REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE MOHAMED BOUDIAF - M'SILA

Faculté des Mathématiques et de l'Informatique

Département d'Informatique

N° :……..

DOMAINE :Mathématiques et Informatique

FILIERE : Informatique

OPTION : Réseau et Technologie de l'Information et de la Communication

Mémoire présenté pour l'obtention
Du diplôme de Master Académique

Par: AICHE ABLA

Intitulé

La notification et l'agrégation des rapports d'échecs à l'aide du routage directionnel et de l'apprentissage automatique dans WSN

Soutenu devant le jury composé de :

Guesmia Salah	Université de M'sila	Président
Ghribi hayet	Université de M'sila	Rapportrice
Amraoui noureddine	Université de M'sila	Examinateur

Année universitaire : 2021 / 2022


بسم الله الرحمن الرحيم

Dédicace

Je dédie ce travail à mes parents qui m'ont toujours offert le bonheur.

Je le dédie à ma sœur, les petits enfants de la famille haithem,abir

Et à ma grande famille, A Tous mes amis et Mes collègues.

A la promo 2021/2022 d'informatique.

Enfin, à toutes celles et tous ceux qui ont contribué de prèsou de loin à l'accomplissement de ce travail.

ABLA

Remerciements

Je tiens avant tout à remercier Dieu le tout puissant de m'avoirdonné la force et la volonté pour achever ce modeste travail.

Je remercie Madame ***ghribi hayet*** *mon encadreuse d'avoirbien dirigé ce travail, avec ses judicieux conseils dont il a faitpreuve durant l'élaboration de notre étude.*

Table des Matières

CHAPITRE 2: LES PANNES ET L'ENERGIE DANS WSN

CHAPITRE 3: L'AGREGATION DES DONNEES DANS WSN

LISTE DES FIGURES

LISTE DES TABLEAUX

INTRODUCTION GENERALE

Introduction générale

Un réseau de capteurs sans fil du futur proche devrait se composer de centaines à des milliers de nœuds sans fil peu coûteux. Chacun avec une certaine puissance de calcul et une capacité de détection fonctionnant en mode sans surveillance .ils sont destines a un large éventail d'applications de détection environnementale, du suivi des véhicules a la surveillance de l'habitat.

Les réseaux de capteurs sont essentiellement base sur les événements .un réseau de capteurs se compose d'un ou plusieurs puits qui s'abonnent a des flux de données spécifiques en exprimant des intérêts ou des requêtes.

Les capteurs du réseau agissent comme des sources qui détectent les événements environnementaux et transmettent les données pertinentes au puits.

En réseau de l'exigence d'un fonctionnement sans surveillances dans des endroits éloignes ou même potentiellement hostiles, les réseaux de capteurs sont extrêmement limites en énergie, cependant étant donne que divers nœud de capteurs détectent souvent des phénomènes communs, dans notre cas les pannes des capteurs, il probable qu'il y ait une certaine redondance dans la notification des pannes.

L'un des techniques de filtrage et de traitement en réseau peuvent aides à conserver les rares ressources énergétiques est l'agrégation, idée est de combiner les données provenant de déférent sources en éliminant la redondance en minimisent le nombre de transmission il donc en économisant de l'énergie.

Ce paradigme déplace l'attention des approches traditionnelles centrées sur l'adresse pour la mise en réseau trouver des routes courtes entre des paires de nœuds finaux adressables vers un approches plus centrée sur les données trouver des routes de plusieurs sources vers une seule destination qui permet la consolidation en réseau des données redondantes[3].

Au cours de cette mémoire nous nous sommes intéressés l'agrégation de donnes dans les réseaux de capteurs sans fil le souci principale est de prolonger la dure de vie de réseau en économisant l'énergie dépensée par chaque nœud capteur du réseau.

Dans l'objective d'amélioration des performances du réseau en terme consommation d'énergie nous concentre sur les techniques de l'agrégation des données

Ce manuscrit est organiser en 4 chapitre, dans le chapitre 1 nous présentons les réseaux de capteurs sans fil et leurs applications en commençant par les divers éléments constitutifs d'un capteur suivi de définir brièvement l'architecture générale d'un réseau de capteur suivi de déférent types de communications et les modèles de transmission des données et déférent classification de réseau selon des critères déférent et classification des protocole de routage .

Dans le chapitre 2 nous exposons de façon générale sur les panne dans réseau de capteur et classifier cette panne selon déférent critères et le processus de tolérance de panne et déférent approches pour détection des panne.

Puis nous étudions l'énergie dans le réseau de capteurs sans fil par présenter les déférent Facteurs intervenants dans la consommation d'énergie et Les méthodes de conservation d'énergie dans les réseaux de capteurs sans fils et signaler les déférentes méthodes proposées pour minimiser l'énergie.

Dans le chapitre 3 nous concentre l'un des méthodes de conservation l'énergie qu'il s'appelle l'agrégation nous essayons présenter un aperçu sur les déférent stratégies et catégories d'agrégation et quelques protocoles d'agrégation.

Dans le chapitre 4 nous avons essaye de mettre en évidence comment utiliser de DRINA pour le problème de notification des pannes avec donner les phases nécessaire.

CHAPITRE 1

GENERALITES SUR WSN

1. Introduction

Les progrès réalisés ces dernières années dans les domaines des techniques de communication sans fil ont permis de voir apparaître un nouveau type de réseau: les réseaux de capteurs sans fil (RCSF). Ces réseaux sont composés d'un ensemble de petits appareils, ou capteurs, possédant des ressources particulièrement limitées, mais qui leur permettent de collecter et transmettre des données environnementales (la température, l'humidité, la présence d'un gaz….etc.) vers un ou plusieurs points de collecte [13].

Dans ce chapitre, nous allons présenter les réseaux de capteurs sans fil : leurs architectures de communication et leurs applications. Nous allons discuter également les principaux facteurs et contraintes qui influencent la conception des réseaux de capteurs sans fil.

2. Histoire des réseaux de capteurs

Dans les années 1990, dans le monde de la recherche, est apparue une idée qui paraissait plutôt un rêve pour cette époque : imaginer un système nerveux central pour la Terre, capable de surveiller en temps réel les événements, ayant comme principaux bénéfices de pouvoir empêcher les accidents et d'économiser l'énergie. (Cette poussière intelligente a mis longtemps à apparaître) dit le professeur Pister, de l'Université de Californie à Berkeley. (J'ai inventé l'expression il y a 14 ans. La poussière vraiment futée a mis le temps, mais elle est finalement arrivée).

Aujourd'hui les réseaux de capteurs sont devenus des systèmes pouvant atteindre un très grand nombre de nœuds, avec une zone de couverture déterminée et déployés d'une manière plus ou moins dense dans un environnement hétérogène dont on mesure ainsi son état global. Les derniers progrès en terme de miniaturisation, ainsi que le remplacement du câblage classique par des technologies de communication radio, ont généré de nouvelles catégories d'applications qui visent de nombreux domaines : l'aéronautique, l'automobile, le médical, l'environnement, etc. De plus, les progrès des communications sans fil permettent aujourd'hui de répondre à des exigences peu envisageables auparavant [13].

3. Présentation des réseaux de capteurs

3.1. Définition d'un capteur

Les capteurs sont des dispositifs électroniques de taille extrêmement réduite avec des ressources très limitées, autonomes, capable de mesurer une valeur physique environnementale (température, lumière, pression, etc.) et de la communiquer à un centre de contrôle via une station de base[13]**.**

3.2. Composants d'un capteur sans fil

Un capteur sans fil est doté, principalement d'une unité de : captage, traitement, communication, stockage et énergie. D'autres modules peuvent être ajoutés selon le domaine d'application comme une unité de localisation, afin d'identifier la position géographique d'un capteur tel qu'un GPS (Global Position System), un mobilisateur pour que les capteurs puissent se déplacer et un générateur de puissance tel que des cellules solaires afin d'alimenter électriquement le capteur sans avoir à changer ses batteries .Ces éléments principaux et optionnels sont visibles sur la figure 1.1[11].

- **Unité de captage (Sensing unit):** elle est constituée de deux composants, un dispositif qui intercepte les données du monde physique et les transforme en signaux analogiques, et un convertisseur analogique/numérique qui transforme ces signaux analogiques en un signal numérique compréhensible par l'unité de traitement.

- **Unité de traitement(Processing unit) :** composée d'un processeur et d'une mémoire intégrant un système d'exploitation spécifique (TinyOS , par exemple). Cette unité possède deux interfaces, une interface pour l'unité d'acquisition et une interface pour l'unité de communication. Elle acquiert les informations en provenance de l'unité d'acquisition et les envoie à l'unité de communication. Cette unité est chargée aussi d'exécuter les protocoles de communications qui permettent de faire collaborer le capteur avec d'autres capteurs. Elle peut aussi analyser les données captées.

- **Unité de communication (Transceiver unit) :** elle est responsable des émissions et réceptions des données sur un medium sans fil. Elle se base sur les technologies sans fil à faible portée de communication, Zigbee, Bluetooth ou Wifi .

- **Unité d'alimentation énergétique (Power Unit) :** un capteur est muni d'une batteriepour alimenter tous ses composants Cependant, à cause de sa taille réduite, la batterie dont il dispose est limitée et généralement irremplaçable. Pour cela, l'énergie est la ressource la plus précieuse puisqu'elle influe directement sur la durée de vie des capteurs, ce qui a rendu l'énergie Comme principale contrainte pour un capteur

  Système de localisation (Location Finding System) : il fournit des informations sur la localisation requise par les techniques de routage.

- **Mobilisateur (Mobilizer) :** il est appelé si le nœud capteur doit être déplacé pour accomplir la requête à traiter.

Figure 1 **Figure1.1 architecture d'un capteur [11]**

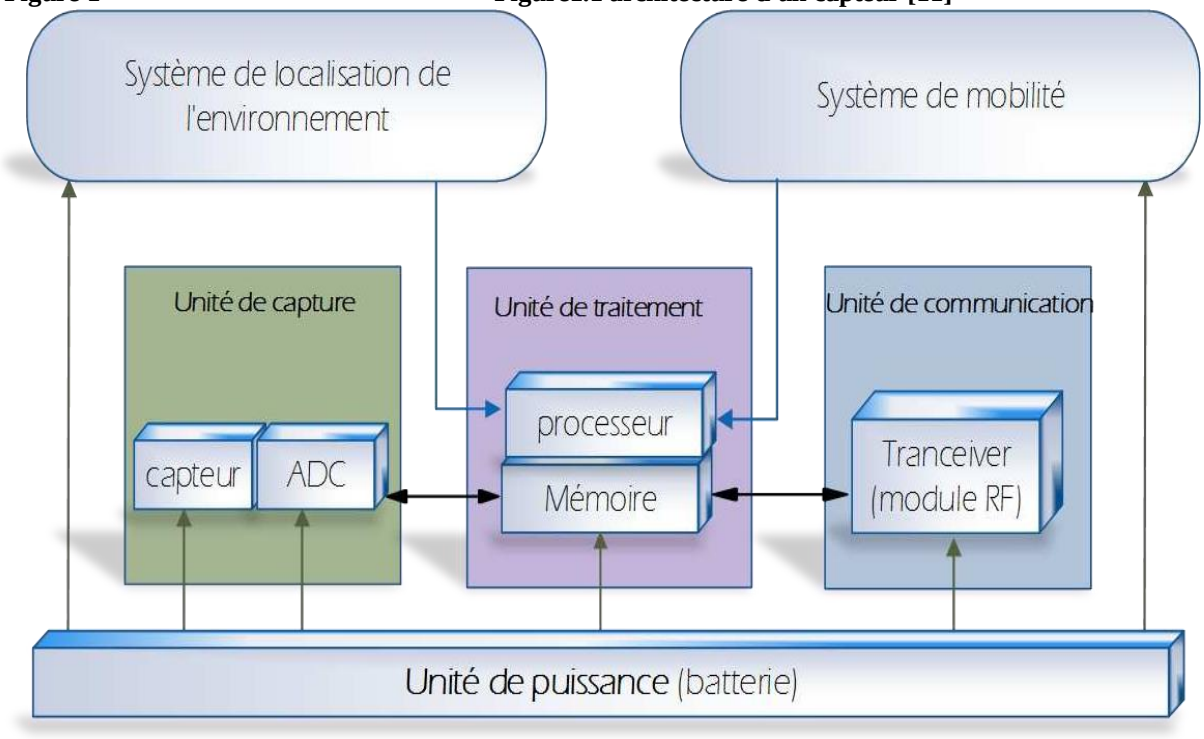


Figure1.1 architecture d'un capteur [11]

3.3.Définition d'un RCSF ou WSN (Wireless Sensor Network)

Un réseau de capteurs sans fil (RCSF) est un type particulier des réseaux ad hoc. Il est composé de centaines ou de milliers d'éléments nommés nœuds ou capteurs placés de manière plus au moins aléatoire. Dans ces réseaux, chaquenœud est capable de surveiller son environnement et de réagir en cas de besoin en envoyant l'information collectée à un ou plusieurs points de collecte, à l'aide d'une connexion sans fil.[13]

3.4.Architecture

L'architecture des réseaux de capteurs sans fils utilise beaucoup de sources. Historiquement, beaucoup du travail relatif a été effectué dans le contexte des réseaux à auto-organisation, mobiles et Ad Hoc Un réseau [17].

- **nœuds :** Sont des capteurs, leur type, leur architecture et leur disposition géographique dépendent de l'exigence de l'application en question. Leur énergie est souvent limitée puisqu'ils sont alimentés par des piles.
- **Sink :** c'est un nœud particulier du réseau. Il est chargé de la collecte des données issues des différents nœuds du réseau. Il doit être toujours actif puisque l'arrivée des informations est aléatoire. C'est pourquoi son énergie doit être illimitée. Dans un réseau de capteur sans fils plus ou moins large et à charge un peu élevée, on peut trouver deux sinks ou plus pour alléger la charge.
- **Centre de traitement des données :** c'est le centre vers lequel les données collectées par le sink sont envoyées. Ce centre a le rôle de regrouper les données issues des nœuds et les traiter de façon à en extraire de l'information utile exploitable. Le centre de traitement peut être éloigné du sink, alors les données doivent être transférées à travers un autre réseau, c'est pourquoi on introduit une passerelle entre le sink et le réseau de transfert pour adapter le type de données au type du canal (comme c'est illustré dans la figure 1.2)

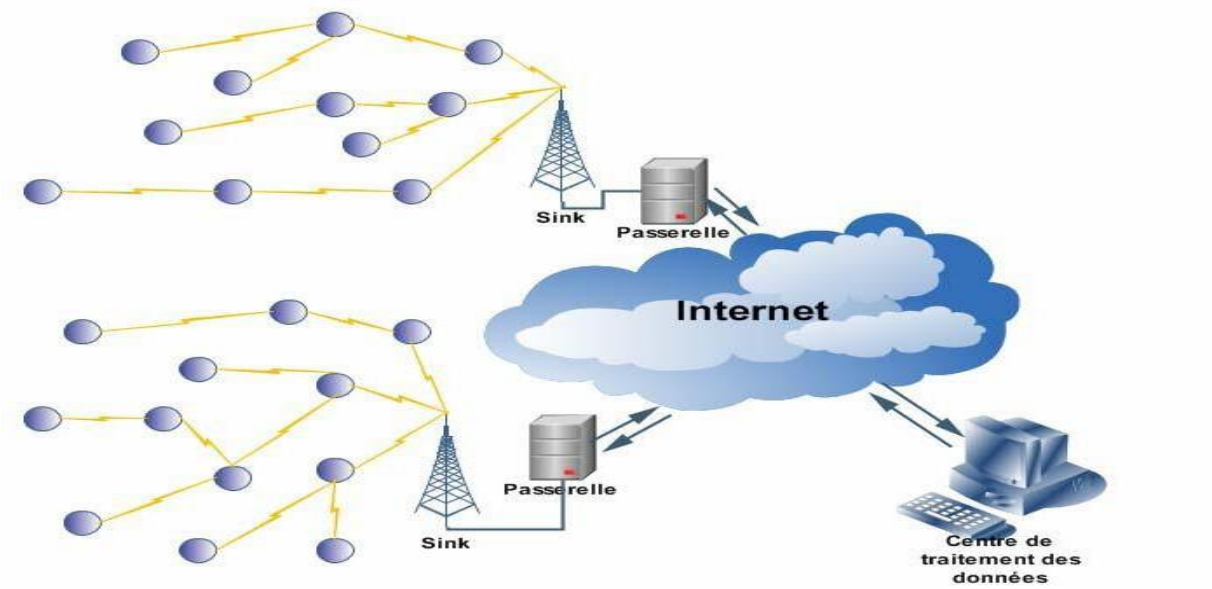


Figure 1.2: Architecture générale d'un réseau de capteurs sans fil [17].

3.5. Types des nœuds

Dans un réseau de capteurs il existe deux types de nœuds : nœud source et nœud sink. Un nœud source est n'importe quelle entité dans le réseau qui peut fournir de l'information, c'est à dire un simple nœud capteur .Un nœud sink est l'entité où les données sont récupérées. Il y a essentiellement trois types de sink [17]:

Un nœud sink est l'entité où les données sont récupérées. Il y a essentiellement trois types de sink :

- Un nœud appartenant au réseau comme n'importe quel autre nœud.
- Une entité extérieure au réseau. Pour ce deuxième cas, le sink peut être un dispositif extérieur, par exemple, un ordinateur portatif ou un PDA interagissant avec le réseau.
- Une passerelle vers un autre réseau tel qu'Internet, où la demande de l'information vient d'un certain centre de traitement lointain

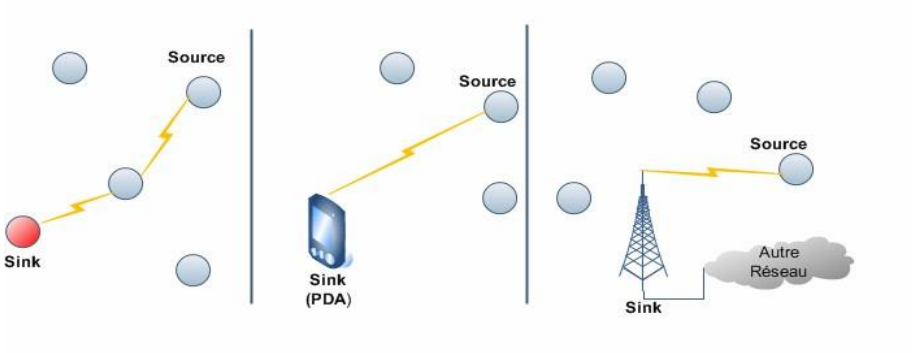


Figure 1.3: Différents types de sink[17].

3.6. Types de communications

Conceptuellement, la communication dans un RCSF peut être classifiée en deux catégories: communication d'application et communication d'infrastructure. La communication d'application concerne essentiellement les données captées ou les informations obtenues à partir des nœuds capteurs dans la perspective d'informer l'utilisateur final sur le phénomène observé. Deux modèles existent pour ce type de communication : modèle coopérative permettant aux nœuds capteurs de communiquer avec d'autres nœuds capteurs pour satisfaire l'objectif de l'utilisateur final, et modèle non coopérative dans lequel les nœuds capteurs n'ont pas besoins de coopérer pour la dissémination des données.

En général, la communication d'infrastructure se réfère aux communications nécessaires pour configurer, maintenir et optimiser certaines opérations. Ces communications sont fortement liées aux spécificités de l'application considérée puisque le réseau doit être capable de configurer lui même afin de satisfaire ces spécificités. La communication d'infrastructure représente les messages de contrôles des protocoles réseau (overhead), il est donc important de la minimiser le plus possible tout en assurant une meilleure communication d'application.

En général, dans un RCSF deux types de nœuds sont reconnus logiquement : les nœuds dont la tâche principale est de transmettre ses propres données collectées (nœuds capteurs) et les nœuds qui assurent essentiellement le relayage des paquets de données (nœuds relais). Ainsi, les données d'un nœud capteur sont routées des nœuds sources vers le Sink via les nœuds relais en créant une topologie multi-sauts. Cette organisation logique permet de dégager quatre types de communications comme le montre la Figure1.4, qui seront pris en compte spécialement par les couches inférieures telles que la sous couche MAC.

- **Communication de type nœud capteur à nœud capteur** : ce type de communication directe est utilisé dans les opérations locales entre nœuds capteurs, par exemple durant les processus de mise en cluster (ou clustering) ou de création de chemins de routage.
- **Communication de type nœud capteur à nœud relais** : dans ce cas, les données collectées sont transmises du nœud capteur vers un nœud relais. Ce type de communication est souvent unicast.
- **Communication de type nœud relais à nœud capteur** : elle est utilisée dans le cas de transmission, souvent multicast, de requêtes (données ou messages de signalisation) formulées par un utilisateur via le Sink et certains nœuds relais pour atteindre un sous ensemble de nœuds capteurs à la fois.
- **Communication de type nœud relais à nœud relais** : les nœuds relais forment en réalité l'épine dorsale (ou backbone) d'un RCSF. La communication entre ces nœuds est dans la plupart des cas unicast. Ces nœuds capteurs sont capables d'effectuer cette activité de relayage du moment que chacun deux est à priori équipé d'une interface sans fil de communication (ou transeiver) [4].

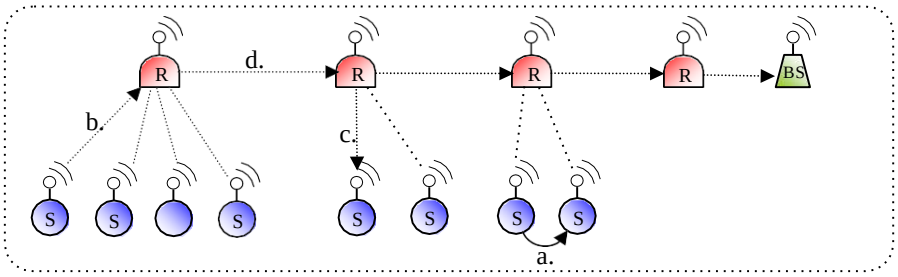


Figure 1.4 : Types de communications dans un RCSF typique [4]

3.7. Les modèles de transmission des données dans les RCSF

La transmission de données dans les réseaux de capteurs peut se faire suivant plusieurs modèles dont on distingue trois essentiels :

3.7.1. modèle driven-event

Au lieu d'avoir un nœud émetteur et un autre récepteur de l'information, on trouve un nœud récepteur (le nœud de contrôle « sink ») et un groupe de nœuds capteurs, se trouvant proche de l'événement, qui sont tous des émetteurs de la même information[17].

L'avantage pour ce modèle, repose essentiellement sur la détection de l'événement et la rapidité des prises des réactions nécessaires pour assurer l'aspect temps réel des applications.

L'inconvénient majeur de ce modèle est la redondance des données, car les nœuds excités par le même événement envoient la même information au « sink ».

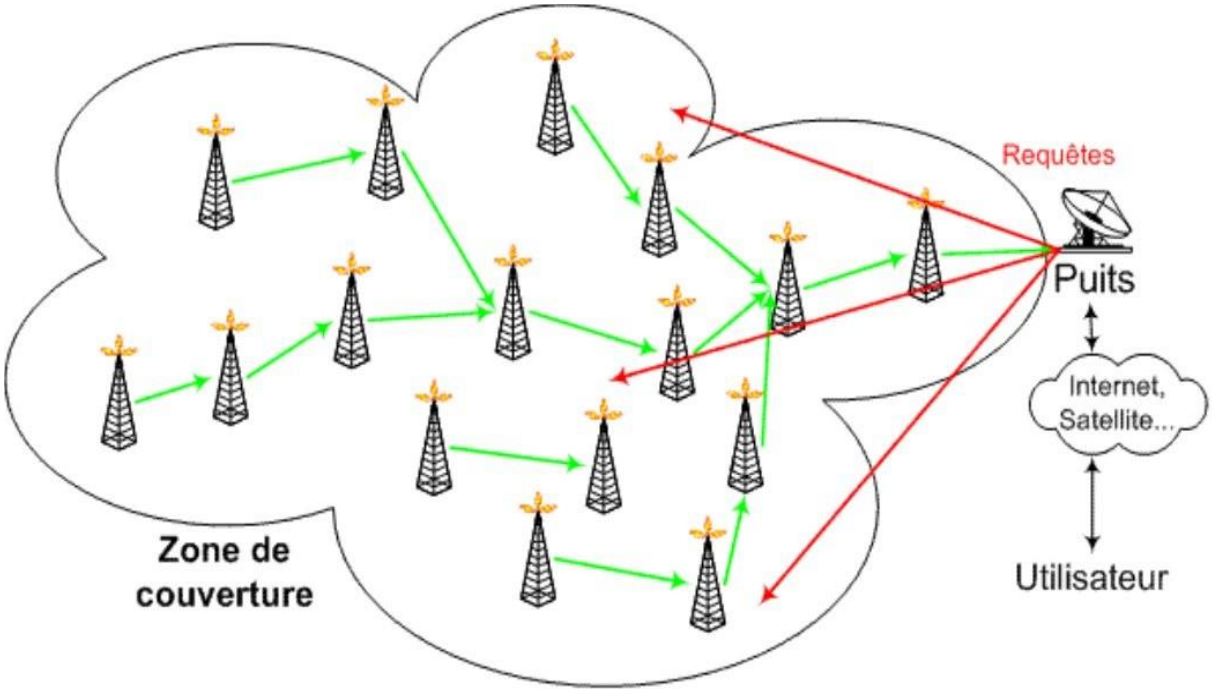


Figure 1.5 : Collection des informations à la demande [13].

