République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Abderrahmane Mira de Béjaïa

Faculté des Sciences Exactes

Département d'Informatique

Mémoire de Master Professionnel

En vue de l'obtention du diplôme master en informatique

Option : Administration et Sécurité des Réseaux

Thème

La tolérance aux pannes dans les réseaux de capteurs sans fil

Présenté par :

BOUKHIAR Amine

Soutenu devant le jury composé de :

Rapporteur	M^{me}. OUYAHIA Samira	Dr	Université A/Mira de Bejaia
Président	M^{me}. BACHIRI Lina	Dr	Université A/Mira de Bejaia
Examinateur	M^{elle}. REBOUH Nadjette	Dr	Université A/Mira de Bejaia

Promotion 2015 – 2016

Remerciements

Je tiens à exprimer ma sincère gratitude envers tout ceux qui m'ont aidés ou ont participé au bon déroulement de ce projet.

Je suis particulièrement reconnaissant à ma promotrice : Mme OUYAHIA Samira d'avoir accepté de m'encadrer et diriger mon travail, je la remercie pour ses qualités humaines et professionnelles, pour sa patience, ses directives, ses remarques constructives et son aide inestimable.

Je tiens à exprimer toute ma grande gratitude aux membres de jury : Mlle REBOUH Nadjette et Mme BACHIRI Lina d'avoir accepté de juger ce travail.

Mes vifs remerciements s'adressent à tous nos enseignants du département d'informatique de l'université Abderrahmane MIRA de Bejaia pour la formation qu'ils ont eu le soin de nous apporter le long de notre cursus universitaire.

Je rends grâce à Dieu, le tout puissant et miséricordieux, de m'avoir donné le savoir, le courage et la force pour mener à bien et à terme ce modeste travail.

Dédicaces

Je dédie ce modeste travail

À mes très chers parents qui ont légué un sens à mon existence, pour leur confiance et leur énorme soutien

À mes merveilleux frères et sœurs pour leur présence et leur appui

À ma famille

À mes précieux amis qui ont toujours cru en moi

Amine

Table des Matières

Liste des figures

Liste des abréviations

ACK Acknowledgment (Acquittement)

CPEQ Cluster-based Periodic Event-driven Query-based

CPU Central Processing Unit

CSMA/CA Carrier Sense Multiple Access / Collusion Avoidance

DIN Dynamic Interference Nullification

EAR Energy Aware Routing

FDMA Frequency Division Multiple Access

HEEC Hierarchical Energy Efficient Clustering

HEER Hybrid Energy Efficient Reactive

IEEE Institute of Electrical and Electronics Engineers

KAT-Mobility K-means And TSP-based Mobility

K–CDS K-Connected K-Dominating Set

LEACH Low-Energy Adaptive Clustering Hierarchy

PEQ Periodic Event-driven Query-based

RAMSS Reliability Availability Maintenability Sefety Security

RCSF Réseaux de Capteur Sans Fil

RMAC Reliable Medium Access Control

RREP Route Replay

RREQ Route Request

TDMA Time Division Multiple Access

TEEN Threshold sensitive Energy Efficient sensor Network protocol

VTRP Variable Transmission Range Protocol

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 d'une unité de calcul, de composants pour la collecte de l'information, et d'une antenne pour transmettre l'information à un centre de contrôle distant. Ces équipements sont appelés nœuds capteurs ou « motes ». Ils ont la capacité de s'auto-organiser pour former un réseau appelé réseau de capteurs. Ces équipements sont généralement déployés dans des environnements hostiles pour surveiller ou collecter de l'information dans un champ de captage. Ils présentent une autonomie d'énergie puisqu'ils sont dotés d'une source d'énergie limitée (batterie) qui est généralement non rechargeable et difficile à la remplacer (1).

En outre, ces nœuds sont sujets à des pannes pour différentes causes (épuisement de l'énergie, écrasement par des animaux, etc). Dans ce cas de figure, il y aurait un grand risque que le réseau perd l'aspect de connectivité et que l'information 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 s'auto-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 connectivité, un autre capteur se trouvant dans son voisinage passe au mode actif pour le remplacer de telle sorte que le réseau soit toujours connecté. Or, dans d'autres cas un capteur peut perdre sa fiabilité et l'information qu'il remonte, est erronée. Dans certaines applications, cette information peut être importante par exemple quand il s'agit de la surveillance d'un patient. De ce fait, la non-fiabilité de l'information 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 l'aspect tolérance aux pannes dans des protocoles et se contentent des mécanismes préventifs par supporter le panne d'un élément, par exemple choisir un deuxième chemin dans un protocole de routage pour tolérer la rupture du chemin principal.

Dans ce travail, nous nous intéressons à proposer une solution pour le problème des nœuds isolés dans le protocole de routage EAR (Enery Aware Routing) qu'il 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 nœud isolé dans le protocole EAR. De ce fait, EAR aura deux mécanismes de tolérance aux pannes préventif (un autre chemin de routage) et curatif (l'augmentation du rayon de transmission).

Pour se faire, nous avons organisé notre travail autour de quatre chapitres encadrés par une introduction et une conclusion :

Le premier s'intitule « généralité sur les réseaux de capteurs », il a pour objectif d'exhiber les réseaux de capteurs sans fil et de présenter leur fonctionnement général, les applications potentielles et les principales caractéristiques.

Le deuxième chapitre est nommé « La tolérance aux pannes dans les réseaux de capteurs », nous présenterons les différentes catégories de pannes qui peuvent survenir durant le cycle de vie d'un réseau de capteurs sans fil, leurs caractéristiques et causes.

L'état de l'art sur les protocoles tolérants aux pannes dans les RCSFs fera l'objet du troisième chapitre.

Le dernier chapitre sera consacré à notre proposition en vu d'améliorer un des protocoles tolérant aux pannes.
Enfin nous conclurons ce travail en résumant les connaissances acquises durant la réalisation de ce projet.

1

Généralités sur les réseaux de capteurs sans fil

Introduction

Les avancées réalisées dans le domaine des technologies de communication sans fil (Wireless Fidelity, Bluetooth,etc.) et de microélectronique (microcontrôleur, Digital Signal Processor,etc.), ont mené à l'apparition de plusieurs nouvelles technologies à un coût de production très réduit, tel que les nœuds capteurs, qui sont capable de générer et d'échanger des données d'une manière autonome et complètement transparente pour les utilisateurs. Les réseaux de capteurs représentent actuellement un nouveau domaine.

Dans ce chapitre, nous présenterons les réseaux de capteurs sans fil, en décrivant leur architecture, leur caractéristiques et nous allons discuter également les principaux facteurs et contraintes qui influencent la conception des réseaux de capteurs sans fil.

1.1 Définition d'un capteur

Un capteur est un dispositif qui transforme l'état d'une grandeur physique observée en une grandeur utilisable, exemple : une tension électrique, une hauteur de mercure, une intensité, la déviation d'une aiguille.

Le capteur se distingue de l'instrument de mesure par le fait qu'il ne s'agit que d'une simple interface entre un processus physique et une information manipulable. Par opposition, l'instrument de mesure est un appareil autonome suffisant à lui-même. Il dispose donc d'un affichage ou d'un système de stockage des données. Ce qui n'est pas forcément le cas du capteur. Les capteurs sont les éléments de base des systèmes d'acquisition de données. Leur mises en œuvre est du domaine de l'instrumentation (2).

1.2 Architecture physique d'un capteur

La figure 1.1 illustre l'architecture physique d'un capteur qui est composé de quatre unités :

Unité d'acquisition: Est composée d'un capteur qui va obtenir des mesures numériques sur les paramètres environnementaux et d'un convertisseur analogique/numérique qui va convertir l'information relevée et la transmettre à l'unité de traitement.

Unité de traitement: Est composée de deux interfaces, une interface pour l'unité d'acquisition et une interface pour l'unité de transmission. Cette unité est également composée d'un processeur et d'un système d'exploitation spécifique. Elle acquiert les informations en provenance de l'unité d'acquisition et les envoie à l'unité de transmission.

Unité de communication: Est responsable de toutes les émissions et réceptions de données via un support de communication radio. Elle peut être de type optique (comme dans les capteurs Smart Dust (3)), ou de type radio-fréquence (MICA2, par exemple).

Ces trois unités sont alimentées par une batterie comme le montre la figure 1.1 :

Unité d'énergie: Il existe une variété d'options pour l'alimentation en énergie pour un nœud capteur. L'option la plus commune est l'utilisation des batteries, d'autres options sont l'énergie de balayage de l'environnement où le nœud capteur est exposé. L'exemple le plus populaire est les piles solaires (4).

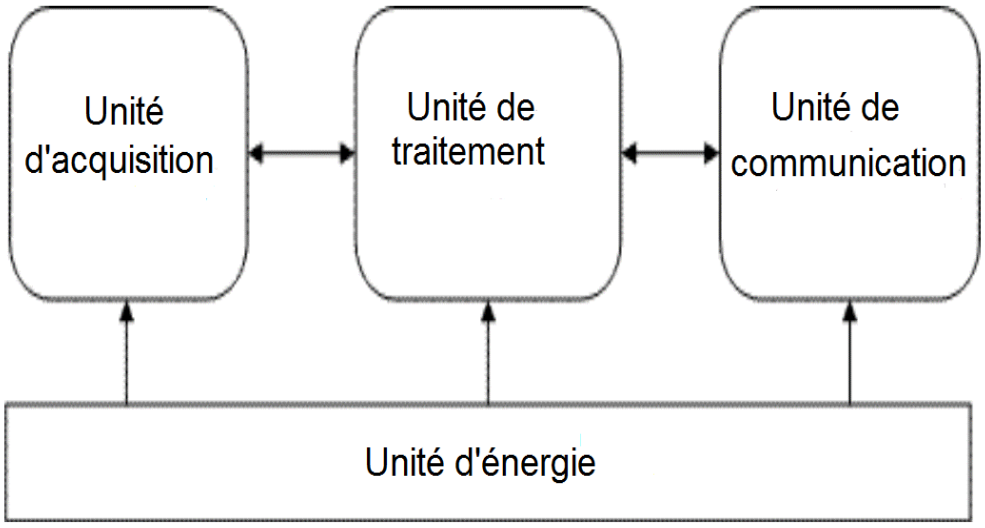


Figure 1.1: Architecture physique d'un capteur.

1.3 Réseaux de capteur sans fil

Un réseau de capteur se définit comme étant un ensemble de capteurs connectés entre eux, où chaque capteur étant muni d'un émetteur-récepteur. Les réseaux de capteurs sans fil(RCSFs)ou Wireless Sensor Networks sont considérés comme un type spécial des réseaux ad hoc où une infrastructure fixe de communication et l'administration centralisée sont absentes et les nœuds jouent, à la fois, le rôle des hôtes et des routeurs. Chaque nœud est capable de surveiller son environnement et de réagir en cas de besoin en envoyant l'information collectée à un ou plusieurs station de base, à l'aide d'une connexion sans fil (5). Comme montré sur la figure 1.2.

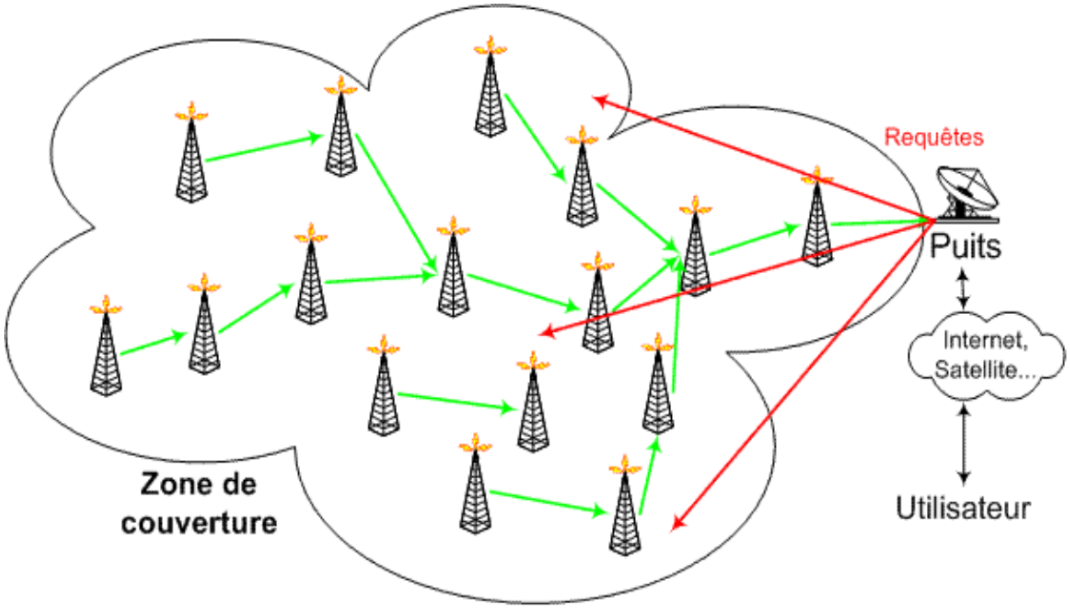


Figure 1.2: Architecture d'un réseau de capteur.

1.4 Caractéristiques et contraintes liées aux réseaux de capteurs sans fil

1.4.1 Le passage à l'échelle

Le nombre de nœuds déployés peut atteindre des millions. Un nombre aussi important de nœuds engendre un trafic énorme dans les réseaux, ce qui entraîne des congestions et des erreurs de communication. Un tel déploiement nécessite que le protocole utilisé pour la communication soit capable de détecter les erreurs et de contrôler les flux et nécessite aussi que la station de base soit équipée d'une capacité suffisante pour accueillir les informations reçues à partir des nœuds capteurs (6). Au futur, les capteurs sans fil sont destinés à avoir des dimensions microscopiques en permettant de les disperser par des milliers voire des dizaines de milliers dans les zones à étudier, ce qui rend ce problème imposant et parmi les plus importants des RCSFs.

1.4.2 L'adressage

Le problème de l'adressage est lié à celui de la mise à l'échelle, le nombre important de capteurs sans fil déployés oblige à se poser des questions sur l'adressage à utiliser. Deux méthodes sont utilisées :

- Identification unique des capteurs : consiste à offrir un identifiant unique à chaque capteur.
- Identification par localisation : consiste à se centrer sur les données en leurs associant un repère spatial.

1.4.3 L'auto-organisation

L'auto organisation s'avère très nécessaire pour ce type de réseau afin de garantir sa maintenance.Vu la topologie instable du réseau de capteur, ce dernier devra être capable de s'auto-organiser pour continuer ses applications.

1.4.4 Les contraintes matérielles

Parmi les contraintes matérielles liées au RCSFs, on peut citer :

La dimension : la taille réduite des nœuds capteurs peut représenter plusieurs avantages, et elle permet un déploiement flexible et simple du réseau. Cependant, la puissance des batteries utilisées pour alimenter les nœuds capteurs est limitée par la petite taille de ces derniers.

La puissance de calculs : les réseaux de capteurs sont différents par rapport aux réseaux traditionnels. Parmi les principaux points de différence, nous pouvons citer la puissance de calcul. Les nœuds capteurs utilisent souvent des microcontrôleurs de faible fréquences.

