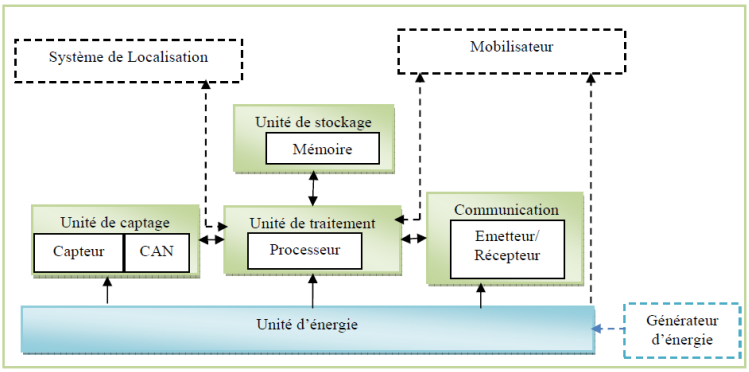

FIGURE 1.2 – Architecture d'un noeud capteur [2].

1.4.5 Architecture de communication d'un RCSF

L'architecture d'un RCSF fournit un prototype nécessaire à la compréhension de ces réseaux et les relations entre les éléments utilisés.

Cette architecture se base sur l'interaction entre les trois éléments suivants :

- **Nœuds :** Sont des capteurs, leur type, leur architecture et leur disposition géographique dépendent de l'exigence de l'application en question. Leur énergie est souvent limitée puisqu'ils sont alimentés par des piles.
- **Zone d'intérêt :** Appelée aussi "champ de captage", c'est une zone géographique où on place les capteurs du réseau pour superviser ou surveiller des phénomènes divers.
- **Stations de base (Sink) :** Nommées aussi nœuds-puits où l'écoulement des données se termine. Ces nœuds-puits sont des nœuds spéciaux qui possèdent plus de ressources matérielles et permettent de collecter et stocker et traiter les informations sorties des capteurs.

L'interaction entre ces éléments suit une séquence d'opérations telles que le

déploiement, la détection d'évènement et la transmission des données [28]. Ces opérations doivent être exécutées dans l'ordre comme montionné dans la (figure 1.3).

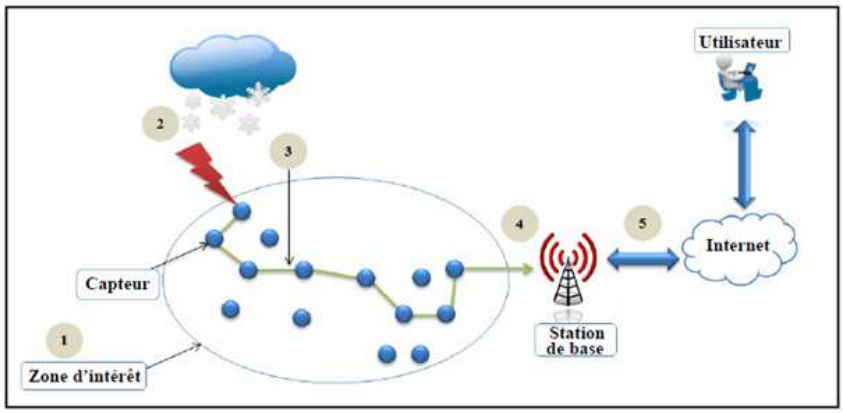

FIGURE 1.3 – Architecture de communication d'un RCSF [28].

La figure 1.3 exprime les points suivants [28] :

1. Les capteurs sont déployés dans la zone d'intérêt de façon aléatoire ou fixe.
2. Lorsqu'un capteur détecte un évènement, il le traite localement pour acquérir des données concernant cet évènement.
3. La transmission des données acquises par le capteur est réalisée par le biais d'une communication multi-sauts où un chemin est créé pendant le passage des messages par plusieurs nœuds.
4. La transmission des données se déroule jusqu'à ce qu'elles atteignent la station de base où l'écoulement des données se termine.
5. La station de base est branchée à une machine puissante via internet pour manipuler et traiter les données récoltées.

1.5 Pile protocolaire d'un RCSF

La pile protocolaire utilisée par les noeuds capteurs, combine l'énergie et le routage, intègre les données avec les protocoles réseaux, communique efficacement à

travers un medium sans fil et promet des efforts coopératifs entre les noeuds capteurs. La pile contient cinq couches : Application, transport, réseau, liaison de données et physique, et trois plans de gestion : D'énergie, de mobilité et de tâches.

1.5.1 Couches de la pile protocolaire

- **Couche application**
  La couche application constitue l'ensemble des applications implémentées sur le RCSF. Ces applications doivent fournir des mécanismes permettant à l'utilisateur d'interagir avec RCSF à travers différentes interfaces, et éventuellement, par l'intermédiaire d'un réseau étendu (par exemple internet). Il s'agit, donc, du niveau le plus proche des utilisateurs, géré directement par les logiciels.[17].
- **Couche transport**
  Elle vérifie le bon acheminement des données et la qualité de transmission dans les RCSFs.La fiabilité de transmission n'est pas majeure, mais les erreurs et les pertes sont tolérées. Le protocole de transport proche du protocole UDP et appelé UDP-Like (User Datagram Protocol Like) est utilisé.
  Cependant, comme le protocole de transport universel est TCP (Transmission Control Protocol), les RCSFs doivent donc posséder, lors d'une communication avec un réseau externe, une interface TCP-spliting pour vérifier la compatibilité entre les deux réseaux communicants [28].
- **Couche réseau**
  Elle s'occupe de l'acheminement de données fournies par la couche transport, établit les routes entre les noeuds capteurs et le noeud puits, et de sélectionner le meilleur chemin en termes d'énergie, de délai de transmission, de débit, etc. Les protocoles de routage conçus pour les RCSFs sont différents de ceux conçus pour les réseaux ad-hoc puisque les RCSFs sont différents selon plusieurs critères à savoire :
  – L'absence d'adressage fixe des noeuds tout en utilisant un adressage basé-attribut.
  – L'établissement des communications multi-sauts.

  - L'établissement des routes liant plusieurs sources en une seule destination pour agréger des données similaires, etc. [27].

- **Couche liaison de données**
  Elle est responsable de l'accès au media physique et la détection et la correction d'erreurs intervenues sur la couche physique.
  De plus, elle établit une communication saut-par-saut entre les noeuds, c'est-à-dire, elle détermine les liens de communication entre eux dans une distance d'un seul saut [17].
- **Couche physique**
  Elle permet de moduler les données et les acheminer dans le media physique tout en choisissant les bonnes fréquences [21].

En plus de ces couches, il existe trois plans de gestion à savoir, voir la figure 1.4 :

1.5.1.1 Plan de gestion d'énergie

Les fonctions intégrées à ce niveau consistent à gérer l'énergie consommée par les capteurs, dès lors, un capteur peut par exemple éteindre son interface de réception dès qu'il reçoit un message d'un noeud voisin afin d'éviter la réception des messages dupliqués. De plus, quand un noeud possède un niveau d'énergie faible, il peut diffuser un message aux autres capteurs pour ne pas participer aux tâches de routage et conserver l'énergie restante aux fonctionnalités de captage [38].

1.5.1.2 Plan de gestion de mobilité

Ce niveau détecte et enregistre tous les mouvements des noeuds capteurs, d'une manière à leur permettre de garder continuellement une route vers l'utilisateur final, et maintenir une image récente sur les noeuds voisins ; cette image est nécessaire pour pouvoir équilibrer l'exécution des tâches et la consommation d'énergie [17].

1.5.1.3 Plan de gestion des tâches

Il équilibre et ordonnance les différentes tâches de captage de données dans une région spécifique, balance les tâches entre les noueds afin d'économiser de l'énergie [21, 17].

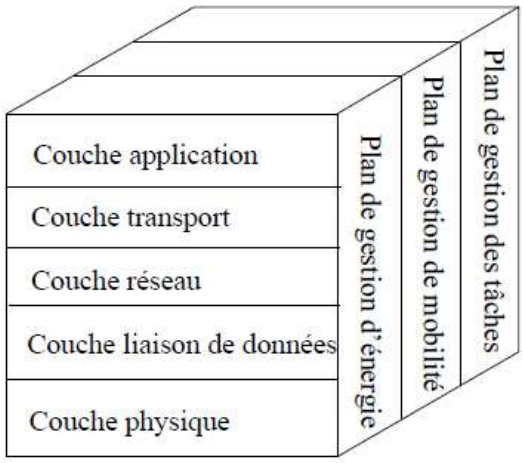

FIGURE 1.4 – Pile protocolaire d'un RCSF [1].

1.6 Facteurs de conception des RCSFs

1.6.1 Passage à l'échelle(scalabilité)

Le nombre des nœuds capteurs déployés dans un RCSF peut être en centaines ou en milliers, suivant l'application, il faut donc que le réseau de capteurs garantisse un bon fonctionnement avec ce nombre important des nœuds et exploite sa nature fortement dense [17].

1.6.2 Coût de production

Le coût global d'un réseau de capteurs est en relation avec le coût de production des capteurs qu'il contient, donc il faut réduire le coût de production des capteurs afin de minimiser le coût globale d'un réseau de capteurs [28].

1.6.3 Sécurité limitée

Comme pour tout réseau sans fil, l'information circule sur une interface partagée et non dédiée. N'importe quel intrus peut alors soit récupérer l'information, soit la modifier ou la rendre inexploitable. C'est pour cela des mesures de sécurité doivent être mise en place pour protéger l'information. Cependant, tous les mécanismes de sécurité sont créés pour des réseaux où les noeuds disposent d'une forte capacité de traitement, ce qui n'est pas le cas des capteurs. À ce jour, très peu de solutions sont adaptées aux capteurs en termes de sécurité [21].

1.6.4 Système d'exploitation

La contrainte énergétique des capteurs exige l'utilisation de systèmes d'exploitation légers tels que TinyOS ou Contiki. Cependant, TinyOS reste toujours le plus utilisé, il est utilisable dans des simulations pour le développement et le test des protocoles des réseaux [1].

1.6.5 Environnement

Les nœuds capteurs doivent être embarqués d'une manière à résister aux différentes situations de leur environnement (forte chaleur, pluie, catastrophe, humidité, etc.) [3].

1.6.6 Moyen de communication

Dans les réseaux de capteurs, le moyen le plus utilisé pour communiquer est la fréquence radio malgré l'existence d'autres moyens comme l'infrarouge, l'optique, et

ceci pour des raisons de faible coût et de facilité d'installation. Il faut, donc, avoir un média de transmission très normé [18].

1.6.7 Faible consommation

L'économie d'énergie est l'une des problématiques majeures dans les RCSF. En effet, la recharge des sources d'énergie est souvent trop coûteuse et parfois impossible, par conséquent il est crucial de minimiser la consommation moyenne des capteurs. Une des alternatives, explorées aujourd'hui par les chercheurs, consiste à extraire l'énergie de l'environnement (lumière intérieure ou extérieure, vibrations mécaniques, bruit acoustique). Ces techniques peuvent grandement améliorer la durée de vie, mais comme la production d'énergie est très faible, une consommation d'énergie des capteurs réduite reste de la plus haute importance [31].

1.6.8 Topologie du réseau

En raison de leur forte densité dans la zone à observer, il faut que les capteurs soient capables d'adapter leur fonctionnement afin de maintenir la topologie souhaitée [9].
La maintenance de la topologie consiste en trois phases [18] :

1. **La phase de déploiement :** Les nœuds sont deployés soit de manière prédéfinie, soit de manière aléatoire (lancés en masse depuis un avion). Il faut alors que ceux-ci s'organisent de manière autonome.
2. **La phase de post-déploiement - exploitation :** La topologie du réseau peut être soumise à des changements dûs à des mouvements de certains nœuds ou bien à des pannes.
3. **La phase de redéploiement :** L'ajout de nouveaux capteurs dans un réseau implique aussi une remise à jour de la topologie.

1.6.9 Tolérance aux pannes

Certains capteurs pourraient être défaillants, bloqués à cause de l'épuisement de leurs batteries, des erreurs de fabrication ou subissent des dommages physiques (écrasés par des animaux ou lorsqu'ils sont jetés par un avion).
La défaillance de ces capteurs ne devrait pas avoir une influence sur le fonctionnement du réseau.
La tolérance aux fautes est la capacité de soutenir les fonctionnalités d'un réseau de capteurs sans causer d'interruption lorsqu'un capteur cesse de fonctionner, ou une autre défaillance peut servenir. Donc, il faut mettre en place des mécanismes qui permettent d'augmenter le taux de disponibilité d'un RCSF [28].

1.7 Domaines d'application des RCSFs

Avant d'entamer les domaines d'application (voir la figure 1.5), il existe des types d'applications qui peuvent être développé pour les RCSFs selon le modèle de communication des données ; on peut citer [18] :

- **Application à la demande :** Les capteurs effectuent des mesures après la réception des ordres, de la part de la station de base.
- **Application périodique :** Il existe des intervalles de temps précis pour déclencher des mesures et envoyer les données vers la station de base de manière périodique.
- **Application événementielles :** Après la détection d'un évènement, le capteur se déclenche pour faire ses mesures.
- **Application hybride :** c'est une combinaison entre les applications à la demande et les applications périodiques.

1.7.1 Applications militaires

Comme pour beaucoup d'autres domaines, les applications militaires ont été les locomotives de la recherche pour les RCSF. Pour les militaires, un réseau de capteurs offre des avantages très précieux :

- Déploiement d'un tel RCSF sur un endroit stratégique ou difficile d'accès.
- Surveillance de toutes les activités des forces des ennemies, l'analyse du terrain avant d'y envoyer des troupes (par la détection d'agents chimiques, biologiques ou de radiations, etc .).
- Détection de la présence des agents chimiques dans l'air ou dans l'eau [17].

1.7.2 Applications environnementales

Il peut s'agir de la surveillance des animaux ou le suivi des conditions de l'environnement telles que :

- Surveiller de larges sites naturels ou industriels qui garantissent l'aspect distribué et une large couverture.
- Signaler un éventuel début d'incendie ou un volcan ou tsunami dans le champ de captage.
- Semer de nœuds capteurs en même temps avec les graines dans les champs agricoles pour pouvoir identifier les zones sèches et rendre l'irrigation plus efficace.
- Déployer des nœuds capteurs sur les sites industriels, les centrales nucléaires ou dans les raffineries de pétrole pour détecter des fuites de produits toxiques (gaz, produits chimiques, éléments radioactifs, pétrole, etc.)[21].

1.7.3 Applications industrielles

les industriels s'intéressent au potentiel des capteurs pour :

- Améliorer les processus de stockage et de livraison.
- Connaître la position, l'état et la direction d'une marchandise.
- Un client attendant une marchandise peut alors avoir un avis de livraison en temps réel et connaître la position des marchandises qu'il a commandées [9].

1.7.4 Applications de transport

Les RCSFs permettent la surveillance des réseaux ferroviaires ou routiers ainsi que d'éventuelles intrusions [3].

