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

**UNIVERSITE IBN KHALDOUN - TIARET**

# MEMOIRE

Présenté à :

FACULTÉ MATHEMATIQUES ET INFORMATIQUE
DÉPARTEMENT DôINFORMATIQUE

Pour lôobtention du diplôme de :

MASTER

**Spécialité :** ***Réseaux et Télécommunications***

**Par :**

***-Laaredj Khaled***

***-Messaoudi Ghalia***

Sur le thème

# Détection des pannes dans les réseaux de capteurs sans fil

Soutenu publiquement le 19 /11 / 2020 à Tiaret devant le jury composé de :

| | | | |
|---|---|---|---|
| *-Mr Mostefaoui Sid Ahmed* | MCB | Université de Tiaret | Président |
| *-Mr Aid Lahcene* | MCB | Université de Tiaret | Encadreur |
| *-Mr Mostefaoui Kadda* | MAA | Université de Tiaret | Examinateur |

2019-2020

# *Dédicaces*

*A ma mère, pour toute de sacrifices consentis, pour mon soutien et mon encourage, que Dieu la guérisse*

*A mon père, à titre posthume, ton souvenir restera à jamais gravé dans ma mémoire.*

*Paix à ton âme.*

*A tous les membres de ma famille :Ma femme, mes enfants TAKI ,Takoua et ANES ,mes frères et sœurs, mes tentes, mes oncles, mes cousins et mes cousines,*

*A toutes mes amies, et mes collègues.*

*A toute la promotion Master Informatique GI-GL-RT*

*A tous ceux que j'aime et qui me sont chères,*

*Je dédie ce travail*

# Remerciements

*Soyons reconnaissants aux personnes qui nous donnent du bonheur ; elles sont les charmants jardiniers par qui nos âmes sont fleuries*

دعونا نكون شاكرين لمن يسعدنا؛ هم البستانيون الساحرون الذين تزهر أرواحنا بواسطتهم.

Marcel Proust (1871-1922).

## Merci !

On voudrait adresser mes vifs remerciements à notre encadreur le Mr Aid Lahcene qui a accepté de me prendre par la main pour faire ce chemin de questionnement jusqu'à son aboutissement.

Pour les nombreux sacrifices qu'il a consentis à l'aboutissement du présent travail qu'il a suivi patiemment, avec doigté et surtout avec le professionnalisme qu'on lui connaît et également pour tous les partages scientifiques et du savoir pour la vie de tous les jours, on lui rends le témoignage de toute notre reconnaissance.

On adresse notre remerciements les plus sincères à toutes les personnes qui nous ont aidée et ont contribué à l'élaboration de ce mémoire.

On tiens également à remercier Mr. MESTEFAOUI SID AHMED Mr. MESTEFAOUI KADA et pour l'honneur qu'il ont fait de présider le jury de soutenance et on les exprime notre profonde gratitude.

Enfin, on n'oubliera pas aussi notre proches, collègue et amis qui m'ont vivement soutenue et encouragée au cours de la réalisation de ce mémoire.

*Merci à vous tous.*

## Abstrait

Dans ce message, nous avons cherché à détecter les défauts et couvrir les erreurs pour éviter tout accident qui pourrait être exposé au réseau, nous avons donc eu recours à des méthodes d'augmentation de la zone de couverture, qui auront un rôle dans la réduction du traitement des données reçues par les capteurs, ce qui conduit à une rationalisation de la consommation d'énergie par les capteurs et donc Entretenir et maintenir le réseau.

Nos travaux s'inscrivent dans le cadre de l'amélioration de la tolérance aux pannes dans le protocole EAR. Dans cette proposition, nous avons cherché à maximiser l'utilisation du réseau en proposant une solution pour gérer les nœuds de capteurs isolés. Pour pallier ce problème, nous avons utilisé l'augmentation de la puissance de transmission des nœuds capteurs sur la base d'une formule inspirée de la progression stochastique

## نبذة مختصرة

استهدفنا في هذه الرسالة كشف الأعطال وتغطية الأخطاء تجنب أي حادث الذي يمكن أن تتعرض له الشبكة, لذلك لجأنا إلى طرق زيادة مجال التغطية والذي سيكون له دور في التقليل من معالجة البيانات التي تتلقاها أجهزة الاستشعار مما يؤدي الى ترشيد استغلال الطاقة من طرف أجهزة الاستشعار و بالتالي المحافظة على الشبكة و ديمومتها .

يقع عملنا في نطاق تحسين التسامح مع الخطأ في بروتوكول EAR. في هذا الاقتراح ، سعينا إلى تعظيم استخدام الشبكة من خلال اقتراح حل لإدارة عقد الاستشعار المعزولة. للتغلب على هذه المشكلة ، استخدمنا الزيادة في قوة الإرسال لعُقد المستشعر بناءً على صيغة مستوحاة من التقدم العشوائي .

## Abstract

In this post we have sought to detect faults and cover errors to avoid any accident that could be exposed to the network, so we have resorted to methods of increasing the coverage area, which will have a role in reducing the processing of data received by the sensors, which leads to a rationalization of the energy consumption by the sensors and therefore Maintain and maintain the network. Our work is part of the improvement of fault tolerance in the EAR protocol. In this proposal, we sought to maximize the use of the network by proposing a solution to manage the isolated sensor nodes.

To overcome this problem, we used the increase in the transmission power of the sensor nodes on the basis of a formula inspired by the stochastic progression

# Table des matières

**LISTE DES FIGURES** ..... **VI**

**LISTE DES TABLEAUX** ..... **VI**

**INTRODUCTION GENERALE** ..... **1**

**I. CHAPITRE 1 CONCEPTS GENERAUX SUR LES RESEAUX DE CAPTEURS** ..... 1

I.1 *INTRODUCTION* ..... 1

I.2 *LES RESEAUX DE CAPTEURS SANS FIL* ..... 1

*I.2.1 Génération des réseaux de capteurs* ..... 1

*I.2.2 Le nœud capteur* ..... 2

*I.2.3 Type de capteurs* ..... 3

*I.2.4 Architecture des réseaux de capteurs* ..... 3

I.3 *APPLICATIONS* ..... 5

I.4 TECHNOLOGIES DE COMMUNICATION DANS LES RCSF ..... 6

I.5 *LES DIFFERENTS FACTEURS DE CONCEPTION* ..... 7

*I.5.1 Tolérance aux pannes* ..... 7

*I.5.2 Topologie du réseau* ..... 7

*I.5.3 Consommation d'énergie* ..... 7

I.6 *CARACTERISTIQUES DES RCSF* ..... 8

I.7 *CONCLUSION* ..... 9

**II. CHAPITRE 2 TOLERANCE AUX PANNES DANS LES RESEAUX DE CAPTEURS** ..... 12

II.1 *INTRODUCTION* ..... 12

II.2 *LES PANNES DANS LES RESEAUX DE CAPTEURS* ..... 12

*II.2.1 Notion de panne (faute, erreur)* ..... 12

*II.2.2 Classification des pannes* ..... 13

*II.2.3 Causes de pannes* ..... 13

II.3 *LA TOLERANCE AUX PANNES* ..... 14

*II.3.1 Définition* ..... 14

*II.3.2 Procédure générale de tolérance aux pannes* ..... 14

*II.3.3 Fonctionnement* ..... 16

II.4 *CLASSIFICATION DES SOLUTIONS DE TOLERANCE AUX PANNES* ..... 16

*II.4.1 Classification temporelle*.....17

*II.4.2 Classification architecturale*.....17

II.5 Protocole des solutions utilisée DANS LES RCSF.....18

*II.5.1 Principes des Techniques de routages*.....18

*II.5.2 Les protocoles de routages proactifs*.....19

*II* 5.2.1. *Le protocole DSDV des données*.....19

*II* 5.2.2. *Le protocole OLSR des données*.....20

*II* 5.2.3. *Le protocole LEERA des données*.....22

*II.5.* 3 *Les protocoles de routages réactifs*.....25

*II.5.* 3.*1 Le protocole DSR*.....25

*II.5.* 3.*2 Le protocole AODV*.....26

*II.5.* 3.*3 Le protocole « Energy aware routing »***EAR***.....28

*II.5.* 3.*4 Le protocole EDSR*.....31

*II.5.4 Les protocoles de routages hybrides*.....34

*II.5.4 .1 Le protocole LEACH*.....34

*II.5.4 .2 Le protocole ELMA*.....36

II.6 CONCLUSION.....40

**III. CHAPITRE 3 Stratégie d'améliorer le protocole de routage EAR**.....41

III.1 INTRODUCTION.....41

III.2 *Ajustement du rayon de transmission pour notre stratégie*.....41

III.3 La stratégie proposée.....42

*III.3 .1* Phase *de gestion de route*.....43

*III.3 .2 Ajustement du rayon de transmission*.....44

*III.3 .3 Exemple illustratif de l'exécution*.....45

III.4 CONCLUSION.....47

**CONCLUSION GENERALE**.....

**REFERENCES BIBLIOGRAPHIQUES**.....

# Liste des figures

Figure I-1: Composants d'un nî ud capteur ..... 2
Figure I-2: Evolution des capteurs ..... 3
Figure I-3: Exemple d'un réseau de capteurs ..... 4
Figure I-4: Topologie hybride d'un RCSF ..... 5
Figure I-5: Applications des réseaux de capteurs ..... 6
Figure II-1 : Classification des pannes ..... 13
Figure II-2: Procédure générale de tolérance aux pannes ..... 14
Figure II-3: Classification des mécanismes à économie dœnergie ..... 15
Figure II-4: Classification des solutions de tolérance aux pannes ..... 16
Figure II-5: Diffusion pure et diffusion en utilisant les MPRs dans OLSR ..... 21
Figure II-6: Schéma de la méthode « Sleep-WakeUp» ..... 23
Figure II-7: Datagramme des messages RTS/CTS ..... 23
Figure II-8: Datagramme avec le STEM pipeline ..... 24
Figure II-9: Protocole DSR : Construction de la route ..... 26
Figure II-10: Protocole DSR : Protocole DSR : Le renvoi du chemin ..... 26
Figure II-11: Fonctionnement du protocole EAR ..... 30
Figure II.12 : Schématisation des zones pour un protocole de routage hybride ..... 35
Figure III-1: Exemple de déplacement du nî ud B ..... 42
Figure III-2: Ajustement du rayon de transmission ..... 43
Figure III-3: Phase initiale ..... 45
Figure III-4: Problème du nî ud isolé ..... 45
Figure III-5: nouveau rayon de transmission ..... 46
Figure III-6: Recouvrement de route ..... 46

# Liste des Tableaux

Tableau I-1: Génération des réseaux de capteurs ..... 3

# Introduction générale

# Introduction générale

L'évolution rapide de la technologie dans le domaine de la communication sans fil et de la micro-électronique, a donné naissance à des équipements miniaturisés dotés dôune unité de calcul, de composants pour la collecte de lôinformation, et dôune antenne pour transmettre lôinformation à un centre de contrôle distant. Ces équipements sont appelés nî uds capteurs ou « motes ». Ils ont la capacité de sôauto-organiser pour former un réseau appelé réseau de capteurs. Ces équipements sont généralement déployés dans des environnements hostiles pour surveiller ou collecter de lôinformation dans un champ de captage. Ils présentent une autonomie dôénergie puisquôils sont dotés dôune source dôénergie limitée (batterie) qui est généralement non rechargeable et difficile à la remplacer. [1]

En outre, ces nî uds sont sujets à des pannes pour différentes causes (épuisement de lôénergie, écrasement par des animaux, etc.é ). Dans ce cas de figure, il y aurait un grand risque que le réseau perd lôaspect de connexité et que lôinformation ne peut pas être transmise au centre de contrôle ou cette information est erronée à cause de la faille des capteurs. Pour faire face à ce type de scénarios, les capteurs sont généralement déployés en grand nombre et ils ont la capacité de sôauto-organiser. Au début, un nombre minimal de capteurs est impliqué dans la formation des réseaux et les autres passent au mode veille pour préserver leurs batteries ce qui permet de prolonger la durée de vie du réseau. Quand un capteur cesse de fonctionner et le réseau perd sa connexité, un autre capteur se trouvant dans son voisinage passe au mode actif pour le remplacer de telle sorte que le réseau soit toujours connexe. Or, dans dôautres cas un capteur peut perdre sa fiabilité et lôinformation quôil remonte, est erronée. Dans certaines applications, cette information peut être importante par exemple quand il sôagit de la surveillance dôun patient. De ce fait, la non- fiabilité de lôinformation peut provoquer un autre traitement qui aura une conséquence négative sur la santé du patient.

Plusieurs protocoles traitant différent problèmes dans les RCSFs ont été proposés dans la littérature (de routage, de qualité de service, etc). Cependant, les chercheurs ne tiennent pas en considération lôaspect tolérance aux pannes dans des protocoles et se contentent des mécanismes préventifs par supporter la panne dôun élément, par exemple choisir un deuxième chemin dans un protocole de routage pour tolérer la rupture du chemin principal

Dans cette optique, on propose de mettre en place une démarche pour le problème des nî uds isolés dans le protocole de routage EAR (Enery Aware Routing) quôil a déjà un mécanisme préventif pour la tolérance dans un chemin de routage principal. Notre solution consiste à augmenter le rayon de transmission par un noeud

isolé dans le protocole EAR. De ce fait, EAR aura deux mécanismes de tolérance aux pannes préventif (un autre chemin de routage) et curatif (lôaugmentation du rayon de transmission).

Pour se faire, on a organisé notre travail autour de trois chapitres encadrés par une introduction et une conclusion :

**Le chapitre 1:** est une introduction aux réseaux de capteurs sans fil, une présentation de leur fonctionnement général, les applications potentielles et les principales caractéristiques.

**Le chapitre 2 :** La tolérance aux pannes dans les réseaux de capteurs sans fil ; dans lequel nous présenterons les différentes catégories de pannes qui peuvent survenir durant le cycle de vie dôun réseau de capteurs sans fil, ainsi quôun survol sur les protocoles tolérants aux pannes dans les RCSFs.

**Le chapitre 3 :** Constitue le cî ur de notre travail. Dans ce chapitre, on propose une solution pour améliorer un des protocoles tolérant aux pannes.

Enfin, on conclue ce mémoire par une conclusion générale et on présente quelques perspectives.

# Chapitre 1

# Concepts généraux sur les réseaux de capteurs

# Chapitre 1 Concepts généraux sur les réseaux de capteurs

## I.1 Introduction

Lôévolution technologique a été marquée par la miniaturisation des équipements. Ces dernières années, il y avait lôapparition des dispositifs à bas coûts intégrant les fonctionnalités de captage, de traitement et de communication. Ces dispositifs sont déployés dans la nature afin de créer un réseau de capteurs à des fins aussi bien de contrôle que de monitorisation. Ils permettent de détecter les changements environnementaux, biologiques, etc.é et les signalent aux autres nî uds selon une architecture flexible du réseau. Les nî uds capteurs donnent la possibilité dôêtre déployés dans des environnements hostiles où lôintervention humaine est quasiment impossible.

## I.2 Les réseaux de capteurs sans fil

Un réseau de capteurs sans fil (RCSF) est un réseau ad hoc avec un grand nombre de nî uds qui sont des micro-capteurs capables de récolter et de transmettre des données environnementales d'une manière autonome. La position de ces nî uds n'est pas obligatoirement prédéterminée. Ils peuvent être aléatoirement dispersés dans une zone géographique, appelée « champ de captage » correspondant au terrain d'intérêt pour le phénomène capté (ex : largage des capteurs par un avion sur un volcan pour étudier les phénomènes vulcanologiques et leurs évolutions, etc...) [2].