3.7.2. Le modèle query-driven

Ce modèle est semblable au modèle driven event sauf que la collecte des informations sur l'état de l'environnement est initiée par des interrogations envoyées par le « sink », on peut utiliser ce modèle pour contrôler et reconfigurer les nœuds. Par exemple, le « sink » peut envoyer des commandes au lieu des interrogations pour modifier le programme d'un noeud capteur, son taux de trafic et son rôle. Seul le nœud capteur jouant le rôle de «sink» est autorisé d'émettre des demandes d'interrogations ou des commandes et ce pour assurer

l'ordre et l'hiérarchie de réseau de capteur[17].

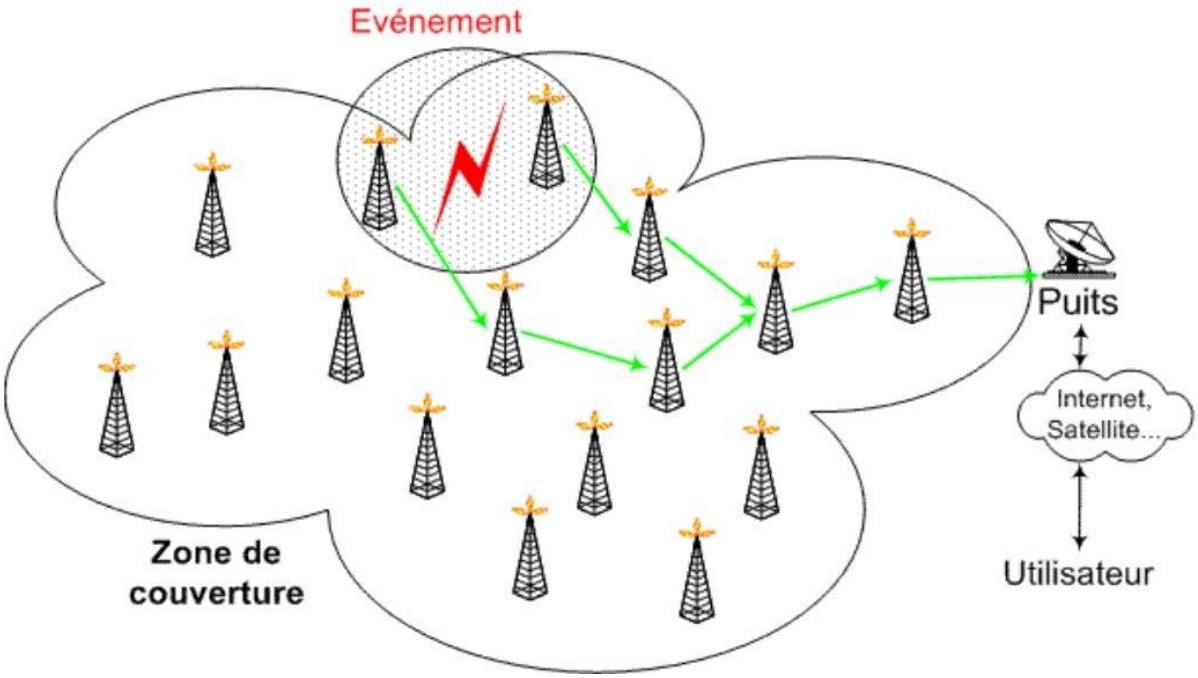


Figure 1.6 : Collection des informations suite à un événement [13].

3.7.3. Le modèle continuous

Dans ce modèle, les nœuds capteurs envoient les informations d'une manière continue au nœud « sink » suivant un volume de trafic prédéterminé [17].

3.7.4. Le modèle hybride

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) [5].

4. Les types des erseaux de capteurs sans fil

Selon des critères bien spécifiques, comme la mobilité, l'homogénéité des nœuds du réseau, la nature de l'application et le type des données captées, les RCSF peuvent être classés en plusieurs classes [19].

4.1. Selon le critère de mobilité

Les nœuds capteurs, ainsi que la station de base dans un réseau de capteurs sans fil peuvent

être stationnaires ou bien mobiles. On parle alors des réseaux de capteurs statiques ou mobiles respectivement.

4.1.1. Les réseaux de capteurs statiques

Dans les réseaux de capteurs statiques, et les nœuds capteurs et la station de base sont stationnaires ; ils gardent leurs positions initiales tout au long de leur durée de vie. Ce type de réseaux de capteurs est bénéfique dans certains types d'applications qui exigent que les capteurs soient placés dans des endroits stratégiques pour les contrôler. En effet, tel type de RCSF est caractérisé par une topologie statique, une localisation facile des nœuds dans le réseau et des techniques de routage assez simples.

4.1.2. Les réseaux de capteurs mobiles

Contrairement aux RCSF statiques, dans les réseaux de capteurs mobiles, les capteurs et/ou la station de base ont la capacité de se mobiliser. La mobilité du capteur se produit soit quand le capteur est collé sur un objet mobile, soit quand le capteur s'auto-déplace (cas d'un capteur muni d'un moteur). La mobilité est indispensable dans les réseaux de capteurs destinés aux applications de suivi, par exemple, quand les capteurs sont embarqués sur des véhicules, ou sur des animaux. Elle est (la mobilité) également avantageuse du point de vue coût d'investissement ; au lieu de déployer plusieurs nœuds statiques, un nombre minime de dispositifs mobiles est suffisant. Cependant, lorsque la mobilité est trop fréquente, elle ne peut être considérée comme un problème secondaire. Ainsi, le changement fréquent de la topologie complique les mécanismes de routage et de localisation.

4.2. Selon le critère de l'homogénéité

Suivant ce critère, on observe deux types des réseaux de capteurs sans fil : les réseaux de capteurs homogènes et les réseaux de capteurs hétérogènes.

4.2.1. Réseaux de capteurs homogènes

Un réseau de capteurs est dit homogène si tous les nœuds capteurs sont équivalents sur le plan capacités et contraintes (faibles ressources et durée de vie courte). C'est le type qu'on trouve souvent dans la majorité des applications des réseaux de capteurs, car ils répondent au besoin d'autonomie.

4.2.2. Les réseaux de capteurs hétérogènes

A l'encontre des réseaux de capteurs homogènes, les réseaux de capteurs hétérogènes comportent deux types de nœuds capteurs : les nœuds capteurs contraints (battery-powered) et les nœuds capteurs puissants non limités en ressources (particulièrement les ressources énergétiques comme ils sont directement liés à un secteur d'alimentation électrique). Dans ce type de RCSF, les nœuds contraints doivent préserver autant que possible leur réserve énergétique en minimisant les tâches les plus coûteuses en énergie tout comme la communication radio. Ainsi, les calculs et les traitements compliqués sont délégués aux nœuds puissants pour équilibrer la charge et maximiser la durée de vie du réseau. Bien que les RCSF hétérogènes soient plus avantageux que les RCSF ordinaires (homogènes), leur adoption est limitée à un nombre réduit d'applications. Cela est dû à la difficulté du déploiement des RCSF hétérogènes dans des milieux hostiles, isolés ou inaccessibles.

4.3. Selon le type de l'application

Le déclenchement du processus de captage de données dans un réseau de capteurs sans fil dépend des exigences applicatives et de l'importance de la donnée captée en elle-même. Donc, on distingue deux types de RCSF : temporels (time-driven) ou évènementiels (event-driven).

4.3.1. Les réseaux de capteurs temporels

Un réseau de capteurs temporel est approprié pour des applications qui nécessitent un prélèvement périodique des données. Tel est le cas par exemple dans les applications de monitoring (feu ou météo). Un écoulement en rafale, périodique, du trafic est très susceptible dans ce type d'applications. Par conséquent, des mécanismes de gestion raisonnable des ressources sont primordiaux.

4.3.2. Réseaux Les de capteurs évènementiels

Dans certaines applications, les capteurs doivent réagir rapidement à des changements brusques des valeurs captées et donner des réponses immédiates à l'occurrence des évènements. Un prélèvement périodique des données est inadapté pour ce type de scénario.

4.4. Selon les données captées

Les données que récoltent les nœuds dans un réseau de capteurs peuvent être de type simple, comme ils peuvent être de type multimédia. De plus, un nœud capteur peut capter un seul type de données (exemple : que la température) ou plusieurs types à la fois (exemple : image, température et humidité).

4.4.1. Les réseaux de capteurs standards

Il s'agit des RCSF ordinaires où les données récoltées sont de types scalaires, comme par exemple : la température, l'humidité, la pression, etc. les RCSF de tel type partagent les caractéristiques déjà mentionnées.

4.4.2.Les réseaux de capteurs multimédia

Certaines applications des réseaux de capteurs, exigent que les données à capter soient de type multimédia (son, image ou vidéo) comme c'est le cas par exemple dans les applications médicales et les applications militaires. Néanmoins, les données multimédia sont reconnues pour être volumineuses et occupent donc, un espace mémoire important. Ainsi, des techniques de représentation différente que celles des données ordinaires sont nécessaires pour les données multimédia. Les réseaux de capteurs multimédia (ou Wireless Multimedia Sensor Networks: WMSN) requièrent des protocoles performants ainsi que des considérations particulières pour répondre à leurs défis en matière de qualité de service et de capacités de traitement exigées. D'autres spécificités liées aux WMSNs sont données ci-dessous :

- **le déploiement** : les nœuds dans les réseaux de capteurs standards sont souvent déployés aléatoirement. En revanche, dans les réseaux de capteurs multimédia, le déploiement des nœuds est généralement précis et étudié d'avance, particulièrement quand il s'agit du captage des images.

- **La puissance de traitement :** les traitements à effectuer sur les données scalaires sont faibles. Néanmoins, pour le cas des données multimédia, les nœuds capteurs effectuent des traitements intensifs ce qui demande plus de performance matérielle.

- **Consommation d'énergie** : puisque la qualité de service et les traitements intensifs sont pratiquement gourmands en énergie, les mécanismes de gestion de la consommation énergétique dans les réseaux de capteurs multimédia doivent être

très efficaces. A cet effet, on note que dans ce cas, le remplacement des batteries des nœuds capteurs est souvent possible (tout dépend de la nature du champ de captage).

- **Qualité de service :** les réseaux de capteurs multimédia revendiquent suffisamment de bande passante ainsi qu'une faible latence pour qu'ils soient opérationnels, ce qui n'est pas le cas dans les réseaux de capteurs standards où la qualité de service est relâchée pour un besoin en un moindre coût et une faible dissipation des ressources.

4.4.3.Les réseaux de capteurs multimodaux

Un nœud capteur dans un RCSF multimodal peut récolter plusieurs informations de types différents où les types peuvent être scalaires ou multimédia. Par exemple, un nœud capteur peut capturer et la température et l'image. Ainsi, un seul nœud capteur multimodal peut remplacer tout un groupe de capteurs ordinaires. Ceci est particulièrement avantageux dans le cas où l'on veut avoir plus d'une information environnementale sur le même endroit d'intérêt [19].

5. Caractéristiques des réseaux de capteur

Parmi les caractéristiques les plus importantes d'un réseau de capteurs, nous citons :

- **La durée de vie limitée :** Les nœuds capteurs sont très limités par la contrainte d'énergie, ils fonctionnent habituellement sans surveillance dans des régions géographiques éloignées. Par conséquent recharger ou remplacer leurs batteries devient quasiment impossible.

- **Ressources limitées :** Habituellement les nœuds capteurs ont une taille très petite, ce facteur de forme limite la quantité de ressources qui peuvent être mises dans ces nœuds. En conséquence, la capacité de traitement et de mémoire est très limitée.

- **Topologie dynamique :** La topologie des réseaux de capteurs change d'une manière fréquente et rapide car: les nœuds capteurs peuvent être déployés dans des environnements hostiles (par exemple un champ de bataille), la défaillance d'un nœud capteur peut donc être très probable. De plus, les nœuds capteurs et les nœuds finaux où ils doivent envoyer l'information capturée peuvent être mobiles.

- **Agrégation des données :**Dans les réseaux de capteurs, les données produites par les nœuds capteurs sont très reliées, ce qui implique l'existence de redondances de données. Une approche répandue consiste à agréger les données au niveau des nœuds intermédiaires afin de réduire la consommation d'énergie lors de la transmission de ces données.

- **La scalabilité :**Les réseaux de capteurs engendrent un très grand nombre de capteurs, ils peuvent atteindre des milliers voir des millions de capteurs. Le défi à relever par les RCSFs est d'être capable de maintenir leurs performances avec ce grand nombre de capteurs.

- **Bande passante limitée :** En raison de la puissance limitée, les nœuds capteurs ne peuvent pas supporter des débits élevés.

- **sécurité physique limitée:** Cela se justifie par les contraintes et limitations physiques qui minimisent le contrôle des données transmises.

6.Pile protocolaire

La pile protocolaire utilisée par la station de base ainsi que tous les autres capteurs illustrés par la figure 1.7. Cette pile de protocoles combine routage et gestion d'énergie et intègre les données avec les protocoles réseau. Elle communique de manière efficace (en terme d'énergie) à travers le support sans fil et favorise les efforts de coopération entre les nœuds-capteurs. La pile protocolaire comprend la couche application, la couche transport, la couche réseau, la couche liaison de donné, la couche physique, le plan de gestion de l'énergie, le plan de gestion de la mobilité et le plan de gestion des tâches. [18]

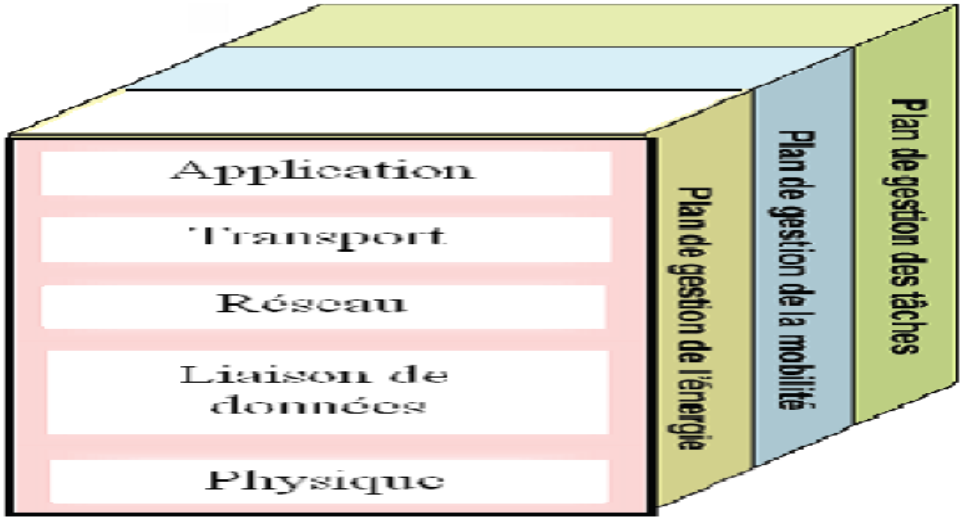


Figure 1.7 : pile protocolaire [18]

7. Domaines d'application des réseaux de capteurs

Dans les paragraphes qui suivent nous présentons quelques exemples de RCSF. Pour éviter toute polémique à ce sujet, nous avons essayé de présenter certaines applications réelles et applicables et d'autres qui peuvent être envisagées pour régler de sérieux problèmes que vie un pays émergent comme le notre [4].

7.1. Applications militaires

Les RCSF sont appliqués avec beaucoup de succès dans la surveillance militaire. Actuellement, ils peuvent être une partie intégrale dans le commandement, le contrôle, la communication, le calcul, l'intelligence, la surveillance, la reconnaissance et l'optimisation. Un exemple de ce type de scénario est illustré dans la Figure 1.7.

Dans un champ de bataille, le déploiement rapide, l'auto-organisation et la tolérance aux fautes du réseau devraient être exigés. Les dispositifs ou les nœuds de capteurs devraient fournir les services suivants :

- La surveillance des forces amies, de l'équipement et des munitions.
- La surveillance des champs de bataille.
- La reconnaissance des forces ennemies.
- Le ciblage.
- L'évaluation des dommages.

- La détection des attaques nucléaires, biologiques et chimiques.

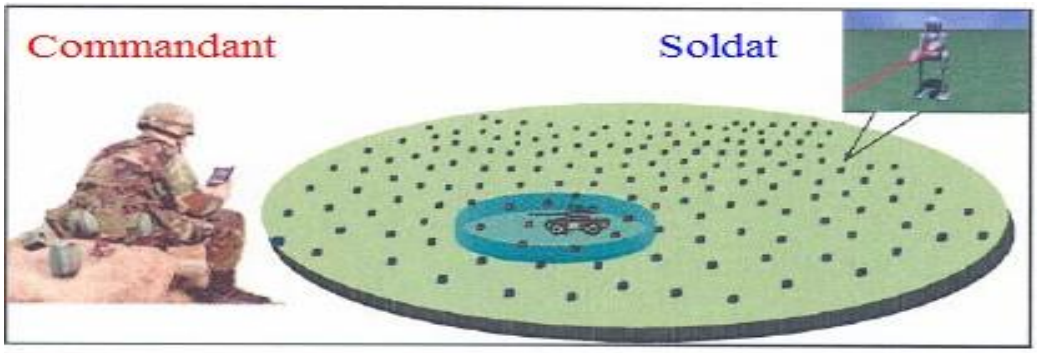


Figure 1.8 : Exemple d'interaction entre un responsable militaire et ses soldats [4].

7.2. Applications environnementales

Quelques applications environnementales des réseaux de capteurs sans fil incluent notamment :

- le dépistage des mouvements des oiseaux, petits animaux et insectes,
- la surveillance environnementale des conditions qui affectent les récoltes et le bétail,
- les macro-instruments pour la surveillance à grande échelle de la terre et l'exploration planétaire,
- la détection des produits chimiques et biologiques,
- l'agriculture avec précision,
- le contrôle de l'environnement marin (capteurs acoustiques), du sol et contextes atmosphériques,
- la détection de feux de forêt,
- la recherche météorologique ou géophysique,
- la détection d'inondation, de tremblements de terre (ex : tsunami), de radiation,
- les études de pollution.

7.2.1. Détection des feux de forêts

Puisque les nœuds capteurs peuvent être stratégiquement, aléatoirement, et en masse déployés dans la forêt, les nœuds capteurs peuvent transmettre l'origine exacte du feu aux gardiens forestiers avant que le feu soit incontrôlable. Des millions de nœuds capteurs peuvent être déployés et intégrés en utilisant les fréquences radio et les systèmes optiques. En outre, ils peuvent être équipés de modules pour recharger les batteries, comme les piles solaires, parce que les capteurs peuvent être laissés sans surveillance pendant des mois et

même des années. Les capteurs devront collaborer entre eux pour mieux capter et surmonter les obstacles comme les arbres et les roches [4].

7.2.2. Détection des inondations

ALERT system [Web25] est un exemple de détection d'inondations, déployé en Europe et aux Etats Unis. Différents types de capteurs sont utilisés pour mesurer le niveau de l'eau, les perturbations et le temps qu'il fait. Ces informations supplémentaires sont ensuite envoyées à un système centralisé de base de données d'une manière prédéfinie [4].

7.2.3. Agriculture de précision

Certains des avantages qu'offre un tel réseau sont la capacité de surveiller le niveau de pesticides dans l'eau potable, le niveau d'érosion du sol et le niveau de pollution atmosphérique.

7.2.4. Le contrôle de l'environnement marin

Un réseau de capteurs acoustiques contient un nombre variable de nœuds et de véhicules qui doivent collaborer pour surveiller une zone donnée. Nous allons voir une partie de la large étendue des applications pour les réseaux sous-marins de détecteurs acoustiques :

- **Surveillance de l'environnement marin** : ceci inclut la surveillance de la pollution (chimique, biologique, nucléaire), la surveillance des courants d'eau et du vent pour disposer des prévisions météorologiques, la détection du changement de climat et sert à mieux comprendre et prévoir les effets des activités humaines sur l'écosystème ainsi que la traque des poissons et des microsystèmes.
- **Exploration sous-marine** : peut aider à détecter les gisements de pétrole sous-marins ou les réservoirs et à déterminer des itinéraires pour la pose de câbles sous-marins et aide dans l'exploration pour les minerais nobles.
- **Prévention des catastrophes** : les réseaux de capteurs qui mesurent l'activité sismique des sites éloignés peut fournir des avertissements de tsunami aux secteurs côtiers ou étudier les effets des tremblements de terre sous-marins.

- **Assistance à la navigation :** des capteurs peuvent être utilisés pour identifier les risques dans les fonds marins, localiser les roches dangereuses, bancs dans les eaux peu profondes ou les épaves submergées.

7.3 Applications sanitaires

Les réseaux de capteurs sont également largement répandus dans le secteur de la santé. Dans certains hôpitaux modernes, des réseaux sont construits pour surveiller des données physiologiques des patients, pour commander la voie d'administration des médicaments et pour surveiller les patients et les médecins à l'intérieur d'un hôpital [4].

La maison de repos à long terme (Long-Term Nursing Home): cette application est dédiée aux soins des personnes âgées. Dans la ville, les caméras dans les fermes, les capteurs de pression, les capteurs d'orientation et les capteurs pour la détection de l'activité des muscles construisent un réseau complexe. Elles soutiennent la détection de chute, la détection d'évanouissement et la surveillance des signes vitaux essentiels. Ces applications réduisent le coût du personnel et accélèrent l'intervention dans les situations d'urgence.

7.4 Applications domestiques

Avec le développement commercial des applications des RCSF, il n'est pas si difficile d'imaginer que les applications domestiques évolueront dans le futur. Plusieurs concepts sont déjà élaborés par les chercheurs et les architectes, comme "Smart Environment : Laboratory résidentiel " et" Smart Kindergarten ". Certains sont même réalisés. Voyons le concept "la maison intelligente ou Smart home" : après une dure journée de travail, tu reviens à la maison. À la porte d'entrée, le capteur te détecte et t'ouvre la porte, puis il allumera la bouilloire électrique pour bouillir de l'eau et mettra le conditionnement d'air en marche. Tu t'assieds dans le sofa, paresseux. La lumière sur la table s'allume automatiquement parce que le capteur de pression sous le coussin a détecté ton poids. La TV est également en marche. À une certaine heure, cinq capteurs dans chaque coin dans la chambre mesurent la température. À l'origine, il y a également un capteur dans l'air conditionné. Mais, il peut seulement obtenir la température au bord de la machine, pas la vraie température dans la chambre. Ainsi, les capteurs dans la chambre détecteront l'environnement. L'air conditionné se tournera vers le mode veille jusqu'à ce que tous les capteurs obtiennent la bonne température. Les lumières dans le couloir, dans les toilettes et le balcon sont toutes équipés d'un capteur et elles peuvent être allumées ou éteintes automatiquement. Même les fenêtres sont également dotées de

capteurs vibratoires, reliés à un poste police pour signaler une intrusion [4].

7.5 Autres applications d'intérêt national

- Surveillance des patients en permanence (population du sud, possibilité d'extraction solaire).
- Utilisation des RCSF pour la prise de décision efficace par les autorités locales et les services annexes dans les environnements urbains complexes (grandes villes : système d'éclairage pour l'économie de l'énergie, gestion de trafic routier pour minimiser les accidents et maîtriser les embouteillages, gestion rationnelle de distribution d'eau potable avec possibilité de détection en temps réel des fuites d'eau d'origine externe, gestion des parking, pollution, détection des feu de forêts ou d'autres endroits sensibles…etc).
- Gestion de l'irrigation (agriculture) dans des zones arides où les conditions d'utilisation d'eau sont très difficiles [4]

Figure 1.9 est une illustration de cet exemple.

- onitoring d'ouvrages d'art tels que les ponts pour sauver des vies humaines (autoroute est-ouest où lenombre de ponts est important, ponts stratégiques dans les agglomérations comme le pont Zabana-ORAN).
- Exploration efficace et économique au sud dans le domaine pétrolier (possibilité d'extraction d'énergie solaire), monitoring des installations pétrolières pour la prédiction des catastrophes (comme celle survenue à Skikda il y a quelques années).

8.Classification des protocoles de routage dans les RCSF

Récemment, les protocoles de routage pour les RCSF ont été largement étudiés, Comme l'illustre la figure II.1, ils peuvent être classés selon plusieurs critères [13] :

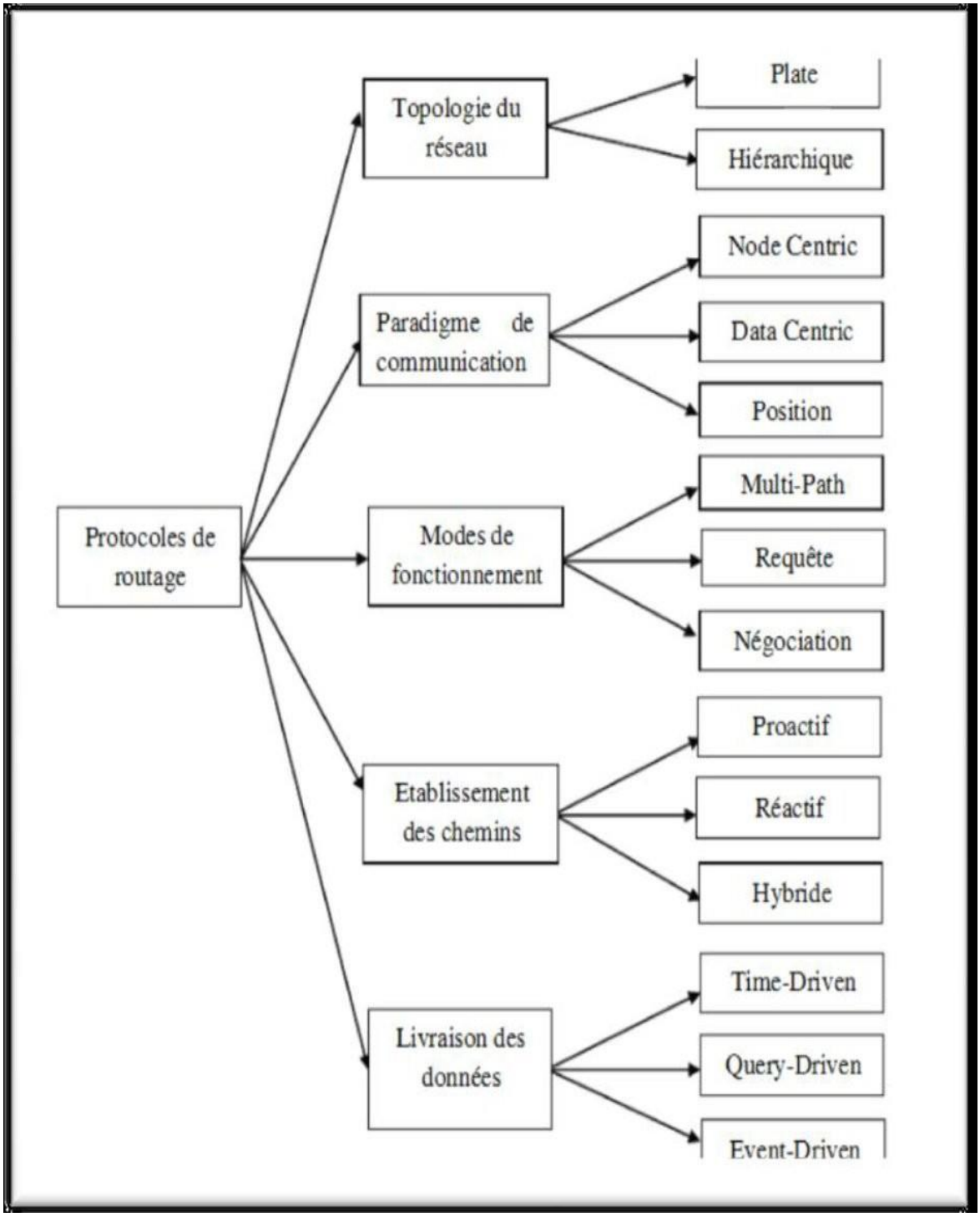


Figure 1.10 : Classification des protocoles de routage dans les RCSF.