1.4.5 L'environnement

Les capteurs sont souvent déployés en masse dans les endroits hostiles tels que les champs de batailles au-del à des lignes des ennemis, à l'intérieure de grandes machines, etc. Par conséquent, ils doivent pouvoir fonctionner sans surveillance dans les régions géographiquement éloignées ou inaccessibles.

1.4.6 La topologie dynamique

La topologie des réseaux de capteurs peut changer au cours du temps pour les raisons suivantes:

- Les nœuds capteurs peuvent être déployés dans des environnements hostiles (champs de batailles par exemple), la défaillance d'un nœud capteur est donc plus probable.
- Un nœud capteur peut devenir non opérationnel à cause de l'expiration de son énergie.
- Dans certaines applications, les nœuds capteurs et la station de base sont mobiles (8).

1.4.7 La consommation d'énergie

Comme les nœuds capteurs sont des composantes microélectroniques, ils sont équipés d'un ou plusieurs batteries normales et irremplaçables, par conséquent cette ressource est la plus précieuse dans les réseaux de capteurs car la durée de vie des nœuds capteurs dépend fortement de la durée de vie de sa batterie. De ce fait, la faible consommation d'énergie est une exigence principale pour les applications où une longue durée de vie de réseau est nécessaire (11).

1.4.8 La tolérance aux pannes

La tolérance aux pannes c'est la capacité de maintenir les fonctionnalités du réseau sans interruption en cas de défaillance d'un nœud capteur. Afin d'assurer la communication entre la station de base et les autres nœuds d'un réseau de capteur, les protocoles de routage sont basés sur la communication multi-sauts. Chaque nœud joue alors, en plus du rôle de source de données, le rôle d'un routeur. Toutefois, ces nœuds sont sujets à de nombreuses pannes, dues principalement à l'épuisement des batteries et aux destructions physiques.Ainsi, la panne de nœuds entraîne la perte des liens de communication et donc un changement significatif dans la topologie globale du réseau. Ceci peut affecter d'une façon considérable la connectivité du réseau et diminuer, en conséquence, sa durée de vie. Ceci est justement l'objet de notre étude dans le chapitre suivant, qui traitera plus en détail la tolérence aux pannes(7).

1.5 Applications des réseaux de capteurs sans fil

1.5.1 Classification des applications

Les réseaux de capteurs sans fil ont été classés parmi les 21 technologies les plus importantes du 21 ème siècle. En effet, la recherche dans le domaine des capteurs est entrain de vivre une révolution importante, ouvrant des perspectives d'impacts significatifs dans de nombreux domaines. Ainsi, on classifie les applications des RCSFs en quatre classes d'applications : orientées temps (time driven), orientées événements (event driven), orientées requêtes (query driven) et hybride (9).

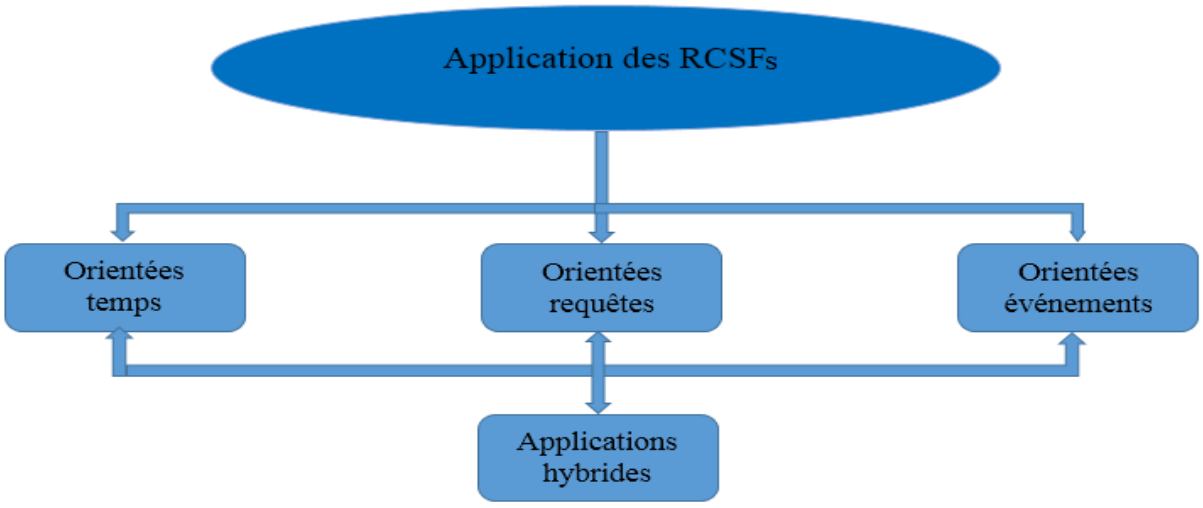


Figure 1.3: Classification des applications des RCSFs.

1.5.1.1 Applications orientées temps

Cette classe représente les applications où l'acquisition et la transmission des données capturées sont liées au temps : instant précis, période d'acquisition. Cette période d'acquisition peut être plus ou moins longue selon l'application (de quelques secondes jusqu'à quelques heures voire des jours). Ainsi, la quantité de données échangée dans le réseau dépend de la périodicité des mesures à effectuer sur l'environnement local. La collecte de données environnementales peut représenter un bon exemple de cette classe d'application dans des domaines variés : agriculture, expérimentation scientifique, etc (9).

1.5.1.2 Applications orientées événements

Dans ce cas, les capteurs envoient leurs données seulement si un événement spécifique se produit. On peut citer l'exemple de surveillance des feux dans les forêts où un capteur envoie des alarmes à la station de base dès que la température dépasse un certain seuil. Au départ, cette classe d'application était conçue à des fins militaires, comme la surveillance du déplacement d'objets dans le champ de bataille. Par la suite, cette classe a rapidement trouvé de nouvelles perspectives comme le contrôle industriel, le contrôle médical des patients, la surveillance d'édifices (barrages, ponts, voies de chemins de fer,etc)(9).

1.5.1.3 Applications orientées requêtes

Dans ce cas, un capteur envoie de l'information uniquement suite à une demande explicite de la station de base. Cette classe d'application est destinée aux applications adaptées à l'utilisateur. Ce dernier peut requérir des informations à partir de certaines régions dans le réseau ou interroger les capteurs pour acquérir des mesures d'intérêts. Dans ce cas, des connaissances sur la topologie du réseau et l'emplacement des capteurs sont nécessaires (9).

1.5.1.4 Applications hybrides

Ce type d'application met en œuvre les trois modes de fonctionnement décrits précédemment. Par exemple, dans un réseau conçu pour le suivi d'objets, le réseau peut combiner entre un réseau de surveillance (time driven) et un réseau de collecte de données par événements (event driven). Par exemple, pendant les longues périodes d'inactivité des capteurs et lorsque aucun objet n'est présent, le réseau peut assurer une fonction de surveillance.

1.5.2 Les domaines d'applications

1.5.2.1 Application militaire

Comme pour de nombreuses autres technologies, le domaine militaire a été le moteur initial pour le développement des réseaux de capteurs (10).

Le déploiement rapide, l'auto organisation et la tolérance aux pannes des réseaux de capteurs sont des caractéristiques qui font de ce type de réseaux un outil appréciable dans un tel domaine. Actuellement, les RCSFs peuvent être une partie intégrante dans le commandement, le contrôle, la communication, la surveillance,etc.

1.5.2.2 Applications médicales

Les réseaux de capteurs sont également largement répandus dans le domaine médical. Cette classe inclut des applications comme : fournir une interface d'aide pour les handicapés, collecter des informations physiologiques humaines de meilleure qualité, et surveiller en permanence les malades et les médecins á l'intérieur de l'hôpital (10).

1.5.2.3 Applications environnementales

Dans ce domaine, les capteurs peuvent être exploités pour détecter les catastrophes naturelles, détecter des fuites des produits toxiques (gaz, produits chimiques, pétrole, etc.) dans des sites industriels tels que les centrales nucléaires et les pétrolières (10).

1.5.2.4 Applications commerciales

Parmi les domaines dans lesquels les réseaux de capteurs ont aussi prouvé leur utilité, on trouve le domaine commercial (10). Dans ce secteur,on peut énumérer plusieurs applications comme la surveillance de l'état du matériel, le contrôle et l'automatisation des processus d'usinage, etc.

1.5.2.5 Applications á la sécurité

Les altérations dans la structure d'un bâtiment, suite à un séisme ou à un vieillissement, peuvent être détectées par des capteurs intégrés dans les murs ou dans le béton. Un RCSF de mouvements peut constituer un système d'alarme distribué qui sert à détecter les intrusions sur un large secteur (10).

1.6 La communication dans les RCSFs

La pile des protocoles utilisés par une station de base ou capteur est donnée dans la figure 1.4. Cette pile combine l'énergie et le routage, intègre les données avec les protocoles réseaux, communique efficacement à travers un médium sans fil et permet des efforts coopératifs entre les nœuds capteurs.

La pile consiste en couches application, transport, réseau, liaison de données, physique et trois plans de gestion d'énergie, de mobilité et de tâche. Les plans de gestion d'énergie,de mobilité et de tâche contrôlent l'énergie, le mouvement et la distribution de tâche au sein d'un nœud capteur. Ces plans aident les nœuds capteurs à coordonner la tâche de capter et minimiser la consommation d'énergie.Ils sont donc nécessaires pour que les nœuds capteurs puissent collaborer ensemble, acheminer les données dans un réseau mobile et partager les ressources entre eux en utilisant efficacement l'énergie disponible. Ainsi, le réseau peut prolonger sa durée de vie (8).

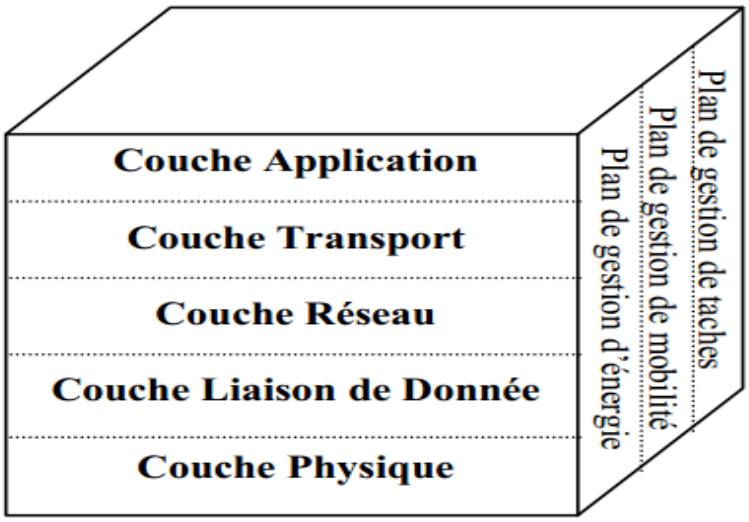


Figure 1.4: La pile protocolaire dans les réseaux de capteurs.

Conclusion

Les réseaux de capteurs sans fil se propagent dans plusieurs domaines d'application. Ils sont devenus indispensables pour les mesures de certaines grandeurs physiques telles que la température, l'humidité, la vibration ou physiologiques. Cependant, les pannes sont inévitables dans ce type de réseaux. Ces pannes peuvent avoir des conséquences catastrophiques. De ce fait, il est nécessaire de prendre en considération l'aspect tolérance aux pannes dans la plupart des protocoles conçus pour les réseaux de capteurs.

Le chapitre suivant sera consacré à la tolérance aux pannes dans les réseaux de capteurs sans fil et son utilité.

2

La tolérance aux pannes

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. Dans ce chapitre, nous parlerons de la tolérance aux pannes dans les systémes distribués puis dans les RCSFs.

2.1 Généralités sur la tolérance aux pannes dans les systèmes distribués

Dans cette partie, nous allons présenter des généralités sur la tolérance aux pannes dans les systèmes distribués. Donc, nous allons introduire une notion importante dans les systèmes distribués, c'est la sûreté de fonctionnement. Après quoi, nous présenterons les mécanismes de la tolérance aux pannes.

2.1.1 Sûreté de fonctionnement

La sûreté de fonctionnement peut être présentée autour des trois notions suivantes: attributs, entraves et moyens. Cette décomposition est schématisée par l'arbre de la figure 2.1 (12).

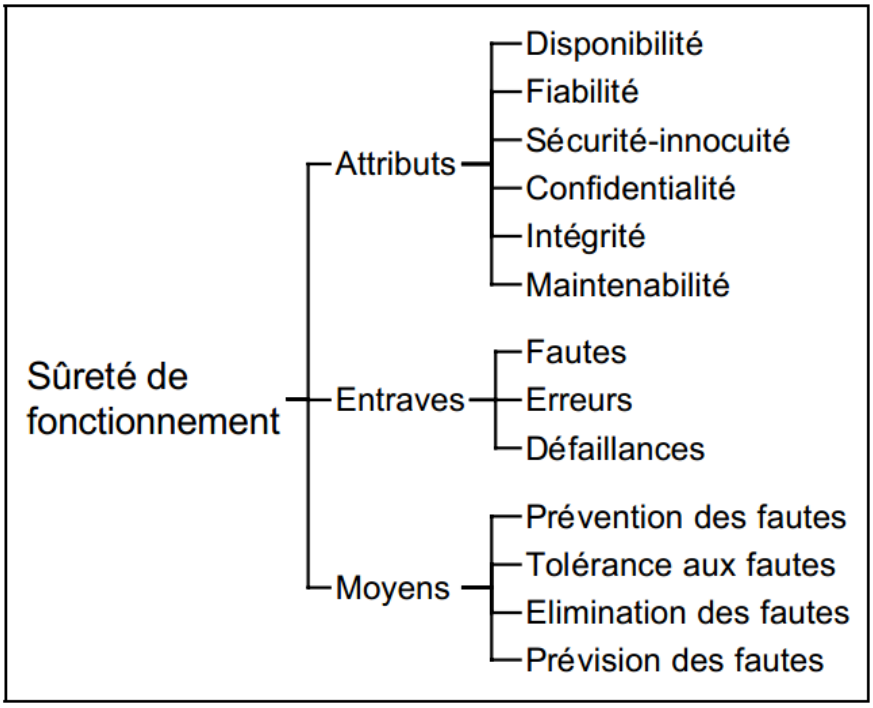


Figure 2.1: L'arbre de la sûreté de fonctionnement.

2.1.1.1 Attributs de la sûreté de fonctionnement

Les attributs de la sûreté de fonctionnement sont parfois appelés FDMS pour Fiabilité, Disponibilité, Maintenabilité et Sécurité (RAMSS pour Reliability, Availability, Maintenability, Safety, Security) (13).

Disponibilité : la disponibilité est l'aptitude d'une entité à être en état d'accomplir une fonction requise dans des conditions données, à un instant donné ou pendant un intervalle de temps donné, en supposant que la fourniture des moyens extérieurs nécessaires soit assurée.

Fiabilité : la fiabilité (reliability) est l'aptitude d'un dispositif à accomplir une fonction requise dans des conditions données pendant une durée donnée.

Sécurité : le réseau de capteurs doit assurer la protection des RCSFs et la diffusion de données (résilience aux attaques). La sécurité est l'aptitude à ne pas provoquer d'accidents catastrophiques.