### I.2.1 Génération des réseaux de capteurs

Les réseaux de capteurs sans fil (RCSF) ont montré leur impact sur notre vie quotidienne. Dans [3], les auteurs ont classé le processus de création de capteurs en trois générations. Le tableau I-1 illustre cette catégorisation des capteurs en des générations.

| Génération | Période | Taille | Poids | Batterie |
|---|---|---|---|---|
| 1er | Les années 80 et 90 | Grande boîte à chaussures | Kilogrammes | Grosse |
| 2e | 2000-2003 | Boîte de cartes | Grammes | AA |
| 3e | 2010 | Particule de poussière | Négligeable | Solaire |

**Tableau I-1: Génération des réseaux de capteurs**

### I.2.2 Le nî ud capteur

Un nî ud capteur est composé de plusieurs modules dont chacun dôeux a une tâche particulière : acquisition, traitement, ou transmission de données. Il comprend également une source dôénergie [4] :

- **Lôunitédôacquisition** : lôunité dôacquisition est composée dôun ou plusieurs capteurs qui effectuent des mesures numériques sur les paramètres environnementaux et dôun

  Convertisseur Analogique/Numérique (CAN) qui convertit lôinformation relevée et a transmettre à lôunité de traitement.

- **Lôunité de traitement:** lôunité de traitement est composée de deux interfaces : une interface pour lôunité dôacquisition et une interface pour lôunité de transmission. Cette unité est également composée dôun processeur et dôun système dôexploitation spécifique. Elle acquiert les informations en provenance de lôunité dôacquisition et les envoie à lôunité de transmission.

- **Lôunité de transmission :** cette unité est responsable de toutes les émissions et réceptions de données via un support de communication radio.

- **Lasourcedôénergie:**Pour alimenter les unités citées ci-dessus, un capteur dispose dôune source dôénergie qui est généralement des piles de type AA.

La figure I.1 [5] illustre lôarchitecture dôun nî ud capteur.

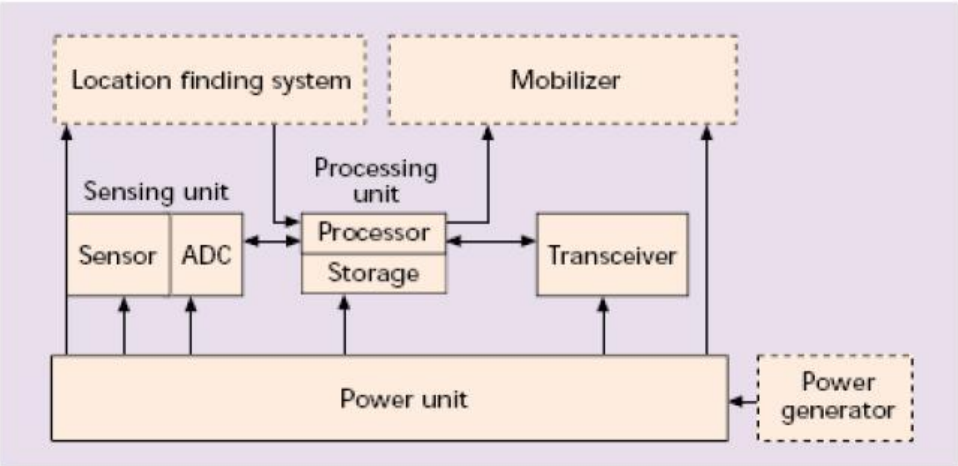


**Figure I-1:Composantsd'un nî ud capteur**

### I.2.3 Type de capteurs

Il existe plusieurs types de capteurs, avec des fonctionnalités diverses et variées. La plupart des capteurs dépendent de l'application pour lesquels ils ont été conçus (capteurs aquatiques, sous-terrain, etc. . .). La figure I.2 [5] illustre l'évolution des capteurs au cours de ces 20 dernières années. Cette représentation met en avant l'importance des travaux de recherche de l'université de Berkeley dans l'essor des réseaux de capteurs, surtout sachant que l'entreprise Xbow2 (aussi appelé Crossbow) qui fait jusqu'à aujourd'hui office de référence dans la fabrication de capteurs.

Les capteurs fabriqués par Xbow au cours des dix dernières années (famille de capteurs Mica et Telos) sont sans aucun doute les plus utilisés dans les expériences et travaux de recherche. Ces capteurs sont capables de mesurer plusieurs métriques et utilisent Chipcon CC2420 qui est devenu le standard au niveau des modules de transmission utilisant le protocole de communication IEEE 802.15..4 [2].

**Figure I-2: Evolution des capteurs**

### I.2.4 Architecture des réseaux de capteurs

Un réseau de capteurs est constitué de milliers de nœuds appelés nœuds capteurs ou tout simplement capteurs, permettant de capter et collecter des événements, d'analyser les traitements et de transmettre les informations recueillies dans différents environnements. Ces nœuds peuvent avoir des positions fixes ou bien être déployés aléatoirement pour surveiller l'environnement. Les communications dans un réseau de capteurs se font souvent d'une manière multisaut jusqu'à la station de base qui est un nœud possédant plus de ressources matérielles et permettant de collecter et stocker les

informations issues des capteurs. En dôautres termes le fonctionnement dôun réseau de capteurs se déroule de la manière suivante : les nî uds sont déployés dans une zo ne appelée zone dôintérêt pour la surveiller. Lorsquôun nî ud détecte un évènement, il le traite localement et lôachemine vers la station de base via une communication multi-saut. Ce processus est illustré dans **la figure 1.3**[5].

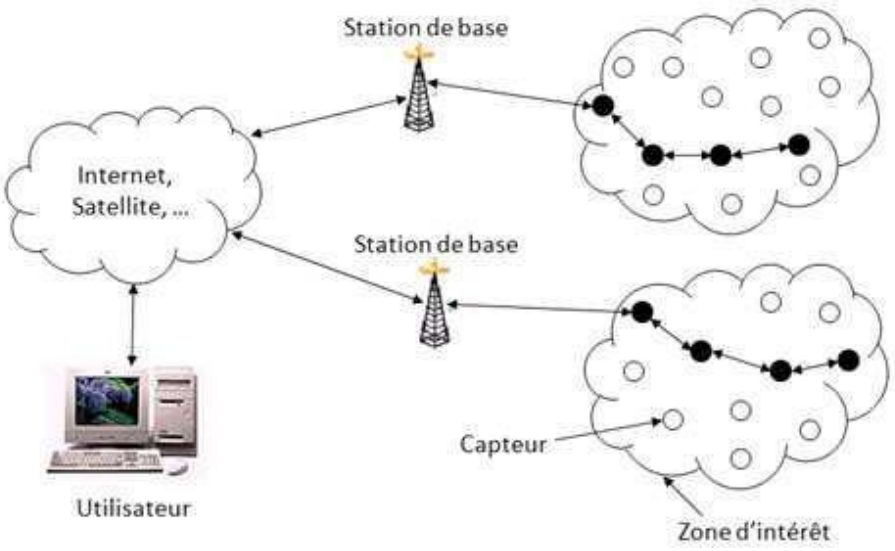


**Figure I-3: Exemple d'un réseau de capteurs**

Il existe plusieurs topologies pour les réseaux de capteurs : [3]

- **Topologie en étoile :** La topologie en étoile est un système uni-saut. Tous les nî uds envoient et reçoivent seulement des données avec la station de base. Cette topologie est simple et elle demande une faible consommation dôénergie.
  Elle est recommandée quand la distance entre les nî uds et la station est limitée.

- **Topologie en toile (Mesh Network) :** La topologie en toile est un système multi-saut dont lequel la communication entre les nî uds et la station de base est possible. Chaque nî ud a plusieurs chemins pour envoyer des données. Cette topologie a plus de possibilités de passer à lôéchelle du réseau, avec redondance et tolérance aux fautes, mais elle demande une consommation dôénergie plus importante.

- **Topologie hybride :** La topologie hybride est un mélange des deux topologies ci-dessus. Les stations de base forment une topologie en toile et les nî uds autour dôelles sont en topologie étoile. Elle assure la minimisation dôénergie dans les réseaux de capteurs. **La figure I.4** [5] illustre cette topologie.

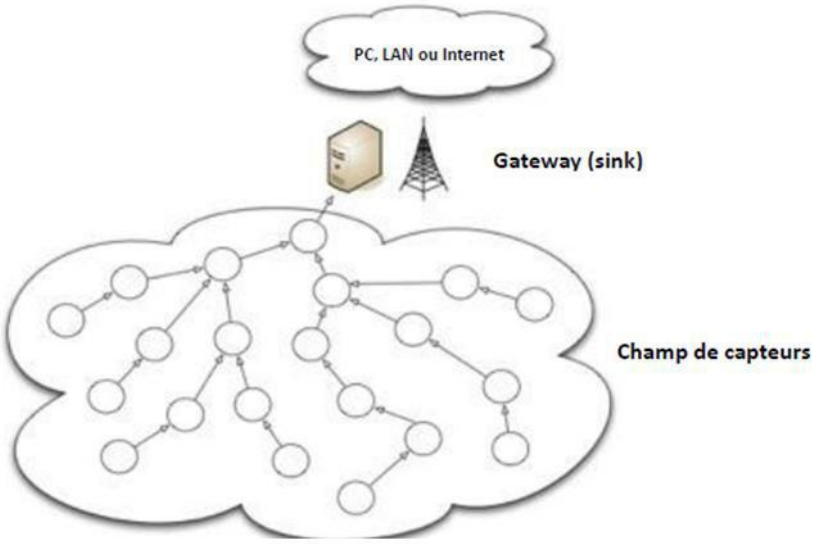


**Figure I-4: Topologie hybride d'un RCSF**

## I.3 Applications

La diminution de taille et de coût des micro-capteurs, l'élargissement de la gamme des types de capteurs disponibles (thermique, optique, vibrations...) et l'évolution des supports de communication sans fil, ont élargi le champ d'applications des réseaux de capteurs. Parmi elles, on cite [6] :

- **Applications militaires :** On peut penser à un réseau de capteurs déployé sur un endroit stratégique afin de surveiller toutes les activités des forces ennemies, ou d'analyser le terrain avant d'y envoyer des troupes (détection d'agents chimiques, biologiques ou de radiations).
- **Applications domestiques :** En plaçant, sur le plafond ou dans le mur, des capteurs, on peut économiser lôénergie en gérant lôéclairage ou le chauffage en fonction de la localisation des personnes.
- **Applications environnementales :** Les réseaux de capteurs sont beaucoup appliqués dans ce domaine pour détecter des incendies, surveiller des catastrophes naturelles, détecter des pollutions et suivre des écosystèmes.

- **Applications agricoles :** Dans les champs agricoles, les capteurs peuvent être semés avec les graines. Ainsi, les zones sèches seront facilement identifiées et l'irrigation sera donc plus efficace et économique.
- **Applications médicales :** Les réseaux de capteurs ont aussi des développements dans le domaine de diagnostic médical. Par exemple, des micro-caméras sont capables, sans avoir recours à la chirurgie, de transmettre des images de l'intérieur d'un corps humain avec une autonomie de 24 heures.
- **Applications de trans port :** Il est possible d'intégrer des nî uds capteurs au processus de stockage et de livraison. Le réseau ainsi formé, pourra être utilisé pour connaître la position, l'état et la direction d'un paquet ou d'une cargaison.

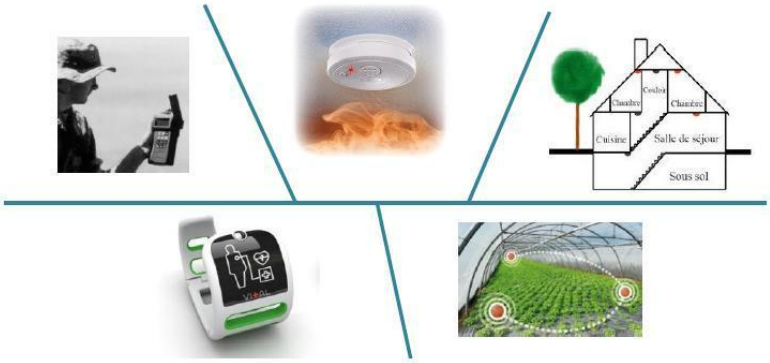


**Figure I-5 : Applications des réseaux de capteurs**

## I.4 Technologies de communication dans les RCSF

- **Bluetooth / IEEE 802.15.4 :** Bluetooth est une spécification de l'industrie des télécommunications. Elle utilise une technique radio courte distance destinée à simplifier les connexions entre les appareils électroniques. Malheureusement, un grand défaut de cette technologie est sa trop grande consommation dœnergie [5].

- **ZigBee / IEEE 802.15.4 :** ZigBee est une norme de transmission de données sans fil permettant la communication de machine à machine. Zigbee offre des débits de données moindres, mais sa très faible consommation électrique et ses coûts de production très bas ont fait dœlle une candidate idéale pour les équipements à ressources limitées.

- **Dash 7 / ISO/IEC 18000-7 :**Dash7 est une nouvelle technologie de communication utilisant la norme ISO/IEC 18000-7. Sa consommation électrique est très faible, la durée de vie de batterie peut arriver à plusieurs années et sa portée est 2km en

outdoor. Elle fournit une faible latence pour le suivi des objets en mouvement et un débit de transmission allant jusqu'à 200kbits/s.

## I.5 Les différents facteurs de conception

La conception des réseaux de capteurs est influencée par de nombreux facteurs comme la tolérance aux pannes, les coûts de déploiement, la consommation dôénergie, lôenvironnement ou la topologie du réseau. Ces facteurs représentent la base de la conception de protocoles ou dôalgorithmes pour les réseaux de capteurs.

### I.5.1 Tolérance aux pannes

Les nî uds peuvent être sujets à des pannes dues à leur fabrication (ce sont des produits de série bon marché, il peut donc y avoir des capteurs défectueux) ou plus fréquemment à un manque dôénergie. En outre, les interactions externes (chocs,

interférences,..) peuvent aussi être la cause de leur dysfonctionnement. De ce fait, afin que les pannes nôaffectent pas la tâche première du réseau, il faut mettre en place des mécanismes qui permettent dôaugmenter le taux de disponibilité dôun réseau de capteurs [5].

### I.5.2 Topologie du réseau

En raison de leur forte densité dans la zone à surveiller, il faut que les nî uds capteurs soient capables dôadapter leur fonctionnement afin de maintenir la topologie souhaitée [7].On distingue généralement trois phases dans la mise en place et lôévolution dôun réseau:

- **Déploiement :** Les nî uds sont soit répartis de manière prédéfinie soit de manière aléatoire (largués en masse depuis un avion). Il faut alors que ceux-ci sôorganisent de manière autonome.
- **Post-Déploiement - Exploitation :** Durant la phase dôexploitation, la topologie du réseau peut être soumise à des changements dus à des modifications de la position des nî uds ou bien à des pannes.
- **Redéploiement :** Lôajout de nouveaux capteurs dans un réseau existant implique aussi une remise à jour de la topologie.

### I.5.3 Consommationdôénergie

Lôéconomie dôénergie est une des problématiques majeures dans les réseaux de capteurs. En effet, la recharge des sources dôénergie est souvent trop coûteuse et parfois impossible. Il faut donc que les capteurs économisent au maximum lôénergie afin de pouvoir fonctionner et garantir une longue durée de vie.[8]

## I.6 Caractéristiques des RCSF

Les principales caractéristiques des réseaux de capteurs se résument dans ce qui suit :

- **Densité importante des nî uds:** Les réseaux de capteurs se composent généralement dôun nombre très important des nî uds pour garantir une couverture totale de la zone surveillée. Ceci engendre un niveau de surveillance élevé et assure une transmission plus fiable des données.
- **Topologie dynamique :** Lôinstabilité de la topologie des réseaux de capteurs est le résultat des trois facteurs essentiels :
  - **La mobilité des nî uds :** les nî uds capteurs peuvent être attachés à des objets mobiles qui se déplacent librement et arbitrairement, introduisant ainsi une topologie instable du réseau.