1.7.5 Applications domestiques

En plaçant, sur le plafond ou dans le mur, des capteurs, on peut économiser l'énergie en gérant l'éclairage ou le chauffage en fonction de la localisation des personnes [17].

1.7.6 Applications liées à la sécurité

Certaines institutions peuvent être suivies en temps réel par des RCSFs pour prévenir d'éventuel vols ou incendie par exemple :

- Détecter les altérations dans la structure d'un pont ou d'un bâtiment, suite à un séisme ou au vieillissement, par des capteurs intégrés dans les murs ou dans le béton.
- Diminuer considérablement les dépenses financières.
- Sécuriser les lieux et les êtres humains tout en garantissant les résultats les plus fiables.
- Surveiller les mouvements afin de constituer un système de détection d'intrusions distribué [21].

1.7.7 Applications médicales

La technologie des RCSFs est utilisée dans les applications de soins sanitaires, telles que [9] :

- Apporter une surveillance permanente des patients grâce à la possibilité de collecter des informations physiologiques de meilleure qualité.
- Faciliter le diagnostic des maladies grâce à des micro-capteurs qui pourront être ingérés ou implantés sous la peau.

– Micro-cameras qui peuvent être ingérées sont capables, sans avoir recours à la chirurgie, de transmettre des images de l'intérieur d'un corps humain.
– Créer une rétine artificielle composée d'une centaine de micro-capteurs pour améliorer la vision de l'œil.

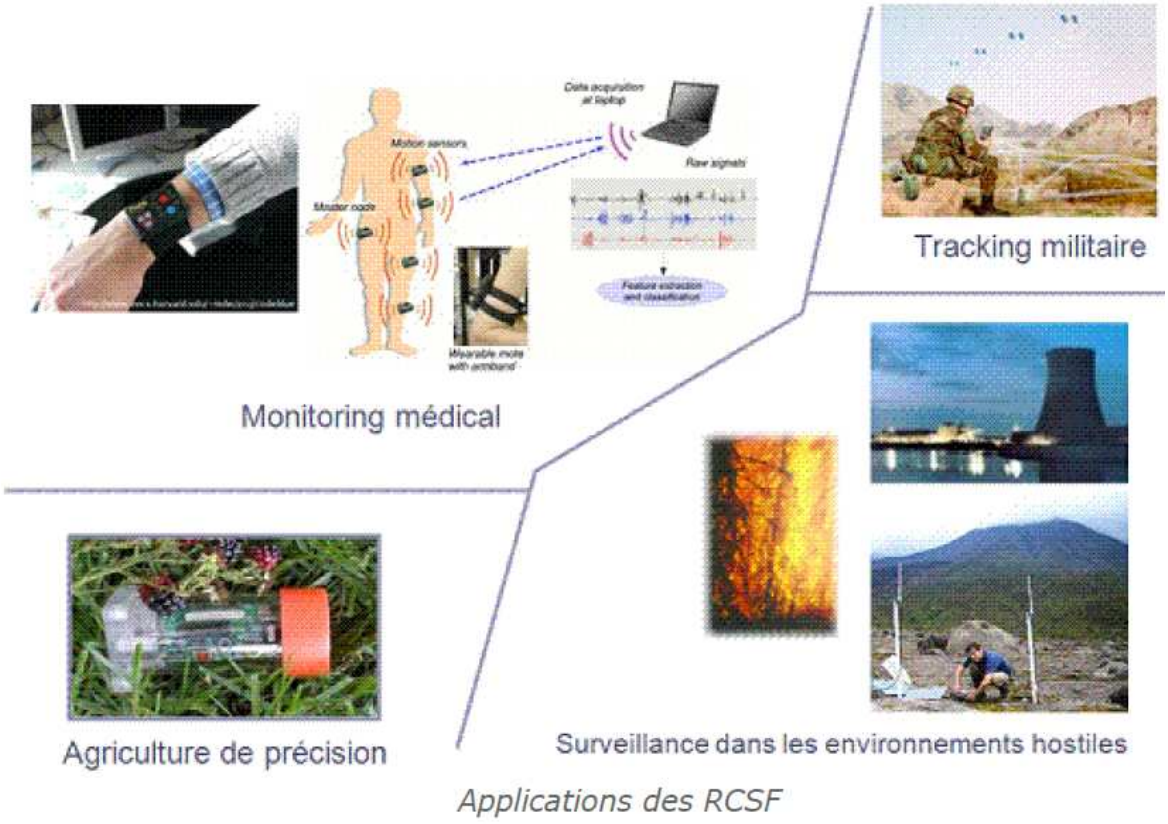

FIGURE 1.5 – Domaines d'applications [21].

1.8 Conclusion

Les RCSFs ont révolutionné le monde de l'électronique et de la télécommunication. Cette nouvelle technologie suscite un intérêt considérable étant donné son utilité et diversité dans les différents domaines de travail. Dans ce cha-

pitre, nous avons donné un bref aperçu sur les RCSF et passer en revue les différents aspects des RCSFs, tel que l'architecture, les facteurs de conception des RCSFs, la communication et les différents domaines d'applications.
Dans le prochaine chapitre, nous détaillerons la notion de tolérance aux pannes dans les RCFSs .

Chapitre 2

Tolérance aux pannes dans les RCSFs

2.1 Introduction

La limitation d'énergie dans les RCSFs, et les environnements hostiles dans lesquels ils pourraient être déployés, sont des facteurs qui rendent ce type de réseaux très vulnérables. Ainsi la perte de connexions sans fil peut être due à une extinction d'un capteur suite à un épuisement de sa batterie, ou tout simplement à une destruction physique accidentelle ou intentionnelle par un ennemi. Par ailleurs, l'absence de sécurité physique pour ce type de capteurs, et la nature vulnérable des communications radios sont des caractéristiques qui augmentent les risques de pannes sur ce type de réseau. Etant donné que les RCSFs reposent sur des protocoles de communication ad hoc, il est donc nécessaire de considérer la tolérance aux pannes comme critère indispensable dans la conception de ces protocoles. La tolérance aux pannes est l'aptitude d'un système informatique à accomplir sa fonction malgré la présence ou l'occurrence de pannes, qu'il s'agisse de dégradations physiques du matériel, de défauts logiciels, d'attaques malveillantes, d'erreurs d'interaction homme machine. Elle apparait comme un moyen de garantir une sûreté de fonctionnement.

Ce chapitre s'articulera sur la notion de tolérance aux pannes dans les RCSFs où nous commencerons par des généralité et les sources possibles de pannes. Ensuite, nous donnerons un état de l'art sur l'ensemble des techeniques existantes qui nous

permettent de détecter les pannes et de garantir la sûreté de fonctionnement dans les RCSFs.

2.2 Sûreté de fonctionnement

La sûreté de fonctionnement est définie par l'aptitude du réseau à maintenir ses fonctionnalités en cas de panne ou anomalie. Elle vise donc à minimiser l'influence de ces pannes sur la tolérance globale du réseau [4].
La figure 2.1 résume les notions associées à la sûreté de fonctionnemne présentées ci-dessous.

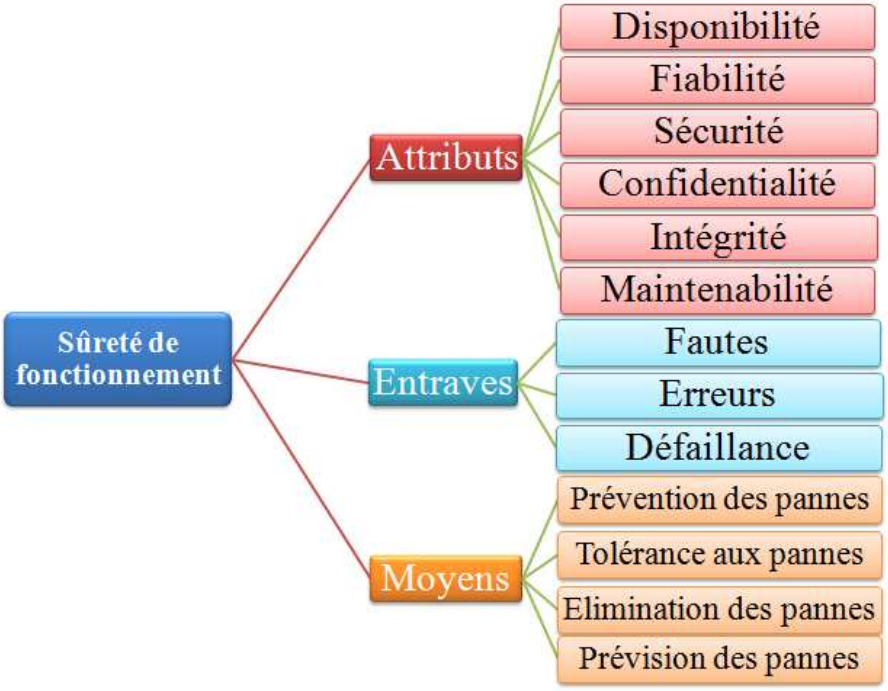

FIGURE 2.1 – Arbre de la sûreté de fonctionnement [24].

2.2.1 Entraves à la sûreté de fonctionnement

Les fautes, les erreurs et les défaillances sont les causes et les conséquences de la non sûreté de fonctionnement, telles que ces dernies sont liées par des relations de causalité [31].

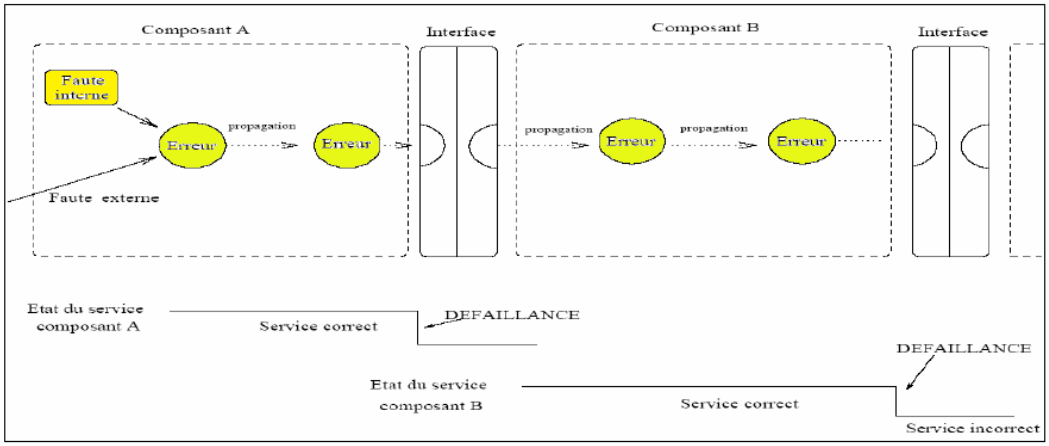

FIGURE 2.2 – Propagation d'une erreur [23].

- **Panne (défaillance)** : il s'agit d'une sortie de dysfonctionnement matériel ou logiciel qui peut causer des erreurs, par exemple un défaut matériel ou un bogue de programme [31].
- **Erreur** : une erreur représente un état invalide du systeme qui peut évenetuellement conduire le système à une défaillance totale [19].
- **Faute** : La faute est la première cause de l'erreur, cette dernière provoque la panne du système [31].

Une erreur est donc la manifestation d'une faute dans le système, et une défaillance est l'effet d'une erreur sur le service. Ceci conduit à la chaîne fondamentale présentée dans le figure 2.3 :

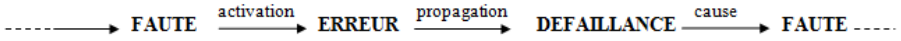

FIGURE 2.3 – La chaine fondamentale des entraves [23].

2.2.2 Attributs de la sûreté de fonctionnement

Les attributs de la sûreté de fonctionnement d'un système mettent plus ou moins l'accent sur les propriétés que doit vérifier la sûreté de fonctionnement du système. Ces attributs permettent d'évaluer la qualité de service fournie par un système. Les attributs de la sûreté de fonctionnement sont défini par :

- **Fiabilité** : cet attribut évalue la continuité du service c'est-à-dire le taux en temps de fonctionnement pendant lequel le système ne subit aucune faute. Une mesure de cette fiabilité concerne le temps entre deux défaillances consécutives (MTBF : temps moyen entre deux défaillances).pour une période de temps de durée t, la MTBF est liée à la fiabilité par une distribution de poisson qui indique la probabilité de ne pas avoir un échec dans l'intervalle de temps [0, t] [12] :

$$R_k(t) = exp^{\lambda_{kt}} \tag{2.1}$$

Où $\lambda_k = 1/MTTF$ est le taux de défaillance du noeud capteur k, t est la période de temps et MTTF est le temps moyen jusqu'à la défaillance ou le temps moyen du bon foctionnement.

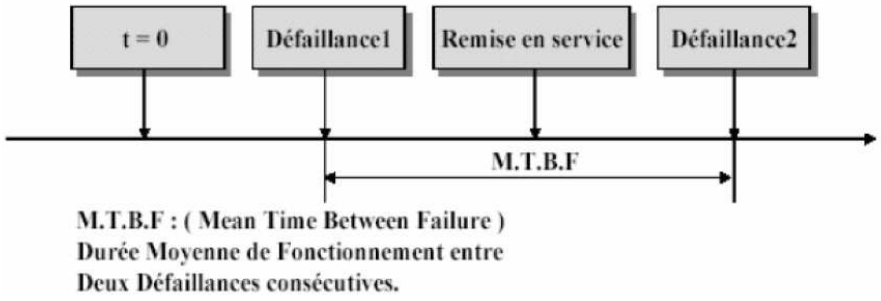

FIGURE 2.4 – Définition de MTBF [25]

- **Disponibilité** : la disponibilité regroupe les notions de fiabilité et de maintenabilité. La disponibilité d'un système est, donc, étroirement liée à la fiabilité, puisqu'elle est définie comme la probabilité pour laquelle le système fonctionne correctement à un moment donné. Elle est liée à la (MTBF : temps moyen entre deux défaillances) et à la durée moyenne de réparation (MTTR : durée moyenne de reprise) par la relation suivante [12, 24] :
  Disponibilité = $MTBF/(MTTR + MTBF)$;
  MTBF= $MTTF + MTTR$;
  Une disponibilité élevée, peut donc, être obtenue par un long MTTF ou par une durée moyenne de reprise MTTR courte. Cette situation est illustrée par la figure 2.5 :

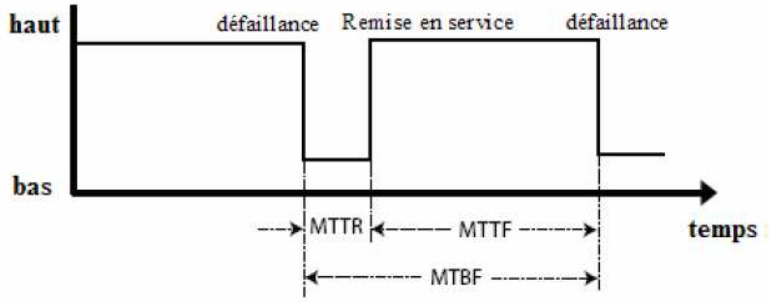

FIGURE 2.5 – Relation entre MTTF, MTTR et MTBF [25]

- **Maintenabilité** : C'est la probabilité que la maintenance d'une entité E,

assurée dans les conditions données avec des moyens et procedures prescrites, s'achève à un instant t2 pour un istant d'occurrence de la défaillance t1. M(t1,t2) = P[entité défaillante à t1 soit réparée à t2] [25].