Maintenabilité : dans les conditions d'utilisation données, la maintenabilité est l'aptitude d'une entité à être maintenue ou rétablie, sur un intervalle de temps donné dans un état dans lequel elle peut accomplir une fonction requise, lorsque la maintenance est accomplie dans des conditions données avec des procédures et des moyens prescrits.

Confidentialité : correspond à l'absence de divulgation non autorisée de l'information.

Intégrité : indique l'absence d'altérations inappropriées de l'information.

2.1.1.2 Entraves à la sûreté de fonctionnement

Les entraves à la sûreté de fonctionnement sont de trois types : les pannes, les erreurs et les défaillances.

1. **La panne :** toute cause (événement, action, circonstance) pouvant provoquer, une erreur menant à la défaillance du système tel qu'il ne se comporte plus d'une manière pré-spécifiée (14). Elle peut être :
   - **Panne permanente :** elle persiste dès qu'elle apparaît jusqu'à la réparation.
   - **Panne transitoire :** elle se produit de manière isolée.
   - **Panne intermittente :** elle se produit aléatoirement plusieurs fois.
2. **L'erreur :** l'erreur est la partie de l'état du système susceptible d'entraîner la défaillance, qui est causée par une faute (15). S'il y a une erreur dans l'état de système, alors il existe une séquence d'actions qui peut être exécutée par le système et qui mènera à la défaillance du système (16).
3. **La défaillance :** la défaillance dénote l'incapacité d'un composant d'exécuter sa fonction en raison des erreurs dans l'élément ou son environnement (17). Quatre sources de faute peuvent causer la défaillance d'un système :
   - Une spécification inadéquate ;
   - Des erreurs de conception dans le logiciel ;
   - Une défaillance de processeur ;
   - Une interférence sur le sous-système de communication ;

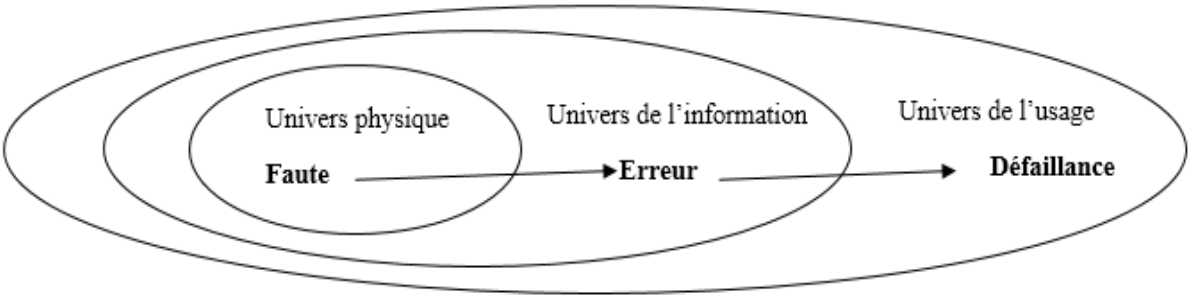


Figure 2.2: De la faute à la défaillance

2.1.1.3 Moyens d'assurer la sûreté de fonctionnement

Les moyens utilisés pour assurer la sûreté de fonctionnement sont définis par les méthodes et les approches utilisées pour assurer cette propriété. Les approches les plus connues sont (13):

La prévention des pannes : qui s'attache aux moyens permettant d'éviter l'occurrence de fautes dans le système. Ce sont généralement les approches de vérification des modèles conceptuels;

L'élimination des pannes : qui se focalise sur les techniques permettant de réduire la présence de fautes ou leurs impacts. Cela est réalisé par des méthodes statiques de preuve de la validité du système (simulation, preuves analytiques, tests, etc.);

La prévision des pannes : qui prédit l'occurrence des fautes (temps, nombre, impact) et leurs conséquences. Ceci est réalisé généralement par des méthodes d'injection de fautes afin de valider le système relativement à ces fautes ;

La tolérance aux pannes : qui essaye de fonctionner en dépit des fautes. Le degré de tolérance aux pannes se mesure par la capacité du système à continuer à délivrer son service en présence de fautes.

2.1.2 Tolérance aux pannes

La tolérance aux fautes est l'ensemble de techniques de conception qui permet à un système de continuer à fonctionner et fournir ses services même en présence de fautes. Elle est mise en œuvre par la détection d'erreur et le rétablissement du système.

2.1.2.1 Détection d'erreurs

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 s'exécutent quand le système est inactif. La détection en ligne vise l'identification de pannes en temps réel et est effectuée simultanément avec l'activité du système. Les formes les plus courantes de détection d'erreur sont : les duplications et les comparaisons, les contrôles temporels, et les contrôles de vraisemblance (18).

La méthode de duplication et comparaison : utilise au moins deux unités redondantes qui doivent être indépendantes vis-à-vis des fautes que l'on souhaite tolérer : typiquement, redondance des composants matériels pour les fautes physiques, et diversification pour des fautes de conception.

Le contrôle temporel : est typiquement utilisé pour détecter la défaillance d'un périphérique en vérifiant que son temps de réponse ne dépasse pas une valeur-seuil, ou pour surveiller périodiquement l'activité d'une unité centrale.

Le contrôle de vraisemblance : cherche à détecter des erreurs en valeur aberrantes pour le système. Il peut être mis en œuvre soit par du matériel pour détecter par exemple des adresses mémoires erronées, soit par du logiciel pour vérifier la conformité des entrées, des sorties ou des variables internes du système par rapport à des invariants.

2.1.2.2 Rétablissement du système

Parmi les techniques de traitement d'erreur, on distingue (19):

1. **La reprise :** qui consiste à sauvegarder périodiquement l'état du système pour le ramener dans un état antérieur à la détection d'erreur.

2. **La poursuite :** qui consiste à créer un nouvel état à partir duquel le système peut continuer à fonctionner de façon acceptable.

3. **La compensation :** qui consiste à utiliser des redondances présentes dans le système pour fournir un service correct en dépit des erreurs. Cette compensation peut être consécutive à une détection d'erreur (détection et compensation), ou appliquée systématiquement (masquage d'erreur). Le traitement de panne peut se faire en quatre phases successives :

   - **Le diagnostic :** a pour but d'identifier la localisation et le type de la faute responsable de l'état erroné du système.
   - **L'isolement :** consiste à exclure la participation du composant erroné de la délivrance du service, par moyen physique ou logiciel.
   - **La reconfiguration :** cherche à compenser l'isolement du composant défaillant, soit en basculant sur des composants redondants, soit en réassignant ses tâches à d'autres composants.
   - **La réinitialisation :** vérifie et met à jour la nouvelle configuration du système.

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

La limitation d'énergie dans les RCSFs, et les environnements hostiles dans lesquels ils pourraient être déployés,sont des facteurs qui rendent ce type de réseaux très vulnérables. Ainsi la perte de connexions sans fil peut être due à une extinction d'un capteur suite à un épuisement de sa batterie ou tout simplement à une destruction physique accidentelle ou intentionnelle par un ennemi. Par ailleurs, l'absence de sécurité physique pour ce type de capteurs et la nature vulnérable des communications radios sont des caractéristiques qui augmentent les risques de pannes sur ce type de réseau. Il est donc nécessaire de considérer la tolérance aux pannes comme critères indispensable dans la conception et la mise en œuvre des protocoles des réseaux de capteurs sans fil.

2.2.1 Sources des pannes dans les réseaux de capteurs

Les réseaux de capteurs sont sujets à une grande variété de fautes et à un manque de fiabilité. Le matériel peu couteux, les ressources limitées et les extrêmes conditions environnementales contribuent tous à causer ces fautes. Plusieurs sources peuvent endommager le bon fonctionnement d'un réseau de capteurs, la figure 2.3 (12) présente une classification des composants d'un RCSF qui peuvent souffrir des fautes.

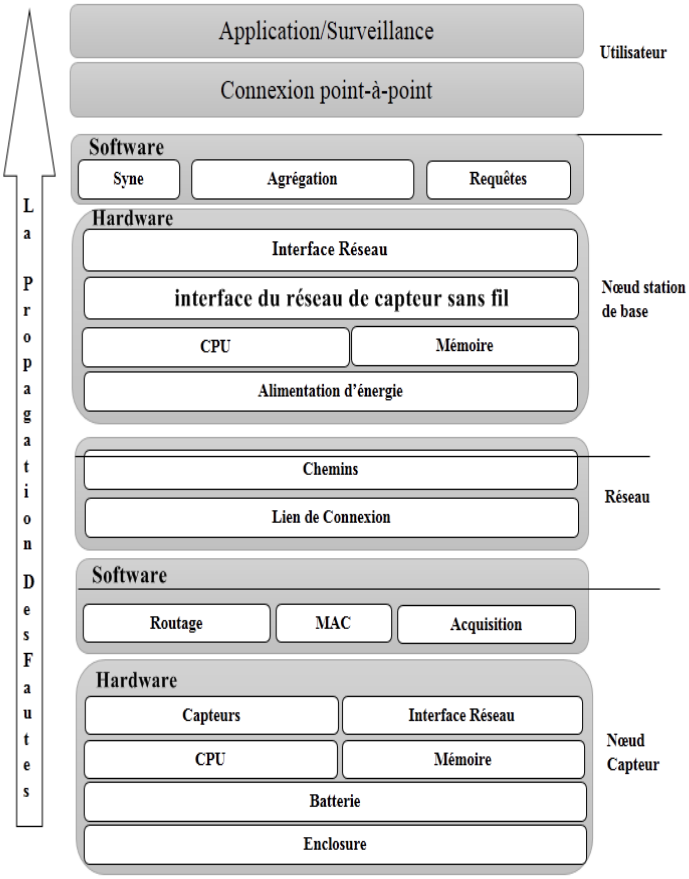


Figure 2.3: Classification et propagation de faute.

2.2.1.1 Pannes au niveau du nœud

Les nœuds ont plusieurs composants matériels et logiciels qui peuvent mal fonctionner. Ce disfonctionnement peut avoir pour origine les conditions extrêmes issues de l'environnement auxquelles sont soumis les nœuds du réseau. Quand la batterie d'un nœud atteint un certain niveau (bas), les captures du nœud peuvent être incorrectes. Comme il est montré dans la figure 2.3, les défaillances matérielles génèrent des défaillances logicielles. Cependant, quelques erreurs matérielles n'affectent pas tous les services d'un nœud, celui-ci peut être utilisé pour d'autres têches par exemple s'occuper du routage des paquets. Les bugs logiciels sont les plus souvent sources d'erreurs dans les réseaux de capteurs. Dans (20), les chercheurs ont remarqué qu'un bug logiciel a causé la plus longue panne du réseau, rendant le système non fonctionnel pendant trois jours jusqu'à la reprogrammation manuelle des nœuds.

2.2.1.2 Pannes au niveau du réseau

Le routage est l'une des fonctions principales des nœuds dans un RCSF. Il est essentiel pour la collecte des données, la distribution, la mise à jour, et la coordination entre les nœuds. Les liens de communications entre les nœuds sont volatiles, le rendement des RCSFs n'est pas toujours constant, le taux de livraison des messages dans les tests du laboratoire ne correspond pas à la réalité. Les interférences radio peuvent causer une faute de connexion entre les nœuds. Une autre source de défaillance de liens d'interconnexion est la collision de messages. Dans (21), les

chercheurs ont observé un potentiel de collisions des messages des nœuds à cause du changement fréquent de topologie. Dans d'autres situations, les nœuds peuvent avoir de bons liens de connexions mais les messages ne sont pas délivrés à cause des erreurs du chemin. Les bugs logiciels dans le routage (couche réseau) peuvent générer des chemins circulaires ou simplement des destinations incorrectes.

2.2.1.3 Pannes au niveau du nœud puit

Les fautes peuvent aussi affecter le noeud station de base. Si ce noeud tombe en panne, même si les noeuds collecteurs fonctionnent correctement, tout le réseau devient inutilisable, car les données collectées ne seront jamais délivrées à l'utilisateur final. La station de base peut être déployé dans un environnement où ils n'y a pas de générateur d'énergie, dans un tel cas, les batteries solaires sont employées pour produire assez d'énergie. Mais en cas de manque d'exposition solaire, cette technique n'est pas efficace, le noeud station de base peut souffrir d'un manque d'énergie (21).

2.2.2 Classification des solutions de tolérance aux pannes dans les RCSFs

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.

2.2.2.1 Classification selon la phase de traitement

Dans cette classification, l'ensemble des algorithmes sont divisés en deux catégories selon la phase de traitement. Si le traitement est effectué avant la panne, on parle donc d'algorithmes préventifs sinon les algorithmes sont dits curatifs.

- **Algorithme préventif :** implémente des techniques tolérantes aux pannes qui tentent de retarder ou éviter tout type d'erreur afin de garder le réseau fonctionnel le plus longtemps possible. La conservation d'énergie, à titre d'exemple, permet de consommer moins d'énergie et évite donc une extinction prématurée de la batterie ce qui offre une tolérence aux panne des nœuds.

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

2.2.2.2 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 d'énergie entre les différents nœuds capteurs, afin de mieux gérer la consommation d'énergie et augmenter ainsi la durée de vie de tout le réseau. En outre, le mécanisme de mise en veille est une technique de gestion de batterie. En effet, les protocoles déterminent des délais de mise en veille des nœuds capteurs inactifs pour une meilleure conservation d'énergie (22).

- **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.) (22).

  1. **Routage multi-chemin :** utilise un algorithme préventif pour déterminer plusieurs chemins depuis chaque capteur vers le nœud puits. Ceci garantit la présence de plus d'un chemin fiable pour la transmission et offre une reprise rapide du transfert en cas de panne sur le chemin principal en choisissant un des chemins qui restent.
  2. **Recouvrement de route :** après la détection de panne, une technique curative permet de créer un nouveau chemin qui soit le plus fiable pour retransmettre les données.
  3. **Allocation de canal :** cette solution est implémentée au niveau de la couche MAC. Elle permet d'effectuer une allocation du canal de transmission d'une manière à diminuer les interférences entre les nœuds voisins et éviter les collisions durant le transfert.
  4. **Mobilité :** certains protocoles proposent comme solution tolérante aux pannes la sélection d'un ensemble de nœuds mobiles chargés de se déplacer entre les capteurs et collecter les données captées. Ceci réduira l'énergie consommée au niveau de chaque capteur en éliminant sa tâche de transmission. Un nœud mobile est généralement doté d'une batterie plus importante que celle d'un nœud capteur.

- **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 (23) :

  1. **Agrégation :** considérée comme approche préventive, l'opération d'agrégation effectue un traitement supplémentaire sur les données brutes captées depuis l'environnement. Un nœud station de base combine les données provenant de plusieurs nœuds en une information significative. Ce qui réduit considérablement la quantité de données transmises en consommant moins d'énergie pour leur dissémination. Ceci permet donc d'augmenter la durée de vie du réseau (23).
  2. **Clustering :** une des importantes approches pour traiter la structure d'un réseau de capteurs est le clustering. Il permet la formation d'un backbone virtuel qui améliore l'utilisation des ressources rares telles que la bande passante et l'énergie. Par ailleurs, le clustering aide à réaliser du multiplexage entre 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 (23).