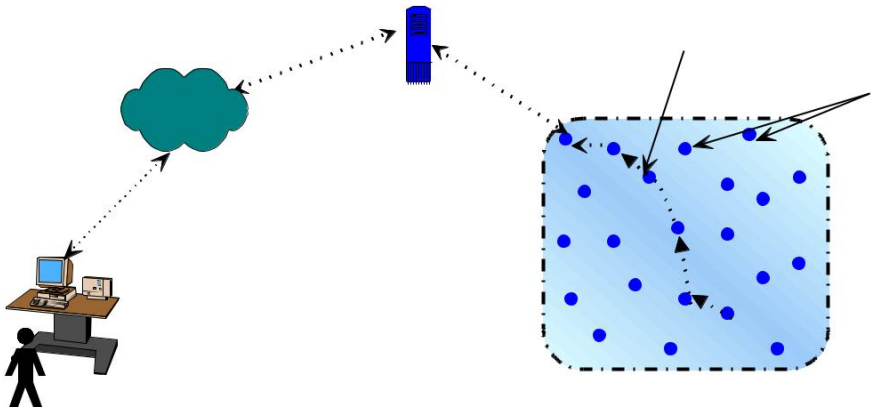

**Figure I-6 : Fonctionnement des réseaux de capteurs**

- **Ladéfaillancedesnî uds:** du fait de lôautonomie énergétique limitée des nî uds, la topologie du réseau nôest pas fixée (les nî uds qui épuisent leur énergie, sont considérés comme des nî uds inexistants).
- **Lôajout de nouveaux nî uds :** de nouveaux nî uds peuvent facilement être rajoutés. Il suffit de placer un nouveau capteur qui soit dans la portée de communication dôau moins dôun autre nî ud capteur du réseau déjà existant.

•**Auto-organisation :** Lôauto organisation sôavère très nécessaire pour ce type de réseaux afin de garantir sa maintenance. Vu les différentes conséquences résultant de lôinstabilité de la topologie du réseau de capteurs, ce dernier devra être capable de sôauto-organiser pour continuer ses applications.

•**Scalabilité :** Les réseaux de capteurs peuvent contenir des centaines voire des milliers de nî uds capteurs [7]. Un nombre aussi important engendre beaucoup de transmissions internodales et nécessite que le nî ud « Sink » soit équipé dôune mémoire importante pour stocker les formations reçues.

## I.7 Conclusion

Dans ce chapitre, on a fait une présentation des réseaux de capteurs, leurs caractéristiques et leurs domaines dôapplications. Cette étude nous permet de poser les briques de base et fédérer quelques concepts nécessaires à la compréhension de la problématique. La flexibilité, la tolérance aux fautes, le prix réduit et le déploiement rapide des réseaux de capteurs offrent des possibilités infinies de développement dans tous les domaines dôapplications. Ceci permet de penser que les réseaux de capteurs feront bientôt partie intégrante de notre vie et satisferont sûrement les plus grands projets.

Dans le chapitre suivant, on aborde les causes de pannes que peut subir un réseau de capteurs ainsi que les approches de tolérance aux pannes et aux fautes dans les RCSF.

# Chapitre2

# La tolérance aux pannes dans les réseaux de capteurs sans fil

# Chapitre 2 Tolérance des pannes dans les réseaux de capteurs

## II.1 Introduction

Certains capteurs 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 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 a pour objectif de maintenir les fonctionnalités du réseau sans interruption due à une panne de certains capteurs.

## II.2 Les pannes dans les réseaux de capteurs

### II.2.1 Notion de panne (faute, erreur)

Dans cette section, on présente quelques notions liées à la tolérance aux fautes dans les RCSF :

- **La défaillance** survient quand le système a un comportement anormal : une erreur est la partie de lôétat du système (par rapport au processus de traitement) qui est susceptible dôentraîner une défaillance. La cause supposée de lôerreur est une faute. Une erreur est donc la manifestation dôune faute dans le système, et une défaillance est donc lôeffet dôune erreur sur le service.
- **Une faute active** lorsquôelle produit une erreur. Elle pourrait être soit une faute interne qui était précédemment dormante côest-à-dire quôelle ne produisait pas dôerreur et qui a été activée par le processus de traitement, soit une faute externe [9].
- **Une faute interne** peut passer, de manière cyclique, de lôétat dormant à lôétat actif. Une erreur est, par nature, temporaire. Elle peut être latente ou détectée: une erreur est latente tant quôelle nôa pas été reconnue en tant que telle; elle est détectée soit par des mécanismes de détection dôerreur qui analysent lôétat du système, soit par lôeffet de lôerreur sur le service (défaillance).

Généralement, une erreur propage dôautres erreurs, nouvelles, dans dôautres parties du système. Une défaillance survient lorsquôune erreur traverse lôinterface système-utilisateur et affecte le service délivré par le système. Si un système peut être considéré comme un ensemble de composants, la conséquence de la défaillance dôun composant est une faute interne pour le système qui le contient, et aussi une faute externe pour le ou les composants qui interagissent avec lui. Ceci conduit à la chaîne fondamentale suivante :

... →défaillance → faute →erreur →défaillance →faute →...

### II.2.2 Classification des pannes

Les pannes qui peuvent survenir dans un réseau de capteurs sans fil, sont classées selon trois critères : durée, cause et comportement. La classification classique est faite selon la nature résultante de la panne ce qui donne deux types de pannes : [10]

- **Pannes catastrophiques** : elles sont inacceptables. Par exemple, les grandeurs pathologiques d'un patient.
- **Pannes non catastrophiques** : elles sont acceptables. La collecte de la température dans un environnement.

La deuxième classification qui suit les trois critères est illustrée dans la figure suivante (Figure II-1) [10]:

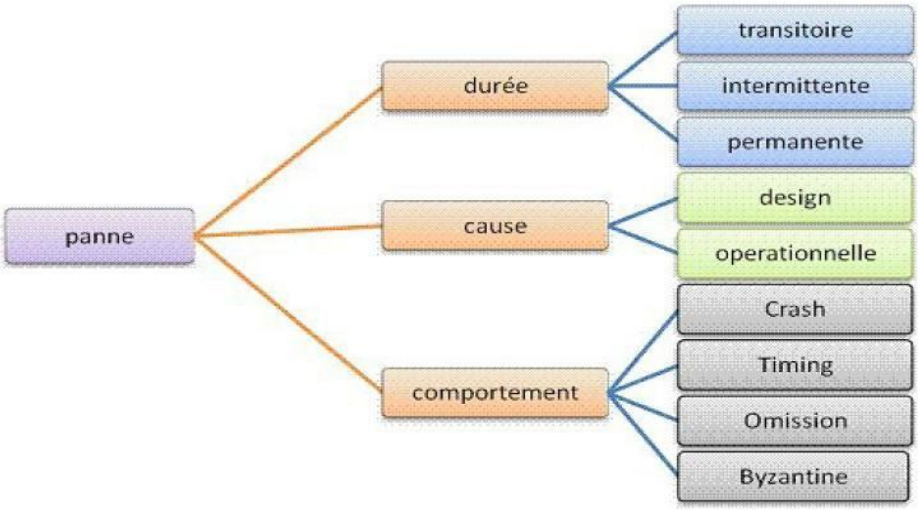


**Figure II-1: Classification des pannes**

### II.2.3 Causes de pannes

Les capteurs peuvent subir des pannes et des défaillances dues à de différentes causes et phénomènes qui peuvent être internes ou externes selon leurs origines. Ces pannes que peut subir un réseau de capteurs peuvent être dues à : [11]

- L'épuisement d'énergie des capteurs.
- Perte de connexion sans fil due à l'épuisement de la batterie d'un capteur.
- Destruction physique (accidentelle ou volontaire).
- Interférences environnementales.

## II.3 La tolérance aux pannes

La limitation dôénergie dans les capteurs sans fil, et les environnements hostiles dans lesquels ils pourraient être déployés, sont des facteurs qui rendent ce type de réseaux non fonctionnels dans certaines périodes. Ainsi, la perte de connexions sans fil peut être due à une extinction dôun capteur suite à un épuisement de sa batterie, ou tout simplement à une destruction physique accidentelle ou intentionnelle par un ennemi. Par ailleurs, la non fiabilité de type de capteurs est une caractéristique qui augmente les risques de pannes sur ce type de réseau.

Etant donné que les réseaux de capteurs reposent sur des protocoles de communications ad hoc, il est donc nécessaire de considérer la tolérance aux pannes comme critère indispensable dans la conception de ces protocoles [12]. En outre, afin dôassurer la communication entre le nî ud collecteur et les autres nî uds dôun réseau de capteurs, les protocoles de routage sont basés sur la communication multi sauts dans laquelle chaque nî ud joue alors, en plus du rôle de source de données, le rôle dôun routeur. Toutefois, ces nî uds sont sujets à de nombreuses pannes, dues principalement à lôépuisement des batteries et aux destructions physiques (par exemple, suite à un écrasement par des animaux). Ainsi, la panne des nî uds entraîne la perte des liens de communications et donc un changement significatif dans la topologie globale du réseau. Ceci peut affecter dôune façon considérable la connectivité du réseau et diminuer, en conséquence, sa durée de vie.

### II.3.1 Définition

La propriété de tolérance aux pannes est définie par lôaptitude du réseau à maintenir ses fonctionnalités, en cas de panne de certains de ses nî uds. Elle vise donc à minimiser lôinfluence de ces pannes sur la tâche globale du réseau [10].

### II.3.2 Procédure générale de tolérance aux pannes

La conception dôune procédure pour la tolérance aux pannes dépend de lôarchitecture et des fonctionnalités du système. Cependant, certaines étapes générales sont exécutées dans la plupart des systèmes comme sôest illustré dans la figure :

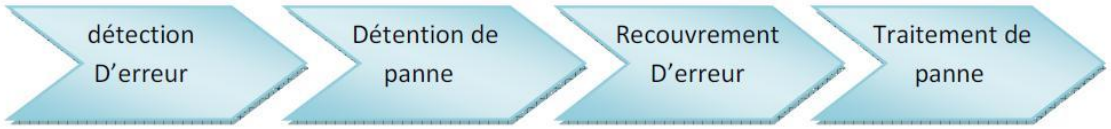


**Figure II-2: Procédure générale de tolérance aux pannes**

- **Détection d'erreur :** C'est la première phase dans chaque schéma de tolérance aux pannes, dans laquelle on reconnaît qu'un événement inattendu s'est produit. Les techniques de détection de pannes sont généralement classifiées en deux catégories : en ligne et autonome (offline). La détection offline est souvent réalisée à l'aide de programmes de diagnostic qui
  Sôexécutent quand le système est inactif alors que la détection en ligne vise l'identification de pannes en temps réel et elle est effectuée simultanément avec l'activité du système.

- **Détention de la panne :** Cette phase établit des limites des effets de la panne sur une zone particulière afin d'empêcher la contamination des autres régions. En cas de détection d'intrusion, par exemple, l'isolation des composants compromis minimise le risque d'attaque des composants encore fonctionnels.
- **Recouvrement d'erreur** d'élimination des effets de panne » et « répétition » C'est la phase dans laquelle on effectue des opérations pannes. Les deux techniques les plus utilisées sont « masquage de

  - **Masquage de panne :** utilise l'information redondante correcte pour éliminer l'impact de l'information erronée.
  - **Répétition :** après que la panne soit détectée, on effectue un nouvel essai pour exécuter une partie du programme, dans l'espoir que la panne soit transitoire.
  -

- **Traitement de panne :** Dans cette phase, la réparation du composant en panne isolé est effectuée. La procédure de réparation dépend du type de la panne. Les pannes permanentes exigent une substitution du composant avec un autre composa nt fonctionnel. Le système doit contenir un ensemble d'éléments redondants (ou en état standby) qui servent à remplacer les capteurs défaillants.

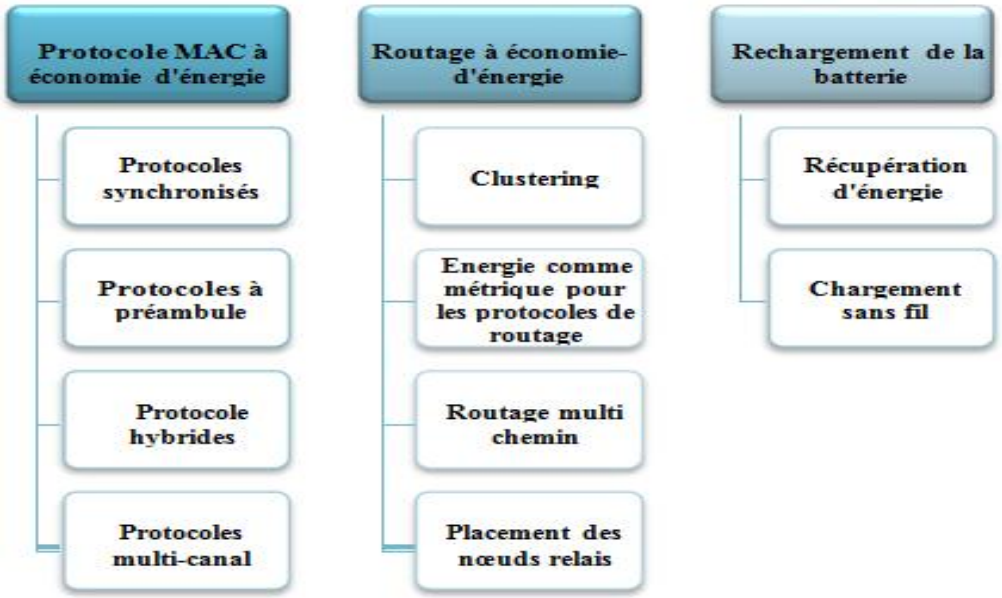


**Figure II.3** : Classification des mécanismes à économie dœnergie.

### II.3.3 Fonctionnement

La propriété de tolérance aux pannes est définie par l'habilité du réseau à maintenir ses fonctionnalités sans interruptions provoquées par la panne des capteurs. Elle vise donc à minimiser l'influence de ces pannes sur la tâche globale du réseau. Cette propriété *R(t)* est modélisée dans [13] par une distribution de poisson où *R(t)* donne la probabilité de ne pas avoir une panne pour un nœud capteur pendant l'intervalle de temps [0,t].

$$R(t) = exp(-\lambda_k t)$$

Où $\lambda_k$ est le taux de pannes du nœud capteur *k*, et *t* est la période de temps.

Les protocoles conçus pour les réseaux de capteurs doivent atteindre le niveau de tolérance aux pannes requit par le réseau, cela dépend essentiellement de l'environnement de déploiement du réseau, des caractéristiques des micro-capteurs, etc. En effet, si le réseau de capteurs est destiné aux environnements avec un faible degré d'interférences, tel que ceux utilisés dans les bâtiments pour surveiller le taux d'humidité et le degré de température, les protocoles utilisés ne doivent pas cibler une grande tolérances aux pannes, car dans ce type de réseaux, il n'existe pas une grande interférence avec l'environnement, et ses nœuds ne sont pas exposés au risque d'endommagement. Par contre, si le réseau est destiné aux applications militaires telle que la surveillance et le contrôle d'un champ de bataille, le niveau de tolérance aux pannes visé par les protocoles employés doit être très élevé, car les nœuds sont exposés à un grand risque d'endommagement par des actions hostiles, et les informations captées sont très critiques. Par conséquent, le niveau de tolérance aux pannes requis dépend de l'application du réseau de capteurs conçu, et les schémas de conception doivent prendre en charge ce paramètre.

## II.4 Classification des solutions de tolérance aux pannes

Les solutions et les approches de tolérance aux pannes peuvent être vues de plusieurs angles différents. De ce fait, un ensemble de critères est défini pour les classifier. Des catégories de trois classifications distinctes peuvent être citées :

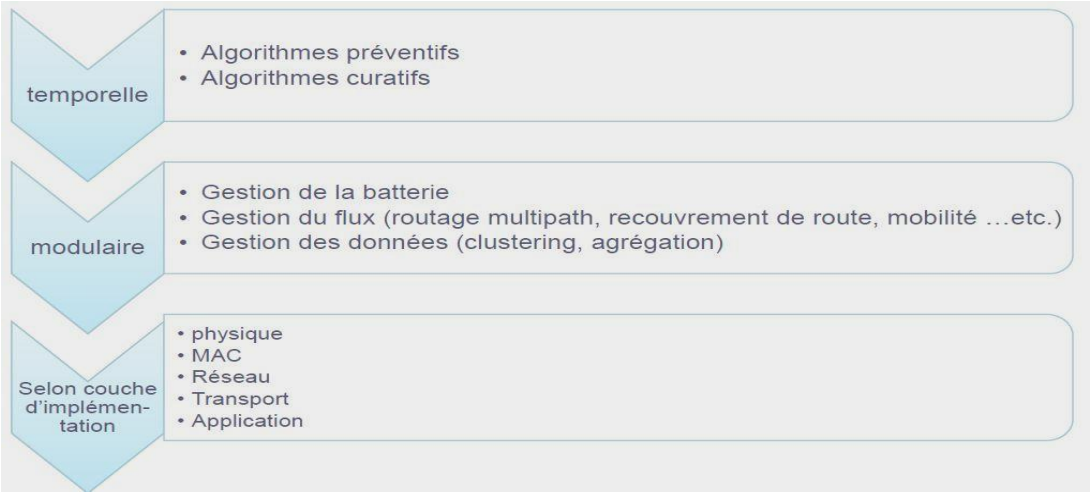


**Figure II-4: Classification des solutions de tolérance aux pannes**

### II.4.1 Classification temporelle

Dans la classification temporelle, nous divisons lœensemble des algorithmes en deux catégories, et cela selon la phase de traitement. Si le traitement est effectué avant la panne, on parle donc dœalgorithmes préventifs sinon les algorithmes sont dits curatifs.