- **Intégrité** : Représente L'assurance à accomplir correctement la mission pour laquelle il a été conçu. Cette assurance implique bien entendu sa capacité à reconnaitre le mode de fonctionnement dans lequel se trouve le système (normal ou anormal) et à signaler ce mode de fonctionnement.
- **Crédibilité** : Elle précise le comportement en cas d'anomalies du système. Elle repose sur la notion d'intégrité et de sécurité[4].
- **Sécurité** : C'est l'ensemble des moyens mises en œuvre pour réduire la vulnérabilité d'un système contre les menaces et les attaques (accidentelle ou intentionnelle) afin d'assurer la confidentialité, l'intégrité et la disponibilité [4].
- **Confidentialité** : Elle correspond à l'absence de divulgation non autorisée de l'information. Cet attribut évalue la capacité du système à fonctionnement en dépit du faut intentionnelles et d'intrusion illégales.

2.2.3 Moyens d'assurer la Sûreté de fonctionnement

Les moyens utilisés pour assurer la sûreté de fonctionnement sont définis par les méthodes et les approches utilisées pour assurer cette propriété, les approches les plus connues sont [24, 13] :

- **Prévention des pannes** : Qui s'attache aux moyens permettant d'éviter l'occurence de fautes dans le système. Ce sont généralement les approches de vérification des modèles conceptuels. Elle repose sur des règles de développement (modularisation, utilisation de langage fortement typé, preuve formelle, etc.).
- **Élimination des pannes** : Une fois une panne détecte et localisée il faut réagisse rapidement. Il peut soit isoler la partie en panne, soit essayer de la réparer. Le but est laissé le système continuer à fonctionner. Une méthode est largement utilisée est la redondance c'est -à-dire que les composants essentiales pour le bon fonctionnement du système sont répliqués pour augmenter sa

fiabilité en cas de pannes sévères. Dans un RCSF les composent a répliqués sont souvent des nœuds assure des services particulier, par exemple les nœuds passerelle dans des protocoles de routage, si le réseau pour laquelle les nœuds sont censés être déployer en masse, car en peut trouver un grand nombre de nœuds qui sont disponible, on peut les utilise soit pour substitue les nœuds en pannes, soit assure simultanément une seule fonctionnalité.

- **Prévision des pannes** : Théoriquement, il est impossible d'éviter complètement les pannes et les anomalies qui surviennent durant le fonctionnement du réseau car ils ne sont pas toujours prévisible. Par contre, il est possible de capturer un état erroné du système et de faire le nécessaire pour qu'il puisse continuer à fonctionner, d'une manière réduite. Après le déploiement et la mise en service d'un réseau, les nœuds doivent effectuer périodiquement des opérations diagnostiques pendant la transmission et le traitement des données lorsqu'une erreur est détectée, ils la signalent immédiatement aux autres nœuds qui s'en occupent pour réagir le plus vite possible.

2.3 Tolérance aux pannes

Elle repésente l'ensemble des techniques permettant à un système de continuer à fonctionner, même en dépit de l'existence de pannes, de l'un de leurs composants. En d'autres termes, le système ne s'arrête pas de fonctionner, qu'il y ait défaillance matérielle ou défaillance logicielle. Un exemple en dehors de l'informatique est celui du véhicule à moteur conçu pour être toujours en état de rouler même si l'un de ses pneus est crevé, elle mise en ouvre par la détection des erreurs et le rétablissement du système[34].

2.3.1 Détection d'erreur

La détection d'erreur est une procédure cruciale sans laquelle le système ne peut pas choisir et prendre la réaction adapté pour minimiser les impacts et les services qu'il fournit risque d'être suspendus.il s'agit généralement d'un diagnostic

de fonctionnement d'un composant spécifique, parfois on essaie aussi d'avoir une prédiction de pannes, c'est-à-dire une analyse symptômes observés.

Dans un réseau de capteurs, les nœuds sont censés être déployés en masse et une maintenance manuelle n'est pas intéressent du tout, car trop couteuse et compliquée. Dans cette section nous présentons un ensemble de techniques qui nous permet d'automatiser la procédure de détection de pannes dans les RCSF.
Diagnostic local : Dans certains cas, un nœud est capable de détecter des erreurs en faisant un diagnostic local. Afin de tester les connexions avec ses voisins, une table de routage contenant les identifiants des voisins est crée en mémoire locale, le noeud diffuse périodiquement des paquets de test aux voisins et attend des réponses. Le nœud est soupçonné d'être isolé, si aucun voisin ne lui répond, ou ils répondent, mais avec une puissance de signal très fiable [39].
Diagnostic en groupe : Il est aussi possible de détecter des erreurs du système causées par des valeurs erronées, si les nœuds disposent d'une valeur de référence. Une application qui est largement utilisée et la collection de données, en supposant que les nœuds qui se trouvent dans la même zone sont censés capturer des valeurs similaires. Si on trouve une valeur qui possède une grande différence par rapport aux autres, cela est souvent considéré comme un symptôme d'erreur[29].

Diagnostic hybride : C'est en effet la combinaison des deux modes de diagnostic, présentés ci dessus. C'est-à-dire que les nœuds effectuent d'abord chacun un diagnostic local, mais il y toujours des chances que les résultats ne soient pas assez précis. Ensuite, les nœuds échangent les résultats de diagnostic local pour faire un diagnostic de groupe[29].

2.3.2 Rétablissement du système

Pour reconstruire un état correct, trois formes de rétablissement du système ont été identifiés : Reprise d'erreur, rétablissement par poursuite, compensation d'erreurs [20].

Reprise d'erreur : Qui consiste à sauvegarder périodiquement l'état du

système pour le ramener dans un état antérieur à partir duquel elle reprend son fonctionnement normal, les principaux inconvénients de la reprise sont la taille des sauvegardes, la difficulté d'effectuer des sauvegardes cohérentes, et le surcoût temporel nécessaire à leur établissement.

Rétablissement par poursuite : Qui consiste à créer un nouvel état à partir duquel le système peut continuer à fonctionner de façon acceptable, ce mode de recouvrement est souvent très dépendant de l'application.

Compensation d'erreurs : Qui consiste à utiliser des redondances présentes dans le système pour fournir un service correct en dépit des erreurs. Cette compensation peut être consécutive à une détection d'erreur (détection et compensation), ou appliquée systématiquement (masquage d'erreur).

2.4 Tolérance aux pannes dans les RCSFs

Dans les réseaux de capteur sans fil, certains noeuds peuvent être bloqués ou tomber en panne à cause d'un manque d'énergie, d'un dégât matériel ou d'une interférence environnementale. La panne d'un noeuds capteur ne doit pas affecter le fonctionnement global de son réseau. C'est le problème de fiabilité ou de tolérance aux pannes. La tolérance aux pannes est donc la capacité de maintenir les fonctionnalités du réseau sans interruption due à une panne d'un noeud capteur.

2.4.1 Source des pannes dans les RCSFs

Une panne est une interruption permanente de la capacité du système à réaliser sa fonction requise. Les pannes dans un RCSF peuvent survenir dans trois niveaux.

2.4.1.1 Panne au niveau du nœud

La défaillance d'un nœud peut être causée par les différents composants matériels ou logiciels. De plus, une défaillance matérielle génére des défaillances logicielles, par exemple quand la batterie d'un nœud atteint un certain niveau (bas),il y a des risques que ses composants ne puissent plus fonctionner correctement. On peut, donc, en déduire que la génération des données erronées est fortement corrélée à l'épuisement de la pile. Cependant, quelques erreurs matérielles n'affectent pas tous les services d'un nœud, celui-ci peut être utilisé pour d'autres tâches par exemple, s'occuper du routage des paquets. Les bugs logiciels sont les plus souvent sources d'erreurs dans les RCSFs. Dans[20], les chercheurs ont remarqué qu'un bug logiciel a causé la plus longue panne du réseau. La propagation des pannes rendant le système non fonctionnel pendant trois jours jusqu'à la reprogrammation manuelle des nœuds [18].

2.4.1.2 Pannes au niveau du réseau

Le routage est l'une des fonctions principales des nœuds dans un RCSF. Il est essentiel pour la collecte des données, la distribution,la mise à jour, et la coordination entre les nœuds. Des défaillance au niveau de routage peuvent engendrer des pertes et de retard de message, les liens de communications entre les nœuds sont volatiles et non très faibles, le rendement des RCSFs n'est pas toujours constant, le taux de la livraison des messages dans les tests du laboratoire ne correspond pas à la réalité. Les interférences radio peuvent causer une faute de connexion entre les nœuds. Une autre source de défaillance de liens d'interconnexion est la collision de messages. Dans [33], les chercheurs ont observé un potentiel de collisions des messages des nœuds à cause du changement fréquent de la topologie. Dans d'autres situations, les nœuds peuvent avoir de bons liens de connexions mais les messages ne sont pas délivrés à cause des erreurs de chemin. Les bugs logiciels dans le routage (couche réseau) peuvent générer des chemins circulaires ou simplement des destinations incorrectes [18].

2.4.1.3 Pannes au niveau de la station de base

La station de base est un composant essentiel dans un RCSF, par conséquent son échec mène à l'échec du réseau en entier si aucun mécanisme de tolérance aux pannes n'est mis en œuvre pour surmonter cet échec. Comme celles des nœuds déployés à distance, les pannes au niveau de la station de base peuvent aussi être causées par des défaillances ou des bogues qui se cachent dans le programme exécuté [18].

2.4.2 Classification des solutions de tolérance aux panne dans les RCSFs

Les protocoles tolérants aux pannes peuvent être vus de plusieurs angles différents. De ce fait, un ensemble de critères est défini pour les classifier. Nous citons, entre autre, des catégories de trois classifications distinctes.

2.4.2.1 Classification selon la phase de traitement

Dans cette classification, nous divisons l'ensemble des algorithmes en deux catégories principales. Si le traitement est effectué avant la panne, on parle donc d'algorithmes préventifs sinon, les algorithmes sont dits curatifs [5].

- **Algorithme préventif** : Il implémente des techniques tolérantes aux pannes qui tentent de retarder ou éviter tout type d'erreur afin de garder le réseau fonctionnel le plus longtemps possible. Nous pouvons distinguer deux niveaux pour les techniques préventives :
  1. **Au niveau de nœud :** La technique vise à prolonger la durée de vie de nœud.
  2. **Au niveau de réseau :** Elle essaye de maximiser la durée de vie de réseau pour assurer la continuité du Capturés de données et de la transmission.
     Parmi les techniques à utiliser,on cite : L'administration des ressources, l'utilisation de stratégie en veille, l'équilibrage de la consommation d'énergie et le calendrier des tâches de réseau est toujours le plus connu.

- **Algorithme curatif** : Il utilise une approche optimiste, où le mécanisme de tolérance aux pannes implémenté n'est exécuté qu'après la détection de pannes. Pour cela, plusieurs algorithmes de recouvrement après l'occurrence des pannes sont proposés dans la littérature, par exemple : Le recouvrement du chemin de routage, l'élection d'un nouvel agrégateur, etc.

2.4.2.2 Classification architecturale

1. **Gestion de la batterie** : Cette catégorie est considérée comme une approche préventive, où les protocoles définissent une distribution uniforme pour la dissipation d'énergie entre les différents noeuds capteurs, afin de mieux gérer la consommation d'énergie et augmenter ainsi la durée de vie de tout le réseau. En outre, le mécanisme de mise en veille est une technique de gestion de batterie. En effet, les protocoles déterminent des délais de mise en veille des noeuds capteurs inactifs pour une meilleure conservation d'énergie [32].
2. **Gestion de flux** : Cette catégorie regroupe les techniques qui définissent des protocoles de gestion de transfert des données (routage, sélection du canal de transmission, etc.). Nous pouvons trouver des approches préventives ou curatives sur les différentes couches (réseau, liaison de données, etc.) telles que[14] :
   -Routage multi-chemin : Il utilise un algorithme préventif pour déterminer plusieurs chemins depuis chaque capteur vers le nœud collecteur. Ceci garantit la présence de plus d'un chemin fiable pour la transmission et offre une reprise rapide du transfert en cas de panne sur le chemin principal et choisissant un des chemins qui restent[26].

   -Recouvrement de routes : Après la détection de panne, une technique curative permet de créer un nouveau chemin qui soit le plus fiable pour retransmettre les données [14].
   -Allocation du canal : Cette solution est implémentée au niveau de la couche MAC, et permet d'effectuer une allocation du canal de transmission d'une manière à diminuer les interférences entre les nœuds voisins et éviter les colli-

sions durant le transfert.

-Mobilité : certains protocoles proposent comme solution tolérante aux pannes la sélection d'un ensemble de nœuds mobiles chargés de se déplacer entre les capteurs et collecter les données captées. Ceci réduira l'énergie consommée au niveau de chaque capteur en éliminant sa tâche de transmission. Un nœud mobile est généralement doté d'une batterie plus importante que celle d'un nœud capteur.

3. **Gestion des données** : Les protocoles classés dans cette catégorie offrent une meilleure gestion de données et de leur traitement. Deux principales sous-catégories sont déterminées [7] :

   -Agrégation : cette approche est considérée comme une approche préventive. Elle permet d'effectuer un traitement supplémentaire sur les données brutes captées depuis l'environnement. Un nœud agrégateur combine les données provenant de plusieurs nœuds en une information significative. Ce qui réduit considérablement la quantité de données transmises en consommant moins d'énergie pour leur dissémination. Ceci permet donc d'augmenter la durée de vie du réseau, en outre, elle essaie d'amortir l'erreur si le résultat de l'agrégation est une moyenne.

   -Clustering : une des importantes approches pour traiter la structure d'un RCSF est le clustering. Il permet la formation d'un backbone virtuel qui améliore l'utilisation des ressources rares telles que la bande passante et l'énergie. Par ailleurs, le clustering aide à réaliser du multiplexage entre les différents clusters. En outre, il améliore les performances des algorithmes de routage. Plusieurs protocoles utilisent cette approche préventive et parfois elle est considérée comme une approche curative[5] .