8.1. Selon la topologie du réseau

La topologie détermine l'organisation des capteurs dans le réseau. Globalement, il existe deux topologies dans les RCSF: La topologie plate et la topologie hiérarchique [13].

8.1.1.Topologie Plate

Un réseau de capteurs sans fil plat est un réseau homogène, où tous les nœuds sont identiques en termes de batterie et des fonctions, excepté le « Sink ». Dans ce type de topologie, les capteurs communiquent entre eux afin d'acheminer l'information au nœud centralisé (station de base). Ce processus d'acheminement d'information peut prendre deux formes : communiquer directement avec la station de base Figure 1.10 (a), ou via un mode multi-sauts Figure 1.10 (b). De plus dans ce type de topologie Figure (a) tous les nœuds peuvent envoyer leurs données à la station de base en utilisant une forte puissance, ceci peut conduire à la diminution de la durée de vie du réseau.

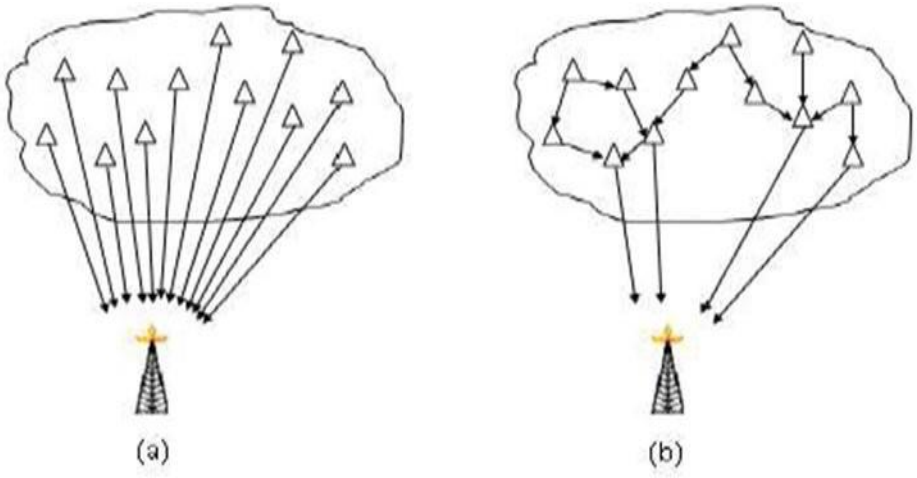


Figure 1.11 : Architecture de communication dans une topologie plate [13].

8.1.2. Topologie hiérarchique

Dans cette architecture, le réseau est constitué d'un ensemble de groupe de capteurs (clusters), tel qu'il est illustré dans la Figure II.3. Le nœud représentant le cluster, appelé cluster-head, a la responsabilité de transmettre les données à la station de base. L'avantage majeur de ce type d'architecture est le prolongement de la durée de vie du réseau de capteurs. Ce résultat est achevé en désignant le cluster-head comme étant le nœud responsable de la transmission des informations (agrégées). Ce procédé est meilleur de celui où tous les nœuds envoient leurs données à un emplacement distant.

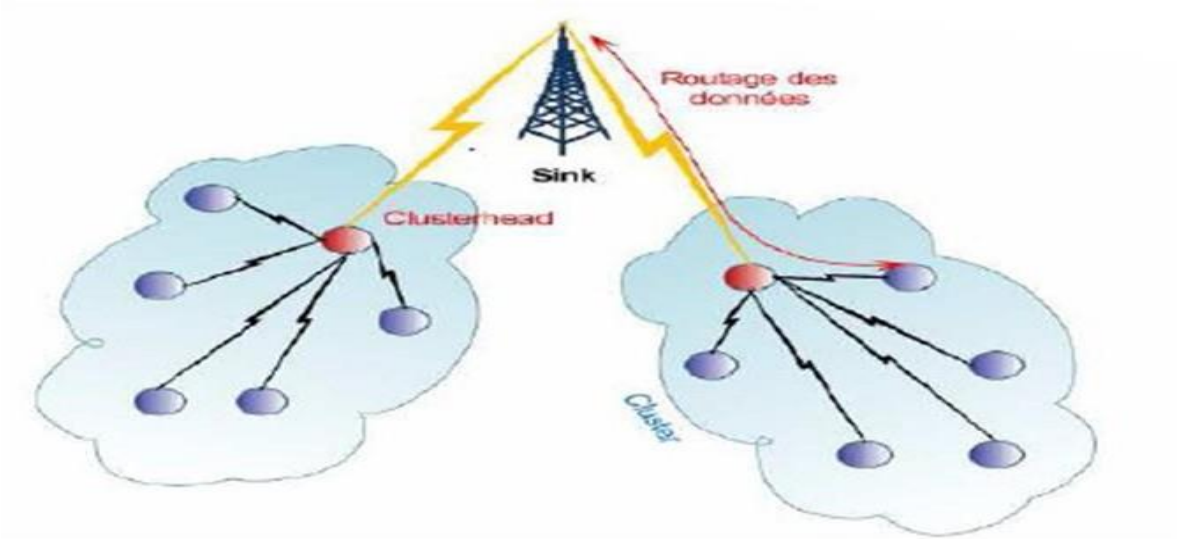


Figure 1.12 : Topologie à base de cluster [13].

8.2. Selon la méthode d'établissement de routes

Suivant la manière de création et de maintien des chemins pendant le routage nous distinguons trois catégories de protocoles de routages : protocoles proactifs, réactifs ou hybrides[13].

8.2.1. Protocole proactif

Ces protocoles de routage essaient de maintenir les meilleurs chemins existants vers toutes les destinations possibles au niveau de chaque nœud du réseau. Les routes sont sauvegardées mêmes si elles ne sont pas utilisées. Chaque nœud du réseau maintient une table de routage pour toutes les destinations indépendamment de l'utilité des routes. Les protocoles proactifs sont adaptés aux applications qui nécessitent un prélèvement périodique des données. Et par conséquent, les capteurs peuvent se mettre en veille pendant les périodes d'inactivité, et n'enclencher leur dispositif de capture qu'à des instants particuliers.

8.2.2. Protocoles réactifs

Ces protocoles (dits aussi, les protocoles de routage à la demande) créent et maintiennent des routes selon les besoins. Lorsque le réseau a besoin d'une route, une procédure de découverte de route est lancée. Ce type de protocoles est pratique pour des applications temps réel où les capteurs doivent réagir immédiatement à des changements soudains des valeurs captées. En effet, un prélèvement périodique des données aurait été inadapté pour ce type de scénarios.

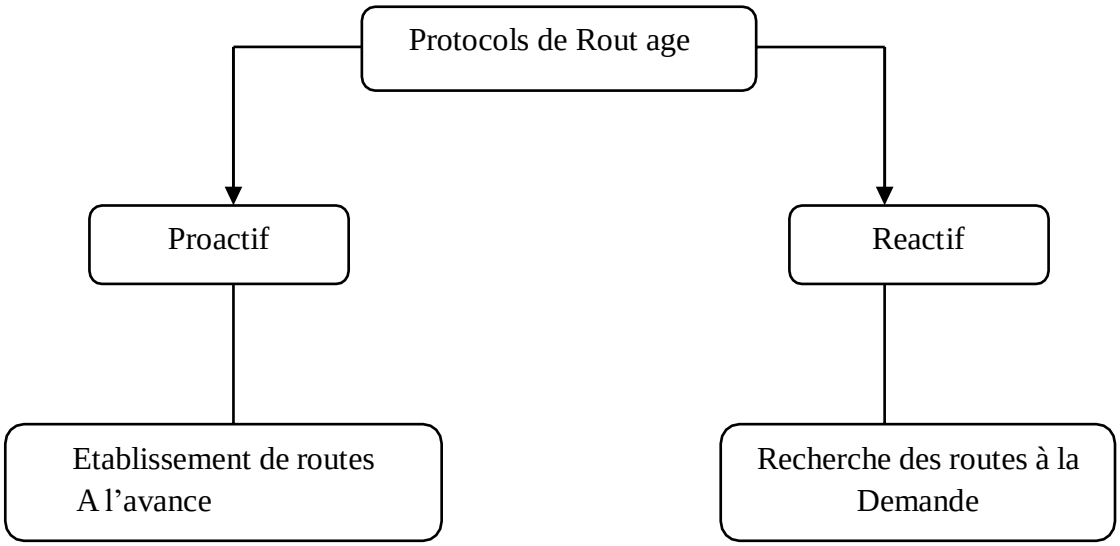


Figure 1.13 Classification selon la méthode d'établissement de routes

8.2.3 Protocoles hybrides

Ces protocoles combinent les deux idées des protocoles proactifs et réactifs. Ils utilisent un protocole proactif pour apprendre le proche voisinage (par exemple le voisinage à deux ou à trois sauts), ainsi ils disposent de routes immédiatement dans le voisinage. Au-delà de la zone du voisinage, le protocole hybride fait appel à un protocole réactif pour chercher des routes.

8.3 Selon les paradigmes de communication

8.3.1Centré-nœuds

Ce paradigme est celui employé dans les réseaux conventionnels, où il est nécessaire de

connaitre et d'identifier les nœuds communicants (comme l'adresse IP). Les réseaux ad hoc utilisent ce genre de paradigme, qui s'intègre bien avec l'utilisation de ce type d'environnement. Cependant pour les réseaux de capteurs, un routage basé sur une identification individuelle des nœuds ne reflète pas l'usage réel du réseau. Pour cela, un autre paradigme a été introduit : Centré-données. Néanmoins, le paradigme Centré-nœuds n'est pas à écarter totalement, car certaines applications nécessitent une interrogation individuelle des capteurs [13].

8.3.2Centré-données

Dans les RCSF, la donnée est généralement plus importante que le nœud lui- même. De ce fait, le routage et l'identification, dans ce paradigme, se font en fonction des données disponibles au niveau des capteurs. Ainsi le système peut être vu comme une base de données distribuée, où les nœuds forment des tables virtuelles, alimentées par les données captées. Le protocole Directed Diffusion (DD) est un exemple des protocoles de routage Centré-données[13].

8.3.3Basé-localisation

Dans cette approche, les positions des nœuds représentent le moyen principal d'adressage et de routage. Dans ce cas, le routage s'effectue grâce à des techniques géométriques afin d'acheminer l'information d'une zone géographique vers une autre. Ce type de mécanismes nécessite le déploiement d'une solution de positionnement, dont le degré de précision requis dépend de l'application ciblée [13].

8.4 .Selon le mode de fonctionnement du protocole

Le mode de fonctionnement définit la manière avec laquelle les données sont propagées dans le réseau. Selon ce critère, les protocoles de routage peuvent êtres classifiées quatre catégories : routage basé sur la qualité de service "QoS" (Quality of Service), routage base sur les requêtes (Query-Based Routing), routage multi-chemins (Multi-Path Routing), et routage basé sur la négociation (Negociation Based Routing).

8.4.1.Routage basé sur la qualité de service

Dans les protocoles de routage basé sur la QoS, le réseau doit équilibrer entre la consommation d'énergie et la qualité de données. En particulier, le réseau doit satisfaire

certaines métriques de QoS, par exemple, retard, énergie, largeur de bande passante, etc. Les protocoles de cette approche sont très recommandés pour les applications de surveillance (centrales nucléaires, applications militaires, etc).

8.4.2.Routage basé sur les requêtes

Dans ce type de routage, le puits génère des requêtes afin d'interroger les capteurs. Ces requêtes sont exprimées soit par un schéma valeur-attribut ou bien en utilisant un langage spécifique (par exemple SQL : Structured Query Language). Les nœuds qui détiennent les données requises doivent les envoyer au nœud demandeur à travers le chemin inverse de la requête. Les requêtes émises par le puits peuvent aussi être ciblées sur des régions spécifiques de réseau [13].

8.4.3. Routage basé sur les multi-chemins

Dans cette catégorie, les protocoles de routage utilisent des chemins multiples plutôt qu'un chemin simple afin d'augmenter la performance du réseau. La fiabilité d'un protocole peut être mesurée par sa capacité à trouver des chemins alternatifs entre la source et la destination en cas de défaillance du chemin primaire. Pour cette raison certains protocoles construisent plusieurs chemins indépendants, c.-à-d. : ils ne partagent qu'un nombre réduit (voir nul) de nœuds. Malgré leur grande tolérance aux pannes, ces protocoles requièrent plus de ressources énergétiques et plus de message de contrôle.

8.4.4. Routage basé sur la négociation

En détectant le même phénomène, les nœuds capteurs inondent le réseau par les mêmes paquets de données. Ce problème de redondance peut être résolu en employant des protocoles de routage basés sur la négociation. En effet, avant de transmettre, les nœuds capteurs négocient entre eux leur données en échangeant des paquets de signalisation spéciales, appelés métadonnées. Ces paquets permettent de vérifier si les nœuds voisins disposent déjà de la donnée à transmettre. Cette procédure garantit que seules les informations utiles seront transmises et élimine la redondance des données.

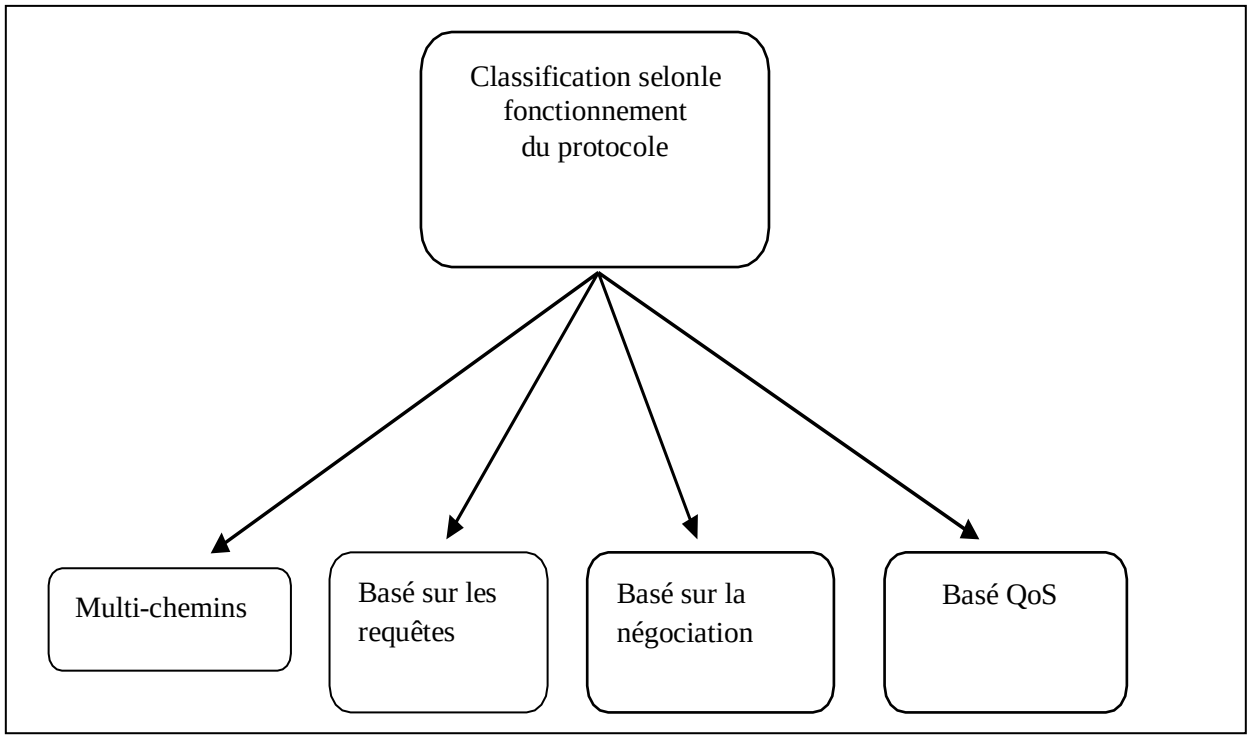


Figure 1.14 Classification selon le mode de fonctionnement du protocole.

8.5. Selon le modèle de livraison de données

Il est possible de distinguer trois modèles de livraison de données : time- driven, query-driven et event-driven [13].

8.5.1. Time-driven

Cette approche consiste à la livraison des données de façon périodique. Cet aspect permet aux capteurs de se mettre en veille pendant les périodes d'inactivité, et n'enclencher leur dispositif de capture qu'à des instants particuliers. Ainsi, la durée de vie du réseau va être allongée. Le modèle time-driven est approprié pour des applications qui nécessitent un prélèvement périodique des données. Par exemple, cela est utile dans des applications de monitoring (feu, météo).

8.5.2. Query-driven

Dans les applications query driven, la collecte d'informations sur l'état de l'environnement et la livraison des données sont initiées par des requêtes envoyées généralement par le nœud puits.

8.5.3. Event-driven

Ce modèle est généralement adopté dans les applications temps-réel où les capteurs doivent réagir immédiatement à des changements soudains des valeurs captées. Dans ce cas, le protocole de routage doit être réactif et doit donner des réponses rapides à l'occurrence d'un certain nombre d'évènements.

9. Métriques de performances

Les métriques de performance suivantes sont les plus utilisées pour évaluer les protocoles des RCSF :

- **Economie d'énergie/durée de vie du réseau :** puisque les nœuds capteurs sont alimentés par des batteries, les protocoles doivent être à économie d'énergie pour maximiser la durée de vie du réseau.

- **Latence :** l'utilisateur final est souvent intéressé d'avoir des informations dans un délai prédéfini sur le phénomène observé. La sémantique précise de cette métrique dépend fortement de l'application.

- **Exactitude ou précision:** une information exacte et précise obtenue via le réseau est un objectif principal de l'utilisateur final. Mais, cette exactitude dépend de l'application considérée. Il faut noter qu'il existe une différence entre l'exactitude,

la latence et l'efficacité énergétique. Une infrastructure donnée doit être adaptative pour permettre à l'application de bénéficier de l'exactitude et de la latence désirée avec une dépense énergétique minimale. Par exemple, l'application peut demander très fréquemment la dissémination des données à partir des mêmes nœuds capteurs. Elle peut aussi diriger la dissémination des données à partir de plusieurs nœuds capteurs avec une même fréquence.

- **Tolérance aux fautes :** les nœuds capteurs sont susceptibles de disparaître et être en dehors du fonctionnement global du réseau par manque d'énergie ou à cause des conditions physiques très sévères qui les entourent. On sait qu'il est difficile parfois impossible de les remplacer. Dans ces conditions, le réseau doit être tolérant aux fautes à un point où les pannes non catastrophiques soient entièrement cachées à l'application. Cette tolérance aux fautes peut être effectuée à l'aide de réplication des données et nécessite par conséquent une dépense énergétique supplémentaire. Une solution intéressante dans ce cas consiste à ne répliquer que les données de haute priorité qui dépend fortement de la spécificité de l'application.

Conclusion

Les réseaux de capteur sans fil présent un intérêt considérable et nouvelle étape dans l'évolution des technologies de l'information et de la communication cette nouvelle technologie suscite croissant vu la diversité de ces applications sante, environnement, industrie .Dans ce première chapitre nous avons présente les réseau de capteurs sans fil leur architecture de communication et leur diverses applications ,nous avons essayé a travers cette chapitre de mettre les point sur les classifications des protocoles de routage dédies aux RCSF selon plusieurs critères.

CHAPITRE 2

LES PANNES ET L'ENERGIE DANS WSN

1. Introduction

Certains capteurs peuvent être bloqués ou tomber en panne à cause d'un manque d'énergie, d'un dégât matériel ou d'une interférence environnementale. La panne d'un capteur ne doit pas affecter le fonctionnement global de son réseau. C'est le problème de fiabilité ou de tolérance aux pannes. La tolérance aux pannes a pour objectif de maintenir les fonctionnalités du réseau sans interruption due à une panne de certains capteurs. [2]

2. Les pannes dans les réseaux de capteurs

2.1Notion de panne (faute, erreur)

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

- **La défaillance** survient quand le système a un comportement anormal : une erreur est la partie de l'état du système (par rapport au processus de traitement) qui est susceptible d'entraîner une défaillance. La cause supposée de l'erreur est une faute. Une erreur est donc la manifestation d'une faute dans le système, et une défaillance est donc l'effet d'une erreur sur le service.

- **Une faute active** lorsqu'elle produit une erreur. Elle pourrait être soit une faute interne qui était précédemment dormante c'est-à-dire qu'elle ne produisait pas d'erreur et qui a été activée par le processus de traitement, soit une faute externe.

- **Une faute interne** peut passer, de manière cyclique, de l'état dormant à l'état actif. Une erreur est, par nature, temporaire. Elle peut être latente ou détectée: une erreur est latente tant qu'elle n'a pas été reconnue en tant que telle; elle est détectée soit par des mécanismes de détection d'erreur qui analysent l'état du système, soit par l'effet de l'erreur sur le service (défaillance).

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

... ⇀défaillance ⇀faute ⇀erreur ⇀défaillance ⇀faute ⇀... [2]

3. Origines des fautes

Les erreurs dans les données peuvent surgir à différents niveaux du système de RCSF. Ces erreurs sont directement liées aux processus d'acquisition et de traitement des données. Elles représentent des défaillances spécifiques aux quatre facteurs principaux suivants : le capteur, les méthodes de mesures, le facteur environnemental, et la communication.

3.1 Le capteur

Le capteur est un dispositif qui transforme les signaux physiques du monde réel en données. Ces appareils ont des capacités pour mesurer, calculer et communiquer les mesures acquises. Nous avons deux aspects importants à considérer : l'état physique du nœud/capteur et la limitation des ressources. Concernant l'état physique du nœud capteur nous considérons que le temps de vie du capteur, son calibrage, la dégradation de l'appareil, le mauvais fonctionnement, ou les erreurs d'installation etc., sont des aspects qui peuvent impacter la qualité des données lors de la prise de mesure. Les ressources du capteur représentent aussi une source d'erreurs. Le fait que les capteurs sont typiquement alimentés par des batteries (souvent non renouvelables), et le changement de ces batteries qui est souvent très délicat, voire impossible selon la localisation du capteur, le milieu d'observation et le type de réseau utilisé, font que la probabilité qu'ils manquent à des tâches prévues n'est pas négligeable. De plus, les limitations des capacités de calcul et stockage réduisent la capacité et la quantité de traitement exécuté au sein des capteurs. Ceci peut générer une perte d'information, de mauvais calculs, l'indisponibilité du capteur, ou encore l'envoi de données au serveur central sans demande directe.

3.2 Les méthodes de mesure

Généralement, les capteurs mesurent un seul élément (i.e. humidité, température…) à la fois, en considérant certaines exceptions (i.e. capteur RDI – pression, champ magnétique, température). Ceci est du au fait que la taille, l'énergie et la capacité de traitement au sein du capteur sont limitées. Ces aspects incitent à utiliser des méthodes de mesure peu coûteuses en termes de capacités (activation par périodes de temps, l'échantillonnage, l'activation par détection des seuils…) en dépit de la fiabilité de la donnée en termes de précision et exactitude de résultats.

3.3 Le facteur environnemental

Les réseaux de capteurs sont souvent déployés dans des zones à risque, donc les conditions de fonctionnement d'un capteur ou d'un réseau de capteur peuvent être affectées par les conditions environnementales (i.e. Inondations, neige, orage, séismes, etc.). De même, les conditions de fonctionnement des capteurs peuvent ne pas être optimales (i.e. températures élevées, excès d'humidité, etc.). Ces facteurs ont un impact important sur la qualité du fonctionnement des capteurs, et par conséquent sur les mesures qu'ils réalisent.

3.4 La communication

Une fois les données collectées (acquises et validées), les capteurs/nœuds capteur utilisent souvent une communication sans-fil pour communiquer les données acquises à un nœud central ou à un serveur. Cependant, cette communication peut être endommagée à cause de mauvaises conditions environnementales, le partage des ressources du capteur (interférence) ou le partage d'une même chaine de communication avec des autres capteurs au sein du réseau (congestion), etc. Une mauvaise communication peut générer des données erronées, données manquantes, des données en retard ou l'indisponibilité des sources. Ces aspects impacteront de façon importante la qualité de l'analyse des données en temps réel.