- ***Algorithme préventif :*** implémente des techniques tolérantes aux pannes qui tentent de retarder ou éviter tout type dœerreur afin de garder le réseau fonctionnel le plus longtemps possible. La conservation dœénergie à titre dœexemple, permet de consommer moins dœénergie et évite donc une extinction prématurée de la batterie ce qui augmente la durée de vie des nî uds.
- ***Algorithme curatif :*** utilise une approche optimiste, où le mécanisme de tolérance aux pannes implémenté nœest exécuté quœaprès la détection de pannes. Pour cela, plusieurs algorithmes de recouvrement après lœoccurrence des pannes sont proposés dans la littérature, par exemple: le recouvrement du chemin de routage, lœélection dœun nouvel agrégateur, etc.

### II.4.2 Classification architecturale

Cette classification traite les différents types de gestion des composants, soit au niveau du capteur individuellement ou bien sur tout le réseau. Nous distinguons trois catégories principales:

- **Gestion de la batterie** : Cette catégorie est considérée comme une approche préventive, où les protocoles définissent une distribution uniforme pour la dissipation dœénergie entre les différents nî uds capteurs ; afin de mieux gérer la consommation dœénergie 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 nî uds capteurs inactifs pour une meilleure conservation dœénergie. [14]

- **Gestion de flux** : Cette catégorie regroupe les techniques qui définissent des protocoles de gestion de transfert des données (routage, sélection de 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-path** : utilise un algorithme préventif pour déterminer plusieurs chemins depuis chaque capteur vers le nî ud collecteur. Ceci garantit la présence de plus dœun chemin fiable pour la transmission et offre une reprise rapide du transfert encas de panne sur le chemin principal et choisissant un des chemins qui restent.

  - **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.

  - **Allocation de canal**: cette solution est implémentée au niveau de la couche MAC. Elle permet dœeffectuer une allocation du canal de transmission dœune manière à diminuer les interférences entre les nî uds voisins et éviter les collisions durant le transfert.

- **Mobilité**: certains protocoles proposent comme solution tolérante aux pannes la sélection dôun ensemble de nî uds mobiles chargés de se déplacer entre les capteurs et collecter les données captées. Ceci réduira lôénergie consommée au niveau de chaque capteur en éliminant sa tâche de transmission. Un nî ud mobile est généralement doté dôune batterie plus importante que celle dôun nî ud capteur.

- **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 [15] :
- **Agrégation**: cette approche est considérée comme une approche préventive. Elle permet dôeffectuer un traitement supplémentaire sur les données brutes captées depuis lôenvironnement. Un nî ud agrégateur combine les données provenant de plusieurs nî uds en une information significative. Ce qui réduit considérablement la quantité de données transmises en consommant moins dôénergie pour leur dissémination. Ceci permet donc dôaugmenter la durée de vie du réseau. En outre, elle aussi dôamortir lôerreur si le résultat de lôagrégation est une moyenne.
- **Clustering** : une des importantes approches pour traiter la structure dôun réseau de capteurs est le clustering. Il permet la formation dôun back one virtuel qui améliore lôutilisation des ressources rares telles que la bande passante et lôénergie. Par ailleurs, le clustering aide à réaliser du multiplexage entre 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 en minimisant l'erreur totale des clusters.
-

## II.5 Protocoles des solutions utilisées dans RCSFs

### II.5.1 Principes des Techniques de routages

La technique de routage est une méthode dôacheminement des données à la bonne destination à travers un réseau de connexion donnée. Le problème de routage au sein des RCSFs est assez complexe et cela est dû essentiellement à lôabsence dôinfrastructure fixe (forêt, mère), de toute administration centralisée et à dôautres défis qui doivent être vérifié.

Le principal défi dans le routage consiste à déterminer un acheminement optimal des paquets à travers le réseau au sens dôun certain critère de performance. En effet, le problème consiste à trouver lôinvestissement de moindre coût en capacités nominales et de réserves qui assure le routage du trafic nominal et garantit sa survie en cas un nî ud ou plusieurs nî uds du réseau ne sont pas fonctionnels.

Le problème qui se pose dans le contexte des réseaux ad hoc est lôadaptation de la méthode dôacheminement utilisée avec le grand nombre dôunités existant dans un environnement caractérisé par de modestes capacités de calcul et de sauvegarde et de changements rapides de topologies.

Il est donc nécessaire que toute conception de protocole de routage doive étudier les problèmes suivants :

- Assurer un routage optimal.
- Minimiser la charge du réseau.
- Offrir un support pour pouvoir effectuer des communications multipoints fiables.
- Offrir une bonne qualité concernant le temps de latenceé etc.

Avant dœentamer la phase de conception dœune technique de routage efficace en énergie, il est nécessaire dœapporter une étude minutieuse des principaux protocoles de routages utilisés dans les RCSFs. Les différents protocoles de routage vont être découpés en trois grandes classes à savoir : les protocoles de routages proactifs, réactifs et les protocoles de routages hybrides.

## II.5.2 Les protocoles de routages proactifs

Lorsque les nî uds de capteur sont déployés sur le terrain, aucun routage vers des nî uds spécifiques ne peut être fait. La solution pour y remédier est dœutiliser pour ce genre de réseau (le réseau ad-hoc) une technique de routage. Les protocoles de routage sont divisés en plusieurs classes. Nous allons exposés dans cette section le principe de fonctionnement des techniques de routages proactifs.

Un protocole de routage proactif permet dœétablir les tables de routage avant toute chose et permet également de connaître, en tout temps, la topologie de notre réseau. Nous allons étudier certains protocoles proactifs qui permettent dœobtenir les tables de routages afin de permettre une communication entre les différents capteurs. Mais également nous ne sommes plus dans un réseau de télécommunications classiques et donc nous devons privilégier certains critères tels que la consommation dœénergie du nî ud mais aussi la consommation dœénergie des nî uds dans tout le réseau.

### II.5.2.1 Le protocole DSDV (Destination Sequenced Distance Vector)

Le DSDV est un protocole de routage à vecteur de distance. Chaque nî ud appartenant au réseau possède une table de routage contenant tous ces nî uds voisins et également le nombre de sauts vers toutes les destinations possibles [16] [17]. Périodiquement, des diffusions sont faites pour actualiser la table de routage. Pour éviter le bouclage (loop-freedom), DSDV utilise les numéros de séquence [18] pour mettre à jour les nouvelles routes qui sont disponibles pour atteindre des nî uds cibles. Une route R est favorisée à une route RNjsi R a un numéro de séquence plus grand que celui de RNj

Si dans le cas où les deux ont un même numéro de séquence, alors la route possédant un minimum de saut est sélectionnée. Le numéro de séquence commence par le nî ud émetteur et est incrémenté pour chaque nouvelle route trouvée. Quand le nî ud trouve une actualisation vers une destination donnée, il met à jour le nombre de sauts vers cette destination et incrémente son numéro de séquence.

Les boucles de routes surviennent après un changement dans la topologie du réseau. Cêst alors que lôutilisation des numéros de séquence est utile car elle rend le DSDV applicable pour une topologie dynamique du réseau. Lôutilisation de mis à jour des numéros de séquence lorsque la topologie change permet au protocole DSDV dêêtre adaptée aux réseaux ad-hoc mobiles. En prenant en considération également que la transmission des mises à jour sont retardée, pour avoir ainsi un effet dôamortissement lorsque la topologie change rapidement.

### II.5.2.2 Le protocole OLSR (Optimized Link State Routing)

Le protocole OLSR est un protocole proactif à états des liens optimisé, il permet également dôavoir des routes de plus court chemin [19] [20]. Dans un protocole à état des liens, tous les nî uds déclarent ses liens directs avec tous ses voisins, par contre dans lôOLSR, les nî uds ne donnent quôune sous-part ie de leurs nî uds voisins à lôaide de la technique des relais multipoints.

**Relais multipoints**

La technique des relais multipoints consiste, pour un nî ud donné, dôignorer une partie de ses liens et des ses voisins directs, qui reviennent souvent dans le calcul des routes du plus court chemin. Donc une partie des voisins dôun nî ud est considéré comme intéressant. Cet ensemble de voisinage choisi de façon à obtenir le voisinage à deux sauts, est appelé ensemble des relais multipoints noté MPR sa dénomination anglophone  Multi-Protocol Router ». Lôutilité de cette technique est de diminuer nettement le trafic pour la diffusion des messages de contrôle dans le réseau, mais également pour diminuer la taille du sous-ensemble des liens diffusés à tout le réseau du faites que les routes sont crées à base des relais multipoints [20].

Lôidée de cette technique est de réduire lôinondation du trafic de contrôle dans un réseau en diminuant les mêmes retransmissions dans la même région. Chaque capteur dans le réseau choisit un ensemble de nî uds dans son entourage pour lesquels les messages seront transmis. Un nî ud

choisit ses MPRs dans son voisinage de manière quôil soit à un saut avec un lien symétrique. Par ce choix, la zone de couverture sera de deux sauts. Les nî uds considérés comme MPR le font savoir à son voisinage par les messages de contrôle envoyés. De cette manière, un nî ud capteur fait savoir au réseau quôil a la possibilité dôatteindre des nî uds qui lôont élu en tant que MPR. Les MPRs ont lôutilité de mettre en place des routes vers toutes les destinations possibles du réseau. En choisissant la route à lôaide des MPRs, on élimine les problèmes liés à la transmission des paquets pour les liens unidirectionnels. Tous les nî uds du réseau gardent des informations sur leurs voisins qui ont été choisis comme MPR.

Un capteur dans le réseau obtient des informations sur ces voisins grâce à des messages de contrôle reçus périodiquement. La figure 2.1 suivante fait la comparaison entre une diffusion pure et la diffusion en utilisant les MPRs. Pour la diffusion pure, dans le but dôatteindre tous les nî uds à trois sauts de la source, la diffusion à besoin de 24 retransmissions du paquet envoyé par la source. Avec lôutilisation des MPRs, il suffit de 11 retransmissions pour atteindre les nî uds à 3 sauts.

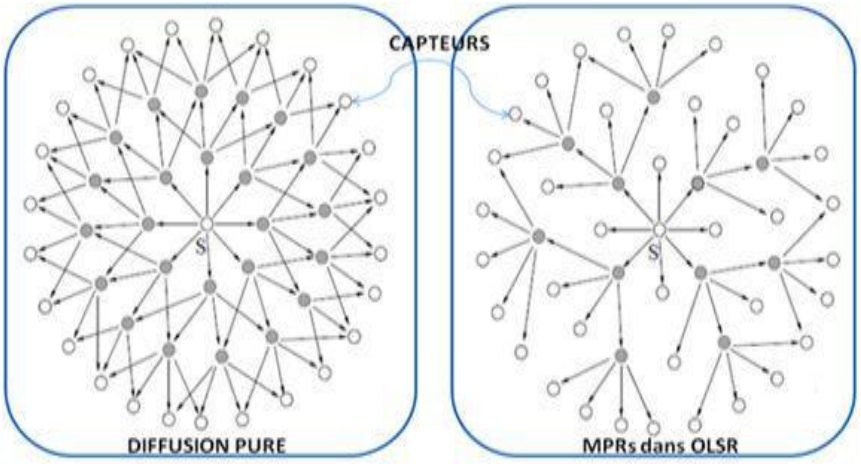


**Figure II.5 ï Diffusion pure et diffusion en utilisant les MPRs dans OLSR.**

**Fonctionnement du protocole OLSR**

OLSR est un protocole de routage proactif très bien adapté aux larges et denses réseaux. Dans ce protocole tous les capteurs servent en tant que routeur et chaque nî ud de ce réseau garde une table de routage de toutes les entrées pour tous les autres entités du réseau. Donc lors dôenvoi dôun paquet de données le nî ud décide lui-même de la route la plus adaptée à prendre.

Dôautres parts, Dans ce type de protocole de routage les capteurs sôéchangent des informations périodiquement pour obtenir les informations nécessaires au choix des relais multipoint et nécessaire également pour le calcul de la table de routage. Les nî uds envoient également des messages « HELLO » périodiquement pour obtenir des informations sur leur voisinage proche. Cela permet à chaque nî ud de choisir son ensemble de relais multipoints.

Il y a un autre type de messages que le protocole OLSR utilise, le message TC (Topologie Control). A lôaide de ce message les relais multipoints sont déclarés périodiquement dans le réseau. Ils sont diffusés en utilisant les relais multipoints et ce qui donne une diffusion contrôlée et optimisée. Les informations diffusées donnent une carte du réseau contenant tous les nî uds de celui-ci mais également un ensemble partiel des liens.

### II.5.2.3 Le protocole LEERA (Localized energy efficient routing for wireless sensor networks)

Dans le cadre de prolonger la durée de vie du réseau, une connaissance de la topologie du réseau est nécessaire mais aussi la connaissance de lôénergie résiduelle dans chaque entité du réseau est primordiale. Cela permet de router lôinformation tout en consommant lôénergie équitablement à travers tous les nî uds du réseau [21].

Pour permettre de connaître lôénergie résiduelle de chaque nî ud, plusieurs méthodes sont utilisées. Chaque nî ud peut diffuser périodiquement la quantité dôénergie disponible quôelle possède mais cela va consommer une grosse quantité dôénergie dans tout le réseau et il y a la possibilité de connaître lôénergie résiduelle des capteurs par des méthodes dôestimations. Dans la partie suivante nous allons étudier les différentes méthodes utilisées dans **le protocole de routage proactif LEERA**.

#### Méthode sleep-wakeup (sommeil-éveil)

Un nî ud sort de lôétat de sommeil lorsquôun événement se produit. Tous les nî uds du réseau possèdent deux antennes de communication. Lôune dôelle permet lôéchange des données et lôautre permet dôéveiller les nî uds pour communiquer des données.