2.4.2.3 Classification selon le niveau d'implémentation

Afin de garantir la fiabilité de transmission, donc, la tolérance aux panne assurée par une phase de prévention de panne avant la transmission (en éjectant des délais d'attente, des mécanismes d'écoute du canal, etc.). Le mécanisme de transmission des données qui se fait grâce à des communications multi sauts est efficace

pour le problème de propagation et des dégradations du signal mais ce type de communication est conforté a des problèmes de choix du meilleur chemin à emprunter pour garantir la livraison des données (qui soit lien fiable et qui consomme moins d'énergie). La tolérance aux panne, assure une fiabilité de délivrance de paquets à la station de base, est traitée au niveau de la couche réseau.

2.5 Conclusion

Dans ce chapitre, nous avons présenté le concept de tolérance aux pannes, ses définitions générales, ses différentes approches proposées. Plus spécialement, nous avons étudié cette notion dans les réseaux de capteurs sans fil. Nous avons vu les différentes pannes qui peuvent affectées ce type de réseau, ainsi nous avons présenté quelques solutions proposées par les chercheurs. Ainsi, nous avons remarqué que la tolérance aux pannes dans un tel système (RCSF) est indispensable pour que le réseau soit toujours fonctionnel.

Dans le chapitre suivant nous présenterons quelques protocoles de routage tolérants aux pannes dans RCSFs.

Chapitre 3

Protocoles de routage tolérants aux pannes dans les RCSFs

3.1 Introduction

Les défaillances dans un RCSF peuvent être engendrées par plusieurs causes, notamment l'épuisement d'énergie, l'endommagement physique, ou les interférences liées à l'environnement. Il résulte de l'occurrence des pannes une difficulté pour acheminer les données collectées vers le puits.
Pour remédier à ce problème, des protocoles de routage tolérants aux pannes ont été proposé dans la littérature. Du fait que la propagation et la délivrance des données dans un RCSF représente les fonctionnalités les plus importantes, ces protocoles doivent prendre en considération toutes les caractéristiques du réseau, afin d'assurer les meilleures performances du réseau : durée de vie, fiabilité, temps de réponse, etc. Dans ce chapitre, nous tenons à présenter quelques protocoles de routage tolérants aux pannes proposés et nous discutons leurs avantages et leurs limites.

3.2 Protocoles de routage tolérants aux pannes

La tolérance aux pannes a connu une importance considérable parmi les différents domaines de recherche dans les réseaux de capteurs sans fil. De ce fait des protocoles tolérants aux pannes ont été proposés afin de garantir le bon fonc-

tionnement du réseau même après la panne de certains de ses composants. dans ce travail nous nous intéressons aux protocoles de routage tolérants aux pannes.Dans ce qui suit, nous présentons les protocoles de routages tolérant aux pannes les plus connus.
Par la suit, nous focalisons seulement notre étude sur ceux appartenant à la classe des protocoles hiérarchique.

3.2.1 Protocole RERP

RERP [26] est un protocole de routage préventif. Il crée à chaque chemin principal un chemin alternatif, la capacité d'un nœud tolérant aux pannes dépend du nombre des nœuds voisins actifs. C'est-à dire si un nœud a N voisins actifs, il peut tolérer N-1 nœuds en pannes. Dans ce protocole la tolérance aux pannes se fait par la diffusion des messages du rapports d'erreurs.

3.2.2 Protocole ENFAT-AODV

Le protocole ENFAT-AODV [16] est un protocole de routage préventif, tolérant aux pannes qui améliore le protocole AODV. IL améliore de la fiabilité et la robustesse du réseau en créant un chemin de secours pour chaque noeud sur un chemin principal de livraison des données, afin de réduire le nombre de paquets perdus à cause de l'échec de chemin et assurer la continuité de livraison des paquets de données même en présence des pannes sur le chemin principal de transmission de données.

3.2.3 Protocole Directed Diffusion (DD)

DD [6] c'est un protocole de routage curatif, Son principe est basé sur la diffusion des intérêts exprimés par le puits. Si une source de données capte un évènement qui répond à cette requête, elle envoie l'information au noeud ayant transmis le message d'intérêt. En outre, ce protocole définit des règles de renforcements positif pour la sélection des chemins de routage et négatif pour renforce un autre chemin en cas de pannes.

3.2.4 Protocole FaT2D

Le protocole FaT2D [6] améliore les performances du protocole DD [6] original, qui permet essentiellement de réduire le temps de reprise, en accélérant la détection puis le recouvrement de la panne. Il définit un nouveau paramètre qui associe à chaque chemin renforcé, un délai de garde pour détecter les éventuelles pannes durant la transmission de données et la diffusion d'un message ExploreRequest pour le recouvrement en cas de panne.

3.2.5 Protocole EAR

Le protocole EAR [30] propose une solution hybride pour la tolérance aux pannes. Pour son principe préventif, EAR définit un mécanisme de recouvrement de pannes afin d'élire un second chemin fiable pour transmettre les données depuis le capteur vers la station de base et d'assurer une bonne tolérance aux pannes. Ce protocole définit deux métriques pour la sélection des meilleures routes à mémoriser. La première métrique est le nombre de sauts dans une route. Ceci permet de choisir le chemin le plus court. En effet, si un chemin échoue à transmettre N paquets consécutifs, il sera mis dans une " liste noire " l'écartant ainsi d'une future utilisation. La deuxième métrique, appelée score de route utilise en cas des pannes au niveau d'un ou de plusieurs de ses noeuds.
Nous présentons ci_dessus quelque protocoles de routage hiérarchique tolérants aux pannes.

3.3 Protocoles hiérarchiques

Cette classe de protocoles de routage s'intéresse a ceux conçus et implémentés dans un réseaux partitionné en groupes des noeuds appelés clusters. Nous détaillons quelques un dans ce qui suit :

3.3.1 Protocole CPEQ (Cluster-based PEQ)

Avant d'entamer la variante CPEQ, nous détaillons son protocole oroginal PEQ [10].

Protocole PEQ

La motivation de cet algorithme vient du besoin de fournir un support pour toutes les contraintes : faible latence, fiabilité, recouvrement rapide en cas de panne et conservation d'énergie. PEQ combine la conservation d'énergie avec le routage multi-chemins en sélectionnant parmi toutes les routes disponibles, celles qui consomment moins d'énergie. En plus de ce mécanisme préventif qui permet un routage fiable, un mécanisme de recouvrement de pannes est implémenté. Ce dernier remplace le chemin en panne par une autre route qui soit de liens fiables et consomme moins d'énergie. Ainsi, le protocole PEQ couvre la procédure de tolérance aux pannes par la gestion de la consommation d'énergie, la sélection des meilleures routes puis leur recouvrement en cas de panne.

Dans le paradigme Publish/subscribe introduit par PEQ pour l'interaction entre la station de base et les capteurs. En effet, les capteurs envoient des notifications d'événements à la station de base, qui va souscrire son intérêt pour certaines de ces informations. Les capteurs concernés publient par la suite l'information désirée.

Les quatre principales phases du protocole sont :

- **Construction de l'arbre de routage**

cet arbre permet de définir les différents chemins multi-sauts possibles pour acheminer les données. La station de base commence le processus en initialisant la variable « saut » à 0, par la suite, chaque capteur prend la valeur du saut actuelle, l'incrémente puis l'envoie à tous ses voisins. Ainsi la valeur au niveau de chaque capteur désigne le nombre nécessaire de sauts pour communiquer avec la station de base. A la fin de cette phase seulement les meilleurs chemins sont enregistrés.

- **Propagation des paquets de souscription**

dans cette étape, après une souscription, par la station de base, des données à transmettre, chaque noeud achemine cette dernière jusqu'au capteur concerné.

- **Transmission de paquets de notification**

chaque capteur envoie selon sa table de routage et l'événement capté, une notification de l'information qu'il a. Pour cela, il utilise le chemin le plus rapide et le moins coûteux en terme d'énergie, le chemin qui est crée vers le puits pour l'envoi du message de notification peut être vu dans la figure 3.3 :

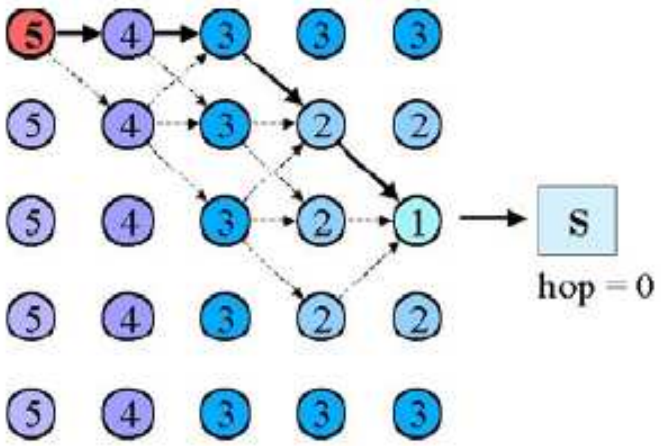

FIGURE 3.1 – Envoi du message de notification [10]

Le chemin utilisé pour transmettre les données du noeud source vers le puits peut également être utilisé pour transmettre la souscription au noeud source, comme montré à la figure 3.4.

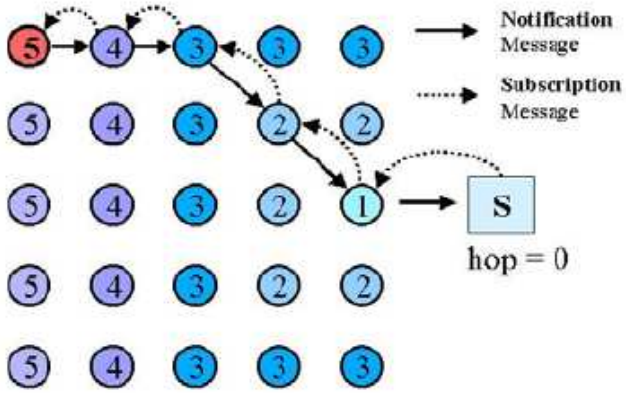

FIGURE 3.2 – Transférer la souscription au noeud source [10]

- **Mécanisme de réparation du chemin**

le recouvrement est effectué après détection de pannes. Un noeud envoie son paquet puis attend un acquittement ACK. S'il est reçu, le message a été bien transmis, sinon une panne est détectée au niveau du chemin de routage. On effectue donc une recherche "SEARCH" pour la sélection d'un autre noeud de destination tout en minimisant le coût du nouveau chemin. Si aucun noeud n'est trouvé (tous les voisins sont détruits) le noeud devient isolé et doit donc augmenter son rayon de transmission radio pour atteindre les voisins lointains. Un chemin perturbé est illustré à la figure 3.5, après la réparation, le chemin est reconstruit comme montre la figure 3.6.

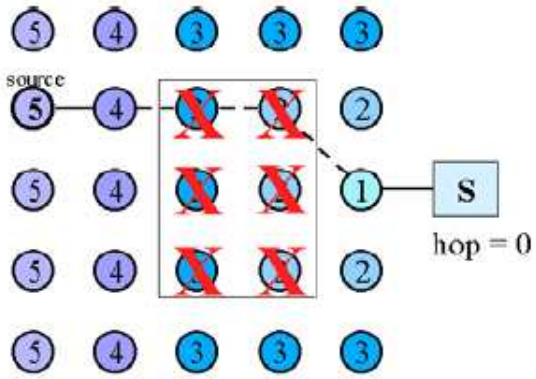

FIGURE 3.3 – Région avec noeuds détruits [10]

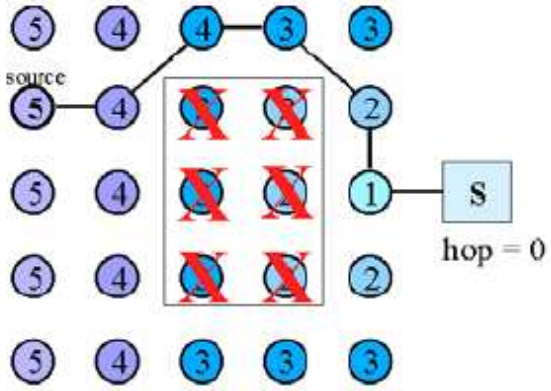

FIGURE 3.4 – Recouvrement de panne [10]

En plus de tous les mécanismes de tolérance aux pannes qu'implémente PEQ, la variante CPEQ [11] ajoute un module de clustering pour offrir une meilleure gestion d'acheminement des données et pour contourner les limites du PEQ à savoir :

- ▷ Le nombre élevé de message échangés.
- ▷ L'unicité du chemin de transmission (aller / retour) épuise rapidement l'énergie des capteurs concernés qui influx sur la durée de vie des nœuds et par conséquent du réseau en entier.

En effet, dans CPEQ, les nœuds ayant plus d'énergie résiduelle sont sélectionnés comme cluster-head. Un cluster-head établit son cluster, et les noeuds envoient leurs données capte au cluster-head qui effectue d'éventuel traitement sur les données brutes puis les achemine vers la SB. Chaque nœud du réseau peut devenir cluster-head pendant une certaine période de temps selon son niveau de batterie. CPEQ se réalise en cinq étapes :

- **Configuration initiale**

Cette phase est basée sur l'algorithme PEQ, où la SB déclenche une inondation pour configurer tout le réseau, â la fin de cette étape, chaque noeud connaît le nombre de sauts nécessaire pour atteindre la SB. En outre, CPEQ introduit un champ additionnel contenant le pourcentage des capteurs qui deviendront des cluster-heads.

- **Sélection du cluster-head**

C'est la phase d'élection des cluster-heads. Après la configuration initiale, chaque noeud génère un nombre aléatoire entre 0 et 1. Si ce nombre est inférieur à une probabilité p (probabilité pour devenir cluster-head), le noeud demande à tous ses voisins immédiats leur niveau de batterie en envoyant un paquet REQ-EN (Request Energy). Chaque voisin répond par un message REP-EN (Reply Energy) contenant son ID et la quantité d'énergie. Le noeud choisit le voisin ayant le maximum d'énergie et diffuse un SET-AGR (Set Aggregator) pour informer tous les noeuds du nouvel cluster-head, un noeud reste dans l'état cluster-head pour un certain temps, et quand ce temps expire, la phase de sélection de cluster-head est exécutée encore une autre fois, les trois étapes de cette phase sont illustrées dans la figure 3.11 :

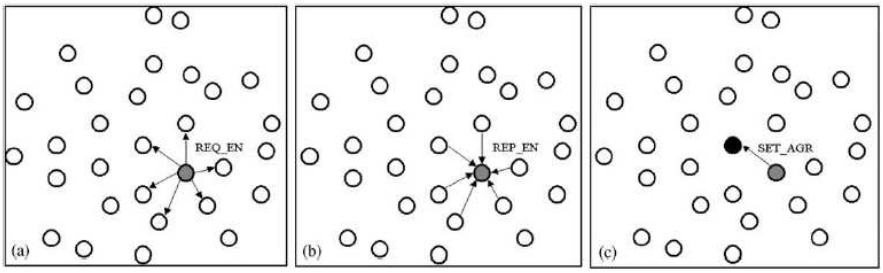

FIGURE 3.5 – Sélection du cluster-head [11]

- **Configuration en cluster**

Cette phase décompose le réseau en un ensemble de clusters. Le nouveau noeud cluster-head sélectionné doit avertir ses voisins de son rôle du cluster-head. De cette manière chaque cluster-head construit son cluster des noeuds. La configuration en clusters est réalisée par l'envoi de messages AGR-NTF (Aggregator Notification) avec un champ TTL pour limiter la propagation du paquet sur les noeuds se trouvant à une distance inférieure ou égale au TTL. Chaque fois qu'un noeud reçoit ce message, il enregistre l'ID du noeud émetteur dans sa table de routage pour déterminer le chemin vers le cluster-head. Si un noeud reçoit plusieurs messages AGR-NTF, il choisit le cluster-head avec le moindre nombre de sauts. La figure 3.1 illustre la configuration en clusters avec un TTL=2.