4. Classification des pannes

Différentes pannes peuvent se produire dans un RCSF, un déplacement d'un nœud peut causer une panne de lien, l'épuisement de la batterie conduit à une panne d'énergie synonyme d'arrêt du nœud, ou bien le nœud se met à envoyer des valeurs aléatoires du à une .Il existe donc différents types de pannes qui peuvent se produire dans un système, un

RCSF en l'occurrence, selon des critères donnés. Dans ce qui suit, une classification des pannes selon trois critères est exposée [15]

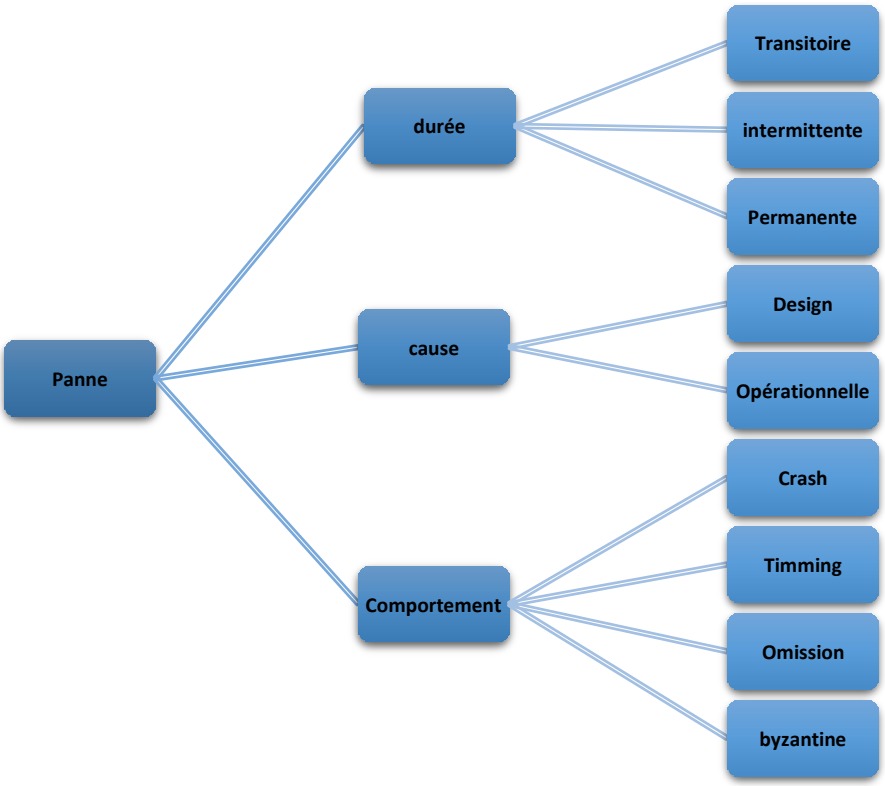


Figure 2.1 : Classification des pannes [19]

4.1Panne selon la dure

Basée sur sa durée, la panne peut être classifiée en [19]:

- **Transitoire :** conséquence d'un impact environnemental temporaire, elle peut éventuellement disparaître sans aucune intervention.
- **Intermittente :** variante de la panne transitoire, elle se produit occasionnellement et de façon imprévisible. Elle est généralement due à l'instabilité de certaines caractéristiques matérielles ou à l'exécution du programme dans un espace particulier de l'environnement.
- **Permanente :** continue et stable dans le temps, la panne permanente persiste tant qu'il n'y a pas d'intervention externe pour l'éliminer. UN changement physique dans un composant provoque une panne matérielle permanente.

4.2Pannes selon la cause

On distingue deux types de pannes selon leur cause [19] :

- **Panne de design :** due à une mauvaise structuration du réseau ou du composant en particulier. En pratique, Ce genre de panne ne devrait pas exister grâce aux tests et simulations avant la réalisation finale du réseau.

- **Panne opérationnelle :** qui se produit durant le fonctionnement du système. Elle est généralement due aux causes physiques. En outre, on peut distinguer, spécialement pour les réseaux de capteurs, trois principales causes :

  - **Energie :** l'épuisement de la batterie cause l'arrêt du capteur. La consommation d'énergie est très importante pour déterminer la durée de vie d'un nœud capteur, et donc de tout le réseau ;
  - **Sécurité** : la destruction physique accidentelle ou intentionnelle par un ennemi peut être une cause de panne. L'absence de sécurité dans les réseaux de capteurs augmente le risque des pannes de ce type ;
  - **Transmission :** la nature vulnérable de transmission radio, la présence d'obstacles dans les environnements hostiles ainsi que les interférences électriques peuvent être la source d'une faute lors du transfert de données.

4.3 Panne selon le comportement

Après l'occurrence d'une panne, on distingue quatre différents comportements possibles du composant concerné[19] :

- **Panne accidentelle (Crash) :** le composant soit, s'arrête complètement de fonctionner ou bien continue mais sans retourner à un état stable (valide).

- **Panne d'omission :** le composant n'est plus capable d'améliorer son service (échec total).

- **Panne de synchronisation (Timing) :** le composant effectue son traitement mais fournit le résultat en retard.

- **Panne Byzantine:** cette panne est de nature arbitraire ; le comportement du composant est donc imprévisible. Due à des attaques très malicieuses, ce type de pannes est considéré le plus difficile à gérer.

5.Définition de la tolérance aux pannes dans un RCSF :

Capacité d'assurer la continuité des fonctionnalités du RCSF sans aucune interruption et sans affecter la tâche globale du réseau, malgré d'éventuelles pannes de nœuds du RSCF[15].

6.Importance de la tolérance aux pannes dans les RCSF

L'importance d'une stratégie de tolérance aux pannes nous permet de distinguer trois sortes de RCSF où celle-ci (tolérance aux pannes) est primordiale [15].

- RCSF critiques
- RCSF à environnement hautement hostile
- RCSF critique à environnement hautement hostile

6.1RCSF critiques

Cette catégorie englobe tous les RCSFs qui sont déployés pour des applications de nature critique ne tolérant aucune interruption momentanée ou permanente du système dans des environnements peu, voir non hostile. Un arrêt de ce genre de RCSF peut avoir des conséquences souvent désastreuses, d'où la nécessité absolue d'avoir une très grande tolérance aux pannes. Nous pouvant citer comme exemple un RCSF pour la surveillance de l'état des patients dans un hôpital ou même chez eux [15].

6.2 RCSF à environnement hautement hostile

Le déploiement de ce genre de RCSF se fait dans des environnements présentant les particularités d'être instables et très risqués pour les nœuds qui composent ces RCSFs, ceci accroit considérablement la probabilité de pannes et de dysfonctionnements dus aux changements imprévisibles de l'environnement, avec souvent l'impossibilité d'interventions post-déploiement. La tolérance aux pannes permet donc la survie du RCSF et de la mission assignée à celui-ci dans de telles situations. Un exemple serait le déploiement d'un RCSF dans une forêt, au pôle nord ou dans un volcan pour la récolte de données scientifiques aidant à la compréhension d'un phénomène donné [15].

6.3 RCSF critiques à environnement hautement hostile

Il s'agit d'une combinaison des deux sortes de RCSF déjà évoqués ci-dessus, là aussi, la tolérance aux pannes s'avère être d'une importance capitale et ne doit plus que jamais être négligée. On peut trouver par exemple ce type de RCSF dans des applications de nature militaire comme la détection de cible et la surveillance dans un champ de bataille, ou encore la détection d'un feu de forêt. Les genres de RCSF cités précédemment mettent en avant l'importance de la présence d'une tolérance aux pannes au même titre que les autres critères nécessaires à la conception d'un RCSF robuste et efficace (sécurité, durée de vie et consommation d'énergie, routage…etc.)[15].

7. Procédure générale de tolérance de panne

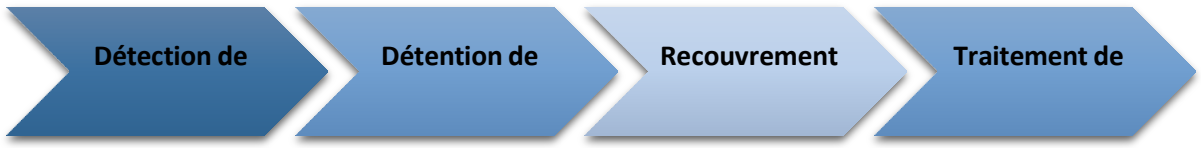


Figure 2.2 : Procédure générale de tolérance aux pannes [19].

7.1 Détection de panne

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 [19].

7.2 Détention de la panne

Cette phase établit des limites des effets de la panne sur une zone particulière afin d'empêcher la contamination des autres régions. En cas de détection d'intrusion, par exemple, l'isolation des composants compromis minimise le risque d'attaque des composants encore fonctionnels [19].

7.3 Recouvrement de panne

C'est la phase dans laquelle on effectue des opérations d'élimination des effets de pannes. Les deux techniques les plus utilisées sont « masquage de panne » qui utilise l'information redondante correcte pour éliminer l'impact de l'information erronée, et « répétition » qui effectue, après la détection d'une panne, un nouvel essai pour exécuter une partie du programme, dans l'espoir que la panne soit transitoire [19].

7.4 Traitement de la panne

Dans cette phase, la réparation du composant en panne est effectuée. La procédure de réparation dépend du type de la panne. Les pannes permanentes exigent une substitution du composant avec un autre composant fonctionnel [19].

8. Les approches de détection des pannes

La détection de pannes est la première phase de gestion de pannes, où un échec inattendu devrait être correctement identifié. Les approches de détection de pannes dans les RCSF sont classées en trois catégories : approche centralisée, distribuée et l'approche par clustering.

8.1 Outil centralisé, actif, à base d'arbre de décision

8.1.1Sympathy

Est un outil de diagnostic centralisé (open source), conçu principalement pour les applications de collecte des données. Chaque nœud du réseau envoie périodiquement au puits les métriques définies par Sympathy. Celles-ci sont récupérées à partir de toutes les couches protocolaires du nœud, et elles sont de trois types : métriques de connectivité (table de routage, liste des voisins), métriques de flux (le nombre des paquets transmis et reçus par

chaque nœud, le nombre des paquets échangés entre chaque nœud et le puits, l'estampille du dernier paquet reçu par le puits pour chaque nœud) et les métriques du nœud (temps de démarrage, le nombre de mauvais et de bons paquets reçus). Le puits collecte les métriques de manière passive en écoutant le trafic écoulé dans le réseau et de manière active car les nœuds envoient explicitement les métriques à chaque période T. La collecte n'est possible que pour les nœuds qui sont au prochain saut du puits. Pour cette raison, la collecte active des métriques est une obligation même si elle est très coûteuse en termes de communication et d'énergie. Une fois les métriques collectées, le puits peut identifier le type de(s) panne(s) produite(s) (franche, omission, synchronisation, transmission), ses causes principales (l'écrasement d'un capteur, le redémarrage du puits, l'absence de voisins, l'absence de route au puits, un mauvais chemin vers le nœud, un mauvais chemin au puits) et ses sources (le nœud lui-même, le réseau ou le puits).

De fait, une panne est détectée quand un capteur (ou un composant d'une application) génère un trafic (métrique flux) inférieur à celui prévu. Ensuite, un arbre de décision est conçu pour faciliter l'analyse des causes des pannes (panne franche du nœud, perte de connectivité, problèmes dans le routage, etc.). Par exemple, si le puits n'a pas reçu un paquet d'un nœud N au bout d'une durée donnée (après laquelle les métriques deviennent invalides) et si le nœud N n'est inclus dans la liste des voisins d'aucun autre nœud du réseau, N est supposé écrasé (panne franche du nœud). Par la suite,

« Sympathy » archive les pannes afin que l'utilisateur puisse effectuer les étapes de reprise convenablement. Comme toute approche centralisée, « Sympathy » induit une surcharge dans la communication (surcharge de 30% du trafic écoulé), ce qui limite le passage à l'échelle. De plus, il nécessite l'instrumentation du code qui le rend vulnérable par rapport aux bugs logiciels du capteur [6].

8.2Outil centralisé, marquage des paquets, à base de modèle d'inférence probabiliste

8.2.1 PAD

Est une approche centralisée à base de modèle d'inférence, conçue pour les applications de collecte des données. Elle collecte les informations de diagnostic par le marquage des paquets. PAD est constitué de quatre composants essentiels :

- Un module de marquage réside à chaque nœud du réseau. Il sert à insérer les champs de diagnostic dans les paquets des données : son identifiant, l'identifiant du nœud source et le numéro de séquence du paquet. Un paquet traversé dans le réseau ne peut être marqué que par un seul nœud choisi en fonction d'un ensemble des règles définies par l'algorithme (Figure 2-3)

- Un module d'analyse des marques réside au niveau du puits. Il analyse les marques, génère la topologie du réseau, détecte des symptômes anormaux (perte, retard, ou duplication des paquets), génère des diagnostics préliminaires (les liens qui provoquent une perte des paquets, modification fréquente du nœud parent, les liens et les nœuds qui sont en bon état à cause de la bonne réception. etc.).

- Un modèle d'inférence probabiliste construit les graphes de dépendances entre les éléments du réseau

- Un moteur d'inférence. Il se base sur un réseau bayésien pour identifier les causes principales des symptômes anormaux. Il produit les diagnostics finals, en se basant sur le modèle d'inférence et les symptômes (négatifs et positifs) générés par le système de marquage.

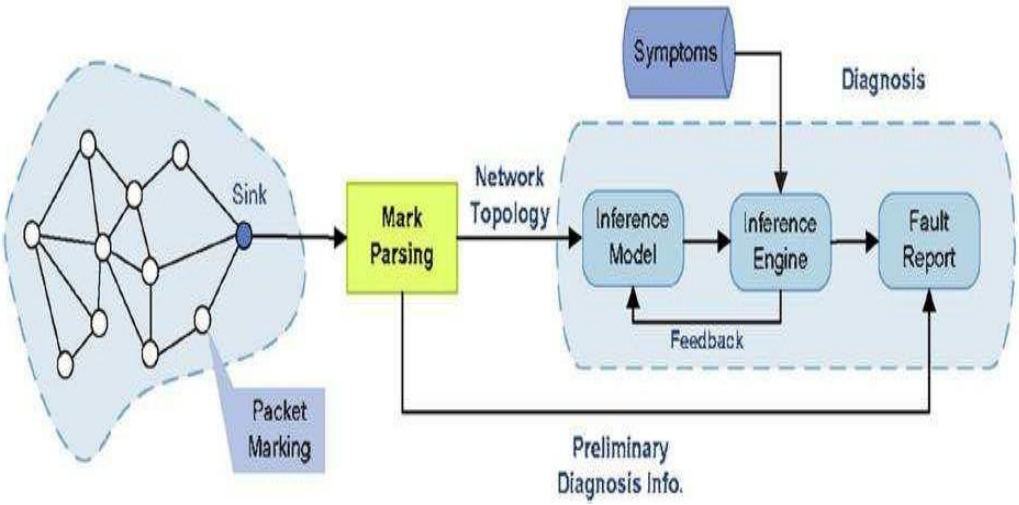


Figure 2.3: PAD Aperçu général du système [6]

Les avantages principaux de cette approche sont la construction dynamique des modèles de fautes et la topologie du réseau, la prédiction de certains types de fautes et d'informations sur l'état du réseau, la gestion efficace de l'énergie et le passage à l'échelle. La gestion de l'énergie est effectuée de manière efficace par l'analyse passive des symptômes observés et par la minimisation de la quantité des informations échangées (2 octects). Cette minimisation est possible grâce au système d'inférence probabiliste qui permet de compléter les informations de diagnostic par déduction des états internes des éléments du réseau.PAD montre une efficacité à identifier les causes des problèmes observés (déplétion rapide de l'énergie, perte des données et retard) dans le cadre du projet « OceanSence ». PAD identifie les fautes de type destruction physique, écrasement de logiciel, fautes au niveau de l'application, congestion et interférence. Les modèles des fautes sont construites en se basant sur les connaissances d'experts de la nature des fautes ou une déduction à partir des données historiques du réseau[6].

8.2.2 AD

présente une approche centralisée et agnostique de diagnostic des fautes. Cette approche n'exige pas une connaissance a priori de l'environnement et des types de fautes qui peuvent apparaître pendant le déploiement du réseau. AD collecte périodiquement vingt deux métriques qu'on peut classifier en quatre catégories : métriques de chronométrage, métriques de trafic, métriques concernant les tâches du système et métriques de connectivité (par exemple, le temps cumulé, le nombre de paquets transmis par un nœud, le nombre de tâches exécutées, le nombre de changements du nœud parent, etc.). AD analyse la corrélation temporelle et/ou spatiale des métriques pour détecter les fautes produites (Figure 2-4). Pour cela, à chaque période T, les corrélations de chaque nœud sont calculées et représentées par une matrice dont chaque élément correspond à une corrélation entre chaque couple de métriques. Un changement significatif entre deux mesures consécutives des corrélations d'un nœud indique la présence d'une faute. En plus de la corrélation temporelle, AD détecte des fautes par la corrélation spatiale entre les nœuds qui ont des fonctionnalités similaires, par exemple les nœuds feuilles du réseau.

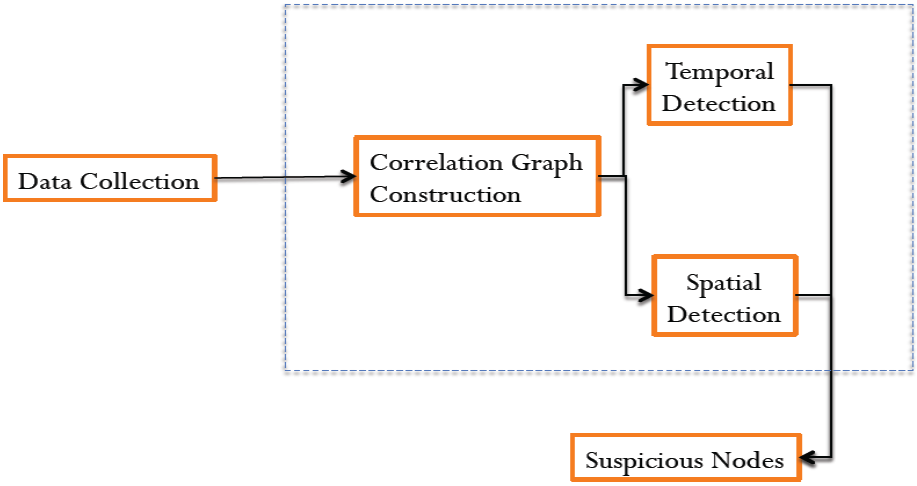


Figure 2.4: Approche agnostique de diagnostic [6]

AD montre une efficacité de détecter des fautes potentielles (« ingress drops », problèmes de routage, problèmes de liens, fautes logicielles) dans le cadre du projet « GreenObs » . Certaines de ces fautes peuvent être détectées par l'observation directe des valeurs anormales de certaines métriques, tandis que d'autres sont détectées par l'observation de la corrélation de certaines métriques. Par exemple, le nombre de paquets transmis par un nœud correct doit être proche du nombre de paquets reçus par les nœuds descendants. AD permet de réduire le taux de faux positifs et négatifs avec une surcharge d'énergie raisonnable où l'ensemble des métriques sont envoyées périodiquement à un nœud central dans un seul paquet.

8.3 Outil centralisé, réseau dédié, à base de modèle

8.3.1 PowerTracer

Introduit un système de diagnostic qui se base sur un modèle de la consommation d'énergie des nœuds. PowerTracer crée des modèles des fautes (modèles de référence) par leur émulation lors d'expériences en laboratoire et par l'utilisation des techniques d'apprentissage (le modèle de chaîne de Markov). Le processus de diagnostic peut être effectué, en quelques minutes, en comparant les modèles de référence aux modèles observés. Ces derniers sont construits selon une fenêtre temporelle, par exemple d'une durée de 30 min, à partir des mesures collectées préalablement du nœud en panne. L'exactitude de l'outil de diagnostic dépend de la taille de l'espace des états de transition de la chaîne de Markov, de l'intervalle d'échantillonnage, et de la taille de la fenêtre temporelle.

L'étude expérimentale montre que l'identification des fautes peut être exacte à 100% avec

un choix convenable de trois facteurs précédents. Cependant la mise en œuvre de PowerTracer nécessite d'installer trois types de composants : un mètre de puissance pour chaque nœud du système et une station de diagnostic qui analyse les traces de puissance collectées à travers des liaisons sans fils de faible bande passante. Ce coût supplémentaire (estimé à 3%) est acceptable par rapport à l'indépendance réalisée du système de diagnostic par rapport au système de surveillé [6].

8.3.2 PD2

Est un outil de diagnostic hybride conçu principalement pour les applications de collecte des données. Il effectue une analyse de la performance des flux des données générées par les nœuds pour isoler les éléments (nœuds, composants matériels ou logiciels) potentiellement défectueux. Pour cela, PD2 identifie chaque flux de données par l'ensemble des composants qu'il traverse à partir du nœud source jusqu'au nœud destination, le puits. Il garde la trace des chemins par un ensemble de règles de dépendances qui relient les différents modules logiciels des nœuds traversés par les flux. Lorsqu'une faute apparaît et provoque un taux de perte et/ou un temps de latence au niveau d'un flux de données, PD2 commence à étudier le problème en parcourant le chemin en sens inverse à partir du nœud puits. Il identifie les éléments défaillants en calculant le taux de perte et le temps de latence de chaque composant du chemin. Une fois les localisations des fautes identifiées, il est possible d'extraire

Des informations du composant défaillant et d'appliquer un raisonnement logique proposé par d'autres outils de débogage (par exemple « Sympathy ») pour identifier les causes des problèmes. C'est de cette manière que PD2 arrive à contrôler la consommation d'énergie en collectant les informations de débogage seulement des éléments défectueux dès que la défaillance d'un élément affecte la performance de l'application [6].

8.4 Outil hybride, réseau de renifleurs, à base d'arbre de décision

8.4.1 SNIF

Est un outil de diagnostic passif et à base d'arbre de décision pour les applications de collecte des données du RCSF. Il consiste à déployer un réseau de renifleurs distribués entre les nœuds capteurs. Les renifleurs écoutent passivement le trafic du réseau de capteurs pour éviter l'impact de l'instrumentation du code et l'envoi des messages explicites sur l'activité du réseau surveillé. Ils analysent le trafic pour extraire les indicateurs de fautes. SNIF peut

identifier des fautes présentes au niveau des nœuds et du réseau. Cependant, certains types de fautes ne peuvent être identifiés directement par l'observation de certains indicateurs (par exemple, la défaillance d'un nœud suite à l'épuisement de l'énergie) ou déduites par l'analyse de plusieurs symptômes observés. Bien que L'approche SNIF induit un coût d'installation supplémentaire et nécessite une compréhension profonde des protocoles utilisés dans le réseau, elle convient à de nombreuses applications pour plusieurs raisons : elle laisse intactes les ressources du système, elle évite l'impact de l'instrumentation de code et de la modification du trafic du réseau et elle garantit la fiabilité du système de diagnostic. Ce dernier n'est pas affecté par les problèmes du réseau des capteurs produits pendant le déploiement.

8.5 Outil hiérarchique, agents mobiles, à base d'arbre de décision

L'approche proposée dans se base sur un ensemble d'agents mobiles en charge de la détection intelligente des pannes et du recouvrement avec une gestion efficace de l'énergie et de la communication. L'architecture du réseau est hiérarchique à trois niveaux : les clusters, formés d'un ensemble de capteurs associés à un « ClusterHead », les « SuperClusters », formés de plusieurs clusters associés à une passerelle (Gateway) et le puits (Figure 2-6). Dans chaque niveau de la hiérarchie se trouvent deux types d'entités mobiles : les renifleurs (sniffers) et les correcteurs (correctors). Le renifleur émigre d'un nœud à un autre pour détecter les pannes et communique au(x) correcteur(s) leur localisation. La reconnaissance des pannes se fait grâce à une base de données distribuée. Cette base est définie partiellement au niveau du « ClusterHead » et des passerelles et elle est complète au niveau du « puits ». Elle décrit en détail les modèles de fautes et la relation qui existe entre les fautes, les erreurs et les défaillances. Les interactions entre les agents mobiles sont inspirées du langage de la danse des abeilles. Celui-ci a l'avantage d'assurer la communication entre les abeilles (agents mobiles) en temps réel et avec une gestion efficace de l'énergie. Les agents mobiles imitent les abeilles dans leur manière de communiquer pour indiquer la source et la qualité de nourriture (panne) en effectuant une danse en rond si la nourriture est à moins de 15 mètres (message Time To Live TTL limité) du nid et une danse de transition pour la source à moins de 50 mètres[6].

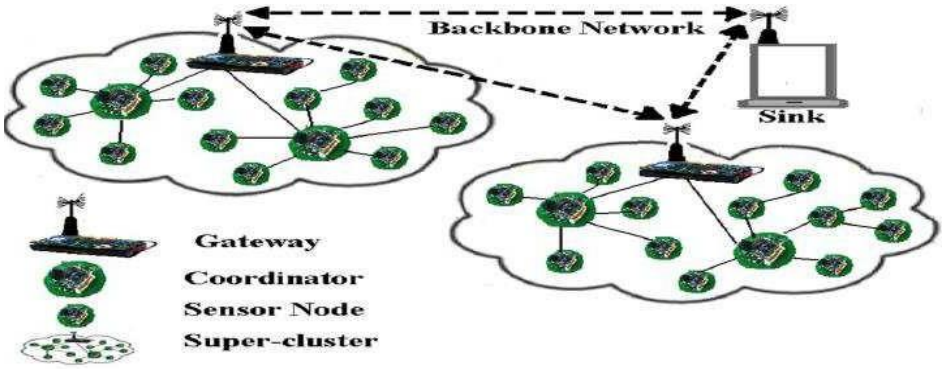


Figure 2.5: Architecture du réseau [6].