Dans le protocole LEERA, il y a lôutilisation de la méthode STEM. Cette méthode utilise les messages RTS/CTS (Ready To Send/Clear To Send).Pour un simple scénario comportant trois nî uds A, B et C nous obtenons le datagramme de la figure suivante [21] :

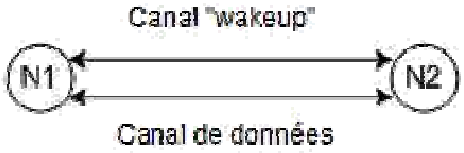


**Figure II.6 : Schéma de la méthode « Sleep-WakeUp».**

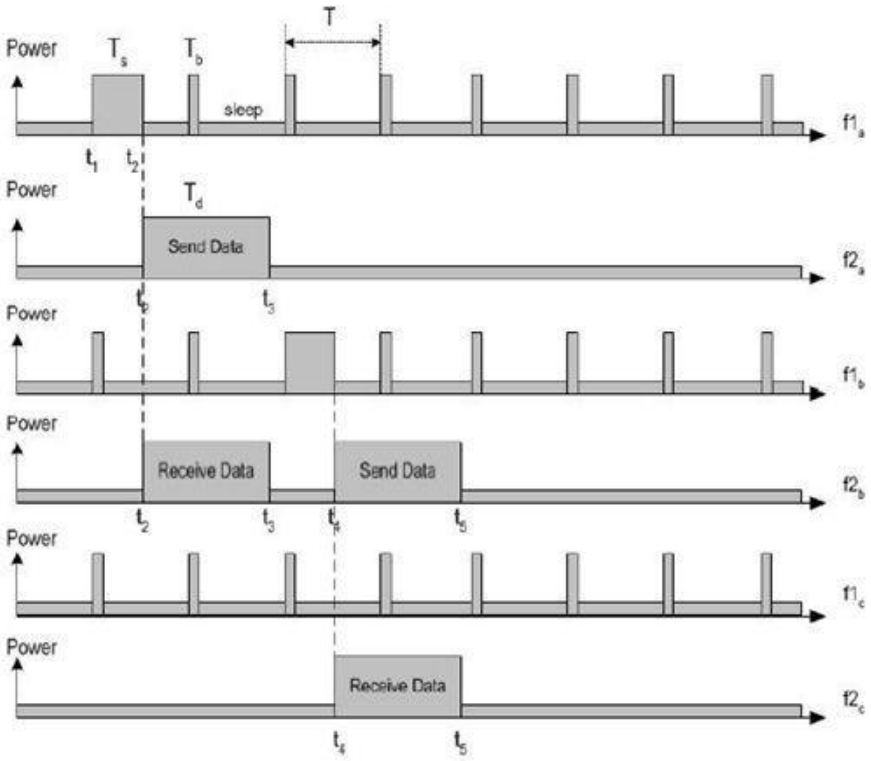


**Figure II.7 : Datagramme des messages RTS/CTS.**

Une amélioration est apportée en utilisant le STEM pipeline (Sparse Topology and Energy Management). Cette méthode permet aux différents nî uds du réseau dô interagir entre eux simultanément. Comme le montre la figure 2.4, dés que le nî ud B reçoit le message RTS, il renvoie un acquittement au nî ud A mais tout en connaissant lô adresse du prochain saut, le nî ud C. Lô adresse est contenue dans le message « RTS » qui circule dans le réseau [21]. Le nî ud C sachant quô il est le prochain nî ud se met en écoute pour recevoir les données du capteur B. Il y a alors un gain dans les attentes de délai et les délais de processus entre les nî uds du réseau.

## Estimation de lôénergie résiduelle

Les décisions de routage peuvent être prises de façons locales. Ces décisions peuvent être assurées de deux façons. Soit les nî uds capteurs diffusent leur niveau dôénergie périodiquement. la deuxième alternative est de recalculer le niveau dôénergie résiduelle des nî uds expéditeurs et receveurs.

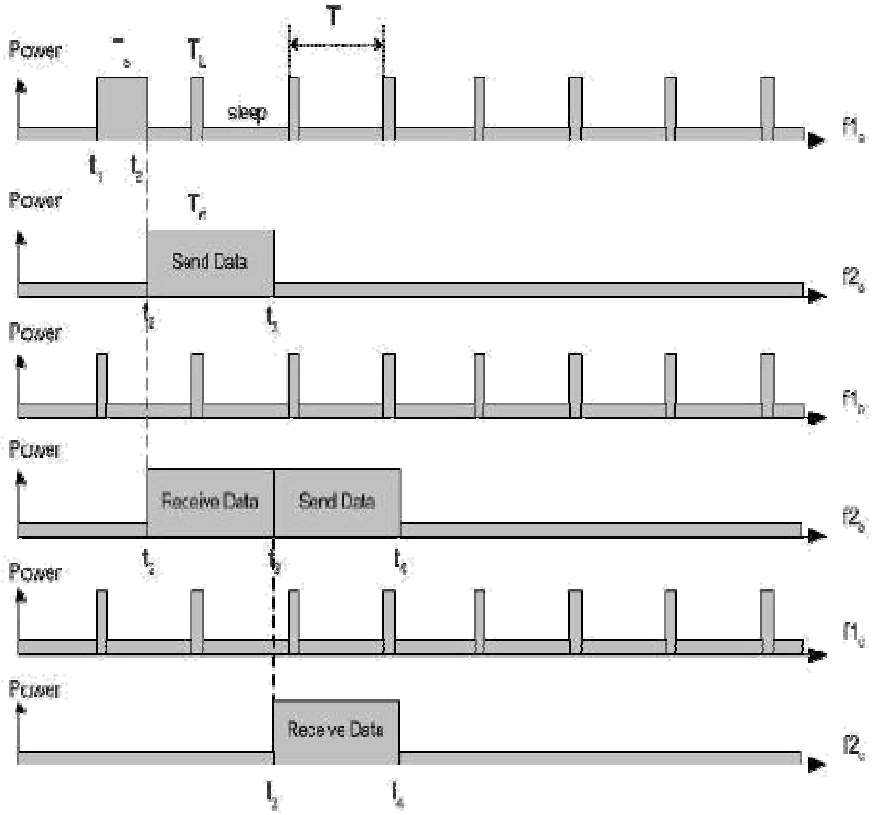


**Figure II.8 :** Datagramme avec le STEM pipeline.

En employant le mécanisme des messages RTS/CTS, tous les capteurs dans la plage de communication peuvent connaître lôénergie résiduelle car les nî uds qui transmettent connaissent les prochains sauts des paquets de données. Grace au message RTS/CTS ils ont également lôinformation de la longueur du paquet de données donc le calcul de lôénergie consommée par lôexpéditeur ou le récepteur peut être calculé par les formules suivantes :

$$E_{transmit} = T_d P_{transmit} \qquad (2.1)$$

$$E_{receive} = T_d P_{receive} \qquad (2.2)$$

### II.5.3 Les protocoles de routages réactifs

La deuxième classe de protocole que nous allons étudier est le protocole de routage réactif. Un protocole réactif permet d'établir une table de routage lorsqu'un nœud capteur décide de transmettre des données (suite à un événement). Il n'a aucune donnée sur le réseau. Ne connaissant pas la topologie de celle-ci ni l'énergie disponible. Le protocole réactif va permettre de rassembler les différentes données des entités du réseau pour déterminer le chemin le plus optimale à prendre afin de communiquer avec un autre nœud du réseau, ou avec le nœud puits (sink).

#### II.5.3.1 Le protocoles DSR (Dynamic Source Routing)

Le protocole « Routage à Source Dynamique » (DSR), est basée sur l'utilisation de la technique « routage source ». Dans cette technique : la source des données détermine la séquence complétée des capteurs à travers lesquelles, les paquets de données seront envoyés [22]. En effet, Pour ce routage, les entêtes des paquets de données possèdent la séquence des nœuds à travers lesquels ils doivent passer. Donc les nœuds intermédiaires, qui se situent entre la source et la destination lors de l'acheminement des informations, garde une trace de leurs voisins intermédiaires pour pouvoir échanger les paquets de données. Bien entendu, il faut qu'également le nœud source ait besoin de connaître l'ordre complet des nœuds jusqu'à la destination.

La demande de route dans DSR se base sur la transmission des paquets Route Request. Lorsqu'un nœud ayant pris connaissance du paquet, il commence à chercher dans sa cachette de route (ou toutes ses routes connues sont stockées) un chemin contenant la destination demandée. Au cas ou aucune route n'est trouvée, le nœud émet le paquet Route Request au nœud suivant tout en lui ajoutant sa propre adresse à la séquence de nœud stocké dans le paquet Route Request. Et ainsi de suite, le paquet est envoyé de nœud en nœud dans le réseau jusqu'à arriver au nœud de destination où alors à un nœud ayant dans sa cachette de route la connaissance du chemin de destination. Si un chemin est trouvé, un paquet Route Reply possédant la séquence de nœud pour atteindre le nœud de destination est renvoyé au nœud source [23].

Pour éviter des inondations inutiles du réseau par des messages Route Request, la méthode de demande de route est initialisée en questionnant le voisinage du nœud source. Cela est permis en envoyant le paquet Route Request avec une limite de saut égale à zéro, pour que celui-ci ne soit pas

la possibilité dêêtre transféré aux voisins. Si aucune route nêest obtenue alors, un nouveau paquet est initialisé et diffusé dans le réseau entier.

Un nî ud capteur DSR a donc la possibilité de connaître des routes en consultant des paquets qui ne lui sont pas adressés. Malgré cela, cette méthode exige un récepteur actif dans le nî ud, qui va être consommatrice dêénergie. Dans les réseaux où les nî uds ont une capacité dêénergie limitée, lêobjectif est de mettre en veille lêémetteur-récepteur afin de sauvegarder lêénergie le plus longtemps possible. La découverte de chemins dans le protocole DSR est illustré dans **la figure 2.5** et **la figure 2.6**

### II.5.3.2 Le protocole AODV (Ad-hoc On Demand Distance Vector)

Le protocole AODV représente essentiellement une amélioration de lêalgorithme DSDV [23]. Le protocole AODV, réduit le nombre de diffusions de messages, et cela, en créant les routes lors du besoin, contrairement au DSDV, qui maintient la totalité des routes. En effet, Le protocole AODV demande une route dêacheminement des données que lorsquêil en a besoin. Il utilise les principes des numéros de séquence de la même façon que DSDV, pour éviter les boucles de routage, maintenir la consistance des informations de routage et obtenir des nouvelles routes dêacheminement des données.

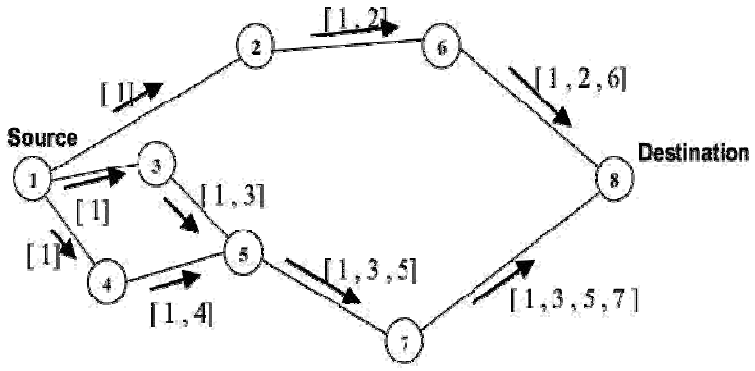


**Figure II.9 :** Protocole DSR Construction de la route.

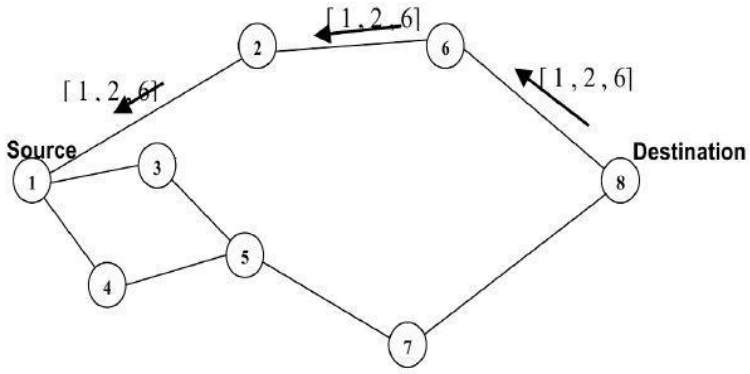


**Figure II.10 :** Protocole DSR : Le renvoi du chemin

Une entrée de la table de routage possède l'adresse de destination, l'adresse du nœud suivant, la distance en nombre de sauts, le numéro de séquence de destination et le temps d'expiration de chaque entrée de table. Quand un nœud ayant besoin d'envoyer des données vers une destination et dont l'entrée dans la table de routage n'existe pas ou est alors expirée, celui-ci diffuse un message de demande de route a son voisinage (RREQ : Route Request message). Pendant son acheminement dans le réseau, le message RREQ crée des entrées temporaires des tables de routage pour la route inverse des nœuds à travers lesquels il passe. Lorsque la destination ou la route d'acheminement est trouvée, la route est rendue accessible par un message RREP (Route Reply) répondant au RREQ du nœud source. Le message répondant au RREQ revient sur le chemin temporaire laissé de celui-ci. Au cours de son chemin inverse vers la source, le RREP créée des entrées pour la destination dans les tables de routage des nœuds intermédiaires. Ces entrées de routage ont une durée déterminée après laquelle elles expirent [24].

Pour le protocole de routage AODV, les différentes phases sont en premier lieu, une diffusion dans le réseau d'une demande de route. Par la suite, le nœud de destination répond au nœud source à l'aide des informations obtenues lors de la demande de route, pour créer une route de la destination à la source. Mais nous devons prendre en compte que le protocole de routage AODV ne donne pas tout le temps le meilleur chemin possible entre la source et la destination. Le voisinage d'un nœud est détecté à l'aide de messages périodiques

• HELLO ». Lorsquôun nî ud utilise un de ces voisins pour lôenvoie des données, et que celui-ci ne reçoit pas le message HELLO, alors le lien est considéré comme brisé et une information de défaillance est envoyée aux voisins étant actifs. La source ayant pour connaissance du lien brisé peut choisir de stopper lôenvoi des données ou de demander une nouvelle route pour acheminer ces informations, en transmettant à nouveau un message RREQ.

### II.5.3.3 Le protocole « Energy Aware Routing »

Lôenergy aware routing est un protocole qui permet de développer la survie dôun réseau pauvre en énergie. Nous parlons dans ce cas dôun protocole réactif [25] [26]. Le problème pour ce genre de protocole est quôil utilise de lôénergie pour créer une route et cela pour chaque communication. Pour résoudre ce problème, nous proposons un nouveau protocole « Energy Aware Routing ». Pour sa réalisation, de multiples chemins sont découverts entre le nî ud source et le nî ud de destination. A chaque fois, des paquets de données sont envoyées de la source à la destination, par un chemin choisi au hasard. Cette technique ressemble à une diffusion (inondation). Ce type de protocole est composé de 3 phases :

**1-Phase dôinstallation**

**Etape 1** : Le nî ud de destination inonde le réseau dans la direction de la source. Il initialise également le coût du domaine avant de lancer sa requête.

$$Cost(ND) = 0 \qquad (2.3)$$

**Etape 2** : Tous les nî uds intermédiaires envoient des requêtes aux voisins pour voir les nî uds qui sont les plus proches du nî ud source et le plus éloigné du nî ud de destination. Ainsi, un nî ud $N_i$ envoie sa demande à un nî ud $N_j$ qui satisfait les exigences suivantes :

$$d(Ni, Ns) Ó d(Nj , Ns) \qquad (2.4)$$

$$d(Ni, Nd ) Ó d(Nj , Nd ) \qquad (2.5)$$

**Etape 3** : En recevant la requête, lôénergie métrique pour le voisin qui a envoyé la demande est calculée et est ajouté au coût total du chemin. Dès lors le nî ud $N_j$ calcule le cout du trajet entre Ni et $N_j$ :

$$C(N_i, N_j) = Cost(_{Ni}) + Metric(N_j , N_i) \qquad (2.6)$$

**Etape 4** : Les chemins qui ont un coût élevés sont rejetés et non ajoutés à la table de routage. Seul les voisins de Ni avec les chemins de faible coût sont ajoutés au tableau de transmission.

$$F\ T_j = \{i/CN_j ,N_i\ \ \grave{O}\breve{U}(min_k CN_j ,N_k )\} \qquad (2.7)$$

**Etape 5** : Le nî ud Nj assigne une probabilité à chacun de ces nî uds voisins Ni dans la table de transfert, avec la probabilité inversement proportionnelle au coût.

$$P_{N_i,N_j} = \frac{\frac{1}{C_{N_j,N_k}}}{\sum_{k\in FT_j} \frac{1}{C_{N_j,N_k}}} \qquad (2.8)$$

**Etape 6** : Ainsi, chaque nî ud Nj a un certain nombre de voisins à travers laquelle elle peut router les paquets vers le nî ud de destination. $N_j$ alors calcule le coût moyen pour atteindre le nî ud de destination en utilisant les voisins qui se trouve dans la table de routage.

$$CostN\ j ,Ni\ = \times\ PN\ j ,NiCNj ,Ni \qquad (2.9)$$

i ú F Tj

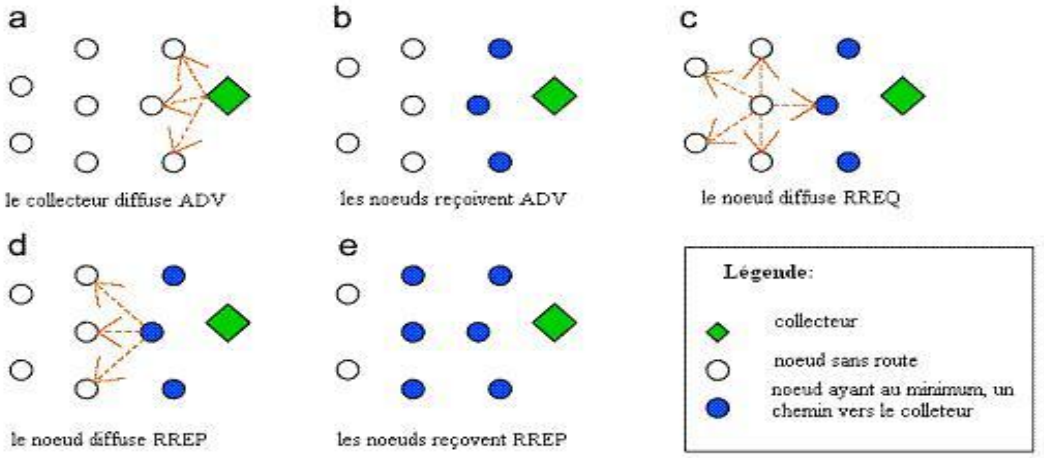


**Figure II.11 : Fonctionnement du protocole** EAR

## Phase de communication des données

**Etape 1 :** Le nî ud source envoie le paquet de données à un voisin quelconque se trouvant dans sa table de routage, avec la probabilité du voisin choisi égale à la probabilité dans la table de transfert.