2.2.2.3 Classification selon le niveau d'implémentation

Cette classification permet de répartir les protocoles sur les différentes couches de l'architecture des réseaux de capteurs. Ainsi, les algorithmes de routage sont au niveau réseau, les techniques de sélection de canal sur la couche MAC, etc.

Conclusion

Dans ce chapitre, nous avons fait le tour sur le concept de tolérance aux pannes, ses définitions générales ainsi que les différentes étapes de sa procédure. Plus spécialement nous avons étudié cette aspect dans les réseaux de capteurs sans fil. Nous avons vu les différentes pannes qui peuvent affectées ce type de réseau.
Ainsi, nous avons remarqué que la tolérance aux pannes dans un tel système (RCSF) est indispensable pour que le réseau soit toujours fonctionnel.

3

Etat de l'art sur les protocoles tolerants aux pannes dans les RCSFs

Introduction

La tolérance aux pannes a connu une importance considérable parmi les différents domaines de recherche dans les réseaux de capteurs sans fil; dus à leurs contraintes d'énergie, d'environnement et de déploiement. Ce dernier, étant d'un coût prohibitif, présente un handicap pour la réorganisation du réseau en cas de panne d'un ou plusieurs de ses capteurs. D'où, il était impératif d'introduire un mécanisme de tolérance aux pannes dans tous les protocoles implémentés au niveau des différentes couches de l'architecture RCSF afin de garantir le bon fonctionnement du réseau même après la faille de certains de ses composants.
Dans ce chapitre, nous avons citer quelques approches de maintien de la connectivité dans les réseaux de capteurs ans fil.

3.1 Approches tolérantes aux pannes dans la couche MAC

Avoir un réseau dense augmente la tolérance aux pannes et la robustesse du système grâce à la notion de redondance. Cependant, une mauvaise gestion peut aboutir à plusieurs collisions durant la transmission aussi bien qu'à la congestion du réseau. D'où, il est impératif de concevoir un protocole MAC au niveau de la couche liaison de données qui garantit la livraison des messages via des liens sans fil. Les solutions de la littérature proposées à ce niveau de couche utilisent un algorithme préventif contre les pannes, c'est-à-dire, éviter les collisions durant la livraison des données (en éjectant des délais d'attente, des mécanismes d'écoute de canal, etc.) afin de garantir la fiabilité de transmission. La tolérance aux pannes est donc assurée par une phase de prévention de pannes avant transmission.

3.1.1 DIN (Dynamic Interference Nullification)

Saffre et al (40), présente un algorithme distribué pour la sélection de canal de transmission avec génération de liens fiables dépourvus d'interférence entre les différents nœuds voisins, afin d'assurer l'émergence du réseau. Ainsi, DIN modélise la tolérance aux pannes par une opération de prévention contre les collisions en évitant au mieux l'effet d'interférence présent entre les voisins directs tout en minimisant la consommation d'énergie au niveau de chaque nœud. Basé sur les deux protocoles FDMA/TDMA, l'algorithme combine la sélection aléatoire d'intervalles de fréquences/temps avec différents niveaux de consommation d'énergie pour la transmission, ceci pour minimiser la probabilité de collision au niveau du récepteur final mais en se basant uniquement sur l'information disponible localement (au niveau des voisins du nœud émetteur).

L'algorithme DIN est modélisé par le problème de coloration de graphe où chaque nœud doit occuper une couleur (ou canal) différente de celle de chacun de ses voisins directs ainsi que les voisins de distance 2 (les voisins de ses voisins) afin d'éviter les interférences au niveau de leur premier voisin commun. La difficulté dans cet algorithme vient de la nécessité d'accomplir cet objectif pour une distribution irrégulière (aléatoire) et imprévisible des composants du réseau de capteurs.

DIN a été simulé dans un réseau militaire pour la détection de mouvement des véhicules ; il a montré une efficacité dans la sélection de canal de transmission en minimisant les interférences ainsi que la consommation d'énergie.

3.1.2 RMAC (Reliable Medium Access Control)

De même que l'algorithme DIN, le protocole RMAC (25) utilise la technique de prévention de collisions pour garantir une transmission fiable des données, et offrir ainsi une bonne tolérance aux pannes dans tout le réseau. Pour cela, RMAC traite les différents problèmes au niveau MAC tels que la congestion, la collision, la latence, puis définit des mécanismes spécifiques basés sur l'approche CSMA/CA, il repose donc sur deux principaux concepts (voir figure 3.1) :

- Mécanisme d'écoute de la porteuse qui assure que le canal est disponible pour la transmission (aucun nœud n'est entrain d'utiliser ce canal) ;
- Utilisation du schéma de retard (backoff) pour réduire le conflit et éviter les collisions. L'idée est de retenir le nœud de l'accès au canal pour une durée aléatoire dans l'espoir que le canal soit libéré après cette période.

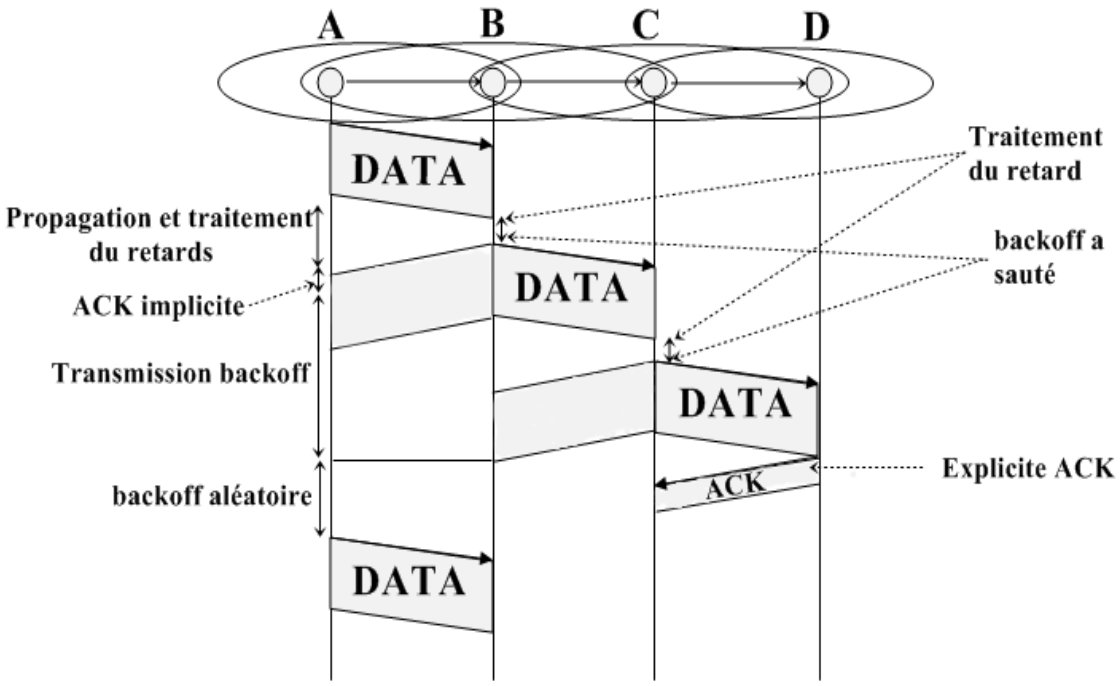


Figure 3.1: RMAC

3.2 Approches tolérantes aux pannes dans la couche réseau

Dans cette section, nous présentons les approches tolérantes aux pannes dans la couche réseau.

Les réseaux de capteurs utilisent une communication multi-sauts. Comparée à une communication sans fil à longue distance, la communication multi-sauts présente une bonne solution pour le problème de propagation de signal et effets de dégradation de signal. De plus, il est recommandé pour ce type de communication de choisir le meilleur chemin qui soit de lien fiable, consomme le moins d'énergie et assure la livraison des données au nœud station de base. Les solutions proposées à ce niveau de couche sont classifiées en trois principales catégories : routage, agrégation et clustering .

3.2.1 Solutions de routage tolérantes aux pannes

Les protocoles de routage permettent de choisir les meilleurs chemins pour acheminer la donnée depuis la source vers l'utilisateur final. Par ailleurs, ils permettent de sélectionner un chemin de secours en cas d'échec d'envoi sur la route principale, à cause d'une panne au niveau d'un ou plusieurs capteurs de cette route.

3.2.1.1 PEQ (Periodic, Event-driven, Query-based)

La motivation de cet algorithme vient du besoin de répondre à toutes les contraintes : faible latence, fiabilité, recouvrement rapide en cas de panne et conservation d'énergie. PEQ(26) combine la conservation d'énergie avec le routage multi-chemins en sélectionnant parmi toutes les routes disponibles, celles qui consomment moins d'énergie. En plus de ce mécanisme préventif

qui permet un routage fiable, un mécanisme de recouvrement de pannes est implémenté. Ce dernier remplace le chemin en panne par une autre route qui soit de liens fiables et consomme moins d'énergie. Ainsi, le protocole PEQ couvre la procédure de tolérance aux pannes par la gestion de la consommation d'énergie, la sélection des meilleures routes puis leur recouvrement en cas de panne (26).
PEQ introduit le paradigme Publish/Subscribe comme montre la figure 3.2 (26) pour l'interaction entre la station de base et les capteurs simples. En effet, les capteurs envoient des notifications d'événements à la station de base, qui va souscrire son intérêt pour certaines de ces informations. Les capteurs concernés publient par la suite l'information désirée.

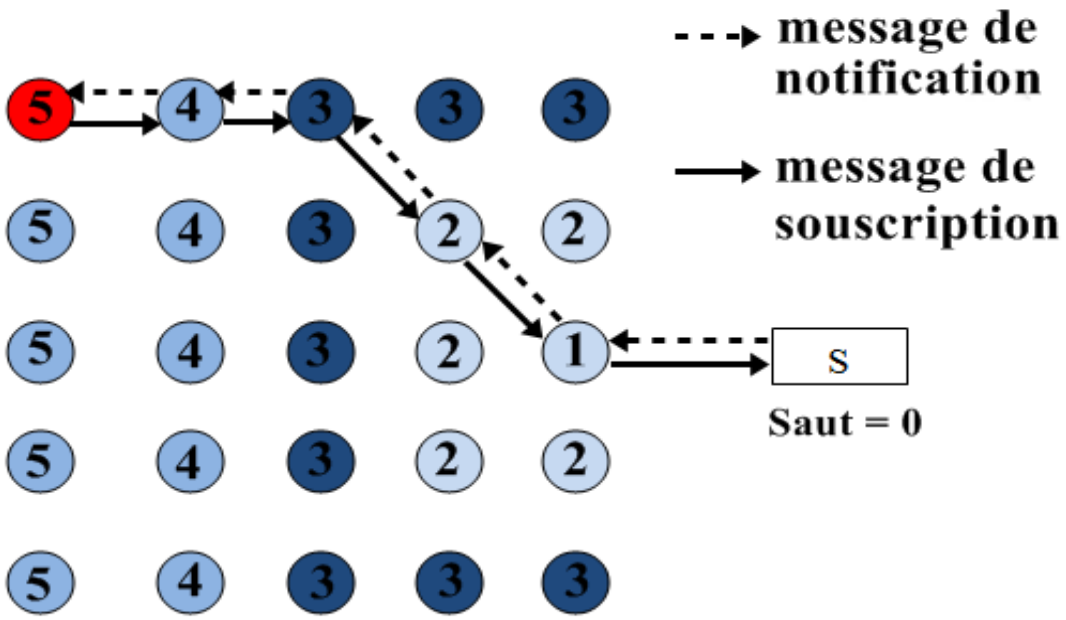


Figure 3.2: Mécanisme Publish/Subscribe

Les quatre principales phases du protocole sont:

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

- **Transmission de paquets de notification :** chaque capteur envoie selon sa table de routage et l'événement capté, une notification de l'information qu'il a à sa disposition. Pour cela, il utilise le chemin le plus rapide et le moins coûteux en terme d'énergie

- **Propagation des paquets de souscription :** dans cette étape, après une souscription, par la station de base, des données à transmettre, chaque capteur achemine cette dernière jusqu'au capteur concerné.
- **Mécanisme de recouvrement de route :** le recouvrement est effectué après détection de pannes (figure 3.3) (26). Un capteur envoie son paquet puis attend un acquittement ACK. S'il le reçoit, le message a été bien transmis, sinon une panne est détectée au niveau du chemin de routage. On effectue donc une recherche "SEARCH" pour la sélection d'un autre capteur destination tout en minimisant le coût du nouveau chemin. Si aucun capteur n'est trouvé (tous les voisins sont détruits) le capteur devient isolé et doit donc augmenter son rayon de transmission radio pour atteindre les capteurs voisins lointains.

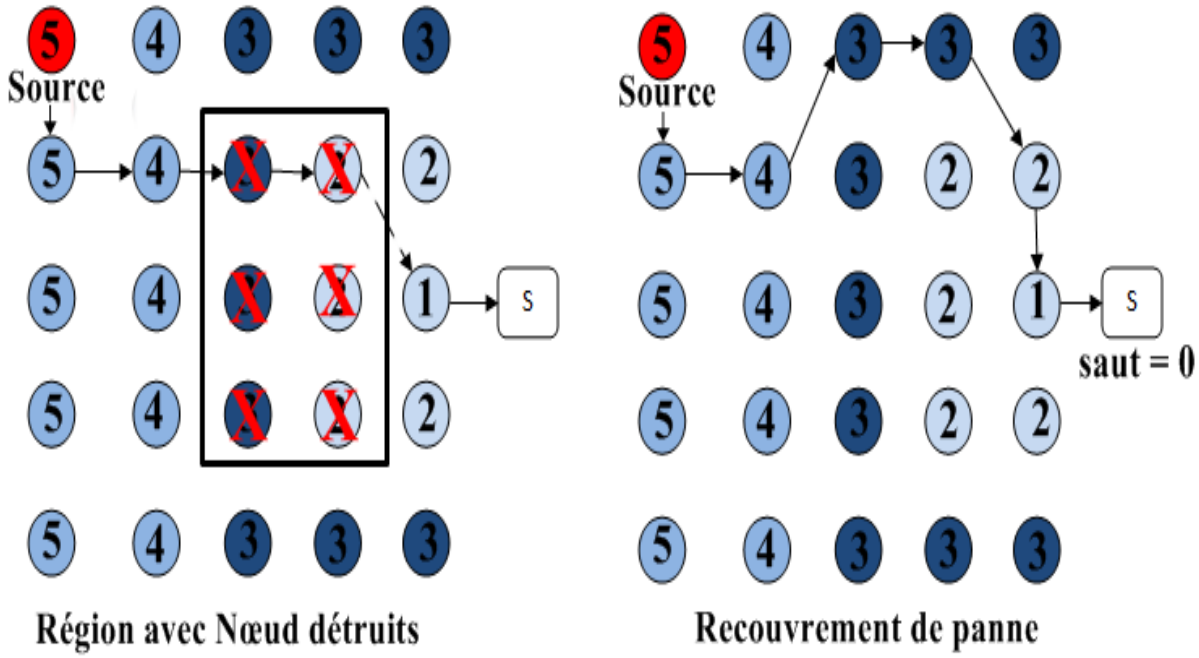


Figure 3.3: Recouvrement de routes dans PEQ

3.2.1.2 Protocole EAR(Energy Aware Routing)

Une solution hybride pour la tolérance aux pannes est proposée dans le protocole EAR qui a un aspect préventif. EAR offre une meilleure conservation d'énergie et définit plusieurs chemins de routage afin de garantir une fiabilité du transport et d'augmenter la durée de vie du réseau. En outre, un mécanisme de recouvrement de pannes est implémenté. Le protocole EAR supporte des réseaux de capteurs avec multiples station de base. Chaque capteur génère un paquet RPT contenant des informations pour les préférences de l'utilisateur. Les paquets RPT peuvent être envoyés vers n'importe quelle station de base. Cependant, pour chaque capteur intermédiaire le protocole de routage choisit le meilleur chemin qui réduit la consommation d'énergie et la latence. EAR s'exécute selon les étapes suivantes (27).