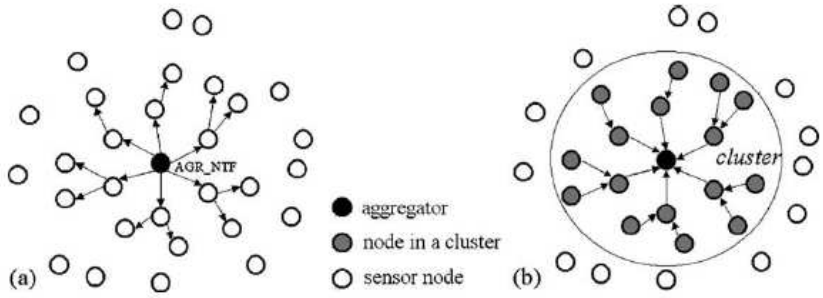

FIGURE 3.6 – Cofiguration d'un cluster [11]

- **Transmission des données au cluster-head**

L'algorithme de routage est le même implémenté dans le protocole PEQ. Chaque noeud utilise sa table de routage pour envoyer la donnée vers son cluster-head. Dans CPEQ le cluster-head peut être considéré comme un noeud puits. Le mécanisme de recouvrement de chemin est aussi hérité du protocole PEQ.

- **Transmission de données à la station de base(SB)**

Après réception des données depuis les capteurs de son cluster, cluster-head doit acheminer ces données à la SB, le cluster-head peut utiliser une fonction d'agrégation ou de fusion de données pour réduire la quantité de paquets qui seront transmis à SB.

CPEQ utilise une communication multi sauts entre le cluster-head et la SB, comme dans la figure 3.12.

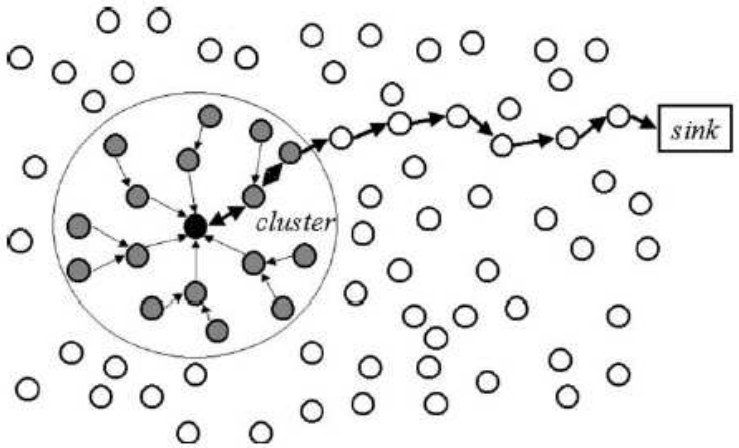

FIGURE 3.7 – Transmission des données vers la station de base [11].

- **Avantages de CPEQ**

▷ Distribuer d'une manière uniforme la dissipation d'énergie entre les noeuds, car chaque noeud sur le réseau peut devenir cluster-head pour une certaine période de temps.

▷ Réduire la latence et le trafic de données dans le réseau par utilisation des clusters.

▷ Réduire la quantité d'informations transmise à la station de base.

- **Limites de CPEQ**

▷ Il est possible que certains noeuds n'appartiennent à aucun cluster.

▷ L'idée d'utilisation des clusters dynamique apporte une charge supplémentaire aux cluster-heads, ainsi que le changement de cluster-head à chaque fois aboutira aux échanges des messages de contrôle, qui augmente la consommation d'énergie.

3.3.2 KAT Mobility

Dans KAT mobiliy (K-means And TSP-based mobility) [22], en plus du clustering, le concept de mobilité est implémenté au niveau des noeuds collecteurs. Ces deux mécanismes, définissent une technique préventive hybride tolérante aux pannes qui offre une meilleure gestion d'énergie et augmente, donc, la durée de vie du réseau. Après la réorganisation du réseau en clusters, la méthode proposée pilote la SB mobile pour se déplacer à travers les centres des clusters en prenant le chemin optimal. La station de base mobile récupère les données depuis les capteurs des clusters visités. Le principe de KAT mobility se résume en deux procédures : clustering et optimisation du chemin de routage. La figure 3.13 illustre le principe de KAT Mobility :

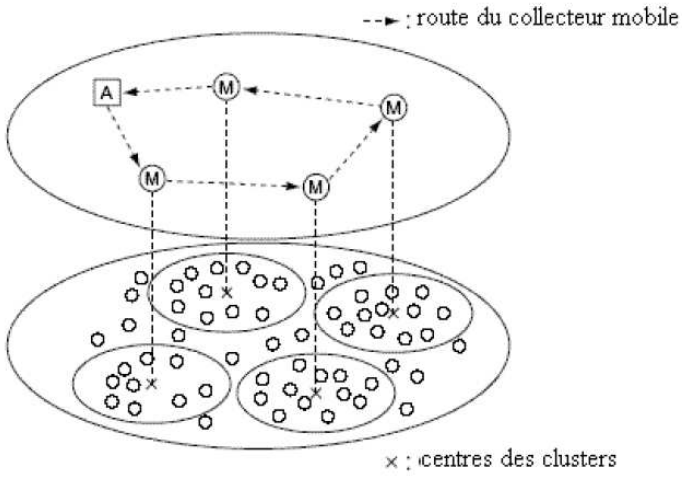

FIGURE 3.8 – Fonctionnement de KAT-Mobility [22]

- **Algorithme de clustering**

Cette procédure divise l'ensemble des N capteurs en k clusters $C_1, C_2, ..C_k$. le coût du cluster est évalué par l'erreur approximative entre le collecteur et les noeud, soit d(x, yi) cette erreur, où x est un noeud capteur, yi est un collecteur (i= 1, 2, ..., k). d(x, yi) est définie par la distance euclidienne entre le capteur et le collecteur. Le

but est, donc, d'affecter chaque capteur à un cluster Ci en minimisant l'erreur totale des clusters.

- **Optimisation d'itinéraire**

Trouver un chemin optimal pour le nœuds mobile est identique au problème du voyageur de commerce TSP . Ainsi, un collecteur représente le voyageur, et les centres des clusters définissent les villes. L'optimisation de la route du collecteur mobile pour visiter tous les noeuds centres des clusters une et une seule fois est équivalente à la recherche du plus court voyage d'un commerçant pour visiter chaque ville une seule fois.

- **Avantages de KAT mobility**

▷ KAT mobility peut fournir une meilleure conservation d'énergie aussi bien qu'une bonne tolérance aux pannes en cas de mal fonctionnement de certains noeud.

▷ KAT mobility représente un nouveau schéma de collecte de données pour les réseaux sans fil.

▷ Les puits mobiles pourraient être considérés des capteurs indépendants des capteurs réguliers, et donc ils peuvent être rechargés et reprogrammés à acquiesce à la mise à jour de la trajectoire.

▷ KAT mobility peut calculer l'itinéraire optimal vers la station de base pour contourner la zone endommagée ou mal fonctionnée.

- **Limites de KATmobility**

▷ Les puits mobiles se déplacent à des vitesses aléatoires et distances loin pour arriver à chaque centre des clusters.

▷ Epuisement rapide de énergie du puits à cause de la mobilité.

3.3.3 Protocole FTMRS

Dans le protocole FTMRS [32], les cluster-head et la station de base sont connectés l'un à l'autre à l'aide des chemins multiples (trois), dont le plus court est principalement utilisé pour acheminer les données vers la SB avec une faible

consommation d'énergie. Les deux autres chemins considérés comme des chemins de secours sont utilisés pour doubler le cheminement principale et tolèrer les pannes.

- **Routage tolérant aux pannes**

Dans FTMRS, chaque nœud de cluster transmet les données au cluster-head. Ce dernier transmet des ACK aux noeuds qui ont envoyé les données. Après il accumule toutes ces données et les transmet vers la station de base. Quand un noeud reçoit des données de ses voisins, il vérifie d'abord ces données reçues et ses propre données captées. Si elles sont les mêmes alors le noeud ne transmet pas les données reçues à d'autres noeuds. Sinon, si les données reçues sont différentes de ses données captées le noeud transmet les données reçues à d'autres noeuds en utilisant le plus court chemin.

- **Détection de faute matérielle d'un nœud**

Dans FTMRS, un nœud collecte les données de ses proches voisins, si elle sont différent a ses propre données captées, il transmet ces données au cluster-head, via le plus court chemin. Si un nœud ne reçoit aucune donnée de ses voisins durant une période de temps, il envoie un message de santé à ses voisins et attend les messages de réponses. Si tous les nœuds voisins répondent à ce message de santé, alors le nœud considère qu'une faute transitoire " un type de défaillance " a été rencontrée dans la dernière transmission. Si d'un autre coté, le nœud ne reçoit aucun message de réponse au message de santé, alors il considère que son chemin de réception est en panne. Sinon si un nœud voisin ne répond pas au message de santé alors le nœud considère que le problème est sur le chemin de transmission de ce nœud voisin, alors il informe tous les nœuds voisins de ce problème. La défaillance du circuit du nœud est détectée par ce nœud lui-même en comparant ses données captées avec celles reçues de ses voisins. Si les informations captées sont inférieures à une valeur de seuil alors le circuit du nœud est dans un état actif. Sinon, le circuit est défaillant.

- **Recouvrement des fautes dans FTMRS**

Selon les composants des nœuds, on peut les catégoriser comme : nœud normal, nœud de trafic, nœud de fin ou nœud mort. Cette catégorisation diminue le nombre des nœuds morts dans le réseau et améliore la durée de vie du réseau. FTMRS réutilise le capteur défectueux selon le type de faute. Si le circuit de capteur est défectueux, donc le capteur est utilisé comme un nœud de trafic. D'autre part, si le circuit de

réception du capteur est défectueux, le capteur est utilisé comme un noeud de fin. Si un nœud détecte que son circuit de transmission, la batterie ou son circuit de microcontrôleur sont défectueux, donc on déclare le nœud comme un nœud mort.

- **Plan de gestion du trafic**

Dans FTMRS, chaque nœud maintient un intervalle de temps entre deux transmissions de paquets de données différentes par le même chemin. Lorsque un capteur reçoit de nouvelles données d'un autre nœud, il vérifie si le plus court chemin est non-défectueux et s'il n'est pas actuellement utilisé, donc les données reçues sont transmises par le plus court chemin. Cependant, si le plus court chemin est utilisé alors il transmet ses nouvelles données par les chemins de secours.

- **Avantages de FTMRS**

▷ FTMRS traite la congestion du trafic de données dans le réseau.
▷ FTMRS réutilise les nœuds en panne.
▷ Dans FTMRS, le pourcentage de la tolérance aux pannes est très élevé comparé à d'autres protocoles tolérants aux pannes.
▷ Le temps de transmission des données dans FTMRS est très rapide avec une très grande efficacité d'énergie.
▷ FTMRS utilise le routage multi-chemins qui tolère les pannes et réduié la consommation d'énergie .
▷ FTMRS contrôle le trafic des données quand les données sont transmises au cluster-head ou à la SB pour eviter les collisions.
▷ FTMRS utilise deux chemins de secours, ce qui augmente la possibilité de recouvrement des pannes.

- **Limites de FTMRS**

▷ Le temps de livraison des données augmente très lentement lorsque des défaillances des noeuds se prominent.
▷ Dans FTMRS, l'énergie globale diminue lorsque la taille du réseau augmente sans aucune défaillance du noeud.
▷ Si le nombre de défaillance des noeuds est élevé, alors la perte d'énergie du réseau est diminuée, car dans ce cas, la livraison des données à la station de base a diminué.

- ▷ La défaillance rapide des cluster-heads.
- ▷ Le maintien d'un chemin de secours exige qu'une partie de l'énergie soit réservée même si le chemin n'est jamais utilisé. De plus, un espace mémoire est autorisé pour maintenir ce chemin de secours qui peut mener à un manque de mémoire.

3.3.4 Comparaison des protocoles présentés

La tolérance aux pannes connait une importance considérable dans les différent domaine de recherche dans les réseaux de capteurs sans fil, de ce fait plusieurs protocoles de routage tolérant aux pannes ont été proposé dans la littérature pour garantir un bon fonctionnement de réseaux et assuré un acheminement efficace de données. Le tableau ci-dessous compare les différents protocoles étudié, dans ce travail en se basant sur etablissement des routes, type de protection, mécanisme de détection des pannes, type dapplication, critère qui augemente la consommation dénergie structure de réseau, type de routage.

Protocole	Etablissement des routes	Type de protection	Mécanisme de détection des pannes	Type dapplication	Critère qui augemente la consommation dénergie	Structure de réseau	Type de routage
RERP	Proactif	Préventif	Par ACK	Even-driven	La diffusion des rapport d'erreur	chaine	Plat
ENFAT AODV	Proactif	Préventif	Par ACK	Even-driven	Inondation des messages de conroles	Grille	Plat
DD	Réactif	Curatif	Exploration périodique	A la demande	Inondation des messages de conroles	Chaine	Plat
FaT2D	Proactif	Curatif	Exploration périodique	A la demande	Inondation des messages de conroles	Chaine	Plat
PEQ	Proactif	Préventif	Par ACK	Hybride	ACK et recouvernement de chemin	Chaine	Plat
EAR	Proactif	Préventif		A la demande		chaine	plat
CEPQ	Hybride	Préventif	Par ACK	Hybride	Par ACK et recouvernement de chemin	cluster	Hiérarchique
KAT MOBILITY	Hybride	Préventif	Par ACK	Hybrid	Par ACK et recouverment de chemin	Cluster	Hiérarchique
FTMRS	Proactif	Préventif	Par envoie des messages de santé	A la demande	Inondation avec des messages de conroles	Cluster	Hiérarchique

TABLE 3.1 – Comparaison entre les protocoles

3.4 Conclusion

Dans ce chapitre nous avons présenté quelques protocoles de routage tolérants aux pannes et nous nous sommes concentrés sur les protocoles hiérarchiques, en présentant leurs avantages et inconvénients, ce qui a donné naissance à un nouveau protocole de routage hiérarchique tolérant aux pannes présenté dans le chapitre suivant.