L'algorithme classifie alors les pannes en trois catégories selon leur gravité : la panne endémique, la panne épidémique et la panne pandémique. La panne est endémique si elle se produit à un taux faible au niveau d'un cluster. Par exemple, le débordement des tampons, le taux d'erreur binaire, etc. Ce type de pannes est traité par des agents mobiles locaux au niveau du

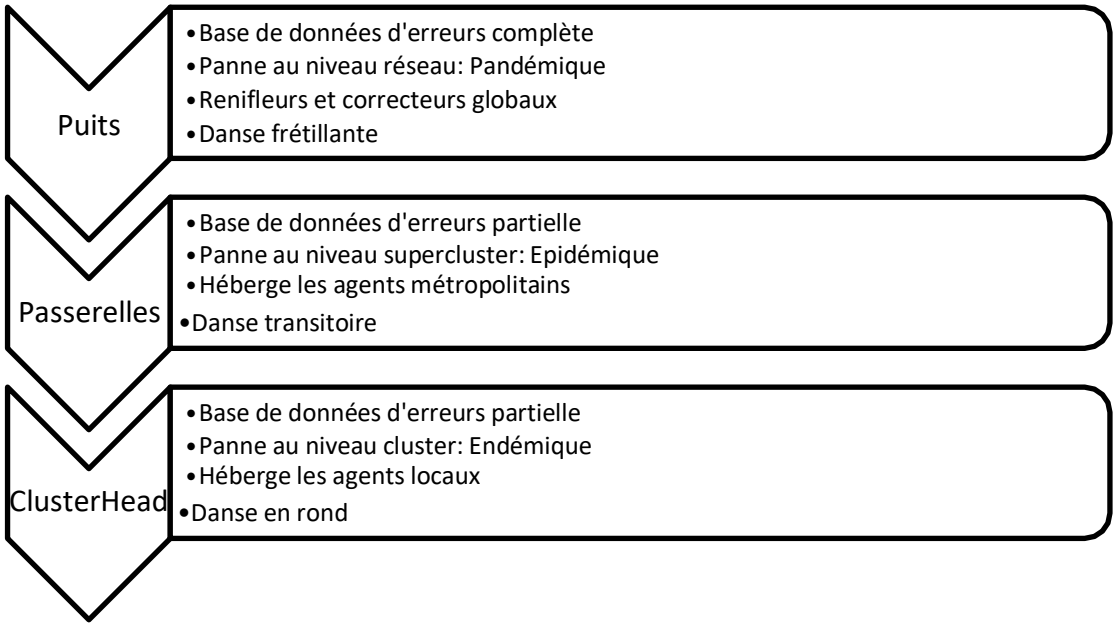


Figure 2 .6 : Traitement hiérarchique des pannes[6].

cluster. La panne est épidémique si elle se produit à un taux plus élevé dans plusieurs clusters du même super cluster. Par exemple, la perte des paquets est considérée du type épidémique lorsqu'elle se produit dans plusieurs clusters et à un taux élevé. Des agents métropolitains, initialement déployés dans les passerelles, interviennent pour traiter ce type de panne. La panne est pandémique lorsqu'elle devient incontrôlable et se produit simultanément dans plusieurs super- clusters du réseau. Le traitement de ce type de panne se fait par des

agents globaux périodiquement les nœuds du cluster pour collecter et sauvegarder les paramètres pertinents à la détection des pannes (la table de routage, la liste des voisins, le temps de démarrage d'un nœud, le niveau d'énergie, etc.).

Il détecte l'erreur lorsqu'il observe un comportement aberrant dans la plupart des paramètres ou découvre une déviation imprévue (dépassement d'un seuil prédéterminé) de la valeur d'un paramètre dans le temps. Par exemple, le niveau d'énergie d'un nœud à un temps T+t est inférieur à celui du temps t. Le traitement des pannes dépend de leur gravité et se passe d'une manière hiérarchique (Figure 2-7). S'il y a une seule défaillance, elle est traitée par le correcteur local. Sinon (défaillances multiples) le détecteur informe les correcteurs du cluster par la « Danse en Rond », diffusion de TTL limitée au cluster, qu'il y a une défaillance de type« endémique » en indiquant la localisation des nœuds affectés. Dans ce cas, les correcteurs visitent les nœuds défectueux pour les traiter. Si l'occurrence d'un même type de défaillance dépasse un seuil prédéterminé, le détecteur local annonce par une« danse de transition », diffusion de TTL limitée au super cluster, qu'il y a une panne du type « épidémique » en indiquant la distance et la direction du cluster affecté. Dans ce cas, les correcteurs des autres clusters se déplacent vers le cluster désigné et participent au traitement

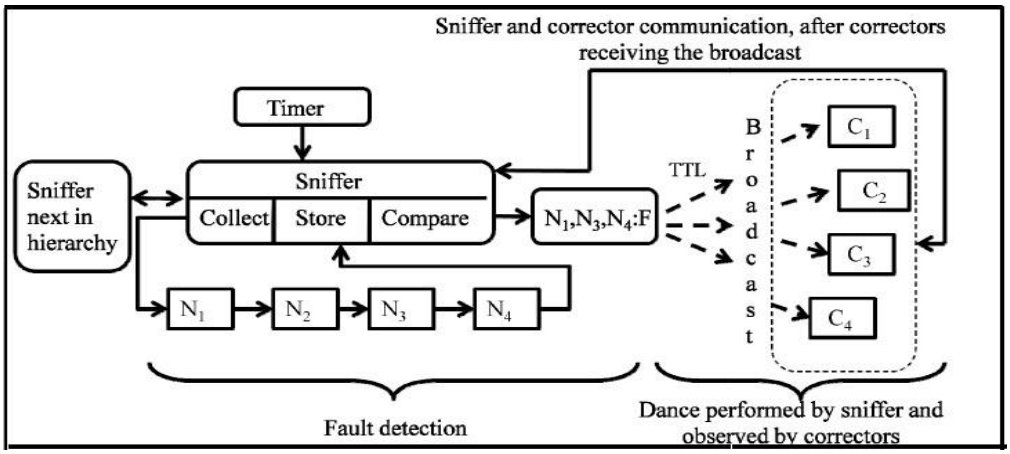


Figure 2.7 : Détecteurs des fautes [6] .

cluster, le renifleur global du puits effectue la « danse frétillante», diffusion de TTL illimitée, indiquant qu'il y a une panne de type « pandémique » et demandant aux détecteurs de répliquer les correcteurs locaux et métropolitains. Une fois la « danse de transition » terminée, le renifleur global demande aux correcteurs répliqués de retourner à l'état normal. Dans la Figure 2-8, le renifleur visite les nœuds N1, N2, N3 et N4. Il collecte des paramètres explicitement (choisis par l'administrateur comme le temps de démarrage, le niveau d'énergie, etc.) ou implicitement (à travers les protocoles de communication comme la

table de routage, la liste des voisins, *etc*.), il les sauvegarde et les compare aux paramètres collectés précédemment. En cas de panne(s), il informe les correcteurs pour entreprendre les actions appropriées. S'il n'arrive pas à détecter une faute liée à une panne observée, il transmet la faute inconnue au renifleur du niveau supérieur de la hiérarchie. L'algorithme gère efficacement l'énergie, par :

- l'introduction des agents mobiles qui permet de déplacer la complexité du routage des nœuds capteurs vers les agents mobiles. Cependant la mobilité induit une surcharge dans la communication, car à chaque fois le « Cluster Head » envoie un renifleur à chaque nœud du cluster et le (s) correcteur (s) visite (nt) le (s) nœud (s) défectueux. La surcharge dépend de la période de la collecte des paramètres (T) et du taux de pannes dans le réseau. T devrait être aussi large que possible pour réduire la surcharge de communication, mais en même temps juste assez petit pour assurer la fiabilité du réseau.

- l'imitation de la nature par le langage « danse des abeilles » le plus efficace pour conserver l'énergie des abeilles. Celles-ci sont très petites et ont des ressources limitées en énergie et en taille (le cas des capteurs). Les abeilles (agents mobiles) ne dansent qu'en cas de besoin (nécessaire) et leur danse n'implique qu'un nombre limité suffisant d'abeilles. L'algorithme essaie de profiter de cela pour les capteurs en diffusant des messages courts, limitant le nombre des messages diffusés le plus possible et en traitant les pannes d'une manière hiérarchique[6].

8.6 Outil distribué, agent mobile, à base d'arbre de décision

8.6.1TinyD2

Est une approche réactive de diagnostic des fautes. Contrairement, aux approches proactives, qui collectent les informations de diagnostic périodiquement des nœuds capteurs, TinyD2 adopte une approche réactive où l'échange d'informations ne commence qu'à la suite d'une détection d'un symptôme anormal. Selon le type de symptôme observé, la décision finale de diagnostic peut être prise localement en fonction des preuves observées sur le nœud local (par exemple, le redémarrage du système, peut être détecté et identifié par le nœud lui même), ou globalement en fonction des informations sur d'autres nœuds du réseau (par exemple, si un nœud détecte la panne franche d'un nœud, il faut vérifier le résultat avec les nœuds voisins).

Dans ce dernier cas, le diagnostic se fait d'une manière incrémentale ou graduelle où chaque nœud effectue une étape intermédiaire de décision jusqu'à l'arrivée au jugement final. Pour cela, chaque nœud maintient un ensemble de détecteurs de fautes dont chacun est représenté par une machine à états finis (Figure 2-14). Ainsi, chaque nœud participe dans le processus de diagnostic en faisant transiter la machine d'un état à un autre sur la base d'informations locales. Le détecteur, un message de petite taille incluant principalement le type de détecteur et son état courant, se déplace continuellement d'un nœud à un autre pour collecter plus d'informations. Dès qu'un nœud arrive à déduire la nature de la faute produite, il informe le puits pendant la phase de la collecte des notifications.

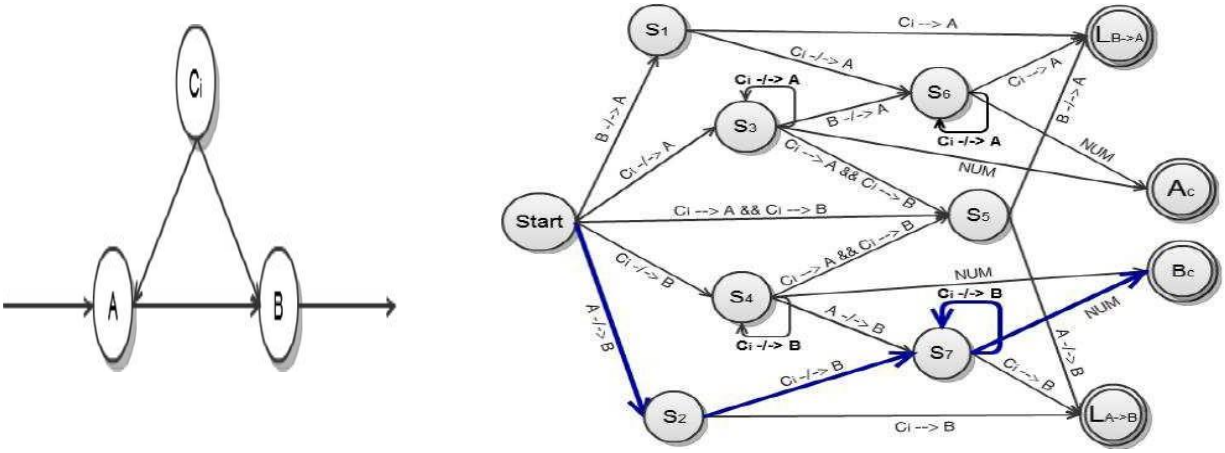


Figure 2-8: Un exemple du détecteur de défaut [6].

Manière incrémentale ou graduelle où chaque nœud effectue une étape intermédiaire de décision jusqu'à l'arrivée au jugement final. Pour cela, chaque nœud maintient un ensemble de détecteurs de fautes dont chacun est représenté par une machine à états finis (Figure 2-9). Ainsi, chaque nœud participe dans le processus de diagnostic en faisant transiter la machine d'un état à un autre sur la base d'informations locales. Le détecteur, un message de petite taille incluant principalement le type de détecteur et son état courant, se déplace continuellement d'un nœud à un autre pour collecter plus d'informations. Dès qu'un nœud arrive à déduire la nature de la faute produite, il informe le puits pendant la phase de la collecte des notifications.

Voici un exemple montrant la coopération entre les nœuds A, B et {Ci}, un groupe de nœuds voisins de A et B, pour identifier la cause d'une retransmission élevée des paquets

détectée sur le lien entre A et B. Le détecteur de la retransmission, détenu par chaque nœud du réseau, est encodé par une machine à états finis. L'état initial (S) représente l'état du nœud A qui crée en premier le détecteur. Les états finaux (LB->A), (Ac), (Bc) et (LA->B) représentent respectivement les causes potentielles du problème détecté : la mauvaise qualité du lien de B vers A, la congestion en A, la congestion en B et la mauvaise qualité du lien de A vers B. Pour passer à l'état suivant (S1, S2, S3 ou S4), le nœud A diffuse un message contenant le type et l'état courant du détecteur aux nœuds voisins. Chacun de ces derniers analyse le message et effectue des transitions en fonction des informations locales de chacun d'eux. Dans ce cas, le nœud B, qui a reçu un nombre des paquets inférieur à celui qui a été prévu au nœud A, fait transiter le détecteur à l'état S2 (signifie qu'il y a un problème de lien de A vers B). Il diffuse un message incluant l'état courant du détecteur S2. Si les nœuds Ci ont réussi à envoyer des paquets au nœud B, on passera à l'état final (LA->B), sinon on déduit qu'il y a une contention en B, l'état (Bc)[6].

8.7Système distribué, à base d'échange de messages (protocole)

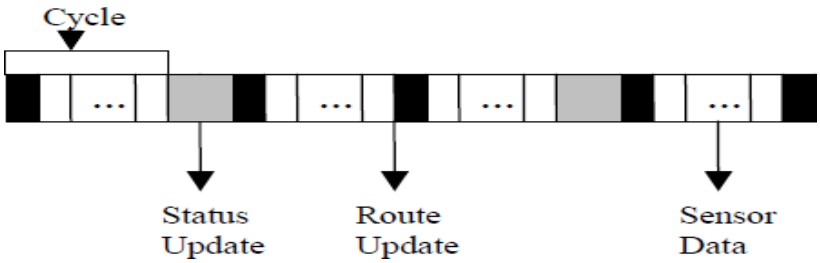
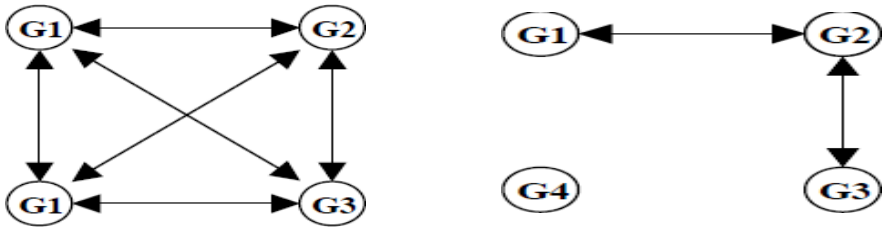


Figure 2.9: Allocation d'un créneau dans les réseaux de capteurs sans fils [6]

Lorsqu'aucune autre passerelle du réseau n'arrive à communiquer avec elle. La détection de panne se base sur un échange des messages de statut entre passerelles et sur un mécanisme de consensus établi entre les passerelles qui sont en état correct. Le protocole de communication utilisé est le « TDMA MAC » qui alloue un créneau pour l'échange du statut de passerelle (Figure 2-10).

Un tableau de connectivité est crée suite à l'échange des messages de statut. Il représente les connexions entre les différentes passerelles et permet la détection de la défaillance d'une passerelle. Prenons les deux exemples suivants. Le Tableau2-1 représente la connectivité du réseau sans défaut de la Figure 2-16 où chaque passerelle peut communiquer avec toutes les autres passerelles ; et le Tableau 2-2 représente le réseau avec défaillances de la Figure 2-11 (b) dans lequel G4 est défectueuse et le lien entre G1 et G4 est rompu. En examinant le

Tableau 2-4, les passerelles G1, G3 et G2 détectent que G4 est défectueuse (pas de communication avec toutes les autres passerelles).



(a) : Passerelles sans défaillances(b) Passerelles avec défaillances

	G1	G2	G3	G4
G1	√	1	1	1
G2	1	√	1	1
G3	1	1	√	1
G4	1	1	1	√

	G1	G2	G3	G4
G1	√	1	0	0
G2	1	√	1	0
G3	0	1	√	0
G4	0	0	0	0

Tableau 1Tableau2-1: Connectivité de l'exemple (a) Tableau 2 Tableau 2-2: Connectivité de l'exemple (b)

Figure 2-10 : Pannes au niveau d'un « cluster head »

Si G4 est défectueuse, les capteurs qui appartiennent à son groupe seront incapables de transmettre leurs données au puits. Le recouvrement consiste à associer ces capteurs à une autre passerelle qui est en bon état. L'approche proposée évite le mécanisme de « Re-clustering » à cause de son coût élevé. Par contre, c'est lors de la phase de l'initialisation du réseau (la phase de formation des clusters) que chaque passerelle maintient une liste des capteurs qu'on peut réassocier en cas de panne dans son groupe [6].

8.8 Outil distribué, actif, à base d'échange des messages

8.8.1Memento

Est un système de détection des défaillances. Les nœuds envoient périodiquement des messages de type « bitmap » à leur nœud parent. Un bitmap de forme 1101110 et de type « alive » signifie que les nœuds 3 et 7 sont défaillants. Les bitmaps de chaque nœud représentent les états des nœuds descendants. Memento incorpore un protocole de communication qui permet de réduire la consommation d'énergie à 80% en comparaison aux méthodes standards de la collecte des données. Ce protocole inclut deux mécanismes :

- Mécanisme d'agrégation : les bitmaps des nœuds descendants sont agrégés au niveau de chaque nœud parent en appliquant l'opérateur binaire « ou ».

- Mécanisme de cache : un nœud parent cache l'état des nœuds descendants. Ces derniers s'abstiennent de transmission s'il n'y a pas de changement des états des nœuds.

Memento n'utilise pas de mécanisme d'acquittement. Par contre, les nœuds envoient d'une manière proactive un certain nombre de messages à chaque intervalle de temps, alors que ce nombre est estimé en fonction de la performance de la qualité de lien et du taux de faux positifs ciblé. Ce dernier est un paramètre de l'algorithme de détection. Memento est indépendant du type de l'application. En outre, il tolère la perte des messages dans la communication multi-saut [6].

9. Le diagnostic des pannes:

10. Classification des approches de diagnostic des pannes

De nombreuses approches ont été développées en vue du diagnostic des défaillances dans le système à base de RCSF. Elles se distinguent par les mécanismes de la collecte des informations du diagnostic et la structure de prise de décision concernant la détection [19].

10.1 Classification selon l'architecture

Selon la structure de la prise de décision et le(s) entité(s) intervenante(s) dans le processus de détection et de diagnostic des défaillances, les auteurs classifient les approches de diagnostic en plusieurs catégories : approche centralisée, approche distribuée, approche hybride et approche au niveau du nœud [19].

- **Approche centralisée** : Elle repose sur un nœud central qui diagnostique les fautes en se basant sur des informations recueillies des nœuds du réseau. Cette approche assure une supervision globale de l'état du réseau permettant de garantir une exactitude quant au diagnostic des problèmes complexes (par exemple, la défaillance des nœuds critiques). Les limites de cette approche sont liées à une dépendance forte due à la centralisation exclusive des opérations de diagnostic. D'une part, cette approche n'est pas robuste vis-à- vis de la perte des messages transmis sur un réseau sans fil de communication multi saut. De plus, l'arrêt

accidentel du point central entraîne également l'arrêt du système de diagnostic. D'autre part, elle est coûteuse en termes de consommation d'énergie, et ne permet pas le passage à l'échelle. L'approche centralisée favorise principalement les réseaux de petite taille.

- **Approche distribuée:** La détection des pannes est réalisée de façon distribuée par l'ensemble des nœuds du réseau. Elle permet d'améliorer la robustesse du système. Cependant, des mécanismes de coopération doivent être mis en œuvre pour assurer la cohérence dans les opérations de gestion exécutées par les nœuds.
- **Approche hybride :** Elle combine le principe des deux approches centralisée et distribuée. Le but est de pouvoir profiter des avantages des deux approches : l'exactitude et la précision des approches centralisées et l'efficacité de la gestion de l'énergie et le passage à l'échelle des approches distribuées**.**
- **Approche de diagnostic au niveau du nœud:** Le diagnostic se base sur des informations sur l'état d'un nœud sans tenir compte du comportement des autres nœuds du réseau. Cette approche ne permet pas le diagnostic des fautes réseaux.

architecture	centralisée	distribuée	hybride
Précision/exactitude	Bonne	Moyenne	Bonne
Consommation d'énergie	Forte	Faible	Moyenne
Passage à l'échelle	Non	Oui	Oui
Robustesse	Non	Oui	Oui
Latence de détection	Bonne	Faible	Faible
Impacts sur la performance du réseau	Oui	Faible ou Moyenne	Moyenne
Complexité d'implémentation	Non	Oui	Oui

Tableau 3Tableau 2. 3 : Comparaison entre les approches centralisées, distribuées et hybrides[19]
]

10.2 Classification selon les techniques de collecte des informations

L'outil de diagnostic récupère les informations sur le système surveillé selon deux approches principales: active et/ou passive [19].

- **Approche active :** Les nœuds génèrent des paquets spécifiques au diagnostic (les paquets de contrôle). La transmission des paquets s'effectue en utilisant le canal de communication principal de l'application. L'approche active est coûteuse en termes de consommation de ressources. Pour cela, certaines solutions introduisent des nœuds « mobiles » dotés de batteries plus puissantes et capables de se déplacer pour récupérer les informations des nœuds du réseau. Cependant, elle ne nécessite pas de matériel supplémentaire pour transmettre les paquets de contrôle.
- **Approche passive :** L'approche passive ne requiert aucune intervention de la part des nœuds du réseau, et ne génère pas de paquets supplémentaires dans le réseau. Elle peut être réalisée par le puits, ou par les nœuds du réseau. Un avantage principal du diagnostic passif est la transparence. Le diagnostic s'effectue sans aucune interférence avec les opérations normales du réseau. Ce qui permet de garder les ressources des nœuds du réseau et la performance globale du système. Un autre avantage est le support d'une grande diversité de plateformes.
- Un autre modèle de l'approche passive, est **l'approche de marquage** des paquets « piggybacking ». Il consiste à insérer les informations de diagnostic dans les paquets de données. Il permet de réduire la consommation de la bande passante, en évitant d'injecter des paquets supplémentaires dans le réseau. L'inconvénient principal du marquage des paquets, est que la taille des informations à insérer est limitée à la taille maximale des paquets.

approche de la collecte d'information	active	passive	marquage
Transparence	Non	Oui	Oui
consommation d'énergie	forte	/	faible
Fiabilité	Faible	élevée	Faible
Support de la mobilité	Oui	non	oui
Passage a l'échelle	/	oui	oui
Domaines d'applications	tout types d'application	Application de la collecte des données	Application de la collecte des données

Tableau 4Tableau 2. 4 : Mécanismes de transmission des informations du diagnostic [19]

11. Quelques exemples d'approches de diagnostic des pannes

La partie logicielle du capteur est déjà tolérante aux pannes et que la majorité des pannes sont des pannes matérielles. Et autre, il suppose que la majorité des pannes sont dues à l'environnement dans lequel les capteurs sont déployés [19].

12. Les approches de recouvrement des pannes des nœuds

Le recouvrement de la panne est l'étape dans laquelle le réseau de capteur est reconfiguré et reconstitué d'une telle façon que les pannes n'influent pas sur les performances du réseau, les approches existantes isolent les nœuds défectueux. Selon Marti, après détection de la panne, le nœud capteur doit choisir un autre voisin pour acheminer ses paquets. Tandis que Win MS a proposé que le nœud central détecte la région faible du réseau (exemple, celle qui a une faible énergie) en comparant l'état actuel du réseau avec un modèle historique donnant des informations sur le réseau (exemple, schéma d'énergie) , après détection il règle les nœuds de cette région de façon à ce qu'ils envoient les informations moins fréquemment qu'avant afin de conserver leur énergie et maximiser ainsi leur durée de vie. Dans autre, quand un nœud passerelle tombe en panne, tous les nœuds du groupe sont réattribués à d'autres passerelles en bon état. Ceci consomme plus de temps vu que tous les membres du groupe sont impliqués dans le processus de rétablissement [19].