**Etape 2** : Chacun des nî uds intermédiaires transmet les paquets de données à un voisin chois au hasard dans la table de transmission, avec la probabilité du voisin choisie étant égale à la probabilité du tableau de transmission.

**Etape 3** : On continue jusquôà ce que le paquet de donnée arrive au nî ud de destination.

## Phase de maintenance

La phase de maintenance des chemins permettant une réception des données des plus optimales des données reste à un niveau minimal.

Nous pouvons en conclure que ce protocole de routage est approprié à la consommation dôénergie et le faible débit du réseau. Lôidée de ce protocole est très simple, les chemins dôaccès utilisant le moins dôénergie nôest pas nécessairement le meilleur pour la santé à long terme du réseau. En utilisant un mécanisme plus simple pour lôenvoie des paquets de données dans le réseau permet de gérer plus équitablement les ressources de chaque nî ud du réseau.

### II.5.3.4 Le protocole EDSR (Energy-aware DSR)

Actuellement, dans le réseau ad hoc, lôalgorithme de routage à propos de lôénergie « Energy-aware DSR » propose deux idées :

- Envoyer des données en consommant le moins dôénergie possible.
- Faire en sorte de prolonger la durée de vie du réseau le plus longtemps possible.

On propose de modifier le protocole de routage classique DSR, en retenant le mécanisme de routage DSR-demand.

Lorsque lôon va choisir une route on prend en compte le minimum de saut possible mais également la consommation dôénergie des nî uds par lesquelles vont être traversées les données ainsi que lôénergie encore disponible à travers le réseau.

On propose un routage basé sur le facteur de priorité dynamique, en essayant de consommer le moins dôénergie possible et en utilisant la capacité des états de liens entre les nî uds.

Å Méthode Ad hoc

On suppose que les données passent par n1, n2, n3 jusquôà nk, avec n1 représente le nî ud de source et nk le nî ud de destination. Lôexpression de lôénergie consommée pour envoyer des données du nî ud « a » au nî ud b » est noté T (ab). Dés lors, toute lôénergie consommée lors de la traversée des données à travers le réseau est :

$$e = \sum_{i=1}^{k-1} T(n_i, n_{i+1}) \qquad (2.10)$$

Optimisation des liens dôénergies Le modèle de la consommation dôénergie est :

$$u(d) = ad^{\alpha} + c \qquad (2.11)$$

Avec, u(d) représente la distance entre les nî uds Ŭ et c sont des constantes. UN algorithme « greedy » pour sauvegarder lôénergie en considérant que le nî ud émetteur connait la position du nî ud récepteur, nous obtenons comme formule :

$$d \leq \alpha \sqrt{\frac{c(1-2^{1-\alpha})}{a}} \qquad (2.12)$$

Il sôagit du minimum de puissance pour une transmission directe.

Le facteur de la priorité des liens

Dans une topologie réseau, il y a plusieurs chemins du nî ud source au nî ud de destination. Nous obtenons la consommation dôunité dôénergie pour chaque route en la calculant. Nous assignons un facteur de priorité dynamique. Le changement de ß se fait suivant la formule suivante [33] :

$$\beta = \left(\frac{c}{\frac{me}{\pi}}\right)^2 \qquad (2.13)$$

Avec :

- c : la capacité du lien de routage
- e : lôexpression de lôénergie consommée par le lien
- m :le nombre de paquet de données envoyées.
- ´ : le nombre de nî uds traversés par ces paquets.

Cela nous donne c/(me?´ qui nous permet de choisir la plus grande capacité de lien avec une faible consommation dôénergie. Cette stratégie nous permet dôavoir une consommation dôénergie équitable sur tout le réseau

, et par la suite une durée de vie du réseau plus longue.

Å Les étapes de lôalgorithme EDSR

Etape 1 : Utilisation du protocole de routage DSR pour trouver le chemin p1 p2, · · · , pk, et maintenir en état le routage de lôinformation.

Initialisation

Etape 2 : Tandis que le routage Pi, i = 1, 2 · · · k faire :

Etape 3 : Optimisé lôénergie de liaison Pi,

Etape 4 : Calculer la capacité Ci de lien Pi,

Etape 5 : Calculer la consommation unitaire dôénergie unitaire ei ,

Etape 6 : Calculer le Pi et le facteur de priorité ßi,

Etape 7 : Lôacheminement suivant Pi+1

**Choix du routage EDSR**

Etape 8 : tandis que S a des données à envoyés faire

Etape 9 : Par rapport à ß, sélectionner le lien de routage Pi avec le facteur de la plus haute priorité ?i,

Etape 10 : Si ei Òci

Etape 11 : Mise en î uvre du transfert sur Pi,

Etape 12 : ci Ŷ ci Ŷ ei

Etape 13 : Calcul du cumul de lôénergie dépensée,

Etape 14 : Calcul du nombre de routes restantes et du nombre de nî uds restants,

Etape 15 : Nouvelle direction de routage, retour à lôétape 1.

Pour ce protocole, il y a eu quelques améliorations par rapport au protocole de routage DSR originale. Ceci est une nouvelle stratégie de routage EDSR. A travers lôoptimisation des liens, et les facteurs de priorité dynamique pour le choix des chemins, nous arrivons à lôobjectif de préserver lôénergie des nî uds et donc de la vie du réseau [27].

## II.5.4 Les protocoles de routages hybrides

Ces protocoles combinent les propriétés de base des deux premières classes de protocoles, en un seul. Autrement dit, ils sont à la fois réactifs et proactifs. Les protocoles hybrides [28] sont utilisés dans un réseau découpé en zone. Ils emploient un protocole proactif dans la zone et un protocole réactif pour les communications interzones [29].

Quand un réseau est constitué de milliers de capteurs, la gestion de l'acheminement des données entre les différents capteurs est coûteuse dans le domaine énergétique et en capacité de stockage. Dans la technique de clustering, les données ne sont pas transmises directement à la station de base mais au Cluster Head (CH) correspondant. A partir de la, le Cluster Head transmet toutes les données agrégées à une station de base distante. Alors nous pouvons en déduire que les Cluster Head reçoivent et transmettent le plus de données dans un cluster est en proie à une grande consommation d'énergie. Donc il est nécessaire de mettre en place des techniques permettant d'éviter à un Cluster Head de consommer sa capacité énergétique totale.

Pour être utilisé, cette technique de partitionnement en plusieurs zones, confère aux nœuds deux tables de routages. La première table aura pour objectif d'acheminer les données à l'intérieur de la zone. Et la deuxième table aura pour but de router les données entre les différentes zones du réseau. Cette deuxième table de routage est utilisée par les nœuds qui sont aux frontières des différentes zones. Ces derniers joueront le rôle de « Gateway » (portes, relais) entres les différentes zones du réseau. La figure suivante donne un exemple la technique de partitionnement en zones dans un réseau de capteurs et l'acheminement d'information entre deux nœuds se situant dans des zones différentes.

### II 5.4.1 Protocole LEACH (Low Energy Adaptive Clustering Hierarchy)

Pour le routage dans les réseaux de capteurs homogènes, un clustering distribué nommé LEACH a été proposé par Heinzelman et al [32]. Cette algorithme choisit aléatoirement les nœuds qui vont être des CHs et donne ce rôle aux différents nœuds suivant la méthode Round-Robin (tourniquet). Cette méthode permet de garantir une consommation de l'énergie équitable entre tous les nœuds d'un même cluster. De plus, afin de minimiser la quantité de

données transmises à la station de base, les Cluster Head agrègent les informations recueillies par les nî uds membres qui sont dans le même cluster, et envoient un paquet agrégé à la station de base. Le protocole LEACH se compose de deux phases à savoir : la phase n´ Setup zĘ dans laquelle les Cluster Head sont choisis et les clusters du réseau sont créés. Et la deuxième phase appelée n´ Steady State zĘ durant laquelle le transfert des données sont envoyés à la station de base. Malgré cela, le protocole de routage

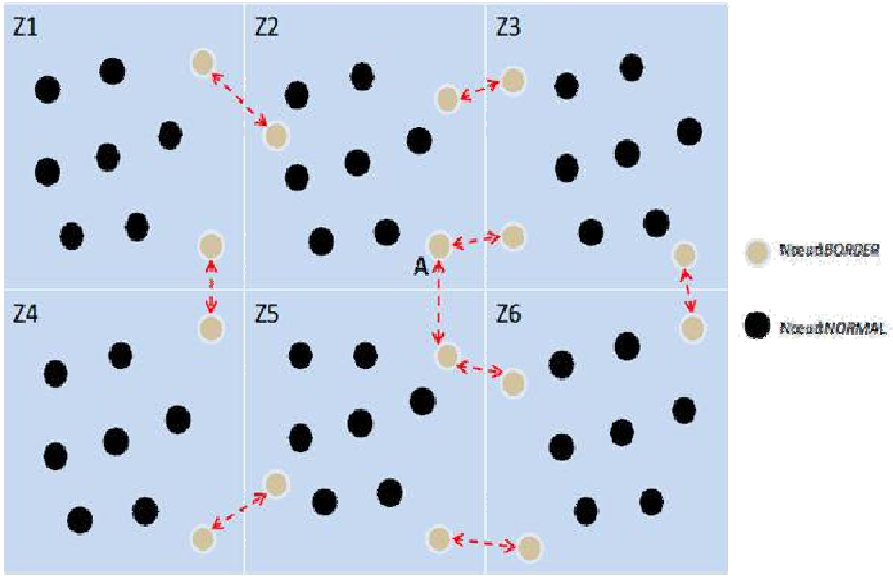


**Figure II.12 : Schématisation des zones pour un protocole de routage hybride.**

LEACH bien quôil puisse allonger la durée de vie du réseau, celui-ci à certaines limites.

Le protocole considère que tous les nî uds du réseau peuvent transmettre des données avec une puissance maximale pour pouvoir atteindre la station de base et que tous les nî uds ont une puissance de calcul permettant de supporter les différentes couches MAC. Donc le protocole LEACH [31] ne correspond pas aux réseaux de très envergure pouvant être déployé sur de grandes zones. Dôautre part, le protocole LEACH choisit aléatoirement les ClusterHeads et ne pose aucune contrainte sur leur distribution ainsi que sur leur niveau dôénergie. Nous pouvons trouver par conséquent des nî uds étant isolés. Dans le protocole LEACH, il y a un rassemblement des données qui est centralisé et se lance périodiquement.

Mais il existe des cas où la transmission périodique des données peut ne pas être négligée car cela épuise rapidement lô énergie des capteurs.

### II 5.4.2 Le Protocole ELMA (Enhanced Lifetime Maximisation Algorithm)

Un nouvel algorithme de routage ELMA [30] (algorithme pour maximiser lôamélioration dôune durée de vie) avec trois versions différentes. Cet algorithme essaie de répartir les charges du trafic sur lô ensemble du réseau et évite ainsi lô épuisement de lô énergie sur lô ensemble des trajets du réseau. Lôun des points principaux de recherche sur les réseaux de capteurs sans fil est le grand nombre de protocole de routage. LEACH est une sorte dôalgorithme de routage hiérarchique basé sur le concept de regroupement. Dans cet algorithme, les nî uds sont classés en différents groupes et dans chaque groupe, lôun des nî uds est sélectionné au hasard pour être le chef du regroupement (cluster) pendant un certain temps. Pour équilibrer la consommation dô énergie des nî uds, le rôle dôun chef de groupe est remis au hasard parmi tous les membres de chaque groupe. Tous les nî uds dôun cluster à lô exception du chef peuvent envoyer des données au nî ud puits (Sink) via le chef du groupe.

Dés lors, la transmission se fait par saut unique à partir des chefs de groupe au nî ud puits. La grosse consommation en puissance énergétique rend lôalgorithme pratique quand il sôagit dôun réseau à grande échelle. On a proposé le protocole multi-hop LEACH. Dans ce protocole, il est supposé que la communication entre le chef du groupe et le puits utilise plusieurs sauts au lieu dôun seul bond comme le modèle LEACH. Le LMAWSN a été proposé par Zytoune, Fakhri et Aboutajdine en 2010. Cet algorithme prend en considération deux paramètres pour sélectionner un chemin avec une énergie de transmission minimum tandis que son objectif global est de repartir les couts de transport dô énergie sur lô ensemble des nî uds du réseau. Pour y parvenir, un nî ud est autorisé à transmettre des données uniquement lorsque son énergie est supérieure à lô énergie moyenne du réseau. Afin de calculer, lô énergie moyenne du réseau, chaque nî ud diffuse périodiquement un paquet contenant son énergie résiduelle.

- Terminologies
- Nous commençons par donner quelques définitions sur les termes utilisées :
- Neighbors Nodes : Tous les nî uds qui peuvent communiquer entre eux.
- Active Nodes : Les nî uds actifs sont des nî uds qui sont en « éveil zĘ». Ils sont sensibles à lôenvironnement (sensibles aux différents événements dans leur environnement), envoie les données aux voisins.
- Idle mode : Les nî uds « ralentis » ne peuvent pas envoyer des données aux nî uds adjacents. Alors la consommation de lôénergie des nî uds « ralenti » est inférieure à celle des nî uds actifs.
- Network life time : Commence à partir du moment que le premier nî ud nôa plus dôénergie. Lôalgorithme proposé de la maximisation de la durée de vie dôun réseau de capteur, ELMA, et ses variantes sont basées sur lôéquilibrage de la consommation dôénergie des nî uds en se concentrant sur la construction de la route entre les nî uds de capteur et le puits.

Le travail effectué utilise la recherche de plusieurs chemins (multi-path fading) noté « mp » et le modèle des canaux libres « fs ». Lorsque la distance entre le nî ud transmetteur et le nî ud receveur dépasse le seuil de distance d0 le modèle des canaux libres est utilisé sinon le multi-path fading est appliqué. le paramètre d0 est donné par lôéquation suivante :

$$d_0 = \sqrt{\frac{E_{fs}}{E_{mp}}} \qquad (2.14)$$

Lôénergie qui va être dépensée par le nî ud transmetteur est donnée par : {

$$E_{tx}(k,d) = \begin{cases} k E_{elec} + k E_{fs} d^2 & si\ d < d_0 \\ k E_{elec} + k E_{mp} d^4 & si\ d \geq d_0 \end{cases} \qquad (2.15)$$

Avec, k : Message de taille k bit.