Chapitre 4

Proposition d'un protocole de routage hiérarchique tolérant aux pannes

4.1 Introduction

Le plus grand défi des chercheurs est de concevoir un protocole de routage efficace qui tolère les pannes, à cause des défaillances qui se manifestent à plusieurs niveaux (nœud, réseau, etc). Dans le chapitre précédent, nous avons présenté quelques protocoles de routage tolérants aux pannes et à partir desquels nous avons tiré quelque idées qui permettent d'améliorer le routage et en même temps la tolérance aux pannes.

Dans ce chapitre, nous proposons un nouveau protocole de routage hiérarchique à basse consommation énergétique, tolérant aux pannes pour les réseaux de capteurs sans fil. Notre intérêt s'est porté sur le routage tolérant aux pannes à travers une description détaillée des différentes phases qui le constitue. L'approche propose basé sur les protocoles de routage tolérants aux pannes qui nous avons étudié, dans le chapitre précédent.

4.2 Protocole de routage hiérarchique tolérant aux pannes

Dans cette section, nous proposons un nouveau protocole de routage dans un RCSF décomposé en clusters et tolérant aux pannes.

4.2.1 Principe de fonctionnement

Le travail proposé dans ce chapitre est un nouveau protocole de routage hiérarchique tolérant aux pannes. Il est a la fois préventif et curatif. Le principe de ce protocole est qu'il s'exécute sur un réseau décomposé en k cluster. Chaque cluster comporte deux clusters heads travaillant alternativement durant des slot de temps définis au préalable par un nœud de cluster. Cette technique augmente la tolérance aux pannes du cluster heads et protège son énergie. Au lancement du protocole de clustérisassions : deux routes sont établies. La première est optimale et utilisé par défaut (primaire). et l'autre est sous optimale et utilisées seulement en cas d'échec de la route primaire. Cette technique curative augment a son tour, le niveau de tolérance aux pannes du protocole et aussi assure un cheminement de données efficace. Le protocole aussi implémente un mécanisme préventif pour tolérer les pannes survenues à n'importe quel moment durant son exécution et recouvre n'importe quelle pannes immédiatement.

4.2.2 Phase d'exécution

Ce protocole se décompose en trois phase d'exécution :

4.2.2.1 Structuration du réseau en clusters

Dans les premiers protocoles de routage hiérarchique, chaque groupe contient un seul cluster-head (CH) et plusieurs membres de groupe (MG). Dans ce type de protocoles, les cluster-heads épuisent leurs batteries beaucoup plus rapidement qu'un membre de groupe (MG) puisqu'un cluster-head (CH) reçoit toutes les données

des membres de son groupe et exécute des tâches d'agrégation et de traitement supplémentaire et aussi de transmission.

La défaillance d'un groupe peut survenir quand le CH épuise sa batterie et ainsi les informations captées par les MG ne seront pas livrées à la station de base. Pour remédier à ce problème, dans la plupart des protocoles de routage hiérarchiques comme LEACH[36], un nouveau cluster-head est re-sélectionné suite à des rotations exécutées après une certaine période de temps. Par conséquent, tous les capteurs jouent le rôle d'un cluster-head, à tour de rôle, afin de retarder la défaillance du groupe. Cependant, le processus de re-sélections d'un cluster-head augmente à son tour la consommation d'énergie puisque chaque rotation engendre des échanges des messages de contrôle. Pour réduire cette consommation d'énergie supplémentaire, nous proposons dans notre protocole de faire deux cluster-head dans chaque cluster repris de [37].
Notre contribution repose sur les hypothèses suivantes :

- Le réseau estcomposé de capteurs ayant un niveau d'énergie différent ;
- Communication par diffusion ;
- Chaque nœud peut ajuster sa portée de transmission ;
- Identificateurs (ID) uniques des nœuds capteurs ;
- Déploiement aléatoire des nœuds capteurs.

- **Phase d'initialisation**

Nous supposons d'abord que le réseau est décomposé en K groupes, K est définie selon la surface et le membre de nœuds. Nous choisissons, alors, aléatoirement K nœuds NCC des K groupes, les noeuds NCC se sont les noeuds qui vont éliré les deux CH (CH1 et CH2) aprés. La sélection du nœud NCC est faite par une affectation d'une constante P à chaque capteur, calculée par P=K /M. Où P dénote la probabilité qu'un capteur soit choisi comme un NCC, M est le nombre total de capteurs dans le réseau[31]. Ainsi, chaque capteur génère un nombre aléatoire entre 0 et 1, le nœud qui produit un nombre inférieur à la probabilité P deviendra un NCC. Ce noeud demandera immédiatement à tous ses voisins leur niveau d'énergie en envoyant un paquet NIV-EN (Niveau d'énergie). Chaque voisin répond par un

message REP-NIV-EN (Réponse Niveau d'énergie) qui contient son identificateur ID et la quantité d'énergie [11]. Le NCC choisit les deux voisins ayant le maximum d'énergie et diffuse un message 'CH-choisis' qui contient les identificateurs des deux nœuds choisis comme cluster-head (CH1 et CH2), voir la (figure 4.1). Chacun des deux nœuds CH1 et CH2 a une chance de devenir un CH actif, pendant un slot de temps S. Le noeud NCC va désigner le premier CH qui va être actif et la durée du slot et envoie ce programme à CH1 et CH2 avec son horloge pour qu'ils se synchronisent entre eux.

Dans le cas où le slot d'un CHx a expiré et ce dernier n'a pas terminé son traitement sur les données, ce CHx envoie ses données vers le CHy qui s'activera après lui. Ensuite, CHx éteindra sa radio et s'endormira, pour que le CH actif continuera le reste du traitement sur les données, aprés il les acheminera vers la SB.

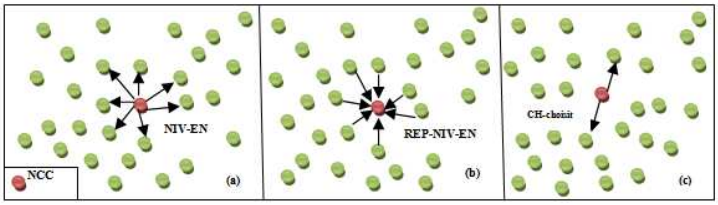

FIGURE 4.1 – Les étapes d'élection de CH1 et CH2

L'Organigramme suivant (figure 4.2) illustre l'élection de deux CHs :

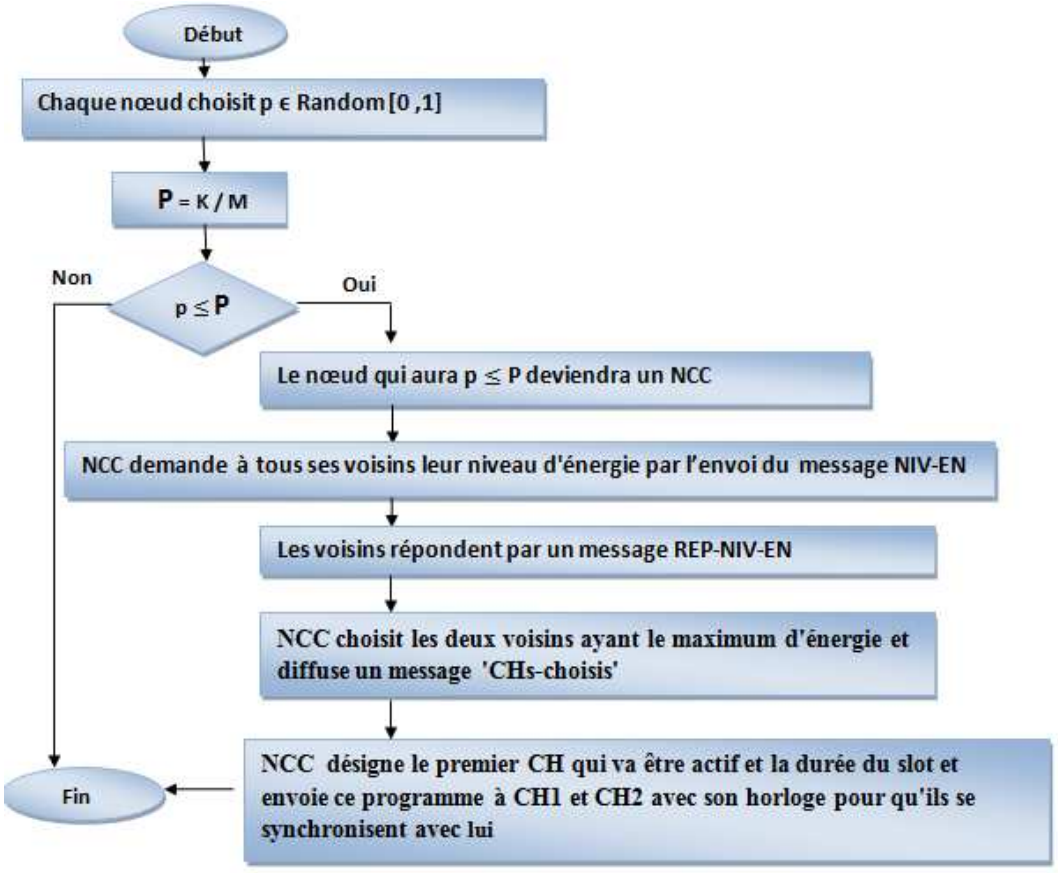

FIGURE 4.2 – Organigramme de l'élection de deux CH

- **Composition des clusters**

Cette étape permet de composier les clusters et de définir une route de chaque nœud capteur vers les deux clusters-heads en minimisant le nombre de messages de contrôle échangés, elle se déroule comme suit : Les deux clusters-heads (CH1 et CH2) choisissent aléatoirement un slot de temps pour envoyer un message (NT-Cluster), pour former le groupe. Le message NT-Cluster contient les champs suivants :

- L'ID du groupe, qui est le même que l'ID du nœud NCC.
- Les identificateurs des deux CHs.
- Un champ "nombre de sauts" initialisé à 0 par les clusters-heads.

- Un champ "niveau d'énergie" qui contient le niveau d'énergie résiduelle du nœud initialisé à 0 par les clusters-heads.
- Le programme d'activation des deux CHs.
- L'horloge pour synchroniser les nœuds membre du groupe.

Un nœud qui reçoit ces messages vérifie le champ "nombre de sauts".
Si le nombre de sauts est égal à 0 il détermine avec quel CH va se joindre, en comparant les forces du signal des messages de groupe (NT-Cluster) reçus des deux CHs, avec la valeur du champ "nombre de sauts" égale à 0. Les membres de groupe joindront le CH duquel ils ont reçu le message NT-Cluster avec la puissance de signal la plus forte, en envoyant des messages "join" qui contiennent les ID des nœuds.
Le message est envoyé selon un durant de temps aléatoirement choisi. Le nœud se synchronise avec le cluster-head choisi et enregistre l'identificateur du cluster qu'il a joint, les identificateurs de ses deux clusters-heads et le programme de leur activation qu'il a récupéré du message "NT-Cluster". En parallèle, le nœud incrémente le champ "nombre de sauts", enregistre son niveau d'énergie résiduelle dans le champs "niveau d'énergie" du message NT-Cluster. Après le nœud ajoute son identificateur au message et le rediffuse à ses voisins.

Dans le cas où le nombre de sauts est supérieur à 0 (ici, on suppose qu'il a reçu un message avec un nombre de sauts égal à 0 et il a envoyé le message "join" vers les clusters-heads choisis), le nœud compare les identificateurs des clusters-heads contenus dans le message avec ceux qu'il a enregistré.
S'ils sont égaux et l'identificateur du cluster-head qui a envoyé le message et différent du cluster-head qu'il a joint, le nœud choisit la route optimale vers le cluster-head qui pas dans son voisinage. Cette route est sélectionnée à travers le voisin qui a un niveau d'énergie maximum et qui est plus proche au cluster-head. Ceci est fait en comparant les champs "nombre de sauts" et "niveau d'énergie" de tous les messages NT-Cluster reçus après l'envoi du message "joint". Après la sélection de la route, le nœud enregistre cette route dans une table de routage "$\mathcal{TR}_{\mathrm{CH}}$" qui contient les champs suivants :

- " ID " : est utilisé pour enregistrer les identifiants des voisins en direction du CH.
- " Distance " : est utilisé pour enregistrer le nombre de sauts vers le CH qui n'a pas joint, est initialisé à 0.
- " Niv-eng " : contient le niveau d'énergie résiduelle de tous les nœuds sur la route sélectionne vers le CH est initialisé à 0.

La figure suivante(figure 4.3) montre la composition d'un cluster :

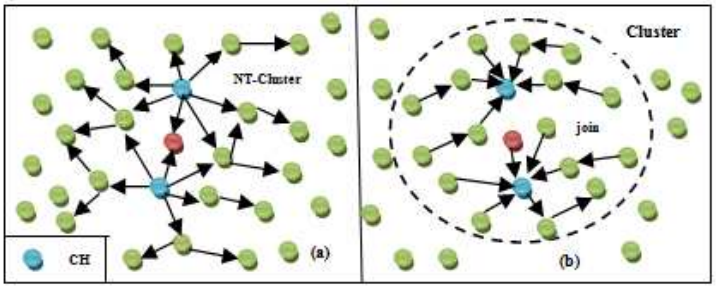

FIGURE 4.3 – Composition d'un cluster

4.2.2.2 Etablissement des routes

La particularité de notre protocole est qu'il utilise uniquement une connaissance du voisinage à un seul saut par rapport au CH , pour construire des clusters à deux sauts contrairement aux autres solutions qui considèrent un voisinage à k sauts.

Dans cette étape, chaque CH sauvegarde deux routes sous-optimal vers la station de base afin de les utiliser comme des route de secours dans le cas où la route primaire est défaillante. Nous présentons les mécanismes de construction des routes et du recouverement en cas de pannes. Ces routes sont utilisées durant les phases d'acheminement des données collectées dans le réseau. Pour établir les différentes routes, depuis tous les clusters-heads jusqu'à la SB, nous proposons l'approche que nous mettons en œuvre en deux phases :

1. Phase de découverte des routes durant laquelle les nœuds capteurs obtiennent

des informations sur leurs voisinages ainsi que leurs nœuds de relai (i.e. le premier voisin direct d'un nœud sur son chemin vers la SB).

2. Phase de maintenance de la route : qui permet aux nœuds de maintenir à jour les informations de routage acquises lors de la phase de découverte de routes.

- **Découverte des routes**

Dans le but de découvrir les routes qui mènent vers la SB, cette dernière initie la l'établissement de routes en envoyant un message de découverte des routes (DEC-R) vers les nœuds capteurs (voir la figure 4.4). Le message DEC-R va contient un champs "nombre de sauts" initialisé à 0 par la SB et un champs "niveau d'énergie" initialisé à 0 par la SB que chaque nœud met à jour avec son niveau d'énergie avant de le rediffuser.