- **Phase d'initialisation :** Cette phase permet la construction de l'arbre de routage contenant tous les chemins possibles pour la dissémination des données. Chaque station de base diffuse un message d'avertissement ADV demandant des paquets RPT. Seuls les capteurs voisins de station de base qui reçoivent le message ADV, enregistrent le chemin dans leur table de routage ; sans qu'ils propagent le message ADV vers les autres capteurs, comme le montrent les étapes "a" et "b" de la figure 3.4. Les autres capteurs envoient une demande RREQ (Route Request) cherchant un chemin vers la station de base (étape c). Si un capteur ayant déjà une route stockée dans sa table, reçoit RREQ, il envoie un paquet RREP (Route Reply) à son capteur voisin concerné par la demande (étapes d , e). Le processus d'initialisation se termine quand chaque capteur reçoit une réponse RREP suite à sa requête RREQ , puis enregistre le chemin dans sa table de routage.

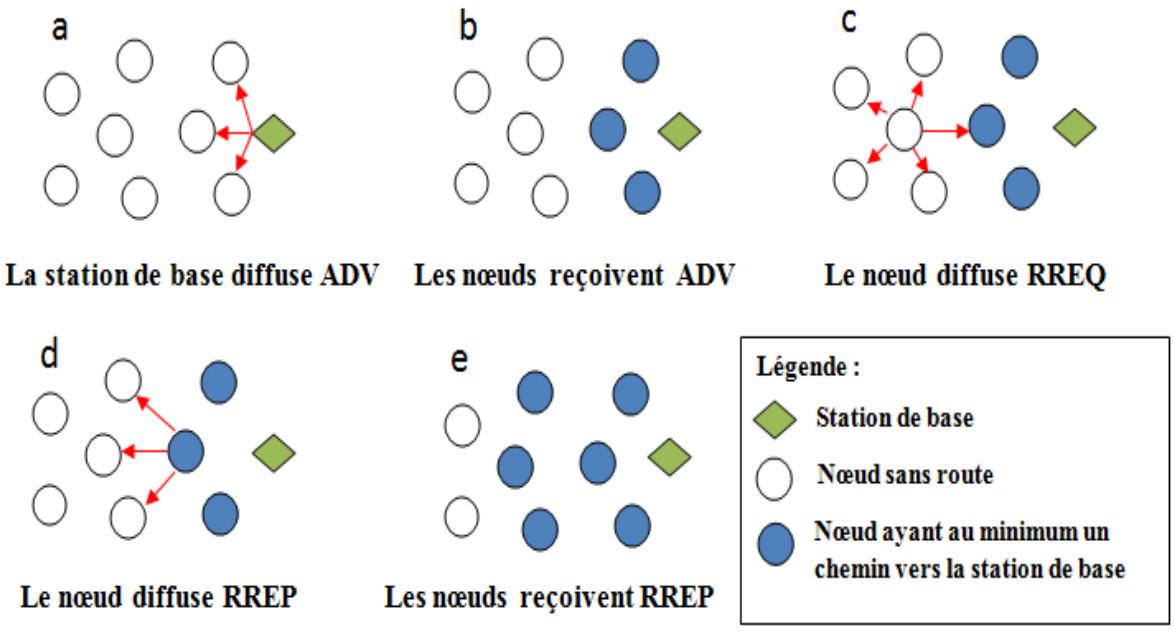


Figure 3.4: Fonctionnement du protocole EAR

- **Phase de gestion de route :** Les micro-capteurs, avec leur mémoire de taille réduite, ne peuvent garder tous les chemins possibles dans leurs tables de routage. Pour cela, et afin d'assurer une bonne tolérance aux pannes, on ne doit garder que les meilleurs chemins. Le protocole EAR 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 RF n'est pas prise en considération, dans ce cas, le plus court chemin n'assure pas forcément la fiabilité de transmission. En effet, si un chemin échoue à transmettre N paquets consécutifs, il sera mis dans une "liste noire" l'écartant ainsi d'une future utilisation. La deuxième métrique, appelée Score de route, est définie comme suit :

$$RS = PE \times WE + PT \times WT$$

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

L'historique enregistré sur l'état du routage dans tout le réseau permet, par conséquence, d'adapter la sélection des chemins en choisissant toujours les meilleurs chemins en termes de fiabilité de liens et de conservation d'énergie. Ceci garantit une bonne tolérance aux pannes en évitant la sélection des mauvaises routes.

- **Phase de dissémination de données :** Après les deux premières étapes, chaque capteur aura au moins un chemin vers la station de base. Les capteurs commencent donc à générer des paquets RPT, et le routage des données utilise la métrique " score de route " pour définir le meilleur chemin à emprunter. En cas où ce dernier présente une panne au niveau d'un ou plusieurs de ses capteurs, un mécanisme de recouvrement de route est exécuté, afin d'élire un second chemin fiable pour transmettre les données depuis le capteur vers la station de bases. Par ailleurs, au moment de sa durée d'inactivité, chaque capteur est mis en veille afin d'épargner davantage son énergie et augmenter ainsi la durée de vie de tout le réseau.

3.2.1.3 VTRP (Variable Transmission Range Protocol)

VTRP (28) est une solution d'ajustement du rayon de transmission pour une meilleure propagation de données. Il permet de remédier au problème d'obstacles en les évitant par l'augmentation du rayon de transmission. Ce dernier augmente la probabilité d'atteindre des capteurs actifs quand le rayon actuel utilisé ne couvre aucun capteur à cause de pannes ou d'inactivité des capteurs voisins ou encore dans le cas des réseaux à faible densité. En outre, VTRP offre une meilleure longévité du réseau en évitant l'utilisation fréquente des capteurs critiques (les voisins proches de la station de base) ceci permet d'alléger leur fonction de routage, conserve leurs batteries et augmente ainsi la durée de vie de tout le réseau. VTRP s'exécute comme suit :

1. **Phase de recherche :** Soient $p1$ et $p2$ deux capteurs du réseau. Dans la phase de recherche, $p2$ utilise une diffusion périodique de message afin de découvrir le nœud $p1$ le plus proche du nœud puit. Cependant, une détection de panne est possible si aucun nœud $p1$ n'est trouvé. Cet échec est causé par l'une des raisons suivantes : soit le nœud $p1$ est mis en veille, soit il est en panne ou bien à cause d'un obstacle qui empêche la communication entre $p1$ et $p2$.

2. **Phase de transmission directe :** En cas où la phase de recherche se termine avec succès, le capteur $p2$ envoie l'information au capteur $p1$.

3. **Phase d'ajustement du rayon de transmission :** Si la phase de recherche échoue (aucun nœud p n'est détecté), $p2$ passe à la phase d'ajustement de son rayon de transmission qui représente le cas de recouvrement après pannes. En effet, chaque capteur maintient un compteur local initialisé à 0. A chaque échec de l'étape de recherche, le compteur est incrémenté, et le rayon de transmission R est modifié. Quatre différentes fonctions sont

définies selon la vitesse de variation du rayon de transmission : linéaire, multiplicative, exponentielle et aléatoire :

- **Progrès constant :** VTRP est convenable dans ce cas de réseaux où un grand nombre de capteurs est compromis ;
- **Progrès multiplicatif :** VTRPm définit un rayon de transmission qui est augmenté d'une manière radicale. Ce changement offre une meilleure probabilité pour trouver des capteurs actifs. En revanche, il requiert une consommation d'énergie plus importante.
- **Progrès exponentiel :** VTRPp est une variante qui augmente le rayon d'une vitesse encore plus rapide ;
- **Progrès aléatoire :** Quand la densité du réseau n'est pas connue au préalable, on utilise l'approche aléatoire VTRPr pour éviter un mauvais comportement du réseau suite à un mauvais choix.

3.2.2 Solutions basées sur le clustering pour la tolérance aux pannes

Les algorithmes proposés dans cette catégorie permettent d'améliorer les performances du processus d'auto-organisation du réseau. Les protocoles du clustering divisent le réseau en un ensemble de clusters ayant chacun un clusterhead qui récupère les données depuis tous les capteurs de son cluster puis les achemine vers la station de base. Cette solution permet de mieux gérer le trafic de réseau et d'alléger la quantité d'informations qui circule, en effectuant des traitements au sein du cluster avant de propager les données vers le reste du réseau pour les transmettre à la station de base (29).

3.2.2.1 Protocole CPEQ

En plus de tous les mécanismes de tolérance aux pannes qu'implémente PEQ (30), la variante CPEQ (Cluster-based PEQ)(30) ajoute un module de clustering pour offrir une meilleure gestion de routage. En effet, les capteurs ayant le plus d'énergie résiduelle sont sélectionnés comme des cluster heads. Un Cluster head établit son cluster, et les capteurs appartenant à ce dernier envoient leurs données au Cluster head qui effectue d'éventuel traitement sur les données brutes puis les achemine vers la station de base. Chaque capteur du réseau peut devenir un Cluster head pendant une certaine période de temps selon son niveau de batterie. Le but principal de CPEQ est de distribuer d'une manière uniforme la dissipation d'énergie entre les capteurs, et de réduire la latence et le trafic de données dans le réseau. Le protocole CPEQ s'exécute en cinq étapes.

- **Configuration initiale :** Cette phase est exécutée de la même manière que dans l'algorithme PEQ, où chaque capteur commence par un mécanisme de diffusion pour configurer tout le réseau et connaître par la suite le nombre de sauts nécessaires pour atteindre la station de base la plus proche. En outre, CPEQ introduit un champ additionnel contenant le pourcentage des capteurs qui deviendront des Cluster heads.

- **Sélection d'un Cluster head :** C'est la phase d'élection des clusterheads. Après la configuration initiale, chaque capteur peut devenir un Cluster head avec un pourcentage

donné. En effet, chaque capteur génère un nombre aléatoire entre 0 et 1. Si ce nombre est inférieur à une probabilité p (probabilité pour devenir un Cluster head), le capteur demande à tous ses voisins directs leur niveau de batterie en envoyant un paquet REQ-EN (Request Energy). Chaque voisin répond par un message REP-EN (Reply Energy) contenant son ID et la quantité d'énergie. Le capteur choisit le voisin ayant le maximum d'énergie et diffuse un SET-AGR (Set Aggregator) pour informer tous les capteurs du nouveau Cluster head. Les trois étapes de cette phase sont illustrées dans la figure suivante (figure 3.5) (28).

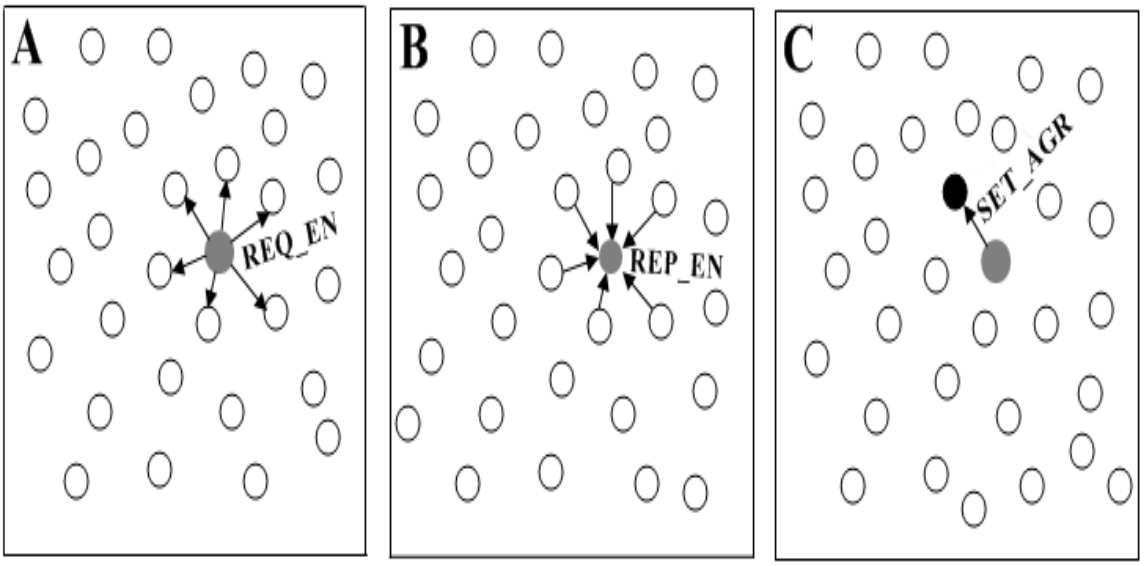


Figure 3.5: Configuration initiale

- **Configuration de clusters :** cette phase divise le réseau en un ensemble de clusters. Le nouveau Cluster head sélectionné doit avertir ses voisins de son rôle d'agrégation. De cette manière, chaque Cluster head construit son cluster. La configuration des clusters est réalisée à l'aide des messages AGR-NTF (Aggregator Notification) avec un champ TTL pour limiter la propagation du paquet sur les capteurs se trouvant à une distance inférieure ou égale au TTL. Chaque fois qu'un capteur reçoit ce message, il enregistre l'ID du capteur émetteur dans sa table de routage pour déterminer le chemin vers le cluster head. Si un capteur reçoit plusieurs messages AGR-NTF, il choisit le Cluster head avec le moindre nombre de sauts. La figure 3.6 (29) illustre la configuration de clusters avec un TTL=2.