Eelec : Energie électronique de la radio. E f s d2 et Emp d4 : Energie amplifiée.

$$E_{rx}(k) = k\ E_{elec} \qquad (2.16)$$

Dôautre part, lôénergie consommée par le nî ud récepteur est :

**La famille dôalgorithme ELMA**

Le principe et lôobjectif de lôalgorithme ELMA est dôune part une consommation équitable de lôénergie entre les nî uds du réseau et dôautre part la construction dôune route entre le nî ud source et le nî ud de destination « puits » (sink). Ils se composent de 5 phases : -

1. Estimation moyenne de lôénergie (Average energy estimation).
2. Détection de lôenvironnement (Sensing the environment)
3. Requête de route (Route request)
4. Réponse de route (Route reply)
5. Transmission des données (des informations). (Data transmission) De plus, lôalgorithme ELMA utilise 4 types de paquets :

1) Réponse de route
2) Paquet dôénergie (résiduel)
3) Paquet de donnée
4) Estimation moyenne de lôénergie

Chaque nî ud du réseau envoie périodiquement le niveau dôénergie restant, grâce aux paquets dôénergie. Tous les nî uds recevant des paquets dôénergie peuvent calculer ou estimer lôénergie résiduelle du réseau. Dans le travail effectué, nous considérons que les nî uds possédant une énergie supérieure à l''énergie moyenne du réseau sont considérés comme des nî uds actifs sinon ils sont considérés comme des nî uds ralentis.

- **Requête de route**

Chaque nî ud du réseau envoie périodiquement au nî ud voisin des paquets de requête de route. Dans celle-ci est ajouté lĠID du nî ud mais également un numéro de séquence du nî ud source. Dans cette partie, si un nî ud reçoit le même paquet par un autre nî ud voisin, celui-ci est négligé et donc cela permet dôéviter la création de boucles dans le réseau.

Nous pouvons avoir des paquets de requête de route qui peuvent sôéloigner du nî ud de destination. Un contrôle de sauts de ces paquets permet dôéviter cela. De plus, seul les nî uds actifs ont la possibilité de transmettre les paquets.

Å **Réponse à la requête**

Dans cette partie, le nî ud attend une période pour recevoir les paquets de requête de route, et choisis la meilleure route possible par rapport à une fonction dôefficacité. Les procédures du nî ud évier lorsquôil reçoit les paquets de requête de routes sont basés sur deux paramètres. Le numéro de séquence et une fonction

Dôefficacité. Le nî ud puits envoie un paquet réponse de requête pour chaque numéro de séquence. Pour une séquence unique, la route est choisie selon le rapport dôefficacité définie par lôéquation suivante :

$$\rho = \frac{E_{total}}{Hop^{\alpha}} \qquad (2.17)$$

Avec : E*total* : représente lôénergie totale de la route.

Hop : représente le nombre de nî ud se trouvant sur cette route.

Ŭ: est une variable définie comme 1 ÒŬÒ2.

Apres avoir définie le meilleur chemin. Une réponse de requête (route reply) est envoyée au nî ud source.

Å Transmission des données

Apres avoir choisi le meilleur chemin. Le nî ud source recevant les paquets de réponse de requête peut son tour calcule le nombre de paquets qui peuvent être envoyé par cette route, en utilisant la fonction de capacité du chemin. Cette fonction est définie par lôéquation suivante :

$$\Phi_P = \frac{E_{min}}{E_{TH}} \qquad (2.18)$$

Avec :

Emin étant lôénergie de consommation la moins élevé utilisé par le nî ud sur cette route.

ET H est le seuil de viabilité.

Le protocole de routage appartient à une famille dôalgorithme de routage qui optimise la durée de vie dôun réseau, ainsi que le nombre de paquets reçus par le nî ud puit. Les algorithmes ELMA sôappliquent à équilibrer les techniques dôestimation moyenne de lôénergie dans un réseau.

# II.6 Conclusion

Dans ce chapitre, nous avons pu énumérés certains protocoles de routages existants les plus connus et les plus citées. Le groupement de ces protocoles on été classés suivant trois grandes familles auxquelles on peut les associer. Cêst-à-dire les protocoles de routage **proactifs, réactifs et hybrides**. Chacune de ces familles possèdent des avantages et des inconvénients qui vont de pair. Pour parvenir à différencier les bonus et malus de chaque protocole de routage, nous devons mettre lôaccent sur les métriques à étudier pour parvenir à un classement des protocoles viables à lôoptimisation de lôénergie. Nous pourrons ainsi utiliser des bribes de ces protocoles pour ainsi parvenir à trouver un protocole servant comme modèle à lôoptimisation de lôénergie pour les réseaux de capteurs sans fil.

Mais avant de pouvoir amener ce projet à terme, il est indispensable de sôintéresser aux fonctionnements de la consommation énergétique dôun capteur dans les différentes phases de son utilisation au sein dôun réseau.

Lôétude de la consommation énergétique est inévitablement liée aux fonctionnements de la communication se déroulant entre les capteurs ainsi que de lôutilisation du module radio dôun nî ud. Mais avant de pouvoir amener ce projet à terme, il est indispensable de sôintéresser aux fonctionnements de la consommation énergétique dôun capteur dans les différentes phases de son utilisation au sein dôun réseau. Lôétude de la consommation énergétique est inévitablement liée aux fonctionnements de la communication se déroulant entre les capteurs ainsi que de lôutilisation du module radio dôun nî ud.

# Chapitre 3

# Stratégie pour améliorer le protocole de routage EAR

# Chapitre 3 : Stratégie pour améliorer le protocole de routage EAR

## III.1 Introduction

Les réseaux de capteurs sans fil, sont destinés à relever des informations dans des environnements hostiles auxquels lôhomme nôa pas toujours accès. Cêst pourquoi on considère quôune fois quôils sont déployés, les capteurs sont autonomes. Leur durée de vie est donc la durée de vie de leur batterie. Le facteur énergie est donc au centre de toutes les préoccupations sur les capteurs : protocoles de routage « économiques », technologie sans fil adaptée, etc.

Il faut minimiser les dépenses énergétiques, car lôénergie est une contrainte clé dans les réseaux de capteurs.

En effet, nous nous somme intéressé au protocole de routage économique EAR (Energy Aware Routing) afin dôaugmenter la capacité de maintenir les fonctionnalités du réseau sans interruption

Dans **EAR** les voisins proches (à un saut) dôun nî ud capteur donné peuvent être fréquemment utilisés lors de lôexécution du protocole de routage. Donc, ces derniers vont subir une plus grosse charge de tâches en jouant le rôle de points relais. Ce qui peut par la suite accentué leurs déperditions en énergie jusquôà épuisement de leurs unités respectives dôénergie. De ce fait, il est possible quôun nî ud capteur nôait aucun nî ud capteur voisin en état de fonctionnement dans son rayon de portée**. EAR** ne propose aucune solution à ce problème.

## III.2 Ajustement du rayon de transmission

Le contrôle de la puissance de transmission ou lôajustement du rayon de transmission est un mécanisme qui a pour objectif la réduction de la consommation dôénergie et par conséquent la durée de vie des batteries. Ceci est très intéressant dans certaines applications ou les nî uds capteurs transmettent des quantités dôinformation assez importante comme cêst le cas dans les réseaux de captures vidéo sans fils [37] par exemple .dans la plus part des applications dans les domaines des RCSFM. Les nî uds capteurs utilisent une puissance de transmission fixe sans prendre en considération la distance entre les nî uds et lôenvironnement de communication. Lôadaptation des puissances de transmission permet dôéconomiser lôénergie surconsommée. La puissance de transmission peut être adaptée selon la distance de communication et le rapport signal sur bruit (***SNR :Signal to Noise Ratio***) ceci est possible grâce à lôexistence sur le marché des modules radio pour les nî uds capteurs de différentes marques qui offres cette possibilité [32].Les transmissions avec une puissance élevée

entrainent plus dôinterférences. Ce qui engendre dôavantage de retransmissions et par conséquent une durée de vie plus courte pour les batteries. Pour assurer une communication fiable et efficace .une faible puissance est suffisante en cas de bonnes conditions du canal de transmission Alors quôune puissance élevée est exigée en cas de mauvaises conditions du canal de transmission ceci est le principe du contrôle de la puissance de transmission routage en tenant compte de l'énergie( EAR).

## III.3 La s*tratégie proposée* :

Dans le but dôaméliorer la tolérance aux pannes du protocole **EAR**, nous avons pensé à traiter le problème des nî uds isolés a cause de défaillance de quelques nî uds relais appartenant aux déférents chemins de routage. Pour cela, nous avons dôajuster le rayon de transmission des nî uds isolé pour trouver de nouveaux nî uds relais.

Lôajustement de rayon de transmission est en effet une propriété quôon retrouve dans quelques protocoles destinés à la tolérance aux pannes dans les réseaux de capteurs tels que DMRF, PEQ et VTRP. Elle est utilisée par ces derniers pour empêcher lôisolement dôun nî ud capteur dans le cas où tous les nî uds voisins se trouvant dans sa zone de transmission sont défectueux pour maintes raisons. Alors, le nî ud doit donc augmenter son rayon de transmission radio pour éviter les nî uds défaillants et atteindre les capteurs voisin lointains.

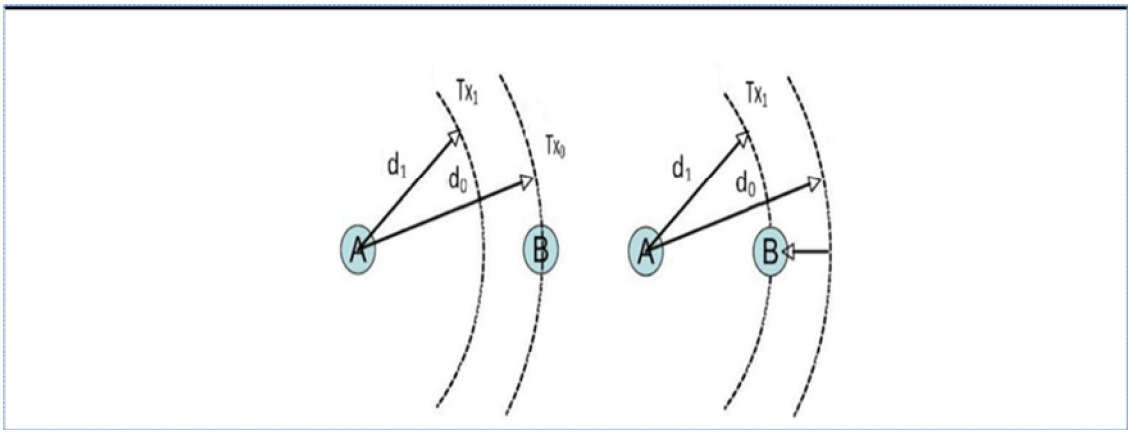


**Figure III.1 :** Exemple de déplacement du nî ud B qui provoque une diminution du niveau de transmission de la source A

### III.3.1 Phase de gestion de route :

Les micro-capteurs, avec leur mémoire de taille réduite, ne peuvent pas garder tous les chemins possibles dans leurs tables de routage. Pour cela, et afin dôassurer une bonne tolérance aux pannes, on ne doit garder que les meilleurs chemins. Le protocole va définit donc 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. Cependant, la qualité des liens nôest pas prise en considération, dans ce cas, le plus court chemin nôassure pas forcément la fiabilité de transmission. En effet, si un chemin échoue à transmettre N paquets consécutifs, il sera mis dans une "liste noire" lôécartant ainsi dôune future utilisation. La deuxième métrique, appelée score de route (RS), est définie comme suit :

RS =PE x WE + PT x WT

Telque :

- PE: niveau de lôénergie du capteur du prochain saut ;
- WE: poids assigné à PE dans lôintervalle [0-1] ;
- PT: taux de succès dans la transmission ;
- WT: poids assigné à PT dans [0-1] tel que (WT + WE = 1);

Dans cette phase, le protocole met à jour la liste des routes dans la table de routage en envoyant un message de contrôle de taille minimale qui est égale à 1 octet. Si un nî ud ne reçoit pas ce message de mise-à-jour de route dôaucun de ses voisins, alors le nî ud se considère isolé et doit augmenter son rayon de transmission pour atteindre des nî uds qui posséderait potentiellement un chemin vers la station de base.

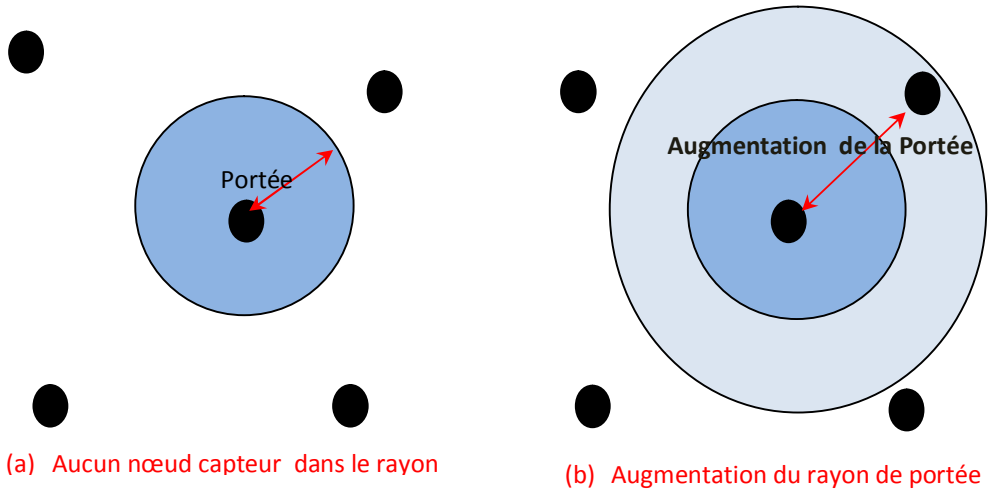


**Figure III.2**: Ajustement du rayon de transmission

## III.3.2 Ajustement du rayon de transmission pour notre stratégie:

Le déploiement de RCSF étant de type aléatoire, sa densité ne peut être connue à lôavance. Alors, nous portons notre choix pour lôajustement du RT sur la fonction avec progrès aléatoire.

$$R_i = R_i\text{-}1 + \delta p$$

$R_i$ représente le nouveau rayon de transmission, $R_i$-1 représente lôancien rayon de transmission, et enfin, $\delta p$ ***(delta)*** représente une valeur aléatoire tel que $\delta p$ ú [ù, Max] choisie selon lôenvironnement Ci-dessous lôalgorithme qui résume le fonctionnement de lôamélioration :

**Repeat**

*ñSending of route update message from neighborsò;*

*(waiting time);*

**If** *no messages received from neighbors* **then**

***Isolated = yes;***

**If** (*Isolated*) **then** $R_i = R_i\text{-}1 + \delta p$

**Else** *Isolated=false* **;**

**End if**

until isolated =false;

***ôôAlgorithme pour lôajustement du Rayon de transmissionôô***

### III.3.3 Exemple illustratif de lœxécution :

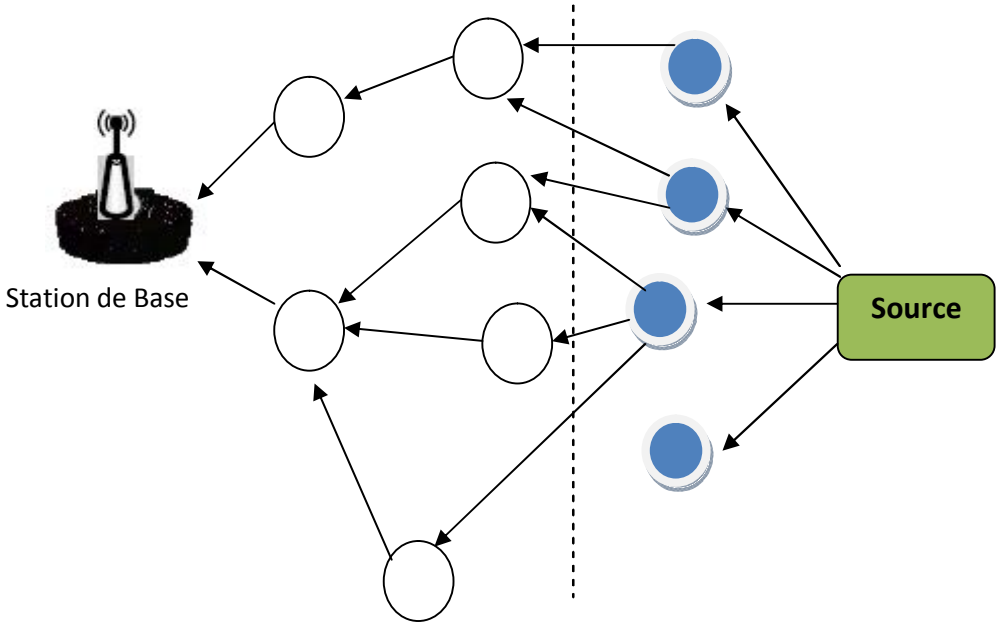


**Figure III.3**: Phase initiale

La **Figure III.2** représente le cas de fonctionnement du protocole lorsquœau moins un des nî uds se trouvant dans la zone de couverture du nî ud source est actif. Dans ce cas, la transmission des données jusquœà la station de base sœeffectuent le plus normalement du monde.