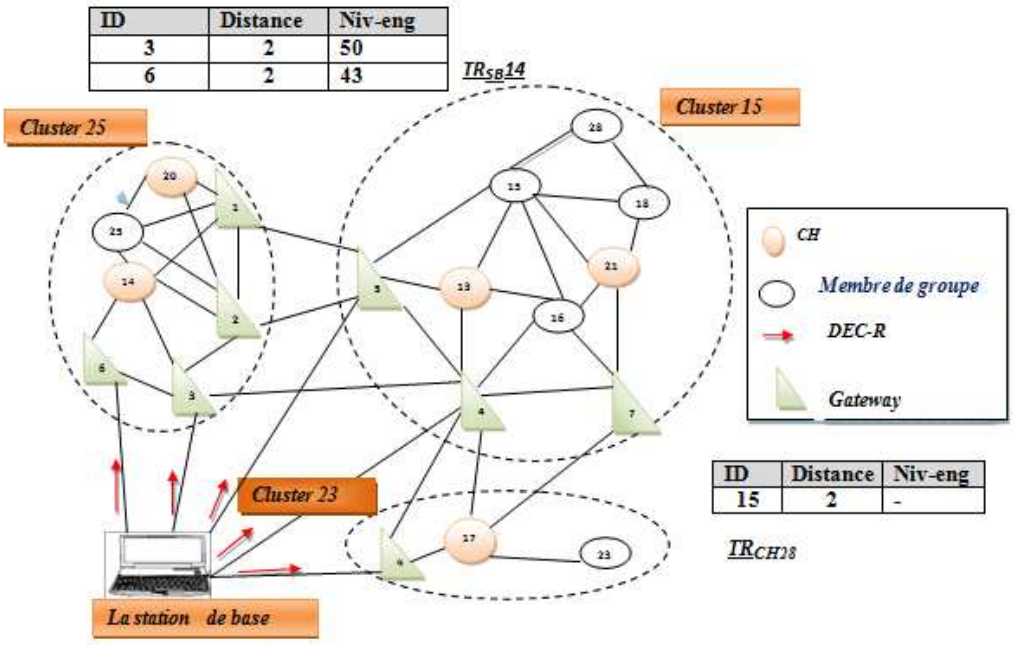

FIGURE 4.4 – Etablissement des routes

Ces messages seront transmis vers les clusters-heads et récolterons dans un vec-

teur toutes les identités des nœuds sur les routes sous-optimaux pour atteindre la SB. Pour ce faire, nous allons suivre le mécanisme du protocole EAR [30] qui fonctionne comme suit : Quand les nœuds voisins à un saut vers la SB reçoivent le message DEC-R de la SB, ils enregistrent dans leurs tables de routage la route vers la SB, incrémente le champs "nombre de sauts" du message DEC-R et mettent à jour le champ "niveau d'énergie" avec leurs niveau d'énergie avant de le rediffuser. Chaque nœud du réseau receveur plusieurs copies du message "DEC-R" de ses voisins, alors il va définir un délai d'attente dès la réception du premier message jusqu'à la réception de la plupart des messages de ses voisins. Ainsi, une fois que le délai a expiré, le nœud choisit comme route primaire la route optimale qui traverse le voisin qui a un niveau d'énergie maximum et le plus proche de la SB. Ceci est fait en comparant les champs "nombre de saut" et "niveau d'énergie" de tous les messages DEC-R reçus. Le nœud doit choisir une route sous-optimale comme route secondaire utilisée en cas de défaillance de la route primaire. Ainsi, il enregistre tous ces informations dans sa table de routage "$\mathcal{TR}_{\mathrm{SB}}$" qui contient les champs suivants :

- " ID " : est utilisé pour enregistrer les identifiants des voisins en direction de la SB sur les deux routes.
- " Distance " : est utilisé pour enregistrer le nombre de sauts vers la SB sur les deux routes initialisé à 0.
- " Niv-eng " : contient le niveau d'énergie résiduelle des nœuds relai sur les deux routes initialisé à 0.

A son tour le nœud incrémente le champ "nombre de sauts" du message et met à jour le champ "niveau d'énergie" avec son niveau d'énergie et rediffuse le message vers ses voisins. Ainsi de suite jusqu'à ce que tous les nœuds du réseau auraient enregistré deux routes vers la SB dans leur table de routage.

- **Maintenance de la route**

Cette fonction est déclenchée dans le cas de détection d'une panne sur une route quelconque. Elle permet de découvrir à nouveau d'autres routes vers la SB. Dans ce cas, le nœud qui a détecté la défaillance d'une route dirige un processus "Découverte de routes" à nouveau visant à trouver de nouveaux chemins alternatifs.

4.2.2.3 Phase de transmission de données

cette phase se décompose en deux phases :

- **Transmission de données vers le clusters-heads**

Chaque nœud collectant les données garde une copie avant de les transmettre au cluster-head par une communication multi-sauts. Cette copie sera supprimée après la réception d'un ACK du cluster-head. Après chaque transmission, le nœud définit un délai d'attente $\mathcal{T}_{\text{fd}}$ [6], pour attendre un ACK du cluster-head, (Comme montré dans la figure suivant(4.5)).

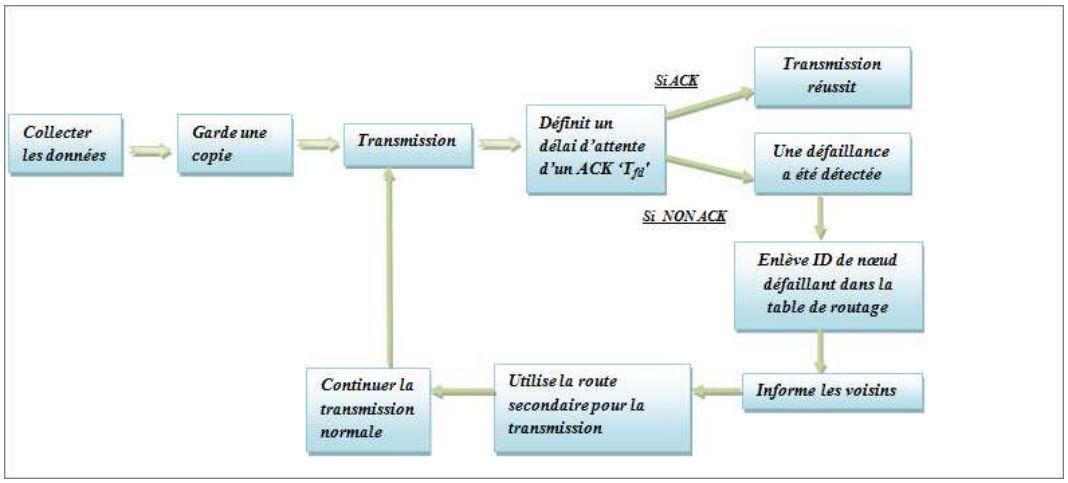

FIGURE 4.5 – Processeus de transmissuin de donnéesvers le CH

$\mathcal{T}_{\text{fd}}$ permet la détection rapide et instantanée des pannes suivies par un recouvrement immédiat. Ce délai est définis et calculé selon : la configuration du réseau, les pertes dues aux transmissions radios, la charge du trafic et la topologie du réseau. Il dépend de la nature de l'application et des caractéristiques du réseau. Selon le programme d'activation des cluster-head, chaque nœud choisit la route optimale menant au cluster-head actif. Dans ce cas, si le cluster-head actif est celui qui a envoyé le message " joint " avant, donc le nœud transmet ces données captées directement à ce CH. Sinon si le CH actif se n'est pas l'émetteur du message " joint " le nœud doit transmettre les informations captées à ce CH en suivant le chemin

optimale enregistré dans sa table de routage "$\mathcal{TR}_{\text{CH}}$".

Les pannes sont détectées lorsque le délai d'attente $\mathcal{T}_{\text{fd}}$ est expiré et aucun ACK n'est reçu. Par conséquent, un problème de communication va avoir lieu avec les voisins. Dans ce cas,et du fait que les distances entre les noeuds appartenant au même cluster sont très courtes, le nœud émetteur doit augmentes son rayon de transmission pour atteindre un autre nœud pour transmettre ses informations captées au cluster-head sans consomme beaucoup d'énergie.
Lorsque le délai d'attente $\mathcal{T}_{\text{fd}}$ est expiré et le nœud émetteur reçoit un ACK du cluster-head, il peut déduire que son paquet a été correctement transmis, dans ce cas le nœud supprime la copie de données gardée.

Pour réduire le nombre de messages envoyé et ainsi réduire la consommation de l'énergie, quand un nœud reçoit des données de ses voisins, il compare d'abord ces données reçues avec ses propres données captées. Si ces deux sont les même, alors le nœud ne transmet pas les données reçues au cluster-head. Sinon si les données reçues sont différentes de ses données, le nœud retransmet les données reçues au cluster-head. La figure (4.6) resume l'étape de transmission de données vers CH actif.

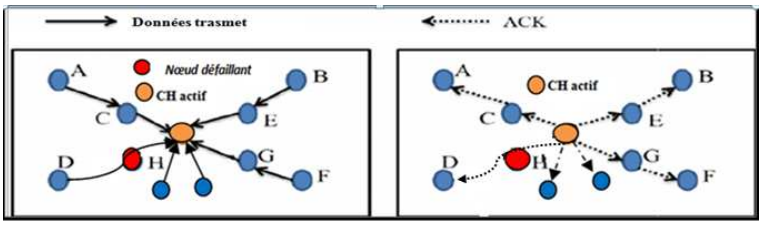

FIGURE 4.6 – Processeus de transmission de données vers le CH actif

- **Transmission de données vers la station de base**

Le cluster head peut utiliser une fonction d'agrégation ou de fusion et de compression de données pour réduire la quantité d'informations transmise. Après le traitement, le cluster-head garde une copie de données avant de les transmettre vers la SB, Cette copie sera supprimée après la réception d'un ACK de la SB, cette

transmission ce fait par une communication multi sauts en suivant la route primaire enregistrée dans sa table de routage. Après la transmission des données le cluster-head définit un délai d'attente $\mathcal{T}_{\text{fdSB}}$, pour attendre un ACK de la SB.
Si le délai d'attente $\mathcal{T}_{\text{fdSB}}$ est expiré et le cluster-head a reçu un ACK du la SB, il peut déduire que son paquet a été correctement transmis, dans ce cas le cluster-head supprime la copie de données gardée. Sinon, si le délai d'attente $\mathcal{T}_{\text{fdSB}}$ est expiré et aucun ACK n'est reçu, le cluster-head utilise la route secondaire pour transmettre les données à la SB, ce mécanisme de recouvrement de route est montré dans la figure (4.7).

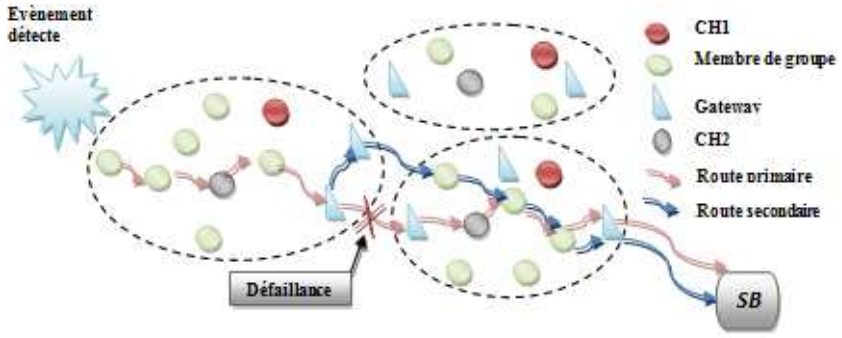

FIGURE 4.7 – Processeus de transmission de données vers la SB

L'organigramme suivant (figure4.8) montrel'étape de transmission de données :

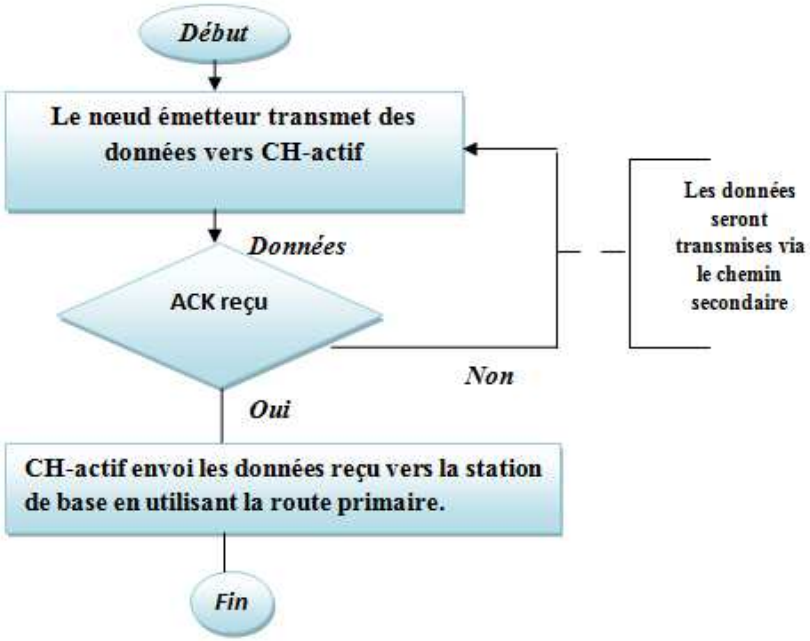

FIGURE 4.8 – Organigramme de transmission des données

4.2.2.4 Phase de Détection et recouvrement de pannes

Typiquement un nœud qui reste passif pendant longtemps doit envoyer un message 'Etat' pour confirmer son statut sain et assurer qu'il est fonctionnel. Si un nœud ne reçoit aucune donnée de ses voisins durant une période de temps, ce nœud envoie un message 'Etat' à ses voisins pour consulter l'état de ses voisins et attend les messages de réponses. De ce fait, on peut détecter les prédictions et les préventions suivantes :

- Si tous les nœuds voisins répondent à ce message, alors le nœud considère qu'une faute transitoire " un type de défaillance " a été rencontré lors de la dernière transmission, la solution consiste à retransmettre la copie du message gardée.
- Si d'un autre côté, le nœud ne reçoit aucun message de réponse à son message

'Etat', alors il considère que son chemin de réception est en panne ou il peut considérer que tous ses voisins sont en pannes ou lui-même est un nœud isolé, donc il doit augmenter son rayon de transmission et prolonge la gamme de communication afin d'atteindre d'autres voisins.