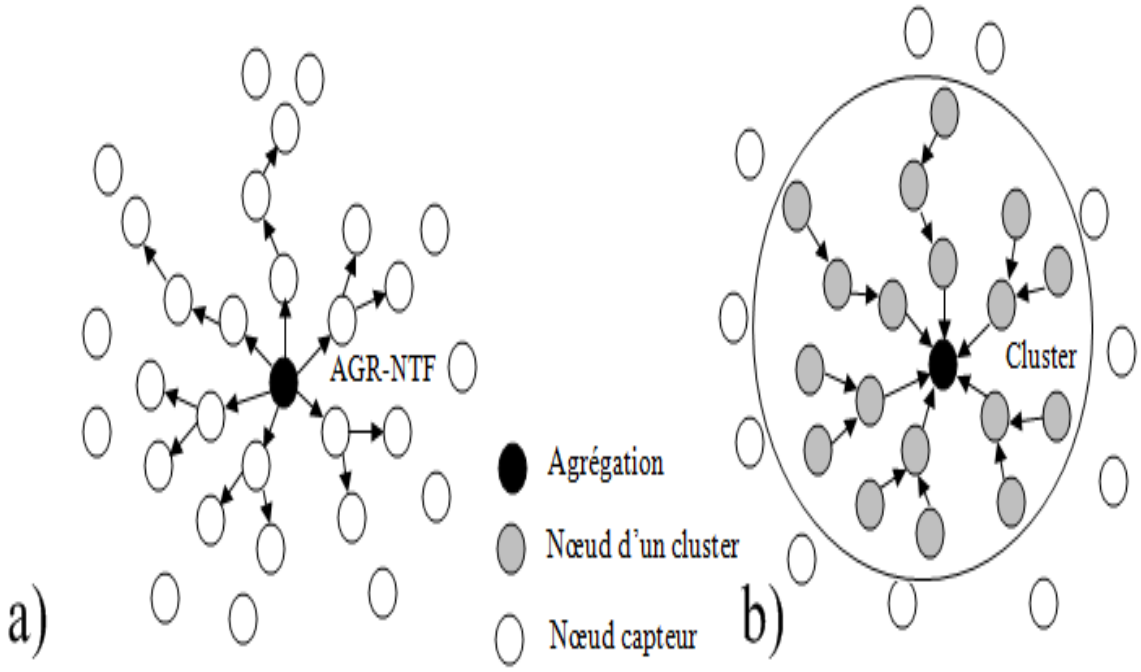


Figure 3.6: Configuration des clusters

- **Transmission de données au clutser head :** l'algorithme de routage des données est le même que celui implémenté dans le protocole PEQ. Chaque capteur utilise sa table de routage pour envoyer la donnée vers son Cluster head. Dans CPEQ, le Cluster head peut être considéré comme une station base. Le mécanisme de recouvrement de chemin est aussi hérité du protocole PEQ.

- **Transmission de données au collecteur :** Aprés réception des données depuis les capteurs de son cluster, le Cluster head doit acheminer ces données à la station de base. CPEQ utilise une communication multi-sauts entre le Cluster head et la station de base comme montre la figure 3.7 (29).

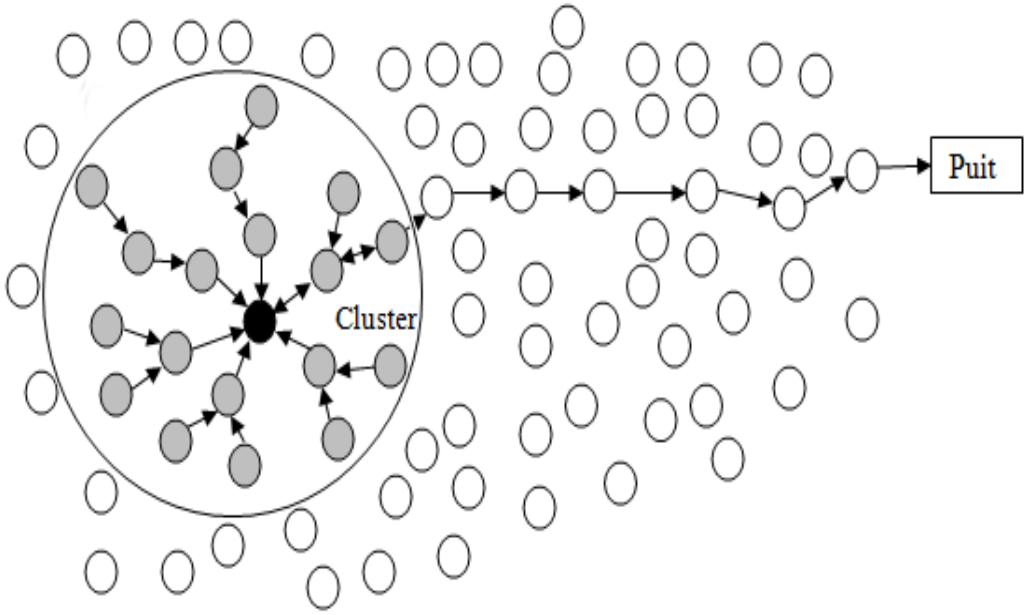


Figure 3.7: Transmission des données à la station de base

3.2.2.2 K-CDS(K-Connected K-Dominating Set)

On modélise un réseau de capteurs par le graphe G = (V, E) où V est l'ensemble des capteurs et E est l'ensemble des liens sans fil entre ces capteurs (30).

- **Définition 1 :** un réseau G est k-connexe s'il n'aura aucune partition quand l'on omet i capteur du graphe (i = 1, 2, ..., k-1),i.e; G est k-connexe si chaque deux capteurs du graphe sont connectés par au moins k chemins disjoints.
- **Définition 2 :** un sous-ensemble V' appartenant à (E) est un k-DS (k-dominating Set) de G si chaque nœud de V qui n'appartient pas à V' a au moins k voisins dans V'. Le k-DS V' devient k-CDS si le sous-graphe $G[V']$ est k-connexe.

L'algorithme K-CDS utilise une approche préventive basée sur le clustering. Il propose une construction d'un ensemble k-connexe dominant k-CDS comme un backbone virtuel pour offrir une efficacité de routage aussi bien qu'une bonne tolérance aux pannes. Pour cela, quatre approches ont été introduites, dont deux sont des algorithmes probabilistes, une est déterministe et la dernière est une hybridation des approches déterministes et probabilistes. Ces quatre approches permettent de considérer différents critéres pour la construction des clusters.

3.2.2.3 KAT-Mobility

Dans KAT-mobiliy (K-means And TSP-based mobility) (31), en plus du clustering, le concept de mobilité est implémenté au niveau de la station de base. Ces deux mécanismes, définissent

une technique préventive hybride tolérante aux pannes qui offre une meilleure gestion d'énergie et augmente donc la durée de vie du réseau. Après réorganisation du réseau en clusters, la méthode proposée pilote la station de base mobile pour se déplacer à travers les centres des clusters en prenant le chemin optimal. La station de base mobile récupère donc les données depuis les capteurs des clusters visités. Le principe de KAT-mobility se résume en deux procédures : clustering et optimisation du routage. La figure 3.8 illustre le principe de KAT-mobility (32).

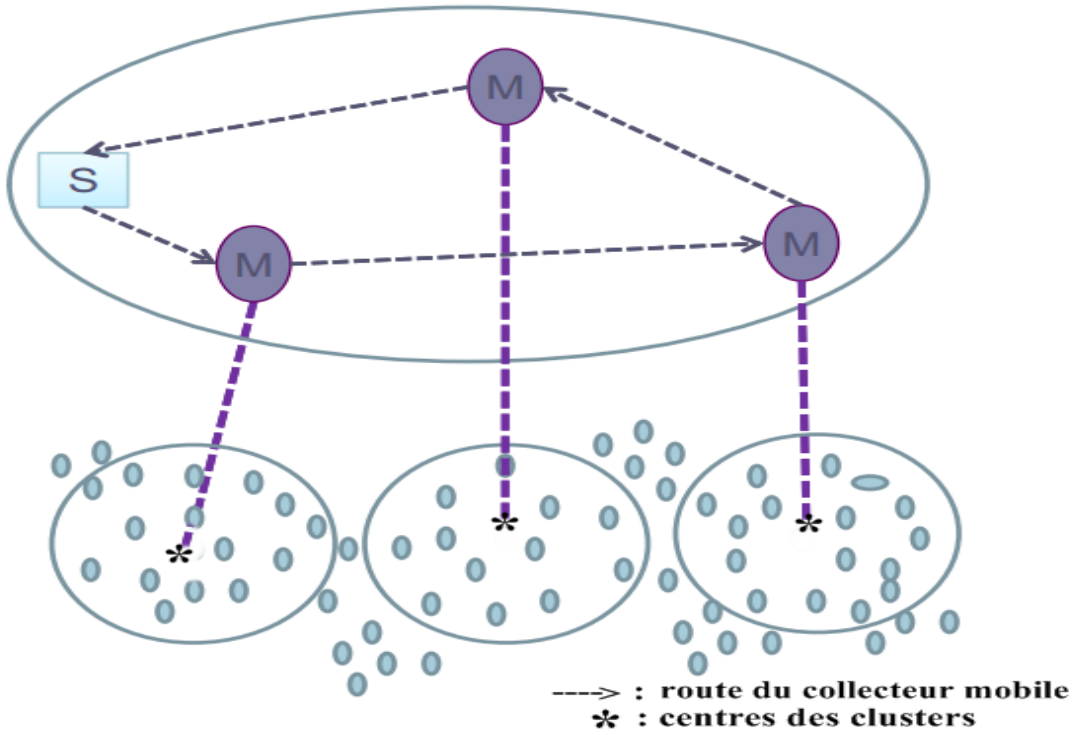


Figure 3.8: Illustration de l'algorithme KAT-mobility

- **Algorithme de clustering:** cette procédure divise l'ensemble des N capteurs en k clusters $C1$, $C2$, ..., Ck. Le coût du cluster est évalué par l'erreur approximative entre la station de base et les nœuds capteurs. Soit d(x, yi) cette distance, où x est un capteur et yi est une station de base (i = 1, 2, ..., k). d(x, yi) est défini par la distance euclidienne entre le capteur et la station de base. Le but est donc, d'affecter chaque capteur à un cluster Ci en minimisant l'erreur totale des clusters.

- **Optimisation du routage :** trouver un chemin optimal pour le nœud mobile est identique au problème du voyageur de commerce (TSP). Ainsi, une station de base représente le voyageur, et les centres des clusters définissent les villes. L'optimisation de la route de station de base mobile pour visiter tous les centres des clusters une et une seule fois est équivalente à la recherche du plus court voyage d'un commerçant pour visiter chaque ville une seule fois.
  Les résultats de simulation ont montré que KAT-mobility peut fournir une meilleure conservation d'énergie aussi bien qu'une bonne tolérance aux pannes en cas de mal fonctionnement de certains capteurs.

3.2.3 Solutions basées sur l'agrégation de données

Minimiser la consommation d'énergie revient à minimiser, entre autre, la quantité de données transmises dans le réseau en particulier les données redondantes. En effet, d'après les statistiques, 70% de l'énergie consommée dans un nœud capteur est due aux transmissions. L'agrégation combine les données provenant de plusieurs capteurs en une information significative, en éliminant ainsi la redondance. Ceci résout le problème d'implosion dans le routage et allège ainsi la congestion du réseau.

3.2.3.1 Classification des protocoles d'agrégation

On peut classer les différentes techniques d'agrégation de données dans les réseaux de capteurs en deux approches, comme illustré par la figue 3.9 (33).

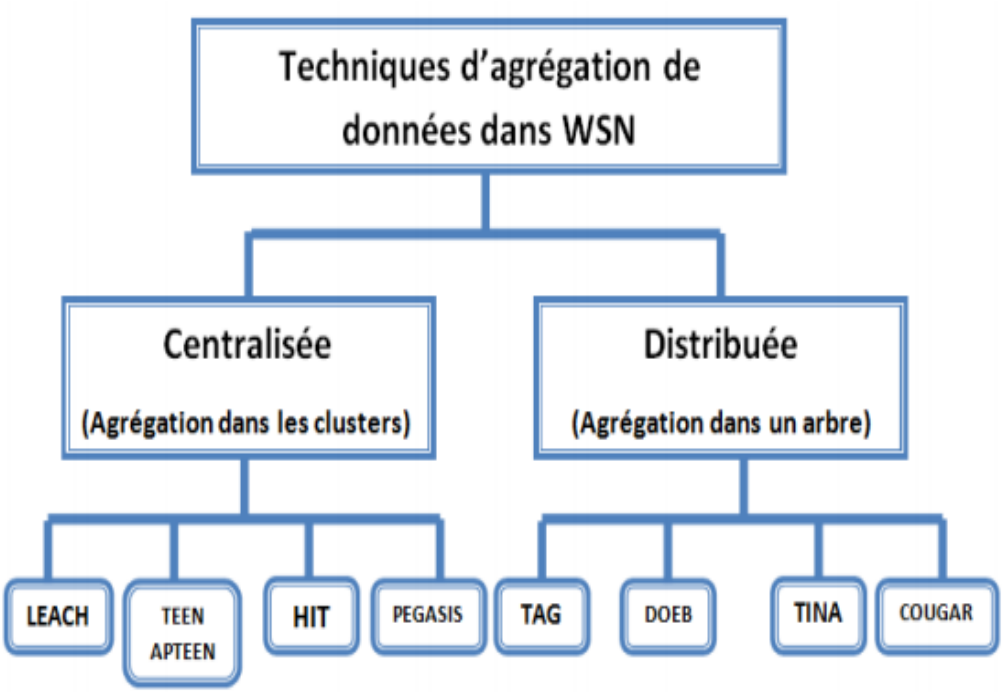


Figure 3.9: Protocoles d'agrégation de données dans les RCSFs

Parmi ces protocoles, on choisit de détailler quelques protocoles les plus courants qui sont : LEACH, TEEN, COUGAR, HEER, HEEC :

- **LEACH (Low-Energy Adaptive Clustering Hierarchy)**

  LEACH est un protocole de routage hiérarchique, employant un procédé de clustering qui divise le réseau en deux niveaux : les cluster-heads et les nœuds membres. Le protocole se déroule en roundes. Chaque round se compose de deux phases : construction et communication (33).

  – **Phase de construction :** Le but de cette phase est la construction des clusters en choisissant les chefs et en établissant la politique d'accès au média au sein de chaque groupe. Cette phase commence par la prise de décision locale pour devenir cluster-head. Chaque nœud n choisit un nombre aléatoire, si ce nombre est inférieur à une valeur $T(n)$, le nœud devient cluster-head. $T(n)$ est définie comme suit :

  $$T(n) = \begin{cases} \dfrac{P}{1 - P \times (r \mod \frac{1}{p})} & \text{si } n \in G \\ 0 & \text{sinon} \end{cases}$$

  avec :

  P : pourcentage désiré de cluster-heads pendant un round

  r : numéro du round.

  G : l'ensemble des nœuds qui n'ont pas été élu cluster heads pendant les $\frac{1}{p}$ rounds précédents. Par la suite, chaque nœud qui s'est élu cluster head émet un message de notification. Les nœuds membres récoltent les messages de notification, et décident leur appartenance à un cluster. La décision est basée sur l'amplitude du signal reçu : le cluster-head ayant le signal le plus fort est choisi (i.e. le plus proche). En cas d'égalité, un Cluster head aléatoire est choisi. Chaque membre informe son Cluster head de sa décision. Toutes les communications précédentes étant faite dans une topologie plate, la méthode CSMA doit être employée. Par la suite, les communications au sein d'un cluster peuvent être faites avec la méthode TDMA. Pour cela, chaque Cluster head établie un programme TDMA pour ses membres, en indiquant pour chaque nœud son slot d'émission. Ce programme est envoyé aux membres.

  – **Phase de communication :** en utilisant le programme TDMA, les membres émettent leurs données captées pendant leurs propres slots. Cela leur permet d'éteindre leur interface de communication en dehors de leurs slots réservés, afin d'économiser leur énergie. Ces informations sont ensuite agrégées, pour être transmises au station de base. Cette communication, entre un cluster-head et la station de base, se fait d'une manière directe, i.e.; le cluster-head adapte son émetteur radio afin d'atteindre directement la station de base.