13. la relation entre les pannes et l'énergie dans WSN

Durant ces dernières décennies, les réseaux de capteurs ont bouleversé le monde. Le besoin d'un suivi continuel des phénomènes naturels et aussi la surveillance dans différents domaines, ont renforcé l'intérêt pour cette nouvelle ère de l'informatique embarquée. En revanche, les réseaux de capteurs souffrent de leurs fragilités et de leurs énergies limitées. Les nœuds capteurs sont alimentés par des batteries limités en énergie. Par ailleurs, le remplacement des batteries n'est pas une solution envisageable pour ces derniers, soit à cause du déploiement aléatoire des capteurs, ou à cause de l'hostilité de l'environnement où ils sont placés. Toutefois, la mort d'un ou plusieurs nœuds capteurs interrompe partiellement la communication dans le réseau. De ce fait, une partie des données collectées sera perdu ce qui en résulte à la mort partielle du réseau. Maximiser la durée de vie du réseau constitue l'un des défis majeur. La maximisation de la durée de vie d'un réseau de capteurs revient à minimiser les différentes sources d'énergies. En fait, un nœud capteur consomme de l'énergie pour accomplir son objectif dans le réseau. Son rôle principal est la collecte, le traitement et la transmission d'un ensemble de grandeur physique sur l'environnement qui l'entoure. Ces trois opérations constituent les principaux facteurs de consommation d'énergie. A partir de là, réduire l'énergie consommée par un nœud capteur reviens à optimiser ces trois taches. Dans ce contexte, plusieurs techniques de conservation d'énergie ont été proposées dans la littérature. Dans ce présent, nous décrirons la problématique de la consommation d'énergie dans les réseaux de capteurs. Nous présenterons aussi un panorama de techniques de conservations d'énergie proposées dans la littérature [5].

14. Facteurs intervenants dans la consommation d'énergie

Il existe des facteurs qui induisent une consommation inutile de l'énergie (surconsommation). Ces facteurs sont nombreux, ils peuvent être engendrés lors de la détection lorsque celle-ci est mal gérée, ou lors de la communication. En effet, la communication est sujette à plusieurs facteurs qui surconsomment de l'énergie surtout coté MAC[5].

14.1Etat du module radio

Le module radio est le composant du nœud capteur le plus consommateur en énergie puisque c'est lui qui assure la communication entre les nœuds. Le module radio opère dans quatre modes de fonctionnement : idle, transmission, réception et sommeil.

- Dans l'état idle : la radio est allumée, mais elle n'est pas employée. En d'autres termes, le nœud capteur n'est ni en train de recevoir ni de transmettre.
- Dans l'état transmission : la radio transmet un paquet. - Dans l'état réception : la radio reçoit un paquet.
- Dans l'état sommeil : la radio est mise hors tension. Il été observé que dans le cas de la plupart des radios que le mode idle induit une consommation d'énergie importante, presque égale à la consommation en mode réception suite à l'écoute inutile du canal de transmission. Ainsi, il est plus judicieux d'éteindre complètement la radio que de la laisser en mode idle quand elle n'est pas utilisée ni pour la transmission ni pour la réception des données.

15. Durée de vie d'un réseau de capteurs

15.1Définition générale

La vie d'un réseau de capteurs correspond à la période de temps durant laquelle le réseau peut, selon le cas, maintenir assez de connectivité, couvrir le domaine entier ou garder le taux de perte d'informations en-dessous d'un certain niveau[7] .

15.2Quelques définitions existantes

il existe plusieurs définitions pour la durée de vie d'un réseau de capteurs :

- La durée jusqu'à ce que le premier nœud épuise toute son énergie,
- La durée jusqu'à ce que le premier cluster head épuise toute son énergie,
- La durée jusqu'à ce qu'il reste au plus une certaine fraction de nœuds survivants dans le réseau,
- Demi-vie du réseau : La durée jusqu'à ce que 50% des nœuds épuisent leurs batteries et s'arrêtent de fonctionner,

- La durée jusqu'à ce que tous les capteurs épuisent leurs énergies;
- La durée jusqu'à ce que le réseau soit partitionné : apparition de la première division du réseau en deux (ou plus). Cela peut correspondre aussi à la mort du premier nœud (si celui-ci tient une position centrale) ou plus tard si la topologie du réseau n’est plus robuste;
- k-couverture: la durée pendant laquelle la zone d'intérêt est couverte par au moins k nœuds;
- 100%-couverture
    - ✓ La durée pendant laquelle chaque cible est couverte par au moins un nœud;
    - ✓ durée pendant laquelle l'ensemble de la zone est couverte par au moins un nœud;
- Couverture
    - ✓ La durée cumulée, au bout de laquelle au moins une portion de la région est couverte par au moins un nœud ;
    - ✓ La durée pendant laquelle la couverture tombe en-dessous d'un seuil prédéfini
    - ✓ La durée de fonctionnement continu du système avant que la couverture ou la proportion de paquets reçus (PDR pour Packet Delivery Ratio) tombent en- dessous d'un seuil prédéfini;
- La durée pendant laquelle un pourcentage donné de nœuds possèdent un chemin vers la Station de Base
- L'espérance de l'intervalle complet pendant lequel la probabilité de garantir simultanément une connectivité et une k-couverture est au moins;
- La durée jusqu'à ce que le réseau ne fournisse plus un taux acceptable de détection d'événements;
- La durée pendant laquelle le réseau satisfait continuellement les besoins de

l'application [3].

16. Formes de dissipation d'énergie

Détecter les évènements dans l'environnement capté, élaborer un traitement de données local et rapide, et transmettre les résultats à l'utilisateur sont les principales tâches d'un nœud capteur dans le réseau de capteurs. Les étapes de consommation d'énergie par ce nœud peuvent être, dès lors, divisées en trois phases : le captage, la communication et le traitement des données [5].

- l'échantillonnage de données et la conversion en un signal électrique,
- le traitement du signale
- conversion du signale de l'analogique au numérique. La plupart des chercheurs partent de l'idée que l'énergie consommée par l'échantillonnage des données est négligeable comparant à la communication.

En revanche, dans certain cas, l'énergie dépensée pour l'échantillonnage peut être dans le même ordre de grandeur ou supérieure à l'énergie consommée lors de la communication. A titre d'exemple : l'utilisation d'un capteur gourmand en énergie, des capteurs actifs (tels que les sonars, les capteurs d'image) ou aussi dans le cas où le temps d'échantillonnage est long. Par ailleurs, L'énergie consommée au moment du captage varie suivant la nature de l'application. La complexité et la nature de l'événement à détecter, joue également un rôle crucial pour déterminer la quantité d'énergie consommée pour l'échantillonnage. Contrôler un événement sporadique1 consomme moins d'énergie qu'un contrôle d'événement constant. Aussi, les environnements contenant un niveau de bruit élevé entraîne l'augmentation de l'énergie nécessaire pour la capture.

16.1L'énergie de traitement (calcul)

Cette unité est constituée d'un microcontrôleur (microprocesseur) et une mémoire. L'énergie résiduelle de cette unité est dépensée lors de la commutation et aux fuites. L'énergie de commutation est déterminée par la tension d'alimentation et la capacité totale commutée au niveau logiciel (en exécutant un logiciel). Par contre, l'énergie de fuite désigne l'énergie consommée par l'unité de calcul dans le cas où aucun traitement n'est effectué. Enfin il est à noter qu'un nœud peut contenir des circuits additionnels pour le

codage/décodage des données, en plus de certain circuits spécifiques aux applications du réseau, dans tous ces cas, la conception des algorithmes et protocoles du réseau est influencée largement par l'énergie consommée par ces circuits. L'énergie de commutation E switch est exprimée comme suit :

$$E_{switch} = C_{tot}\, V_{dd}^2 \qquad \ldots\ldots \text{ equation } (1)$$

Où : C_{tot} est la capacité totale commutée par le calcul, V^2_{dd} est l'alimentation du voltage

16.2 Accès au support de transmission

La couche MAC à un rôle très important pour la minimisation de l'énergie consommée. Un protocole MAC économe en énergie essaie d'utiliser le moins souvent possible le module radio. Les modules radio peuvent avoir plusieurs niveaux de consommation quand ils ne sont pas en mode émission ou réception, moins le nœud consomme moins il est réactif, c'est pour cela que les différents états existent pour assurer une flexibilité selon le degré de réactivité demandé par la couche MAC. L'utilisation inutile du module provient de six sources essentielles : la retransmission, l'écoute passive, l'écoute abusive, la surcharge, la surémission et la taille des paquets.

16.3La retransmission

Les nœuds capteurs utilisent généralement une seule antenne radio, cependant ils partagent le même canal de transmission. La transmission simultanée des paquets par les nœuds voisins peut engendrer des collisions. Ainsi une quantité des données transmises sera perdu. La retransmission de ses données perdues générera une perte significative de l'énergie. - L'écoute passive (idle listening).

16.4 L'écoute passive du canal radio

Dans l'attente d'une éventuelle réception (le mode idle décrit précédemment) engendre une perte importante des capacités des nœuds en termes d'énergie. Ceci est couteux et inutile dans le cas des réseaux à faible charge de trafic. De ce fait, basculer les nœuds capteurs en mode sommeil est une solution mais la transition entre les modes consomme également de l'énergie. Pour cette raison la fréquence de transition entre les modes doit rester raisonnable.

16.5 L'écoute abusive (overhearing)

L'écoute abusive se produit quand un nœud reçoit des paquets qui ne lui sont pas destinés (figure 2.12). Le coût de l'écoute abusive peut être important dans le cas d'un réseau dense et avec une charge de trafic importante.

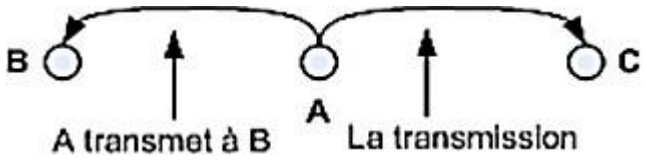


Figure 2.11 L'écoute abusive dans une transmission

Plusieurs protocoles de la couche MAC, utilisent les paquets de contrôle pour maintenir une bonne communication entre les nœuds (signalisation, connectivité, établissement de plan d'accès et évitement de collisions). L'échange de paquets nécessite une énergie additionnelle. Par ailleurs, comme ces paquets ne transportent pas directement des données, ils réduisent également le débit utile effectif.

16.6 La surémission (Overemitting)

Le phénomène de surémission est produit quand des nœuds envoient des messages à des destinations qui ne sont pas prêtes à les recevoir, en effet ces messages sont considérés inutiles et consomment d'avantage de l'énergie.

16.7 La taille des paquets

La taille des paquets à un effet sur la consommation d'énergie. En effet, si la taille des paquets est réduite, le nombre de paquets de contrôle échangés augmente ce qui génèrera un overhead. Dans le cas contraire, une taille grande des paquets nécessite l'utilisation d'une grande puissance de transmission.

16.8Demonstration

Dans le cas de dépense énergétique individuelle d'un nœud capteur, la plupart des études ont montré, comme l'illustre la Figure 2.13, que le composant interne qui consomme le plus d'énergie est le module radio 1 et plus précisément l'opération de transmission (un facteur est souvent avancé : 1.4 :1.05 :1 respectivement pour les opérations transmission, réception et écoute de la porteuse (idle). Il faut donc, comme première mesure d'optimisation, diminuer le

plus possible les transmissions d'un nœud capteur ou transmettre des messages moins cours à des petites distances (car la taille d'un message et la distance séparant deux nœuds communicants est en relation proportionnelle avec la consommation de l'énergie). Parfois on préfère avancer ce slogan : « il vaut mieux effectuer autant de traitements localement et communiquer rarement » du moment qu'un traitement coûte moins cher qu'une communication2 (La technologie a avancé à tel point que la quantité d'énergie consommée par un bit pour une simple transmission est équivalente à celle consommée par le traitement de ce même bit plusieurs milliers de fois). Un nœud capteur dans un état

« Écoute de la porteuse du signal » (idle mode) consomme presque la même quantité d'énergie comme s'il est récepteur (d'où le facteur 1.05:1), car son module radio écoute en permanence la porteuse du signal pour savoir s'il est ou non récepteur. Dans ce cas, il serait plus avantageux de mettre le nœud en mode veille (sleep mode) pour une période donnée dictée par un mécanisme de synchronisation adéquat, du moment qu'il ne fait rien. Cette notion de cycle d'activité (duty cycle) qu'il faut impérativement minimiser concerne également d'autres composants internes des nœuds capteurs d'un RCSF : le microcontrôleur, la mémoire, le module de capture et d'autres circuiteries annexes comme par exemple les modules de mobilité, de localisation, …etc.[4]

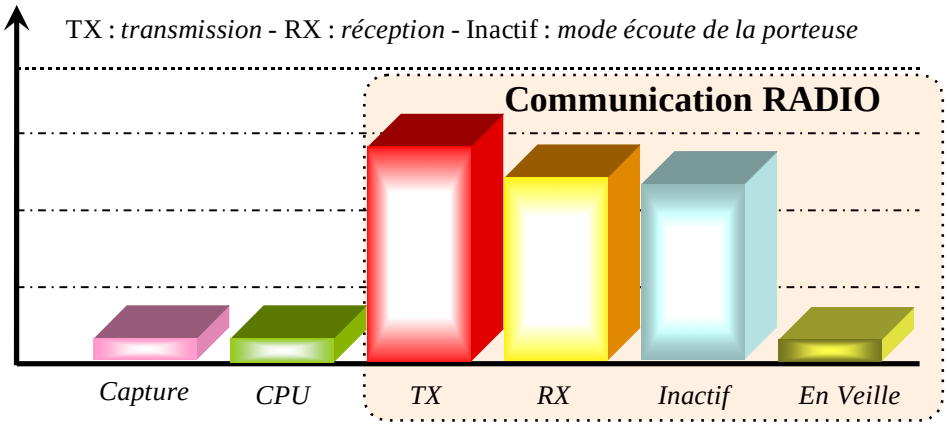


Figure 2.12 : Niveaux de consommation d'énergie au sein d'un nœud capteur [4].

16.9Les méthodes de conservation d'énergie dans les réseaux de capteurs sans fils

Comme on la déjà cité en introduction, les trois taches principales, d'un nœud capteur, qui consomment de l'énergie sont: la capture, le traitement et la communication. La consommation d'énergie du module de détection dépend de la spécificité du capteur [5]. Dans de nombreux cas, elle est négligeable par rapport à l'énergie consommée par le module de traitement et par-dessus tout, le module de communication. Dans d'autre cas, l'énergie dépensée par la détection peut être comparable ou supérieure à celle dépensée par la transmission. Plusieurs approches ont été proposées afin d'optimiser l'énergie au niveau de ces trois tâches. Par ailleurs, plusieurs classifications de ces dernières ont été proposées dans la littérature. Comme montrée dans la (figure 2.14).

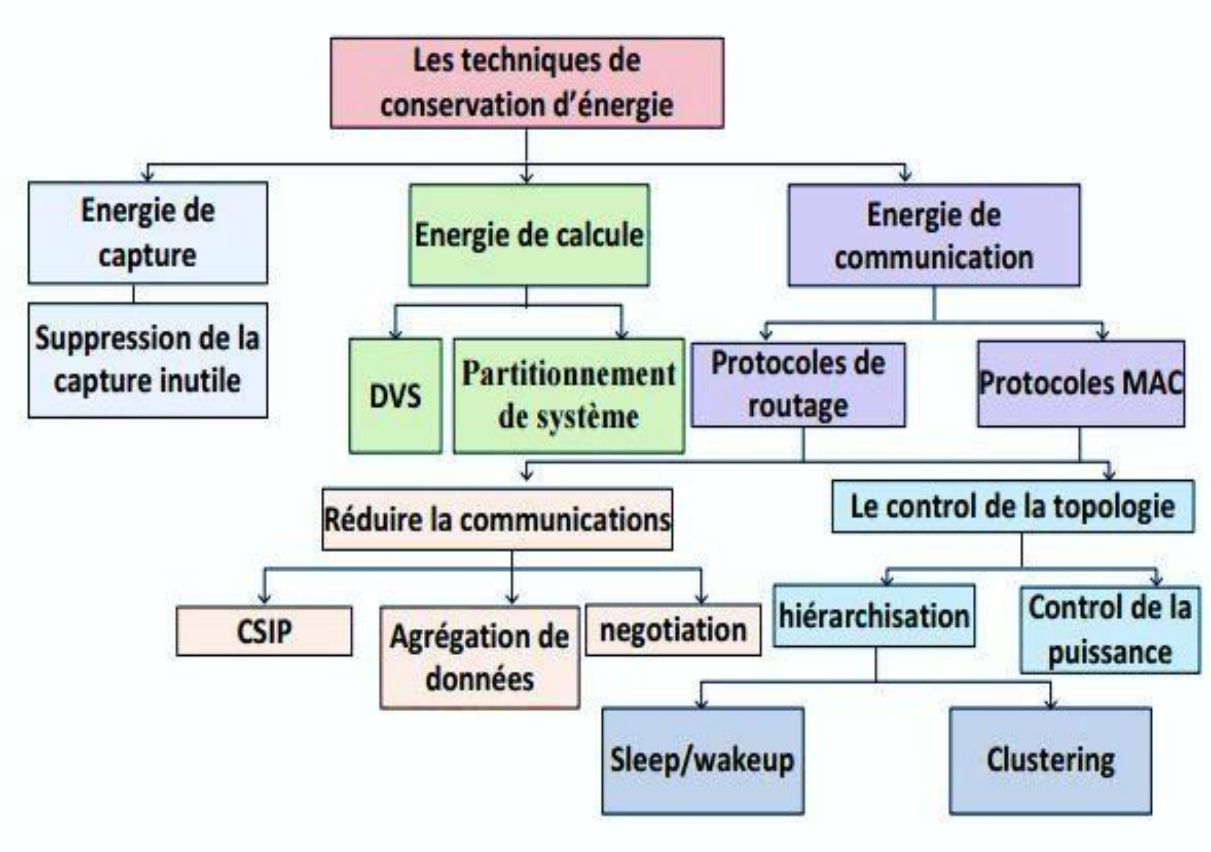


Figure 2.13 Les méthodes de conservation d'énergie dans les réseaux de capteurs sans fil [5]

17. Méthodes proposées pour minimiser l'énergie de communication

Des mesures expérimentales ont montré que généralement c'est la transmission des données qui consomme le plus d'énergie. Comme cité précédemment cette dernière est influencé par plusieurs facteurs qui ont un lien très étroit avec la couche MAC et la couche

réseau. De ce fait, la conception des protocoles de conservation d'énergie doit prendre en considération les contraintes liées à la couche MAC et réseau. La minimisation de l'énergie dépensée côté MAC et réseau peut être atteinte soit en réduisant le nombre d'émission/réception des messages ou par le contrôle de la topologie. Réduire le nombre de communication Réduire le nombre de communication signifie moins d'utilisation de la radio. Ainsi, la consommation d'énergie peut être optimisée d'une manière significative, la réduction du nombre de communication peut être achevée grâce des techniques par exemple Agrégation des données.

Conclusion

Les pannes peuvent survenir par manque d'énergie ou en raison de dommages physiques ou d'interférences environnementales. En effet, la panne de quelques nœuds entraine la perte des liens de communication et ainsi un changement significatif dans la topologie du réseau. Prendre en compte la conservation d'énergie. Ils doivent intégrer des mécanismes qui permettent aux utilisateurs de prolonger la durée de vie du réseau en entier, car chaque nœud est alimenté par une source d'énergie limitée et généralement irremplaçable. Dans un nœud capteur, l'énergie est consommée en assurant les fonctions suivantes : la capture, le calcul (traitement) et la communication. Cette dernière représente une grande portion de l'énergie totale consommée. De ce fait, la communauté de recherche est en train de développer et de raffiner plusieurs techniques de conservation d'énergie. La minimisation de cette énergie est liée aux différents protocoles qui se basent sur plusieurs techniques telles que l'agrégation de données qui fera l'objet de notre prochain chapitre.

CHAPITRE 3

L’AGREGATION DES DONNEES DANS WSN

1. Introduction

Les réseaux de capteurs sans fil (WSN) comprennent plusieurs nœuds de capteurs qui détectent et mesurent les données environnementales et les signalent au puits ou à la station de base. Ces nœuds de capteurs détectent les informations similaires et l'envoie au nœud récepteur. Cela entraîne une redondance au niveau du nœud récepteur. Les nœuds récepteurs consomment plus d'énergie pour traiter ces paquets redondants. Comme les nœuds de capteur ont une puissance de batterie limitée et un petit stockage de données, la majeure partie de la puissance de la batterie est gaspillée en éliminant la redondance au niveau du nœud récepteur et raccourcit la durée de vie du réseau. Donc pour conserver l'énergie d'un nœud et pour améliorer la durée de vie du WSN, nous avons besoin d'une technique pour éliminer les données détectées redondantes et l'agrégation de valeurs de capteurs similaires afin de réduire la surcharge de communication. L'agrégation de données est un moyen efficace de réduire l'énorme volume de données générées dans les WSN en éliminant la redondance entre les réseaux de capteurs sans fil. Dans ce chapitre, nous sommes concentrés sur l'importance de la technique d'agrégation de données et sur les différents protocoles d'agrégation de données basés sur le réseau.

Les réseaux de capteurs sans fil sont constitués de capteurs multifonctionnels densément déployés, à faible coût et à faible consommation. Dans les WSN, la fonction de base des réseaux de capteurs comprend la détection collaborative, l'échantillonnage, le calcul et la diffusion des informations détectées. Les nœuds de capteurs ont une puissance de batterie limitée qui ne permet ni de recharger ni de réapprovisionner le nœud de la batterie une fois qu'il est déployé sur le terrain. Dans un WSN déployé, la communication des nœuds avec dans leur portée radio et la collecte de données consomment plus d'énergie. Il est donc nécessaire de réduire la consommation d'énergie à chaque nœud de capteur pour augmenter la durée de vie du réseau WSN. Cela peut être accompli en supprimant les informations redondantes dans le réseau sans fil. Parce que la majeure partie de l'énergie d'un nœud est gaspillée lors du traitement des données redondantes. Ainsi, l'élimination de la redondance est l'une des solutions pour améliorer la durée de vie du réseau.

Un nœud de capteur est un petit appareil composé de trois parties

- Les données sont collectées à partir de l'environnement physique à l'aide du sous-système de détection.
- Manipulation et stockage des données à l'aide du sous-système de traitement.
- Transmission de données à l'aide d'un sous-système de communication sans fil.

2. Motivation:

Un réseau de capteurs sans fil se compose d'un grand nombre de nœuds contraints en ressources, en termes de puissance de traitements, capacité de stockage, et bande passante de communication, dues à leur taille minuscule ainsi que l'énergie limitée.

En effet, les redondances qui surviennent dans le réseau pourraient avoir un impact négatif sur ces ressources: gaspillage d'énergie et de la bande passante, par exemple. Donc, il est impératif de développer une technique permettant la réduction de ces redondances: l'agrégation de données. Pour surmonter ce problème, il est essentiel de connaitre ces contraintes et comment il introduit cette technique d'agrégation dans les RCSFs[9].

3. Fusion de données et Agrégation de données:

De nombreuses définitions ont été attribuées à la fusion de données, dite aussi fusion d'information, au fil du temps. Selon Hall et Llinas , la fusion de données est la combinaison des données provenant de capteurs multiples et d'autres informations pertinentes fournies par des bases de données associées afin d'aboutir à une meilleure exactitude et des inférences plus spécifiques que celles qui pourraient être atteintes par l'utilisation d'un seul capteur. Dans ce cas, la fusion est réalisée avec l'objectif d'améliorer la précision.

En particulier, pour les réseaux de capteurs sans fil, les données peuvent être fusionnées avec au moins deux objectifs: amélioration de la précision et économie d'énergie.

Par la suite, le terme agrégation de données est devenu populaire dans la communauté de réseaux de capteurs sans fil comme synonyme de fusion de donnée, mais cela doit être évité

car il ne se réfère qu'à une instance de la fusion: le résumé.Selon Van Renesse, l'agrégation est la capacité de résumer. Ce qui signifie que le volume de données manipulées est réduit à l'aide des fonctions de synthèse, tels que le maximum et la moyenne. [9].

4. Définition d’agrégation

Les nœuds qui se trouvent dans la même portée radio peuvent détecter les données redondantes et les transmettre au nœud récepteur. Il est alors difficile pour le nœud récepteur de gérer une telle quantité de données. Ce problème peut être résolu par une approche basée sur les données appelée « agrégation de données ». L'agrégation de données d'approche est le mécanisme d'économie d'énergie. Il s'agit du processus consistant à combiner les données provenant de diverses sources et à les acheminer après avoir supprimé la redondance, de manière à améliorer la durée de vie globale du réseau. Cela peut considérablement aider à réduire la consommation en éliminant les données redondantes.

La fonctionnalité d'agrégation de données est effectuée en continu afin d'améliorer la bande passante et l'utilisation de l'énergie, mais elle peut avoir un impact négatif sur d'autres mesures de performance telles que le délai, la précision, la tolérance aux pannes, etc. Cependant, l'objectif de l'agrégation de données est d'éliminer les éléments redondants. Transmission de données et améliore la durée de vie du réseau. Plusieurs techniques ont été présentées pour une collecte de données efficace dans WSN, qui concernent l'amélioration de la durée de vie du réseau. La figure 1 représente le processus d'agrégation de données.

En tant qu'approche traditionnelle dans WSN, les nœuds envoient des données individuellement lorsque la station de base demande un réseau. Mais dans l'approche d'agrégation de données, l'agrégateur, un nœud spécial est utilisé pour collecter les données de ses stations voisines, les ajouter et transmettre ces données combinées à la station de base, c'est-à-dire le nœud récepteur de manière multi-sauts. L'aspect principal de l'agrégation de données est de collecter et d'agréger les données d'une manière économe en énergie permettant d'augmenter la durée de vie du réseau. L'agrégation de données est un processus de composition du paquet transmis, dans le sens où le paquet ne doit contenir que les informations nécessaires et aucune donnée redondante. Lors de la conception d'algorithmes d'agrégation de données, certaines des exigences supplémentaires à prendre en compte, telles que, ils doivent prendre en compte les

capacités énergétiques des dispositifs de détection, les ressources énergétiques et les capacités de calcul. Et aussi la topologie du réseau à considérer.