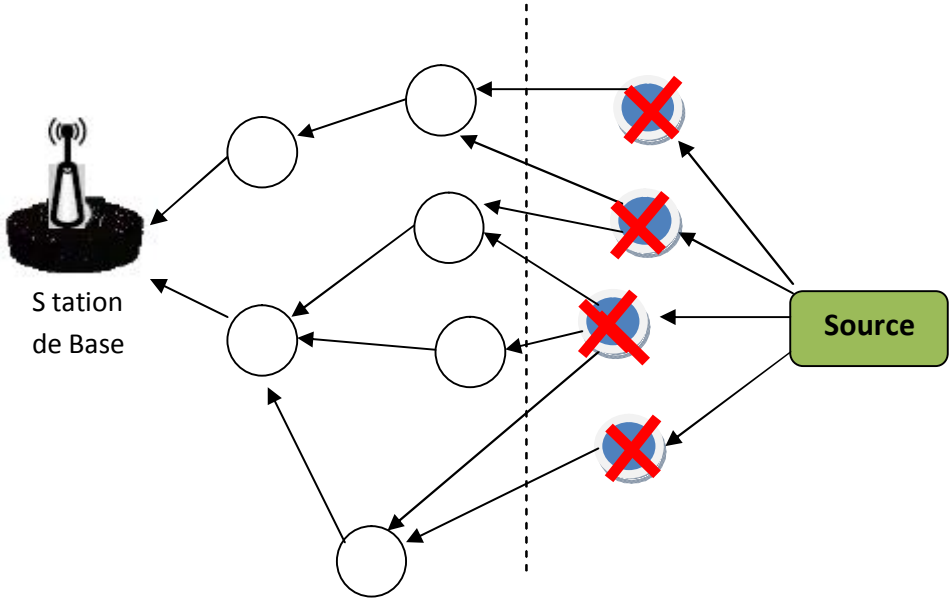


**Figure III.4**: Problème du nî ud isolé

La **Figure III.4** illustre le cas où le nœud source n'obtient aucun message de mise-à-jour de route de la part des nœuds capteurs se trouvant dans sa zone de couverture. Ce dernier ce retrouve isolé.

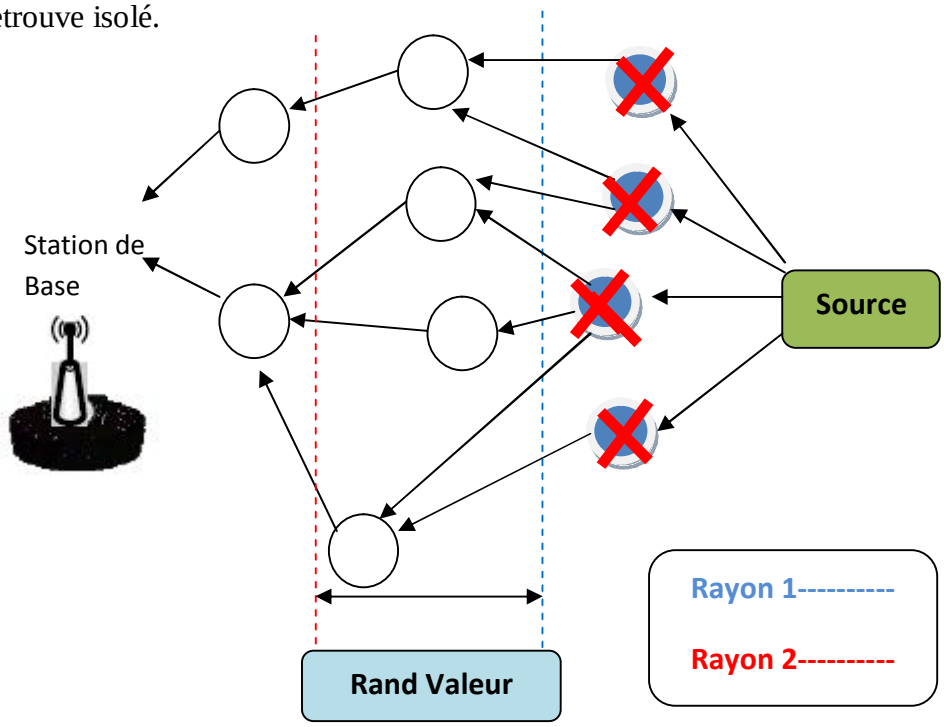


**Figure III.5**: nouveau rayon de transmission

La **Figure III.5** montre l'étape de l'augmentation du rayon de transmission après n'avoir reçu aucun message de mise à jour de routes de la part des voisins du nœud.

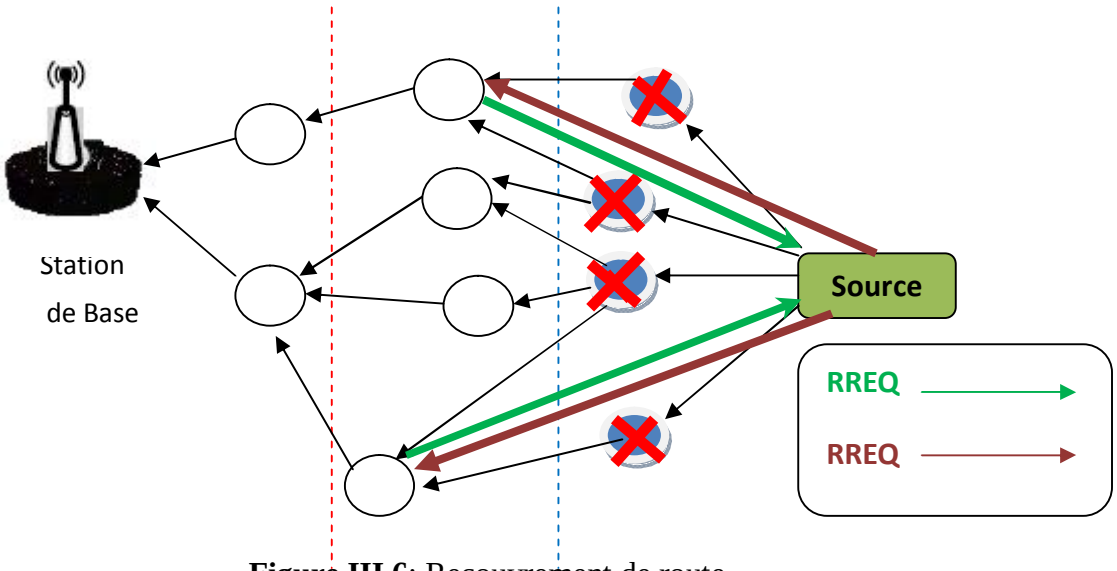


**Figure III.6**: Recouvrement de route

Etant isolé, le nœud capteur doit augmenter son rayon de transmission (vu que tous les nœuds voisin sont détruits) et cela afin de pouvoir atteindre les nœuds voisins lointains pour qu'il puisse transmettre les données à la station de base. (Voir **Figure III.6**)

## III.4 Conclusion

Notre travail rentre dans le cadre de lôamélioration de la tolérance aux pannes du protocole EAR. Dans cette proposition, nous avons cherché à maximiser lôexploitation du réseau en proposant une solution à la gestion des nî uds capteurs isolés. Afin de palier à ce problème, nous avons utilisé lôaugmentation de la puissance de transmission des nî uds capteurs afin de garder le réseau active et minimiser la consommation dôénergie au niveau de capteur pour quôil soit toujours en service et détecté les pannes en plus.

# Conclusion générale

# Conclusion générale

Les réseaux de capteurs sont composés d'un très grand nombre de dispositifs de communication ultra petits, autonomes avec des ressources de calcul et d'énergie limitées. Ils sont actuellement considérés comme l'une des technologies qui bouleverse notre façon de vivre, grâce à leur utilisation dans différents domaines d'application. Cependant, les réseaux de capteurs sans fil rencontrent plusieurs problèmes 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, etc... Par ailleurs, ces réseaux sont caractérisés par les pannes des nî uds qui peuvent causer un dysfonctionnement du réseau en entier. Dans cette optique, il est commode de proposer des techniques qui permettent de prévoir les pannes à une étape précoce.

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 techniques tolérantes aux pannes.

Dans ce mémoire, on a réalisé une application qui permet de détecter les pannes dans leurs débuts. Cette détection permet à des applications sensibles d'éviter des catastrophes.

En perspectives, on propose d'implémenter des techniques d'analyse de données quand les données sont nombreuses et variées.

# Bibliographie

# Références bibliographiques


[1] AKYILDIZ (I. F.), SU (W.), SANKARASUBRAMANIAM (Y.) et CAYIRCI.(E.), ñWireless sensor networks: a surveyò, *IEEE Communications Magazine*, vol. 40, no 8, p. 102ï 114, August 2002.

[2] Julien BEAUDAUX,« Partitionnement logique dans les réseaux de capteurs sans fil», Mémoire de Master, Université de Strasbourg, Laboratoire des Sciences de lõImage de lõInformatique et de la Télédétection, 2010.

[3] LEHSAINI Mohamed, «Diffusion et couverture basées sur le clustering dans les réseaux de capteurs : application à la domotique », Thèse de Doctorat, Université A.B Tlemcen et Université de Franche-Comté, Tlemcen, 2009.

[4] DHIBEYA, «Routage avec QoS temps réel dans les réseaux de capteurs », Rapport de projet de fin dõétudes, École supérieure des communications, Tunis, 2007.

[5] Yacine CHALLAL, Hatem BETTAHAR, Abdelmadjid BOUABDALLAH, «Les Réseaux de capteurs (WSN: Wireless Sensor Networks) », Rapport interne, Université de Technologie de Compiègne, France, 2008.

[6] MAKHOUL Abdallah, « Réseaux de capteurs : localisation, couverture et fusion de données ».Thèse de Doctorat, Université de Franche-Comté, 2008.

[7] Claude CASTELLUCCIA, « La Sécurité des Capteurs et Réseaux de Capteurs », Projet Planete, INRIA, Juin 2008.

[8] Mathieu BADNET et Nicolas BELLOIR «Réseaux de capteurs : Mise en place dõune plate forme de test et dõexpérimentation», Mémoire de Master Technologie de lõInternet, France, 2005/2006.

[9] Ali MAHMOUD, Annette BOHM and Magnus JONSON. ñWireless sensor networks for surveillance applications - A comparative survey of MAC protocolsò. In Proceedings of the 4$^{th}$ International Conférence on Wireless and Mobile Communications (ICWMCõ08), pp399ï 403, Washington, DC, USA, 2008.John

[10] Paul WALTERS ,òWireless Sensor Network Security: A Surveyò,

[11] Boucif Amar et BENSABAR,« Introduction à la sécurité des réseaux de capteurs sans fil» Cours, laboratoire de Mathématiques et Informatique Appliquées LAMIA,Uni versité du Québec à Trois Rivières.

[12] Du W., Deng J., Han, Y. S. and P. Varshney «A witness-based approach for data fusion assurance in wireless sensor networks» In IEEE Global Communications Conférence (GLOBECOM), Vol. 3, pp. 1435ï 1439, 2003.

[13] HOBLOS G., STAROSWIECKI M., AITOUCHA A. « Sur la Tolérance aux Fautes de Capteurs et d'Actionneurs », Journal Européen des Systèmes Automatisés, vol. 35, n°3, 331-352, 2001.

[14] KACIMI Rahim, « Techniques de conservation dôénergie dans les réseaux de capteurs sans fil », Thèse de Doctorat, Université de Toulouse, 2009.
[15] Ioannis Parissis LCIS & Claudia Roncancio LIG « ARTEcoApplications à base de Réseaux de capteurs Tolérantes aux Fautes &Energétiquement économiques », Mémoire, Grenoble Institue of Technology, France, 2011.
[16] Thibault BERNARD, « Marches aléatoires et mot circulant adaptabilités et tolérance aux pannes dans les environnements distribués », Thèse, Université de Reims-Champagne-Ardenne, 2011.
[17] Azzedine Boukerche, Richard Werner Nelem Pazzi, Regina Borges Araujo ñA Fast and Reliable Protocol for Wireless Sensor Networks in Critical Conditions Monitoring Applications*òpaper : MSWiMô04 Copyright 2004 ACM 1-58113-953-5/04/0010,Canada, 2004.
[18] Habib M. Ammari, « Challenges and Opportunities of Connected K-Covered Wireless Sensor Networks », Livre, 2009.
[19] François Taïani Marc-OlivierKillijian,Jean-Charles Fabre «Intergiciels pour la tolérance aux fautes Etat de lôart et défis » Revue des sciences et technologies de l'information, série TSI, Éditions Hermès Lavoisier, Vol. 25, n. 5, juin-juillet 2006,
599-630 (32p.), doi: http://dx.doi.org/10.3166/tsi.25.599-630.
[20] Crossbow. MICA2 Data sheet. [Online] 2009.
[21] D. Braginsky and D. Estrin, ñRumor routing algorithm for sensor networks,ò in Proceedings of the 1st ACM International Workshop onWireless Sensor Networks and Applications, pp. 22ï 31, Atlanta, Ga, USA, September 2002.
[22] Pravin Bhagwat Charles E.Perkins.Highly dynamic destination-sequenced distance-vector routing(dsdv) for mobile computers.ACM SIGCOMM Computer Communication Review, 24, 1999.
[23] Deshpande P.P. Gireesh Hegde B. Chetan, B.M and S Srinivas. Analysis of dsdv and aodv for disaster management system in coal mines. IEEE Wireless Communications, Networking and Mobile Computing (WiCOM), Sept. 2011.
[24] A. Boukerche, al. A new energy eccient and fault-tolerant protocol for data propagation in smart dust networks using varying transmission range, Journal of computer communications, 29(4) : pages 477-489, 2006.
[25] H. Karl and Willig. Protocols and Architecture for Wireless Sensor Networks. John Wiley and Sons, Hoboken, 2005.
[26] CAldric Adjih Anis Laouiti. Mesures de performances du protocole olsr. projet hipercom. Technical report, Project-Team Hipercom, INRIA, 2003.
[27] P. Jacquet et T. Clausen. Optimized link state routing protocol (olsr). Technical report, IETF RFC3626, Octobre 2003.
[28] A.H. Cevik, T. Zaim. Localized energy efficient routing for wireless sensor networks. IEEE International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS), 2011.

[29] David A. Maltz David B. Johnson and Josh Broch. The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks. In Mobile Computing, Kluwer Academic Publisher, 1996.

[30] A. Almutairi and T. Hendawy. Performance comparison of dynamic source routing in ad-hoc networks. IEEE-GCC Conférence, 2011.

[31] S. R. Das. C. E. Perkins, E. M. Royer. Ad hoc on demand distance vector (aodv) routing. In IETF, Internet Draft, draft-ietf-manet-aodv-05.txt, 2003.

[32] M Shah, R.C. ; Rabaey. Energy aware routing for low energy ad hoc sensor networks. IEEE Wireless Communications and Networking Conférences, 1, 2002.

[33] Pankaj Sharma Charu Gupta. Implémentation of energy aware routing protocol for mobile ad hoc net- works. International Journal of Advanced Research in Computer Science and Software Engineering, 3, 2013.

[34] Nini Wei ; Yi Song. An energy-aware routing strategy based on dynamic priority factor in ad hoc networks. International Conférence on Information Technology, Computer Engineering and Management Sciences (ICM), 2, 2011

[35] J. Chang-jiang et Z. Ying X. Min, S. Weiren. Energy efficient clustering algorithm for maximizing lifetime of wireless sensor networks. International Journal of Electronics and Communications, 64(4), 2010.

[36] H. Balakrishnan. W.R. Heinzelman, A. Chandrakasan. Energy-efficient communication protocol for wireless microsensor networks. Proceedings of the IEEE Hawaii International Conference on System Sciences, 2, 2000