- Si un nœud voisin de ce nœud ne répond pas au message 'Etat' alors le nœud considère que le problème est sur le chemin de transmission de ce nœud ou le nœud lui-même est en panne. Alors, le noeud supprime l'ID de noeud défaillant dans sa table de routage et aprés il informe tous les nœuds voisins de ce problème pour supprimer l'ID de ce nœud dans leurs tables de routage.
- La défaillance du circuit est détectée par le nœud lui-même en comparant ses données captées avec celles reçues de ses voisins. S'ils sont égales ou presque égales alors le circuit du nœud est dans un état actif. Sinon, le circuit est défaillant, alors il informe tous les nœuds voisins de ce problème. Par conséquent ses voisins suppriment l'ID de ce nœud dans leurs tables de routage.
- Si l'énergie restante d'un nœud est inférieure à une valeur critique (seuil), le nœud en question envoie un message du batterie critique à ses voisins. Les nœuds qui ont reçu ce message enlèvent l'ID du nœud défaillant de leurs tables de routage.

L'organigramme suivant (figure 4.9) montre la détection et le recouvrement des pannes :

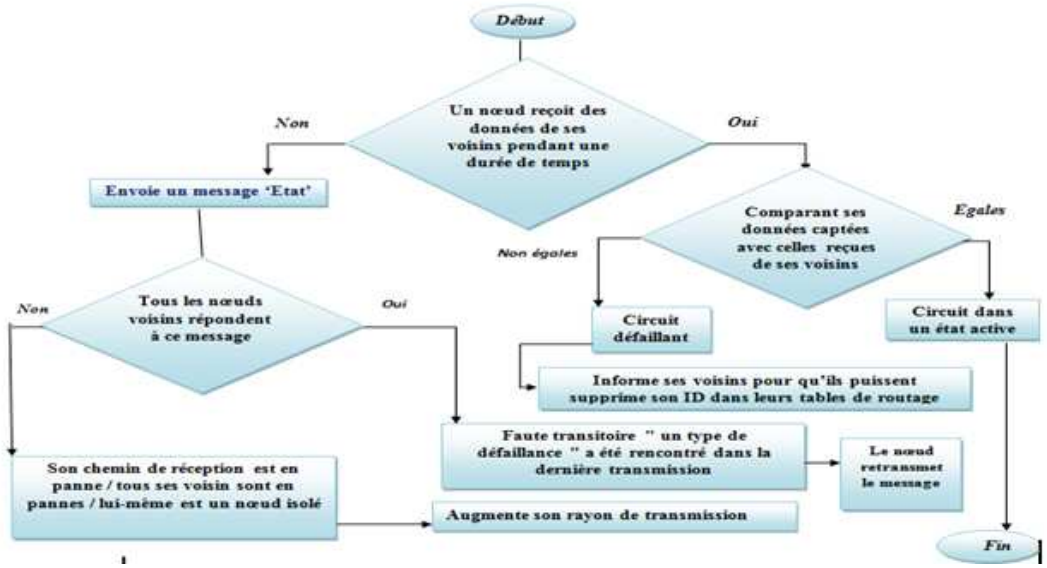

FIGURE 4.9 – Organigramme de détection de pannes et de recouvrement

4.2.3 Etude critique du protocole proposé

Dans ce qui suit, nous présenterons quelques avantages et inconvenients de notre protocole :

Avantages

- Recouvrement de route, ce qui permet la reprise de l'activité après pannes.
- Optimisation de la consommation d'énergie à travers l'utilisation de deux CH et le chemin optimal.
- Tous les traitements de données telles que la fusion et l'agrégation de données sont locaux au cluster d'où réduction de la quantité d'informations transmise à la SB.
- Le pourcentage de detection et de recouvrement aux pannes est trés efficace.
- l'utilisation du routage multi-chemins permet de tolèrer les pannes et réduire la consommation d'énergie .

– Les données sont transmises a la SB avec le minimum d'énergie et de temps.

Limites

– le nombre élevé de messages de contrôle surcharge le réseau qui peut engendré une congestion et aussi augmente la consommation d'énergie.
– Le maintien d'un chemin altérnatif exige qu'une partie de l'énergie sera lui consacré.
– La structure de données utilisée dans l'algorithme utilise plusieurs tables qui nécessitent beaucoup d'espace mémoire alorsque le capteurs a un espace mémoire limité.

4.3 Conclusion

Dans ce chapitre, nous avons proposé un nouveau protocole de routage hiérarchique tolérant aux pannes. Ce protocole et a la fois préventif et curatif. Par conséquent, le niveau de tolérance aux pannes est très élevé et aussi la manière d'acheminement de donnés est très efficace.

Conclusion et perspectives

L'essor des réseaux de capteurs sans fil (RCSF) au cours des dernières années est principalement dû aux fonctionnalités qu'ils offrent à divers domaine (militaire, médicale, etc.). Tout fois, les RCSFs doivent faire face à de nombreux défis qui affectent leur bon fonctionnement dû à leurs caractéristiques, tels que les limitations de batterie, le type de communication, les environnements hostiles où sont déployés les capteurs ou encore leur faible coût. Par ailleurs, ces réseaux sont caractérisés par les pannes des nœuds qui peuvent causer un dysfonctionnement du réseau en entier. Dans cette optique, il est commode de proposer des protocoles de routage tolérants aux pannes. Une panne au niveau d'un capteur peut se produire à cause d'une perte de connexions sans fil due à l'extinction du capteur suite à l'épuisement de sa batterie, ou tout simplement à une destruction physique accidentelle ou intentionnelle par un ennemi. Par conséquence, il faut faire face à ces pannes en proposant des protocoles tolérants aux pannes.

Dans ce mémoire, nous avons réalisé une étude pour atteindre un routage efficace avec tolérance aux pannes dans les réseaux de capteurs sans fil. Cet aspect est fondamental pour ce genre de réseau où le routage se réalise en collaboration avec les différents nœuds du réseau. De ce fait, un protocole de routage doit prendre en compte les contraintes matérielles d'un capteur : une batterie faible, une capacité de stockage modeste, une bande passante faible, etc. L'approche clustérisée qui permet de partitionner le réseau en zones, est une approche prometteuse. Pour atteindre cet objectif, nous avons proposé un nouveau protocole hiérarchique de routage qui tolère les pannes qui vise à résoudre certaines limites sur des protocoles que nous

avant étudier telle que l'épuisement d'énergie rapide d'un cluster head, la perte des données, etc.

Le principe de ce protocole est qu'il s'exécute sur un réseau décomposé en k cluster. Chaque cluster comporte deux clusters heads travaillant alternativement durant des slot de temps définis au préalable par un nœud de cluster. Cette technique augmente la tolérance aux pannes du cluster heads et protège son énergie. Au lancement du protocole de clustérisassions : trois routes sont établies. La première est optimale et utilisé par défaut (primaire). Les deux autre sont sous optimales et sont utilisées seulement en cas d'échec de la route primaire. Cette technique curative augment a son tour, le niveau de tolérance aux pannes du protocole et aussi assure un cheminement de données efficace. Le protocole aussi implémente un mécanisme préventif pour tolérer les pannes survenues à n'importe quel moment durant son exécution et recouvre n'importe quelle pannes immédiatement.

En guise de perspectives, nous souhaitons evaluer les performences de notre proposition et proposer des ameliorations pour minimiser le nombre de messages de contrôle échangés et aussi contrôler le problème de congestion survenu.

Bibliographie

[1] A. Affoua. *Réseaux de capteurs sans fil étendus dédiés aux collectes de données environnementales*. Thèse de doctorat, Université de Clermont II, 2016.

[2] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor networks :a survey. *Jurnal of Computer Networks*, pages 393–422, 2002.

[3] S. Athmani. Protocole de sécurité pour les réseaux de capteurs sans fil. Mémoire de Master, Université de Batna, 2010.

[4] A. Avizienis, J-C. Laprie, B. Randell, and C. Land-wehr. Basic concepts and taxonomy of dependable and secure computing. *Jurnal of IEEE Transactions on Dependable and Secure Computing*, pages 11–33, 2004.

[5] A. Benahmed. Détection préventive de pannes guidée par les données dans les réseaux de capteurs sans fil. Mémoire de Master, Université de Tlemcen, 2013.

[6] F.Z. Benhamida and Y. Challal. Fault tolerant directed diffusion for wireless sensor networks. *Jurnal of IEEE*, pages 1–6, 2010.

[7] T. Bernard. *Marches aléatoires et mot circulant adaptabilités et tolérance aux pannes dans les environnements distribués*. Thèse de doctorat, Université de Reims-Champagne-Ardenne, 2011.

[8] D. Boubiche. Protocole de routage pour les réseaux de capteurs sans fil. Mémoire de Master, Université de Batna, 2008.

[9] A. Boudjaadar. Plateforme basée agents pour l'aide à la conception et la simulation des réseaux de capteurs sans fil. Mémoire de Master, Université de Skikda, 2010.

[10] A. Boukerche, R.W.N. Pazzi, and R.B. Araujo. A fast and reliable protocol for wireless sensor networks in critical conditions monitoring applications. *Jurnal of parallel and Distributed*, pages 157–164, 2004.

[11] A. Boukerchea, R.W.N. Pazzia, and R.B. Araujob. Fault-tolerant wireless sensor network routing protocols for the supervision of context-aware physical environments. *Jurnal of parallel and Distributed*, pages 586—-599, 2006.

[12] T. Carpentier. *Placement De Capteurs Pour La Surveillance Des Processus Complexes*. Thèse de doctorat, Université LILLE, 1999.

[13] T. Carpentier. *Placement de capteurs pour la surveillance des processus complexes*. Thése de doctorat, Université de LILLE, 1999.

[14] Y. Challal. Les réseaux de capteurs (wireless sensor networks). Technical report, Université de technologie de compiègne, France, 2016.

[15] Y. Challal, H. Bettahar, and A. Bouabdallah. Les réseaux de capteurs (wireless sensor networks). Technical report, Université de technologie de compiègne, France, 2008.

[16] Z. Che-Aron, W. Al-Khateeb, and F. Anwar. The enhanced fault-tolerance mechanism of aodv routing protocol for wireless sensor network. *Journal of Computer Science and Network Security*, pages 41–50, 2010.

[17] S. Chelloug. *Optimisation d'énergie dans les algorithmes de routage pour réseaux mobile*. Thése de doctorat, Université de Constantine, 2013.

[18] S. Chouikhi, I. Korbi, and L.A. Saidane. A survey on fault tolerance in small and large scale wireless sensor networks. *Jurnal of Comput. Commun*, pages 22–37, 2015.

[19] C. Delbé. Tolérance aux pannes pour objets actifs asynchrones : protocole, modèle et expérimentations. Mémoire de Master, Université de Nice, France, 2007.

[20] M. Ruiz O. Marcillo-J. Johnson J. Lees G. Werner-Allen, K. Lorincz and M. Welsh. Deploying a wireless sensor network on an active volcano. *Jurnal of IEEE Internet Computing*, 2006.

[21] M. Hadjila. *Protocoles de routage economes en energie pour les réseaux de capateurs sans fil*. Thèse de doctorat, Université de Tlemcen, 2014.

[22] N. Hidehisa, A. Nirwan, J. Abbas, and K. Nei. Fault-resilient sensing in wireless sensor networks. *Jurnal of Comput. Commun*, pages 2375–2384, 2007.

[23] S. Jafar. Programmation des systèmes parallèles distribués : tolérance aux pannes, résilience et adaptabilité. Mémoire de Master, l'École Doctorale de Mathématiques, Sciences et Technologies de l'Information, Informatique, 2006.

[24] Y. Deswarte J-C Fabre J-C. Laprie D. Powell J.Arlat, Y. Crouzet. Tolérance aux fautes. *Jurnal of Vuibert*, pages 240–270, 2006.

[25] k. Benahmed. Approche théorie du graphe pour les surveillances d'un réseau de capteurs sans fil. Mémoire de Magistèr, Université D'oran, 2007.

[26] K. Kulothungan, J. Angel Arul Jothi, and A. Kannan. An adaptive fault tolerant routing protocol with error reporting scheme for wireless sensor networks. *Jurnal of Scientific Research*, 2011.

[27] M. Lehsaini. *Diffusion couverture basées sur le clustering dans les réseaux de capteurs*. Thèse de doctorat, Université de France, 2009.

[28] S. Maarouf and S. Ouadah. implémentation et évaluation des schémas de routage sur une plateforme réelle de réseaux de capteurs sans fil. Mémoire de Master, Université de Tlemcen, 2014.

[29] L.I. Niar. Analyse graphique por la serveillance dans un réseau de capteurs sans fil. Mémoire de Magistèr, Université d'Oran, 2012.

[30] N. Pais, K. Cetin, F. J Velez, N. Prasad, and R. Prasad. Cost-benefit aware routing protocol for wireless sensor networks with hybrid energy storage system. *Jurnal of Green Engineering*, pages 189–208, 2011.

[31] S. Peng and C. Ping Low. Energy neutral clustering for energy harvesting wireless sensors networks. *Jurnal of Ad Hoc Netw*, pages 1–16, 2015.

[32] C. Prasenjit, S. Tuhina, and B. Indrajit. Fault-tolerant multipath routing scheme for energy efficient wireless sensor networks. *Jurnal of CoRR*, pages 33–45, 2013.

[33] A.M. Mainwaring R. Szewczyk, J. Polastre and D.E. Culler. Lessons from a sensor network expedition. *Jurnal of EWSN*, 2004.

[34] R. Strog. Problems in fault tolérant distributed systems répartis. *Jurnal of IEEE*, pages 16–22, 1985.

[35] C. Titouna. La tolérance aux pannes dans les réseaux de capteurs sans fil. Mémoire de Magistèr, Université de M'SILA, 2012.

[36] B. Heinzelman Wendi, A.P. Chandrakasan, and H. Balakrishnan. An application-specific protocol architecture for wireless microsensor networks. *Jurnal of Trans. Wireless. Comm*, pages 660–670, 2002.

[37] D. Kim Y. Alemu, J. Koh. A hierarchical multi-parent cluster-based data aggregation framework for wsns. *Jurnal of IEEE*, pages 153–160, 2010.

[38] Y. Younes. Minimisation d'énergie dans un réseau de capteurs. Mémoire de Master, Université de TIZI-OUZO, 2012.

[39] A. Zemmar. Tolérance aux défaillances dans les réseaux de capteurs sans fil. Mémoire de Magistèr, Université de Bejaia, 2008.

RÉSUMÉ

Concourir un protocole de routage tolerant aux pannes dans un RCSf est un grand defi pour les chercheurs.
ce mémoire propose un nouveau protocole de routage hiérarchique tolerant aux pannes dans les RCSFS. Il est à la fois preventif et curatif. Ces deux caractéristiques augmentent parralèlement le niveau de tolerence aux pannes du protocole et assurent un routage efficace de données.

Mots clés : Tolerence aux pannes, RCSF, routage hiérarchique.

ABSTRACT

Fault tolerant routing protocol in an RCSf is a great challenge for researchers. This paper proposes a new hierarchical routing protocol tolerant to breakdowns in the RCSFS. It is both preventive and curative. These two features inherently increase the tolerance level of the protocol breakdowns and ensure efficient data routing.

Key words : Fault tolerance, RCSF, hierarchical routing.