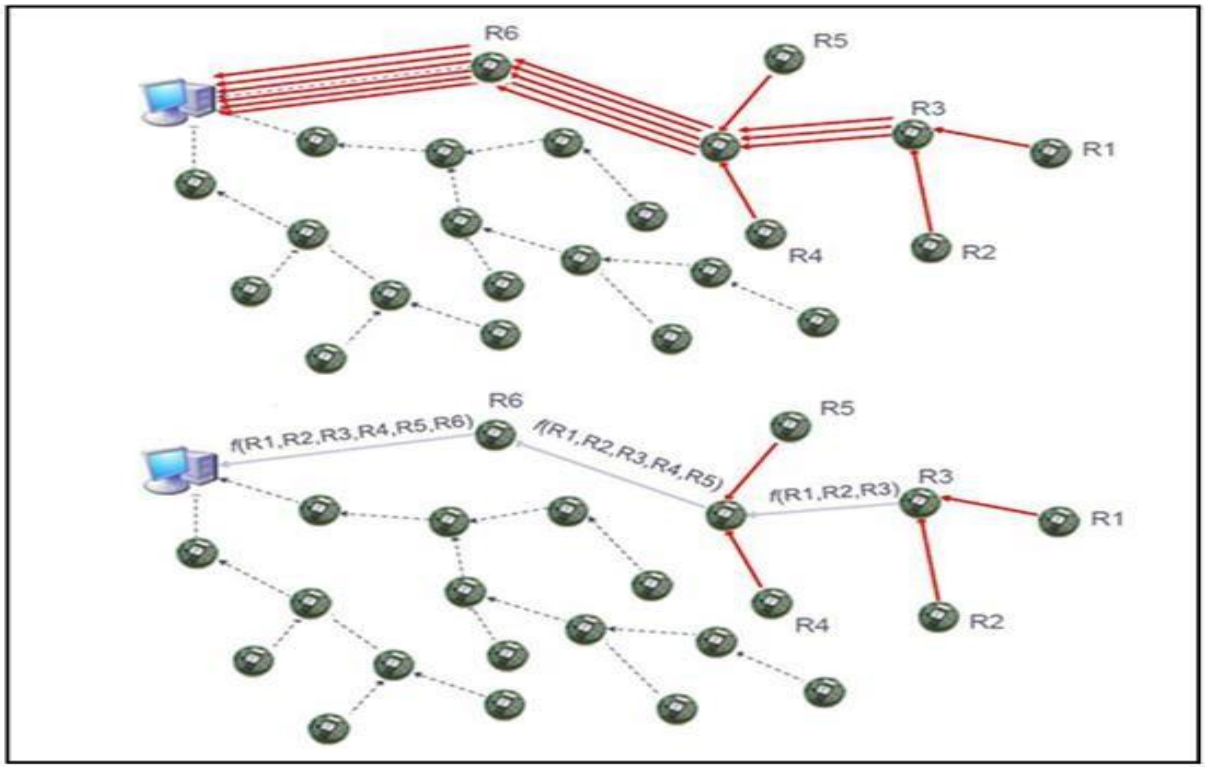
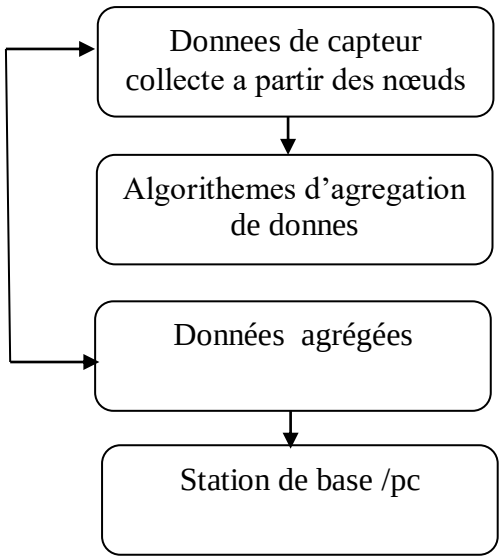


Figure 3.1: Exemple d'agrégation de données

La figure précédente illustre un exemple d'agrégation de données dans un réseau de capteurs sans fil. Au total, 18 messages sont envoyés sur le réseau.

Après l'utilisation du mécanisme d'agrégation de données, on obtient un total de 7 messages uniquement.



La figure 3.2 montre l'architecture générale de l'agrégation de données. [16]

5. catégories d'agrégation de données

Nous pouvons classer trois catégories d'agrégation de données: la structure d'agrégation, la fonction d'agrégation et la planification de l'agrégation [8].

- Où agréger est l'objectif de **la structure d'agrégation.** Cette catégorie définit la manière dont les données agrégées sont acheminées vers le récepteur en utilisant ou en créant une structure de réseau, et la structure doit déclencher l'agrégation dans le réseau. Fondamentalement, la structure d'agrégation trouve plusieurs nœuds de capteurs en tant qu'agrégateurs ou nœuds de passerelle pour traiter les données brutes, et les informations agrégées seront transférées via la structure. La structure d'agrégation ressemble plus à un routage centré sur les données, ce qui permet aux nœuds de relayer les données avec plus d'informations. La structure d'agrégation liée à la littérature propose des structures basées sur une hiérarchie ou une colonne vertébrale pour transmettre des données agrégées.

- Comment agréger est défini à l'aide de **la fonction d'agrégation**. Ce problème est la partie la plus importante pour l'agrégation de données, qui se concentre sur la façon dont les nœuds de capteurs agrègent les données brutes dans un résumé. Une fonction d'agrégation efficace et utile aide les nœuds de capteurs à réduire considérablement la consommation d'énergie. Nous avons mentionné ci-dessus qu'il existe deux corrélations (c'est-à-dire des corrélations temporelles et spatiales) dans les données brutes, et la fonction d'agrégation des données bénéficie principalement de ces corrélations. Fondamentalement, des opérations simples sont utilisées comme fonctions d'agrégation (basées sur la corrélation temporelle), telles que Average, MAX(MIN), SUM, COUNT et Median. Comme exigences de fidélité de récupération, des fonctions d'agrégation plus compliquées sont proposées.

- Le moment de l'agrégation est concerné par **la planification de l'agréation.** L'agrégation de données doit traiter les données puis les transmettre, ce qui entraîne un retard entre le nœud source et le puits. Un ordonnancement d'agrégation est proposé pour résoudre ce problème. Plus précisément, la planification de l'agrégation définit quand un nœud capteur doit agréger les données et quand le nœud doit transmettre les données. L'objectif de la planification d'agrégation est de réduire le retard causé par l'agrégation des données.

5.1 La structure d'agrégation

La structure d'agrégation organise les nœuds de capteurs pour effectuer une agrégation dans le réseau. Il définit principalement le chemin d'agrégation des données et les emplacements des agrégateurs. Les paquets de données des nœuds sources sont relayés sur une structure vers le puits, et la structure doit permettre d'agréger davantage de données le long de cette structure. En fait, le moyen le plus simple d'agréger les données de la source au puits consiste à présélectionner des nœuds qui ont fonctionné comme nœuds d'agrégation ou de passerelle, et à prédéfinir une direction préférée à suivre lors de la transmission des données.

5.1.1Stratégies d'agrégation des données

Il existe plusieurs stratégies d'agrégation dont certaines sont énumérées ci- dessous [16]:

5.1.1.1Approche centralisée

Dans cette approche, chaque nœud de capteur envoie ses données détectées à un nœud central (station de base) via le chemin le plus court possible. Tous les nœuds capteurs envoient simplement les paquets de données à un nœud, qui est le plus puissant parmi tous les autres nœuds. Ce nœud est appelé nœud agrégateur ou nœud d'en-tête. Ce nœud agrège les données provenant d'autres nœuds et les données résultantes seront envoyées sous la forme d'un seul paquet.

5.1.1.2Approche en réseau

L'agrégation en réseau est une approche globale pour la collecte et le traitement des données au niveau des nœuds intermédiaires et l'acheminement des informations via un réseau multi-sauts. Le principal de cette approche est de réduire la consommation d'énergie. Il existe deux types d'agrégation en réseau.

- **Avec réduction de taille**: la du paquet à transmettre au nœud récepteur est réduite en combinant et en compressant les paquets de données reçus par le nœud capteur de ses voisins.

- **Sans réduction de taille :** Ici, sans traitement de la valeur des données, les paquets des différents nœuds voisins sont fusionnés en un seul paquet.

5.1.1.3 Structures basées sur la hiérarchie

Les structures basées sur la hiérarchie font que les nœuds de capteur forment une forme hiérarchique, telle qu'un arbre ou un cluster. Les données sont transférées des nœuds de niveau inférieur vers les nœuds de niveau supérieur, et l'agrégation sera réalisée par les nœuds de niveau supérieur. Dans une structure arborescente, les nœuds enfants envoient des informations aux nœuds parents et l'agrégation est réalisée par les nœuds parents. Dans la structure basée sur le cluster, les nœuds membres du cluster rapportent les données au chef de cluster, et l'agrégation sera effectuée par le chef de cluster. Dans ce qui suit, nous passons principalement en revue les structures arborescentes et basées sur les clusters.

5.1.1.4Approche arborescente

Dans cette approche, un arbre d'agrégation de données (DAT) est encadré et ici, pour chaque transmission de données, un arbre couvrant minimum est construit. Chaque nœud d'un réseau a une relation parent-enfant dans laquelle les données sont transmises selon une approche ascendante. Les données commencent à circuler des nœuds feuilles vers le récepteur nœud et l'agrégation des données est effectuée par les nœuds parents du réseau.

5.1.1.5 Approche basée sur les clusters

Ici, l'ensemble du réseau est divisé en plusieurs clusters. Chaque cluster est composé de plusieurs nœuds de capteurs. Le chef de cluster est sélectionné parmi les nœuds capteurs au sein d'un cluster. Le rôle d'agrégateur est assuré par le chef de cluster qui agrège les données reçues et envoyées au puits. Par cette approche, la surcharge de bande passante est minimisée car le nombre total de paquets à transmettre est inférieur. Plusieurs approches basées sur les clusters pour la collecte de données ont été proposées pour WSN. Le regroupement réduit la transmission directe vers la station de base par l'agrégation des données du réseau ainsi que la consommation d'énergie en réduisant la distance de transmission.

5.1.1.6 Structures basées sur la dorsale

Les structures basées sur le squelette sont également fréquemment étudiées dans WSN. L'idée sous- jacente est de définir le chemin de la dorsale ou l'ensemble dominant connecté dans le réseau. Tous les autres nœuds peuvent transmettre des données à partir de celui-ci, et les nœuds du backbone sont responsables de l'agrégation des informations. Ce type de structures facilite également le processus de diffusion des données et est utile pour les applications de puits mobiles. [8]

6. Exemples des protocoles

6.1 Le Tiny AGgregation (TAG)

un protocole centré sur les données, est basé sur une structure arborescente et spécifiquement conçu pour les applications de surveillance. Il y a deux phases pour TAG, l'une est la phase de distribution, l'autre est la phase de collecte. Pendant la phase de distribution, le puits diffus des requêtes au nœud de capteur cible. À partir du message de requête, la route du puits au capteur est construite. Pendant la phase de collecte, chaque parent

doit attendre les données de tous ses enfants avant de pouvoir envoyer ses informations agrégées dans l'arborescence. Le créneau horaire est utilisé pour chaque nœud, une fois le temps écoulé, le nœud peut se mettre en veille pour économiser de l'énergie. L'agrégation des données peut être réalisée sur des nœuds intermédiaires par des opérations simples (par exemple, Moyenne, Max, Min). Comme indiqué ci-dessus, nous savons que TAG a deux exigences: premièrement, le récepteur peut envoyer des demandes de requête à tous les nœuds du réseau, deuxièmement, chaque nœud a au moins une route vers le puits. Ainsi, TAG peut être inefficace pour les topologies dynamiques ou les défaillances de liaison. [8]

6.2Energy Aware Data Aggregation (EADA)

Combine une structure de grille avec un arbre de diffusion de données à la demande. Dans chaque cellule de grille, le nœud avec l'énergie résiduelle maximale est sélectionné comme nœud passerelle qui est responsable de l'agrégation des données générées dans la cellule de grille. Le puits inonde les requêtes de données à travers des passerelles restreintes sur un secteur circulaire vers la zone d'intérêt. Une fois que la requête entre dans la zone d'intérêt, la passerelle d'entrée devient la racine d'un arbre nouvellement construit qui couvre tous les nœuds de la zone d'intérêt. Les données agrégées sont ensuite diffusées via l'inverse de la route de requête vers le récepteur. Si l'énergie de la passerelle racine descend en dessous d'un certain seuil, la passerelle avec le maximum d'énergie restante dans la zone d'intérêt est sélectionnée comme nouvelle racine et un nouvel arbre est formé. Cependant, l'établissement et le maintien d'un arbre distinct pour chaque zone d'intérêt peut augmenter la consommation globale d'énergie dans le réseau. [8]

6.4 Protocole LEACH (Low Energy Adaptive Clustering Hierarchy)

Pour le routage dans les réseaux de capteurs homogènes, un clustering distribué nommé LEACH a été proposé par Heinzelman et al. Cette algorithme choisit aléatoirement les nœuds qui vont être des CHs et donne ce rôle aux différents nœuds suivant la méthode Round-Robin (tourniquet). Cette méthode permet de garantir une consommation de l'énergie équitable entre tous les nœuds d'un même cluster. De plus, afin de minimiser la quantité de données transmises à la station de base, les ClusterHead agrègent les informations recueillies par les nœuds membres qui sont dans le même cluster, et envoient un paquet agrégé à la station de base. Le protocole LEACH se compose de deux phases à savoir : la phase n´ Set-up z˙ dans laquelle les ClusterHeads sont choisis et les clusters du réseau sont créés. Et la deuxième

phase appelée n´ Steady State z˙ durant laquelle le transfert des données sont envoyés à la station de base. Malgré cela, le protocole de routage LEACH bien qu'il puisse allonger la durée de vie du réseau, celui-ci à certaines limites.

Le protocole considère que tous les nœuds du réseau peuvent transmettre des données avec une puissance maximale pour pouvoir atteindre la station de base et que tous les nœuds ont une puissance de calcul permet- tant de supporter les différentes couches MAC. Donc le protocole LEACH ne correspond pas aux réseaux de très envergure pouvant être déployé sur de grandes zones. D'autre part, le protocole LEACH choisit aléatoirement les ClusterHeads et ne pose aucune contrainte sur leur distribution ainsi que sur leur niveau d'énergie. Nous pouvons trouver par conséquent des nœuds étant isolés. Dans le protocole LEACH, il y a un rassemblement des données qui est centralisé et se lance périodiquement. Mais il existe des cas où la transmission périodique des données peut ne pas être négligée car cela épuise rapidement l'énergie des capteurs. [12]

6.5 PEGASIS (Power-Efficient Gathering in Sensor Information Systems)

Lindsey et Raghavendra ont proposé une version améliorée de LEACH appelée PEGASIS. L'idée principale de PEGASIS est de former une chaîne entre les nœuds de sorte que chaque nœud reçoive de et communique à un voisin proche (Voir Figure 4.2). Les données collectées sont transmises d'un nœud à un autre qui les agrège jusqu'à ce qu'elles arrivent à un nœud particulier qui les transmet à la station de base. Les nœuds qui transmettent les données à la station de base, sont choisis tour à tour selon une politique round-robin dans le but de réduire l'énergie moyenne dépensée par un nœud durant une période (round). Contrairement à LEACH, PEGASIS évite la formation des clusters et procure à un seul nœud dans la chaîne l'envoi de données à la station de base. D'ailleurs, PEGASIS suppose que les nœuds sont capables de modifier leur puissance de transmission [1].

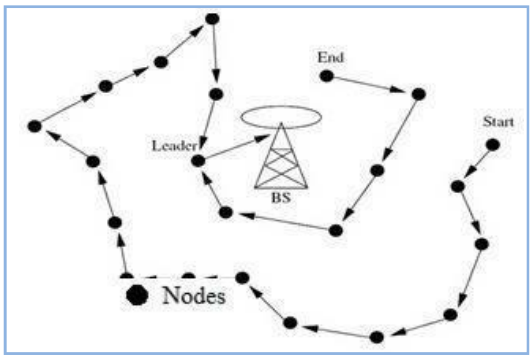


Figure 3.3 : Illustration du protocole PEGASIS [1]

6.6 DRINA: Data Routing for In-Network Aggregation for WSN

L'algorithme DRINA est une technique basée sur les clusters [14]. Ce l'objectif principal est de construire un arbre de routage et de trouver le plus court chemin qui relie tous les nœuds source au puits en maximisant l'agrégation de données. Un cluster est formé, lorsque les données sont envoyées du nœud source au nœud récepteur. Ensuite, la tête de cluster est choisie. Ce chef de cluster agrège les données des nœuds restants dans cluster et forme le chemin le plus court jusqu'au nœud récepteur. Coût de l'arborescence de communication et de routage est moindre pour DRINA. À construire l'arborescence de routage dans DRINA les rôles suivants sont considéré:

- **Collaborateur :** il détecte un événement et envoie les données collectées vers le nœud coordinateur.
- **Coordinateur :** il agrège les données du collaborateur et l'envoie au nœud récepteur.
- **Relais :** c'est un nœud intérieur et transmet les données au puits nœud.
- **Sink** : il reçoit les données du collaborateur et du coordinateur nœuds

6.6.1.les phases de l'algorithemes de DRINA

Il y a trois phases d'algorithme DRINA :

- **Construction de l'arbre Hop :** il s'agit d'un arbre construit du capteur au nœud puits. La distance est calculée de tous les nœuds au nœud puits dans hops.HCM (message de configuration de saut) est envoyé par le nœud puits à tous les autres nœuds via l'inondation. Il y a deux champs dans le message HCM : l'un est l'ID de nœud pour l'identification du nœud et l'autre est le champ Hop to Tree qui stocke la distance en sauts depuis le nœud où le message HCM est produit.La valeur initiale de Hop to Tree est 1 au nœud récepteur et infinie à tous les autres nœuds. Cette valeur est transmise par le nœud puits à tous les nœuds du réseau qui comparent leur valeur à celle-ci et stockent la plus petite des deux valeurs. Le champ ID est également mis à jour. Les messages HCM sont également relayés avec de nouvelles

valeurs et cela continue jusqu'à ce que tout le réseau soit configuré.

- **Formation du cluster :** dans cette phase, le cluster est formé et le chef de cluster est sélectionné. Pour les nœuds qui détectent le même événement, l'algorithme d'élection du leader commence. Au début, le nœud coordinateur est proche du nœud récepteur dans les sauts, tandis que dans d'autres événements, le nœud leader est proche de la route établie. S'il y a une égalité entre deux nœuds, celui avec le plus petit ID ou avec plus d'énergie sera le leader. L'avantage est que les informations collectées par les nœuds qui détectent le même événement sont agrégées en un point appelé point d'agrégation et sont très efficaces.

- **Formation des mises à jour du routeur et de l'arborescence de sauts :** dans cette phase, du coordinateur au nœud récepteur, un té de routage est établi. Le nœud coordinateur envoie REM (message d'établissement de route) à son nœud voisin pour former un arbre de routage. Le nœud voisin est celui qui est le plus proche du chef de cluster en sauts. Ce nœud continue d'envoyer un message REM à son nœud voisin et le processus se poursuit jusqu'à ce qu'un chemin soit établi entre le nœud leader et le nœud récepteur. Le cheminement est illustré à la figure 4.3.

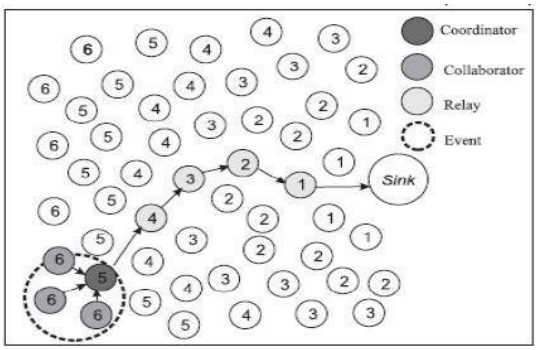


Figure 3.4 : Arborescence du routeur du nœud leader au nœud récepteur

Les routes du nœud source au nœud récepteur sont créées en sélectionnant le voisin le plus proche à chaque saut. Le voisin le plus proche est choisi comme suit :

- dans le cas d'un événement, le nœud proche du puits dans les sauts est choisi.

- pour plus de deux événements, le nœud voisin est celui qui se dirige vers le nœud le plus proche faisant partie de la route établie. Il est montré dans la figure ci-dessous

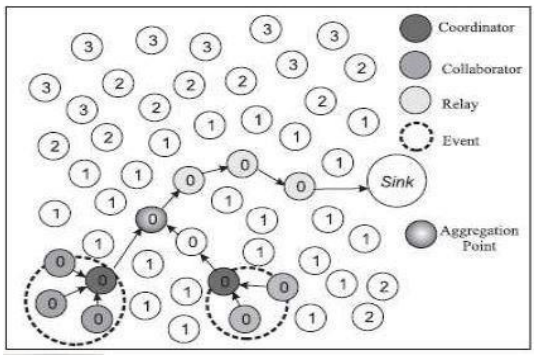


Figure3 .5 un itinéraire établi vers l'itinéraire précédent

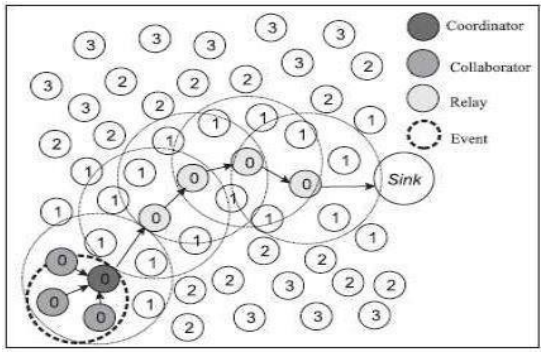


Figure3.6 Mise à jour de l'arbre du houblon

- **Mécanisme de réparation des pannes** : Drina dispose également d'un mécanisme de réparation des pannes pour surmonter les perturbations des communications. Il dispose d'un mécanisme de réparation de route basé sur ACK. Le paquet de données est envoyé par le nœud relais chaque fois qu'il veut transmettre des données à son prochain nœud de saut. Il définit le délai d'attente pour la transmission de chaque paquet de données et attend l'accusé de réception.

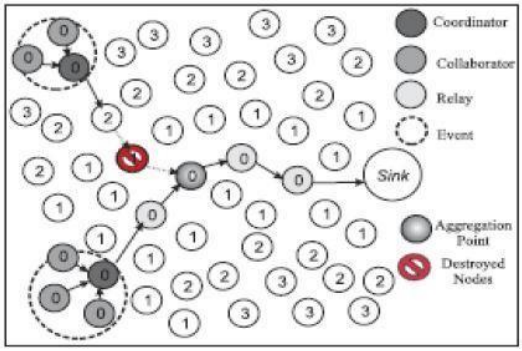


Figure3.7 Région avec nœuds détruits

Si aucun accusé de réception n'est reçu, il considère le nœud particulier comme un nœud défaillant et sélectionne un nouveau nœud. Lorsque ce mécanisme de réparation de route est appliqué, un nouveau chemin partiel est reconstruit. Lorsque ce mécanisme de réparation de route est appliqué, un nouveau chemin partiel est reconstruit.

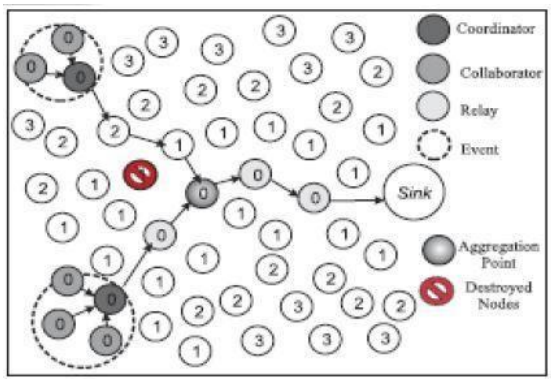


Figure3.8 Chemin réparé

Ainsi, DRINA gère le mécanisme de réparation de route grâce auquel il fournit une communication fiable dans des environnements dynamiques.

Comme DRINA prend en charge l'agrégation dans le réseau, il offre un meilleur taux de livraison des paquets de débit et un délai de bout en bout. Il fonctionne bien avec le mécanisme de réparation d'itinéraire et possède certaines fonctionnalités telles qu'un nombre maximal d'itinéraires qui se chevauchent, moins de messages pour la construction d'arborescence de routage, un taux d'agrégation élevé et une transmission fiable. De plus, la sécurité est un facteur clé dans tout réseau, DRINA aide donc à atteindre deux objectifs fondamentaux de sécurité, à savoir l'authentification et la confidentialité. Ainsi, la mise en œuvre de DRINA dans les réseaux de capteurs peut améliorer la durée de vie du réseau en réduisant la consommation d'énergie.

7. Fonctions d'agrégation des données

Les fonctions d'agrégation se concentrent sur la façon de faire l'agrégation, qui est la façon de traiter données brutes dans un résumé. Comme, il existe deux types de corrélations dans les données brutes : la corrélation temporelle et la corrélation spatiale. Corrélation temporelle existe dans les données collectées par un nœud de capteur à différents instants; et la corrélation spatiale se produit souvent lorsque les données sont collectées à partir de nœuds de capteurs locaux voisins. Correspondant aux deux corrélations, nous définissons deux types de fonctions d'agrégation : fonctions de prévision et de compression. L'agrégation des données

de prévision utilise des modèles de prédiction ou des données empiriques pour prédire le suivant, tout en comprimant l'agrégation, s'engage à compresser l'information. Plusieurs opérations simples, telles que Average, MAX, MIN, COUNT, SUM, etc., peuvent être traités comme n'importe quel type.

de fonction de prévision ou de compression. Prenons Moyenne comme exemple, la valeur moyenne de certaines données peut être utilisée pour prédire les données suivantes, et aussi peut être vu comme une donnée compressée

7.1Fonctions d'agrégation de données de base

Les fonctions d'agrégation de base sont des opérations simples. Nous introduisons les opérations usuelles qui sont souvent utilisés dans des applications pratiques. Tout d'abord, moyen, il est facile à mettre en œuvre sur un nœud capteur. Supposons que les données brutes soient représentées par vt au temps t, noté (vt ,t).fonction de moyenne peut obtenir une valeur agrégée telle que:

$$\text{Fmoyenv} = \frac{\text{v1} + \cdots \ldots \text{vt}}{\text{t}} \qquad (2)$$

Où v est la valeur moyenne de t données brutes.