- **TEEN (Threshold sensitive Energy Efficient sensor Network protocol)**

  En utilisant TDMA, le protocole LEACH est destiné aux applications time-driven. Dans ce type d'application, la donnée est propagée d'une manière périodique. Cependant, ce genre de protocole est inadapté pour les applications event-driven, où un comportement

réactif est nécessaire pour le bon fonctionnement du système. TEEN a été développé pour améliorer LEACH afin de répondre aux exigences des applications event-driven, (34). La majorité du comportement de TEEN est semblable au protocole LEACH. Cependant, quelques différences existent. Les Cluster heads élus ne transmettent pas un programme TDMA, mais émettent un message contenant les informations suivantes :

- Attributs : représentent la tâche demandée au capteur.
- Hard threshold (HT) : détermine la valeur critique après laquelle les membres doivent envoyer leur rapports de données.
- Soft threshold (ST) : spécifie le changement minimal obligeant le nœud à envoyer un nouveau rapport.

Donc, lorsqu'un nœud s'aperçoit que la valeur captée a dépassé HT, il doit émettre un rapport au Cluster head. Il ne réémet un nouveau rapport que si la valeur change radicalement, i.e, la différence dépasse ST. Ce mécanisme permet d'implémenter un comportement réactif, tout en limitant le nombre de messages utilisés.

- **COUGAR**

Dans Cougar, les données produites par le réseau de capteurs sont modélisées comme une table relationnelle. Dans cette table, chacun des attributs représente soit des informations sur le capteur ou bien des données produites par ce capteur. L'approche Cougar fournit une agrégation partielle au niveau des capteurs. Chaque capteur maintient une liste d'attente contenant les capteurs fils qui doivent lui envoyer les paquets. Le capteur n'émet le paquet agrégé au prochain saut que s'il a reçu les paquets de tous les capteurs de la liste d'attente. Cependant, un capteur peut devenir inaccessible à cause du mouvement ou d'un problème de batterie. Pour cela, Cougar utilise un Timer afin d'éviter une attente indéfinie (33).

- **HEER(Hybrid Energy Efficient Reactive):**

Le protocole HEER (Hybrid Energy Efficient Reactive)(37) est conçu pour prolonger la vie et la stabilité du réseau en réduisant la consommation d'énergie. Dans HEER, la sélection du Cluster-Head se fait en se basant sur le ratio d'énergie résiduelle du nœud et de l'énergie moyenne du réseau. HEER utilise les énergies résiduelles et internes du nœud pour devenir un Cluster-Head. Les performances de HEER sont bien meilleures dans le cas des applications critiques en termes de temps et réduit également les non-transmissions avec l'aide les valeurs- seuil du seuil dur, seuil mou pour conserver plus d'énergie. La valeur de CVcurrent sur laquelle la première transmission se produit est stockée en valeur mesurée appelée variable interne SV. Lorsque cette condition devient vraie: $CV \geq HT$ alors il ne réduit pas de transmissions et d'autres transmissions sont réduits lorsque $CV - SV \geq ST$.

- **HEEC (Hierarchical Energy Efficient Clustering):**
Proposé très récemment en l'an 2015 par P. Rajeshwari et al. Dans (38) HEEC (Hierarchical Energy Efficient Clustering) réalise de bonnes performances en termes de réduction de la consommation d'énergie élevée et l'augmentation du temps de vie des réseaux de capteurs.

Il minimise également la charge de manière égale entre tous les nœuds.

Dans HEEC (38), la sélection du CH est effectuée par la SB, puis l'arbre de routage est construit et la méthode DSDV (Destination Sequence Distance Vector Routing) est adoptée pour le choix des chemin optimal. Le CH analyse tous les chemins et sélectionne le plus optimal depuis la source jusqu'à la destination.
Le concept de réélection de Cluster-Heads est également introduit :

- **Etape 01 :** initialement la SB choisit le nœud le plus proche possédant le plus haut niveau d'énergie résiduelle.
- **Etape 02 :** a travers chaque round, la SB vérifie si le niveau d'énergie du CH du tour précédent est suffisant dans le but de transférer les paquet de données. Dans le cas contraire aller à l'étape 03.
- **Etape 03 :** la station de base analyse à nouveaux le niveau d'énergie ainsi que la distance et la vivacité des nœuds du réseau.
- **Etape 04 :** le nœud capteur satisfaisant au mieux ces paramètres est élu.
- **Etape 05 :** l'identité du nouveau CH est diffusée aux restes des nœuds des nœuds du réseau, puis ces deniers construisent leurs nouvelle table de nœud voisins et sélectionne leurs CHs.

Conclusion

Dans ce chapitre, nous avons présenté quelques solutions de tolérance aux pannes dans les réseaux de capteurs sans fil (MAC, routage, etc.). Les solutions de routage présentent une approche importante pour la dissémination des données dans les RCSFs. l'intégration des mécanismes de tolérance aux pannes est une bonne tentative pour tolérer les pannes des composants des RCSFs.

4

Proposition d'un protocole de routage tolérant aux pannes dans les RCSFs

Introduction

Etant donné les différents domaines sensibles auxquels peuvent s'appliquer les RCSF, les protocoles de routage dévelopés pour ces derniers deviennent un élément essentiel et indispensable pour acheminer les données tout en tenant compte de l'economisation de l'énergie.

Après avoir abordé quelques protocoles de routage et solutions de tolérance aux pannes proposés pour les RCSFs, nous avons opté pour le protocole intitulé EAR " Energy Aware Routing " et proposé une amélioration dans le but d'augmenter le degré de tolérance aux pannes pour une meilleure propagation de données.

4.1 Motivation

Dans EAR les voisins proches (à un saut) d'un nœud capteur donné peuvent être fréquemment utilisés lors de l'exécution 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 jusqu'à épuisement de leurs unités respectives d'énergie. De ce fait, il est possible qu'un nœud capteur n'ait aucun nœud capteur voisin en état de fonctionnement dans son rayon de portée. EAR ne propose aucune solution à ce problème.

Après cette analyse du problème, nous remarquons que la tolérance aux fautes du protocole EAR peut être améliorée.

Dans la section suivante, une amélioration du protocole EAR visant une meilleure tolérance au problème introduit précédemment est introduite.

4.2 Proposition d'une amélioration du protocole EAR appelé EAR-INR (Energy Aware Routing-Isolated Node Recovery)

Dans le but d'améliorer la tolérance aux pannes du protocole EAR, nous avons pensé à traiter le problème des nœuds isolés a cause de defaillance de quelques nœuds relais appartenant aux différents chemins de routage. Pour cela, nous avons choisi dans EAR-INR d'ajuster le rayon de transmission des nœuds isolé pour trouver de nouveaux nœuds relais.

L'ajustement de rayon de transmission est en effet une propriété qu'on retrouve dans quelques protocoles destinés à la tolérance aux pannes dans les réseaux de capteurs tels que DMRF(39), PEQ(26) et VTRP(28). Elle est utilisée par ces derniers pour empêcher l'isolement d'un nœud capteur dans le cas où tous les nœuds voisins se trouvant dans sa zone de transmission sont défectueux pour maintes raisons. Alors, le nœud doit donc augmenter son rayon de transmission radio pour éviter les nœuds défaillants et atteindre les capteurs voisin lointains. (Voir figure 4.1)

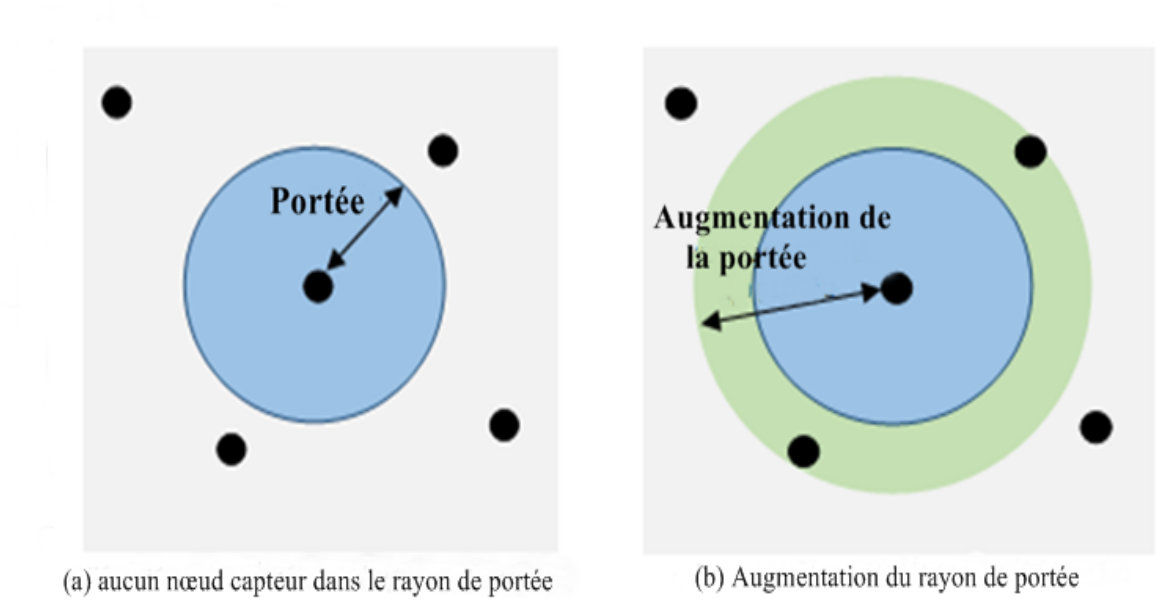
EAR-INR se compose des mêmes phases qu'EAR, auquel nous ajoutons le mécanisme précédemment cité pendant la deuxième phase, c'est-à-dire celle de la gestion des routes.

4.2.1 Phase de gestion de route améliorée

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 d'assurer une bonne tolérance aux pannes, on ne doit garder que les meilleurs chemins. Le protocole EAR-INR 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 n'est pas prise en considération, dans ce cas, le plus court chemin n'assure pas forcément la fiabilité de transmission. En effet, si un chemin échoue à transmettre N paquets consécutifs, il sera mis dans une "liste noire" l'écartant ainsi d'une future utilisation. La deuxième métrique, appelée score de route (RS), est définie comme suit :

$$RS = PE \times WE + PT \times WT$$

Dans cette phase, EAR-INR met à jour la liste des routes dans la table de routage en envoyant un messagede contrôle de taille minimale qui est égale à 1 octet. Si un nœud ne reçcoit pas ce message de mise-à-jour de route d'aucun de ses voisins, alors le nœud se considère isolé et doit augmenter son rayon de transmission pour atteindre des nœuds qui posséderait potentiellement un chemin vers la station de base.



(a) aucun nœud capteur dans le rayon de portée (b) Augmentation du rayon de portée

Figure 4.1: Ajustement du rayon de transmission

4.2.1.1 ajustement du rayon de transmission du noeud isolé :

Le déploiement de RCSF étant de type aléatoire, sa densité ne peut être connue à l'avance. Alors, nous portons notre choix pour l'ajustement du RT sur la fonction avec progrès aléatoire de VTRPr(28) qui se révèle être la plus appropriée dans ce cas précis.

$$R_{new} = R_{old} + rand$$

R_{new} représente le nouveau rayon de transmission, R_{old} représente l'ancien rayon de transmission, et enfin, $rand$ représente une valeur aléatoire choisie selon l'environnement Ci-dessous l'algorithme qui résume le fonctionnement de l'amélioration :

Repeter ;

Envois de message de mise à jour des routes de la part des voisins ;

Attente délais ;

Si (aucun msg reçu des voisins) **alors**

Isolé = oui ;

Si (isolé) **alors** $R_{new} = R_{old} + rand$;

Fin si ;

Sinon isolé = non ;

Fin si ;

jusqu'à isolé == non ;

Figure 4.2: Algorithme résumant le fontionement de l'amélioration

4.3 Exemple illustratif de l'exécution de EAR-INR

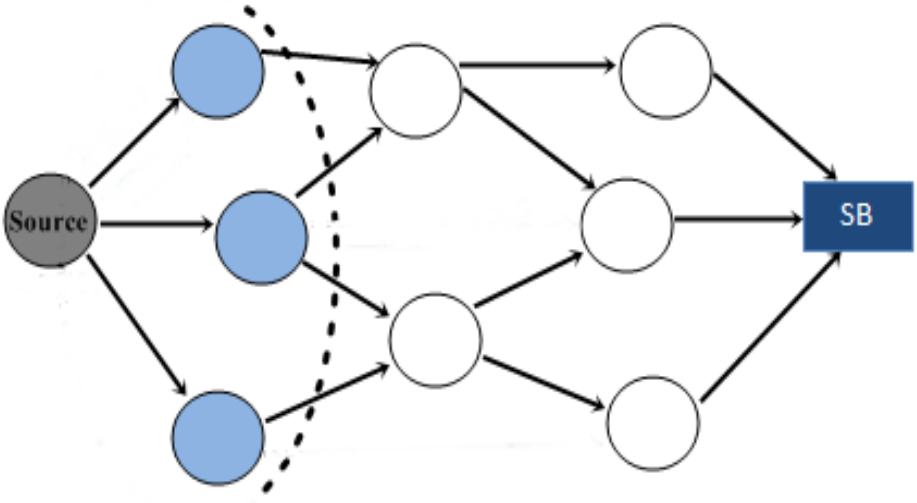


Figure 4.3: Phase initiale

La figure 4.3 représente le cas de fonctionnement du protocole EAR-INR lorsque au moins un des nœuds se trouvant dans la zone de couverture du nœud source est actif. Dans ce cas, la transmission des données jusqu'à la station de base s'effectuent le plus normalement du monde.

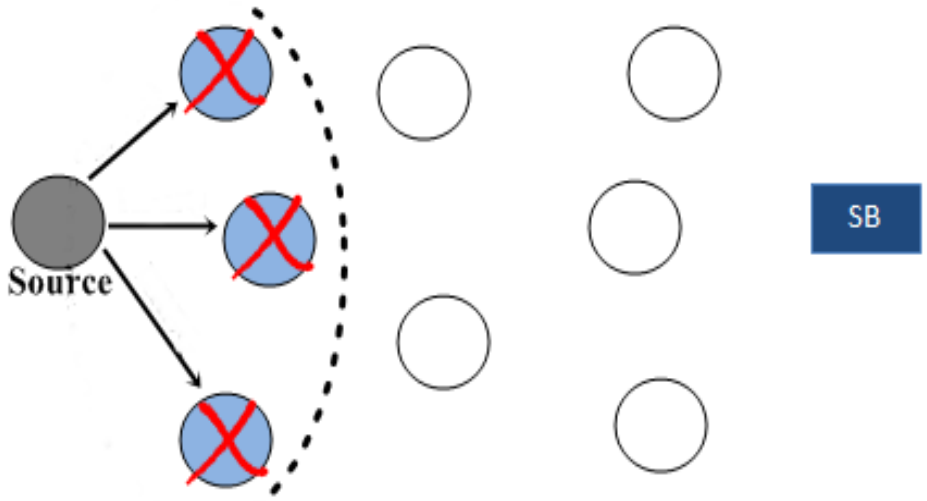


Figure 4.4: Problème du noeud isolé

La figure 4.4 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.

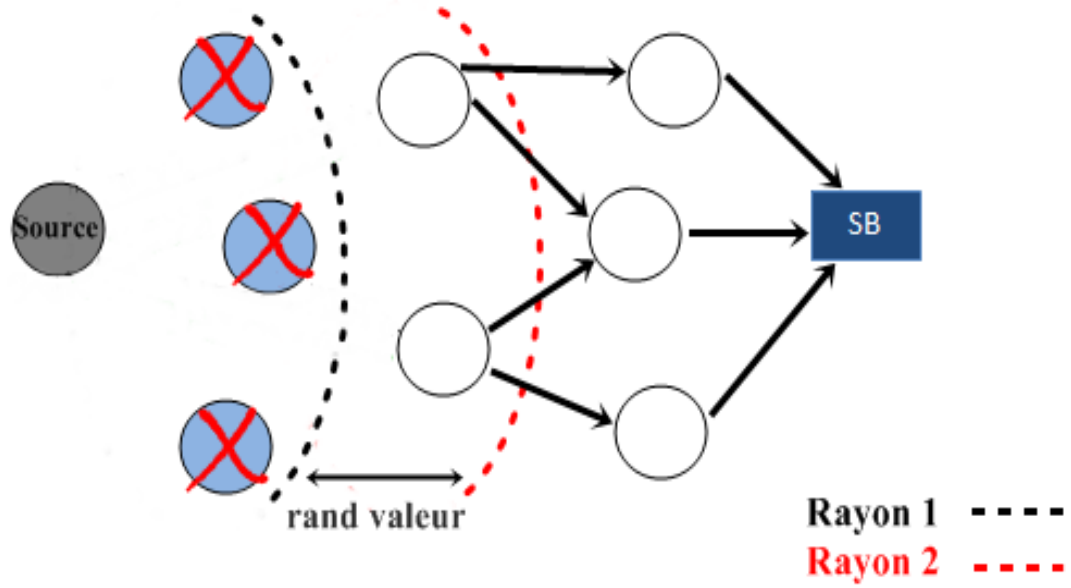


Figure 4.5: nouveau rayon de transmission

La figure 4.5 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 voisin du nœud.

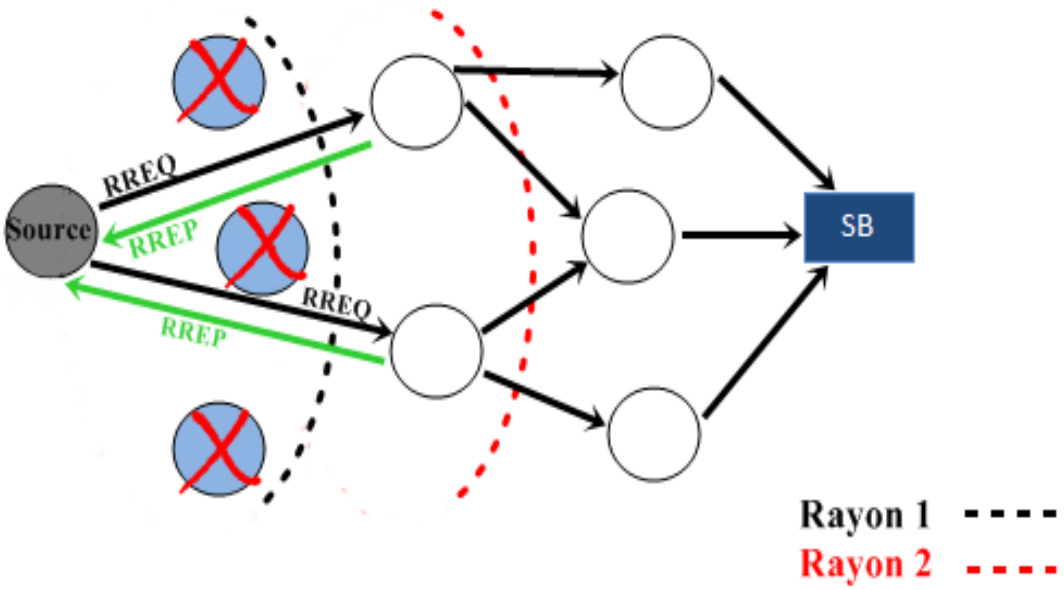


Figure 4.6: Recouvrement de route

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 4.6)

Conclusion

Notre travail rentre dans le cadre de l'amélioration de la tolérance aux pannes du protocole EAR. Dans cette proposition, nous avons cherché à maximiser l'exploitation du réseau en proposant une solution à la gestion des nœuds capteurs isolés. Afin de palier à ce problème, nous avons utilisé l'augmentation de la puissance de transmission des nœuds capteurs en se basant sur une formule inspirée du progrès aléatoire de VRTP.

CONCLUSION GÉNÉRALE

Sans être exhaustif, ce travail a donné un panorama des principales notions relatives aux réseaux de capteurs sans fil. Cependant, une attention particulière a été portée aux mécanismes de tolérance aux pannes, ils sont au cœur du travail réalisé.

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 batteries, le type de communication, les environnements hostiles où sont déployés les capteurs, etc. Par ailleurs, ces réseaux sont caractérisés par les pannes des nœuds qui peuvent causer un dysfonctionnement du réseau en entier. Dans cette optique, il est commode de proposer des techniques qui permettent de prévoir les pannes à une étape précoce ou de réparer la panne en temps réel ou encore tolérer la panne.

Une panne au niveau d'un capteur peut se produire à cause d'une perte de connexion 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 étudié les différentes causes de pannes qui peuvent survenir durant la vie d'un réseau de capteurs sans fil. Puis on a étudié les différents protocoles de routage dédiés à la tolérance aux pannes, ensuite on s'est focalisé en particulier sur le protocole EAR (Energy Aware Routing) pour lequel on a apporté une amélioration qui consiste à ajuster le rayon de transmission d'une telle façon que la propagation de données soit bien meilleure et évitant aussi la mise à mort du réseau de capteurs.

Cette expérience a été enrichissante à plus d'un point dans les travaux réalisés, on a pu approfondir nos connaissances dans un domaine que ne connaissions pas encore.

Bibliographie

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor networks: a survey", IEEE Communications Magazine, 40(8) : pages 102–114, August 2002.

[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor networks : A survey. Computer Networks (Elsevier), 38(4) : pages 393-422, March 2002.

[3] Kristofer, Pister. http://robotics.eecs.berkeley.edu/ pister/SmartDust/. SmartDust. [En ligne] 2001.

[4] Crossbow. MICA2 Data sheet. [Online] 2009. http://www.xbow.com/products/Product_pdf_files/Wireless_pdf/MICA2_Datasheet

[5] C. Basile, M. O. Killian & D. Powell. A survey of dependability issues in mobile wireless networks , Tech. Report 02637, LAAS, Toulouse, 2002.

[6] C. Castelluccia, La Sécurité des Capteurs et Réseaux de Capteurs , Projet Planete, INRIA, Juin 2008.

[7] Y. Challal, H. Bettahar, A. Bouabdllah. Les Réseaux de capteurs (WSN : Wireless Sensor Networks) , Rapport Interne, Université de Technologie de Compiègne, France, 2008.

[8]] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks , IEEE Communications Magazine , 40(8): pages 102-114, Georgia Institute of Technology, Atlanta, USA. Août 2002.

[9] M. Ilyas and I. Mahgoub. Handbook of sensor networks Compact wireless and wired Sensing Systems, ISBN 08493196864. CRC PRESS LLS, USA, 2005.

[10] A. MAKHOUL. Réseaux de capteurs : localisation, couverture et fusion de données . Thèse de Doctorat, Université de Franche-Comté France, 2008.

[11] M. BADNET et N. BELLOIR. Réseaux de capteurs : Mise en place d'une plate forme de test et d'expérimentation, Mémoire de Master Technologie de l'Internet, France, 2005/2006.

[12] J-C. Laprie. Surete de fonctionnement des Systemes : concepts de base et terminologie, Revue de L'électricité et de l'electronique, volume 11 : page 95-105, Déc 2004.

[13] J. Kamimura, N. Wakamiya and M. Murata. Energy-Efficient Clustering Method for Data Gathering in Sensor Networks. Osaka University, Japan. 2004.

[14] A. Arora et all. Gonda : Closure And Convergence : A Foundation Of Fault-Tolerrant Computing. IEEE Transaction on Software Engineering, 19(11) : pages 1015-1027. 1993.

[15] A. Postma. Classes of Byzantine Fault-Tolerant algorithms for dependable distributed systèms, Ph. D thesis, University of Twente, Enschede, The Netherlands, 1998.

[16] G. L. Lann, P. Minet et D. Powell. Tolerance Aux Fautes Et Systemes Repartis : Concepts Et Mecanizmes. Rapport de recherche INRIA N° 2108. 1993.

[17] V. P. Neison, Fault-Tolerant Computing : Fundamental Concepts. IEEE Computer, (23)7. 1990.

[18] J. Wakerly. Error Detecting Codes, s Self-Checking Circuits and Applications, pages 231, Elsevier North-Holland, New York, NY, USA, 1978.

[19] G. Muller, M. Banâtre, N. Peyrouse, B. Rochat. Lessons from FTM : An Experiment in the Design and Implementation of a Low Cost Fault Tolerant System IEEE Transactions on Reliability , 45(11) : pages 332-340, juin 1996.

[20] G. Werner-Allen, K. Lorincz, M. Ruiz, O. Marcillo, J. Johnson, J. Lees, and M. Welsh. Deploying a wireless sensor network on an active volcano. IEEE Internet Computing, volume 11, pages 18–25, 2006.

[21] R. Szewczyk, J. Polastre, A. M. Mainwaring, and D. E. Culler. Lessons from a Sensor Network Expedition. In WSNE, pages 307–322, 2004.

[22] K. Rahim. Techniques de conservation d'énergie dans les réseaux de capteurs sans fil, Thèse de Doctorat, Université de Toulouse, 2009.

[23] B. Thibault. Marches aléatoires et mot circulant adaptabilités et tolérance aux pannes dans les environnements distribués, Thèse, Université de Reims-Champagne-Ardenne, 2011.

[24] A. Boukerche, I. Chatzigiannakisb, S. Nikoletseas. A new energy efficient and fault-tolerant protocol for data propagation in smart dust networks using varying transmission range, 2006. volume 29 : pages 477-489.

[25] S. Yessad, F. Nait-Abdesselam, T. Taleb et S. Bensaou. "R-MAC : Reservation Medium Access Control Protocol for Wireless Sensor Networks. In Proceedings of the 32nd IEEE Conference on Local Computer Networks (LCN2007, Pages 719-724, Dublin, Ireland, 2007.

[26] A. Boukerche et al, A Fast and Reliable Protocol for Wireless Sensor Networks in Critical Conditions Monitoring Applications, International Conference (MSWiM'04), Canada, 2004.

[27] Nuno André Saraiva Pais, Routing Protocol For Wireless Sensor Networks with Hybrid Energy Storage System, Master Thesis, Institute of Electronic Systems Aalborg University, Denmark, September 2009.

[28] A. Boukerche, al. A new energy efficient 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.

[29] H . M. Ammari. Challenges and Opportunities of Connected K-Covered Wireless Sensor Networks, Livre, 2009.

[30] F. Dai, J Wu. On constructing k-connected k-dominating set in wireless ad hoc and sensor networks, Journal of Parallel and Distributed Computing, 66(7) : pages 947-958, July 2006.

[31] N. Hidehisa et al. Fault-resilient sensing in wireless sensor networks, Journal of Computer communications, 30(11-12): pages 2375-2384, 2007.

[32] A. MAKHOUL. Réseaux de capteurs : localisation, couverture et fusion de données. Thèse de Doctorat, Université de Franche-Comté France, 2008.

[33] N. Dhibeya. Routage avec QoS temps réel dans les réseaux de capteurs, Rapport de projet de fin d'études, Ecole supérieure des communications, Tunis, 2007.

[34] F. Taïani, M. OlivierKillijian. J. Ch. Fabre, Intergiciels pour la tolérance aux fautes Etat de l'art et défis, Revue des sciences et technologies de l'information, série TSI, Éditions Hermès Lavoisier, 25(5) : pages 599-630, juin-juillet 2006.

[35] L. Keong, L. Huan et P. Yi. An efficient and reliable routing protocol for wireless sensor networks. In Proceedings of the First International IEEE WoWMoM Workshop on Autonomic Communications and Computing (ACC'05), Taormina, Italy, pages 512–516, June 2005.

[36] L. Huan and P. Yi, L. Keong. An Efficient and Reliable Routing Protocol for Wireless Sensor Networks, Proceedings of the First International IEEE WoWMoM Workshop on Autonomic Communications and Computing (ACC'05), 2005.

[37] S. Sharma et M. Sharma. Ans Improvement for HEER Protocol in Wireless Sensor Network, International Journal of Computer Science and Information Technologies, 5(3) : pages 3399-3402, 2014.

[38] P. Rajechwari, B. Shanthini, and M. Prince. Hierachical energy efficient clustering multiple clustering algorithm for wsn. Middle-Easte Journal of Scientific Research, 23(6) : pages 108-117, 2015.

[39] Guowei Wu, ChiLin, Feng Xia, Lin Yao, il Zhang et Liu Bing. Saut dynamique en temps réel Fault-Tolerant protocole de routage pour les réseaux de capteurs sans fil. De la Fondation nationale des sciences naturelles de Chine par la concession numéro60703101 et n 60903153 (2010).

[40] Yacine CHALLAL. Réseaux de capteur sans fils. [Online] 2010. https://moodle.utc.fr/file.php/498/SupportWeb/co/Module-RCSF-92.html

Résumé

La durée de vie d'un réseau de capteurs sans fil dépend de plusieurs facteurs (la durée de vie du nœud, des chemins, etc.). Plusieurs facteurs peuvent être l'origine d'une défaillance dans un réseau de capteurs par exemple : manque d'énergie d'un nœud significatif, infection d'un nœud par un programme malveillant, une défaillance physique ou logique d'un nœud primaire, etc. Ces défaillance peuvent nécessiter dans quelques cas la reconfiguration du réseau, qui génère un «Overhead» important ou dans d'autre cas, l'échec de la tâche affectée à ce réseau. L'objectif de ce projet de fin d'études est de chercher une stratégie de tolérance aux pannes pour remédier au problème de défaillance dans un RCSF.

Mots clé : réseaux de capteurs sans fil, connectivité, défaillance, tolérance aux pannes.

Abstract

The lifespan of a network of sensors without wire depends on several factors (lifespan of the node, the ways, etc). Several factors can be the origin of a failure in a network of sensors for example: miss energy of a significant node, infection of a node by a malevolent program, a physical or logical failure of a primary education node, etc These failure can require in some cases the reconfiguration of the network, which generates an important "Overhead" or in other case, the failure of the task assigned to this network. The objective of this project of end of studies is to seek a strategy of fault-tolerance to cure the problem of failure in a WSN.

Keywords : networks of wireless sensors, connectivity, failure, fault tolerance.