Deuxièmement, **MAX** (resp. **MIN**), maximum (resp. minimum) est principalement utilisé dans les applications d'alarme. Ces applications n'ont pas besoin de connaître les données brutes, mais si les données brutes est trop élevé (resp. trop faible) pour leurs besoins, ils doivent déclencher une alerte. Fonction de MAX (resp. MIN) peut être formulé comme :

Fmax vmax = MAX{v0, ……., vt} (3)

Fmin vmin = MIN{v0,…… , vt} (4)

Il y a aussi des opérations comme COUNT (qui est utilisé pour compter le nombre de données collectées), Médiane (la médiane valeur des données collectées) et ainsi de suite. Les inconvénients de ces fonctions sont qu'elles ne peuvent pas garantir l'exactitude selon un seuil d'erreur donné. L'application peut choisissez l'un d'entre eux pour atteindre l'efficacité énergétique et économiser la capacité du réseau si la précision n'est pas une exigence absolue.

7.2Agrégation des données de prévision

Les fonctions d'agrégation de prévision bénéficient des corrélations temporelles des données brutes. Les séries de données d'un nœud de capteur (telles que la température, l'humidité) montrent souvent que le la valeur actuelle des données est liée à la précédente (identique ou similaire) et signifie et la variance de l'ensemble de données ne changent souvent pas. Une telle série de données est stationnaire, qui peut être prédit avec précision.

L'agrégation des prévisions est un nom générique pour les fonctions qui prédisent les données à l'aide de plusieurs modèles ou méthodes. Comme le puits peut récupérer les données haute fidélité des modèles ou méthodes, les nœuds capteurs n'ont pas besoin d'envoyer toutes les données brutes au puits, ce qui réduire le nombre de transmissions et donc économiser de l'énergie.

8. Objectifs de l'agrégation des données

- **Économie d'énergie** l'agrégation de données réduit les transmissions redondantes ou corrélées dans un réseau, ce qui minimise directement la consommation d'énergie pour l'ensemble du réseau. Étant donné que la limitation de l'énergie est une contrainte principale pour WSN, la conception de l'agrégation des données devrait mettre l'économie d'énergie au centre des préoccupations.

- **Précision des données :** La précision des données est la précision entre les données récupérées 3 et les données brutes. Les nœuds capteurs agrègent les données brutes dans un résumé qui peut perdre plusieurs informations. Ainsi, il est raisonnable que les données récupérées côté puits aient une certaine déviation comparant aux données brutes. Ainsi, comment économiser de l'énergie avec une précision acceptable est une exigence générale à prendre en compte pour toutes les applications.

- **conomie de capacité du réseau :** les contraintes de bande passante des nœuds de capteurs limitent la capacité de travail du réseau des WSN, donc comment économiser la capacité a également été fréquemment étudiée. En envoyant moins de paquets au récepteur, l'agrégation des données peut économiser la capacité du réseau. De plus, la quantité de capacité de réseau économisée peut être considérée comme une métrique pour évaluer un protocole d'agrégation. Ainsi, nous devons

également prendre en compte l'objectif d'économiser la capacité du réseau lors de la conception d'un protocole d'agrégation.

Conclusion

L'agrégation de données est une technique prometteuse dans les réseaux de capteurs sans fil, permettant un gain important de ressources épuisées en raison des redondances et la surcharge du réseau. Dans ce chapitre, nous avons défini le processus d'agrégation tout en précisant son principe de fonctionnement. Puis, nous avons établi une étude détaillée sue cette technique, qui a permis de distinguer ses différentes stratégies et catégories et approches. Par la suite, nous avons établi un état de l'art de quelques protocoles utilisant cette technique. Et d'après cette étude, en explicitant quelques avantages. Dans la suite de ce travail, nous allons proposer un protocole d'agrégation de données drivée de DRINA appliquer pour minimiser le nombre des messages redondantes (rapports d’échecs) qu’il utilisent dans la notification des pannes en wsn .

CHAPITRE 4

LA NOTIFICATION ET L'AGREGATION DES RAPPORTS D'ECHECS DANS WSN

1. Introduction

Un très grand nombre de travaux de recherche dans les RCSFs se concentrent sur la contrainte d'énergie afin de concevoir des algorithmes et des protocoles spécifiques à ces réseaux optimisant au maximum la conservation d'énergie [9]. La notification des pannes est une tâche très importante intégrée dans plusieurs protocoles de détection et de traitement de panne.

On exploitant les techniques d'agrégation intégré dans le protocole DRINA, et nous essayons donner une solution approprie avec notre problème la notification des panne dans les réseaux de capteurs avec les phases suivantes: la construction de l'arbre de routage et la détection des panne avec la construction du cluster et élection de chef cluster et l'agrégation au niveau du cluster et finalement la livraison fiable des paquets au sink.

2. La relation entre les pannes et l'agrégation

Les capteurs de réseau sans fil caractérisent par des ressources limitées par exemple l'énergie qui conduit aux échecs, alors, pour assurer la continuité de fonctionnalité de RCSF sans aucune interruption et sans affecter la tache globale du réseau il faut notifier le sink sur la position de cette panne pour prendre la décision. Malheureusement, la panne est considérée comme un évènement qui peuvent être détectée ou observée par plusieurs capteurs voisins.

On appelle ce phénomène la redondance. La relay et la transmission d'une information redondante expire l'énergie du réseau. Afin de minimiser la consommation d'énergie il faut minimiser le nombre de messages d'échecs, Parmi les solutions existantes on mentionne l'agrégation. Malgré ces avantages, l'agrégation pour la notification des pannes peut être un outil strict qui élimine la redondance mais qui minimise aussi la qualité de l'information reçu. Pour cette raison, on propose dans ce travail une solution qui minimise la redondance au lieu de la éliminée, on exploitant le principe de protocole DRINA.

3. L'infrastructure de routage

L'algorithme proposé considère les rôles suivants dans la création de l'infrastructure de routage

- **Collaborateur** : un nœud qui détecte un événement et rapporte les données recueillies à un nœud coordinateur.

- **Coordinateur :** un nœud qui détecte également un événement et qui est chargé de rassembler toutes les données collectées envoyées par les nœuds collaborateurs, de les agréger et d'envoyer le résultat vers le nœud récepteur.

- **Sink :** nœud intéressé à recevoir des données d'un ensemble de nœuds coordinateur et collaborateur
- **Relay** : un nœud qui transfère les données vers le puits.

4. les phases d'algoritheme de DRINA

L'algorithme DRINA peut être divisé en trois phases.

- **la phase 1**

l'arbre de saut des nœuds capteurs au nœud récepteur est construit. Dans cette phase, le nœud récepteur commence à construire l'arbre de saut qui sera utilisé par les coordinateurs à des fins de transfert de données.

- **La phase 2**

Consiste en la formation du cluster et l'élection du chef de cluster parmi les nœuds qui ont détecté l'occurrence d'un nouvel événement (capteur en panne) dans le réseau.

- **la phase 3**

Est responsable à la fois de la mise en place d'une nouvelle route pour la livraison fiable des paquets et de la mise à jour de l'arbre de saut.

4.1 Phase 1 : Construire l'arbre de houblon

Dans cette phase, la distance du puits à chaque nœud est calculée en sauts [10]. Cette phase est déclenchée par l'envoi par le nœud puits, au moyen d'une inondation, du message de configuration de saut (HCM) à tous les nœuds du réseau. Le message HCM contient deux champs: ID et HopToTree, où ID est l'identifiant du nœud qui a lancé ou retransmis le message HCM et HopToTree est la distance, en sauts, par laquelle un message HCM est

passé. La valeur HopToTree commence par la valeur 1 au niveau du puits, qui la transmet à ses voisins (au début, tous les nœuds définissent le HopToTree à l'infini). Chaque nœud, à la réception du message HCM, vérifie si la valeur de HopToTree dans le message HCM est inférieure à la valeur de HopToTree qu'il a stockée et si la valeur de FirstSending est vraie, comme indiqué dans l'algorithme 1 - ligne 3. Si cela condition est vraie alors le nœud met à jour la valeur de la variable NextHop avec la valeur du champ ID du message HCM, ainsi que la valeur de la variable HopToTree, et les valeurs des champs ID et HopToTree du message HCM. Le nœud relaie également le message HCM, comme indiqué dans Algorithme 1 - Ligne 8. Sinon, si cette condition est fausse, ce qui signifie que le nœud a déjà reçu le HCM par une distance raccourcie, alors le nœud rejette le message HCM reçu, comme indiqué dans Algorithme 1 - Ligne 12. Les étapes décrites ci-dessus se répètent jusqu'à ce que l'ensemble du réseau soit configuré.

Avant que le premier événement n'ait lieu, il n'y a pas de route établie et la variable HopToTree stocke la plus petite distance jusqu'au puits. Lors de la première occurrence d'événement, HopToTree sera toujours la plus petite distance; cependant, un nouveau parcours sera établi. Après le premier événement, le HopToTree stocke la plus petite des deux valeurs: la distance au puits ou la distance à l'itinéraire déjà établi le plus proche.

4.1.1Algorithme1: Phase de configuration de l'arborescence du houblon

Algorithm 1: Hop Tree Configuration Phase[10]

```
1   Node sink sends a broadcast of HCM messageswith the value of HopToTree = 1;
    // Ru is the set of nodes that received the message HCM
2   for each u ∈ Ru do
3       if HopToTree(u) > HopToTree(HCM) and FirstSending(u) then
4           NextHopu ← IDHCM;
5           HopToTreeu ← HopToTreeHCM + 1 ;
            // Node u updates the value of the ID field in the message HCM
6           IDHCM ← IDu ;
            // Node u updates the value of the HopToTree field in the message HCM
7           HopToTreeHCM ← HopToTreeu ;
8           Node u sends a broadcast message of the HCM with the new values;
9           FirstSendingu ← false ;
            end
11          else
12              Node u discards the received message HCM;

13      end
14  end
```

4.2 Phase 2 : detection la panne et Formation de cluster et élection du leader

Lorsqu'un un capteur en panne (événement) est détecté par un ou plusieurs nœuds, l'algorithme d'élection du leader démarre et les nœuds de détection seront en cours d'exécution pour le leadership (coordinateur de groupe); ce processus est décrit dans l'algorithme 2. Pour cette élection, tous les nœuds de détection sont éligibles. S'il s'agit du premier événement, le nœud leader sera celui qui est le plus proche du nœud récepteur. Sinon, le leader sera le nœud le plus proche d'une route déjà établie (Algorithme 2, Lignes 7 à 9). En cas d'égalité, c'est-à-dire que deux nœuds simultanés ou plus ont la même distance en sauts vers le puits (ou vers une route établie), le nœud avec le plus petit ID conserve son éligibilité, comme indiqué dans les lignes 11 à 13 de l'algorithme 2 Une autre possibilité est d'utiliser le niveau d'énergie comme critère de départage.

4.2.1Algorithm 2: Cluster formation and leader élection

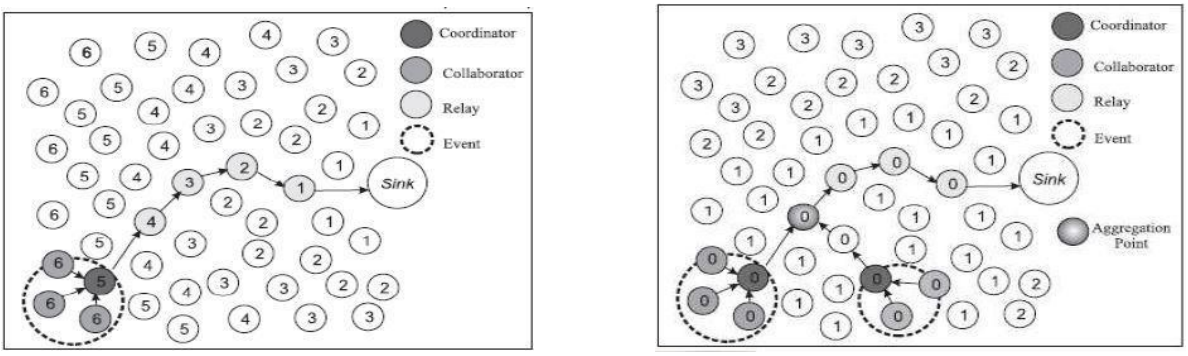
```
1   Input: S // Set of nodes that detected the event
2   Output: u // A node of the set S is elected leader of the group
3   for each u ∈ S do
4   |   role u ← coordinator;
    |   // Node u sends message MCC in broadcast
5   |   Announcement of event detection;
    |   // Nu is the set of neighbors of node u ∈ S
6   |   for each w ∈ Nu do
7   |   |   if HopToTree(u) > HopToTree(w) then
8   |   |   |   roleu ← collaborator ;
9   |   |   |   Node u retransmits the MCC message received from node w ;
10  |   |   end
11  |   |   else if HopToTree(u) = HopToTree(w) ∧ ID(u) > ID(w) then
12  |   |   |   roleu ← collaborator ;
13  |   |   |   Node u retransmits the MCC message received from node w;
14  |   |   end
15  |   |   else
16  |   |   |   Node u discards the MCC message received from w;
17  |   |   end
18  |   end
19 end
```

A la fin de l'algorithme d'élection, un seul nœud du groupe sera déclaré leader (coordinateur). Les nœuds restants qui ont détecté le même événement seront les collaborateurs. Le Coordonnateur recueille les informations recueillies par les Collaborateurs et les envoie à l'évier. Un avantage clé de cet algorithme est que toutes les informations recueillies par le les nœuds détectant le même événement seront agrégés en un seul nœud (le coordinateur), qui est plus efficace que les autres mécanismes d'agrégation (par exemple, agrégation opportuniste)[10].Notre modification sur cette algorithme le processus agrégation ce fait la phase construire cluster et élection Head cluster au lieu faire la 'agrégation a la phase suivante construire la route pour passer le message rapport d'échec .l'agrégation se fait par le nœud coordinateur si arrive plusieurs message de collaborateurs portent le même information sur le position de panne il choisis une seul information éviter la redondance qui consommer plus énergie .

```
Algorithm 2: Cluster formation and leader election
1     Input: S // Set of nodes that detected the event
2     Output: u // A node of the set S is elected leader of the group
3     for each u ∈ S do
4     |   roleu ← coordinator;
      |   // Node u sends message MCC in broadcast
5     |   Announcement of event detection ;
      |  // Nu is the set of neighbors of node u ∈ S
6     |   foreach w ∈ Nu do
7     |   |   if HopToTree(u) > HopToTree(w) then
8     |   |   |   roleu ← collaborator ;
9     |   |   |   Node u retransmits the MCC message received from node w ;
10    |   |   end
11    |   |   else if HopToTree(u) = HopToTree(w) ∧ ID(u) > ID(w) then
12    |   |   |   roleu ← collaborator ;
13    |   |   |   Node u retransmits the MCC message received from node w;
14    |   |   end
15    |   |   else
16    |   |   |   Node u discards the MCC message received from w;
17    |   |   end
18    |   end
19 end
20    repeat
      |   //sons u is the number of collaborator of u
21    |   if sons u>1then
22    |   |   Aggregates all data and sends it to the nexthopu;
23    |   |       Execute the mechanism of Section 3.4
24    |   end
25    |   else
26    |   |   Send data to coordinator and  nexthopu;
27    |   |       Execute the mechanism of Section 3.4
28    |   end
33 until there find node breakdown µ
```

4.3phase 3 : Formation de routage et mises à jour de Hop Tree.

Le chef de groupe élu, tel que décrit dans l'algorithme 2, commence établissant la nouvelle voie pour la diffusion de l'événement. Cette processus est décrit dans l'Algorithme 3, (Lignes 2 à 10). Pour que, le coordinateur envoie un message d'établissement de route à son nœud NextHop. Lorsque le nœud NextHop reçoit un message d'établissement de route, il retransmet le message à son NextHop et démarre le processus de mise à jour de l'arborescence des sauts. Ces les étapes sont répétées jusqu'à ce que le puits soit atteint ou qu'un nœud qui fait partie d'un itinéraire déjà établi est trouvé. Les parcours sont créés en choisissant le meilleur voisin à chaque saut. La les choix du meilleur voisin sont doubles: (i) lorsque le premier événement se produit, le nœud qui mène au chemin le plus court vers le puits est choisi (Figure 2(a)); et (ii) après la survenance de événements ultérieurs, le meilleur voisin est celui qui mène à le nœud le plus proche qui fait déjà partie d'une route établie (Figure 2(b)). Ce processus tend à augmenter l'agrégation points, en veillant à ce qu'ils se produisent aussi près que possible des événements. La route résultante est un arbre qui relie le coordinateur nœuds à l'évier. Lorsque la route est établie, l'arborescence du houblon la phase de mise à jour est lancée. L'objectif principal de cette phase est de mettre à jour la valeur HopToTree de tous les nœuds afin qu'ils puissent prendre compte tenu de l'itinéraire nouvellement établi. C'est fait par les nouveaux nœuds relais qui font partie d'une route établie. Ces nœuds envoient un message HCM (au moyen d'une inondation) pour la mise à jour du saut (Figure 2(b)). Le coût total de ce processus est identique à une inondation, c'est-à-dire que chaque nœud sera envoyer un seul paquet. Cet algorithme pour la mise à jour du saut suit les mêmes principes de l'algorithme de construction d'arbre de saut, décrit à la section 3.1 [10]



(a)exemple d'arbre de routage vers 1evenement (b) exemple d'arbre de routage vers 1evenement

Figure4.1 Mise à jour de l'arbre du houblon

4.4Mécanisme de réparation d'itinéraire

La route créée pour envoyer les données vers le nœud puits est unique et efficace puisqu'elle maximise les points d'agrégation et, par conséquent, la fusion de l'information. Cependant, parce que cette route est unique, toute défaillance dans l'un de ses nœuds entraînera une perturbation, empêchant la livraison de plusieurs données d'événement collectées. Les causes possibles d'échec comprennent une faible consommation d'énergie, une destruction physique et un blocage de la communication. Algorithmes tolérants aux pannes pour les WSN ont été proposés dans la littérature. Certains sont basés sur des mécanismes d'inondation périodiques et enracinés au puits, pour réparer les chemins cassés et découvrir de nouvelles routes pour acheminer le trafic autour des nœuds défectueux. Ce mécanisme n'est pas satisfaisant en termes d'économie d'énergie car il gaspille beaucoup d'énergie avec la réparation des messages. De plus, pendant la période d'inondation du réseau, ces algorithmes sont incapables d'acheminer les données autour des nœuds défaillants, ce qui entraîne des pertes de données. Notre algorithme DRINA offre un mécanisme de réparation de route superposé, basé sur ACK, qui se compose de deux parties : la détection de panne au nœud NextHop et la sélection d'un nouveau NextHop.Lorsqu'un nœud relais doit transmettre des données à son nœud NextHop, il envoie simplement le paquet de données, définit un délai d'attente et attend la retransmission du paquet de données par son NextHop. Cette retransmission est également considérée comme un message ACK. Si l'expéditeur reçoit son ACK du nœud NextHop, il peut en déduire que le nœud NextHop est actif et, pour l'instant, tout va bien. Cependant, si le nœud expéditeur ne reçoit pas l'ACK du nœud NextHop dans le délai d'attente prédéterminé, il considère ce nœud comme étant hors ligne et un autre doit être sélectionné comme nouveau nœud NextHop. Pour cela, l'expéditeur choisit le voisin avec le niveau de saut vers l'arborescence le plus bas pour être son nouveau NextHop; en cas d'égalité, il choisit le voisin avec le niveau d'énergie le plus élevé. Après cela, l'expéditeur met à jour sa table de routage pour faciliter le transfert des paquets suivants. À titre d'exemple, un itinéraire interrompu est illustré à la figure 3(a). Une fois le mécanisme de réparation appliqué, un nouveau chemin partiellement reconstruit est créé, comme illustré à la figure 3(b)[10].

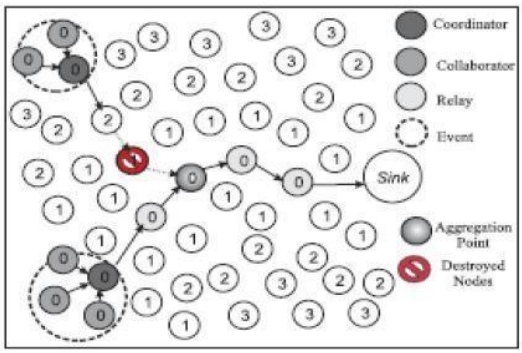


Figure4.2 Région avec nœuds détruits

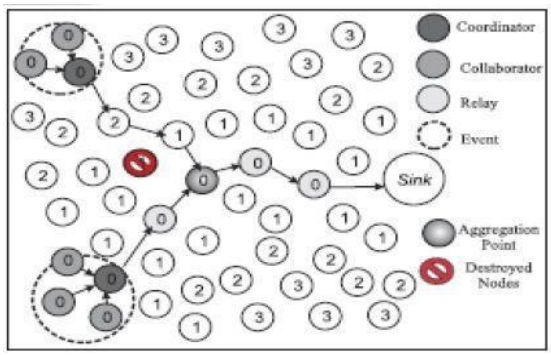


Figure4.3 Chemin réparé

Conclusion

Dans cette chapitre nous avons essaye de mettre en évidence sur le mode d'emploi de l'utilisation de DRINA pour le problème de notification des pannes avec donner les phases nécessaire.

CONCLUSION GENERALE

CONCLUSION GENERALE

Les réseaux de capteurs sans fil constituent une voie de recherche très importante à explorer, ils sont adaptés aux divers domaines de notre quotidien. En effet, une multiplicité de travaux a été mise en place pour remédier aux limites et améliorer leurs performances. L'un des principaux problèmes que nous pouvions rencontrer dans ce type de réseau est la panne des capteurs des réseaux sans fil causée par l'existance de données redondantes .le résultat la consommation importante de la ressource énergétique, la redondance est liée a la nature de ces réseaux, principalement à leur mode de déploiement.

L'existence ou l'échange de données redondantes ou fortement corrélées dans le réseau influe négativement sur ses différentes ressources: la bande passante et l'énergie qui représente une ressource critique dans les réseaux de capteurs sans fil. Il est donc nécessaire de développer et mettre en place des protocoles permettant de conserver cette ressource et assurer le bon fonctionnement du réseau entier

Travailler sur un domaine de recherche comme les réseaux de capteurs, exige la prise en compte des différentes contraintes qui lui sont liées. Ce qui présente des difficultés lors de la phase d'implémentation. Avec la motivation que nous avions eue pour mener ce travail, nous avons finalement donné une vision simple sur la solution qui faire une balance entre l'énergie et donnes par appliquer un technique permet éviter la redondance et conservation ressource critique l'énergie.

Apres la recherche dans les cause des pannes on trouve permet les causes est la communication entre les capteurs si il exist des données redondantes il exprimer plus consommation des énergies alors tombe en panne, alors pour la bonne fonctionne il faut informer le sink pour prendre la decision possible l'information arrive plusieurs fois pour protect le sink tombe en panne alors on applique une technique permet éviter la redondance cette technique est l'agrégation.

On applique le protocole DRINA sur la notification des rapports d'échecs dans wsn par faire une modification avec faire une adaptation sur le sujet de cette mémoire

Aussi, nous prévoyons continuer à découvrir et à explorer des autres techniques et d'autres protocoles aident trouver une solution parfait.

BIBIOGRAPHIE

[1] A .HANNECHE, Conception d'un nouveau protocole pour les réseaux de capteurs sans fils, mémoire master, Université L'arbi Ben M'hidi Oum El Bouaghi, 2021.

[2] A.BENAHMED DAHO, Détection préventive de pannes guidée par les données dans les réseaux de capteurs sans fil, mémoire master, Université Abou Bakr Belkaid– Tlemcen Faculté des Sciences,2014.

[3] A.TOKE , PROF.HASHMI S.A, A Data Centric in Drina: Network Aggregation in Wireless Sensor Networks, International Journal of Wireless Communications and Networking Technologies, Volume 4, No.3, April - May 2015,pp.57-62.

[4] B. KECHAR, Problématique de la consommation d'énergie dans les réseaux de capteurs sans fil, thèse doctorat, université d'oran,2010.

[5] C. Gherbi, Algorithme de routage pour les réseaux de capteurs avec prise en charge de la consommation d'énergie, these doctorat, UNIVERSITE LARBI BEN M'HIDI OUM EL BOUAGHI, 2017.

[6] D. Hamdan, Detection et diagnostic des fautes dans des systemes a base de reseaux de capteurs sansfil, these doctorat, Universite de Grenoble, 2013.

[7] H. GHRIBI, Traitement de pannes isolées dans les réseaux de capteurs et de robots sans fil(WSRN), mémoire magistère, USTHB, 2015.

[8] J. CUI, Data aggregation in Wireless Sensor Networks,these doctorat, INSA de Lyon,2016

[9] K. CHEMOUN, Proposition et implémentation d'un protocole d'agrégation de données basé sur l'approche de clustering dans les RCSFs, mémoire master2, Université Mouloud Mammeri de Tizi-Ouzou,2013.

[10] L.Villas, Azzedine Boukerche,HeitorS.Ramos, Horacio A. B. F. de Oliveira,Regina B. de Araujo and Antonio A. F. Loureiro, DRINA: A Lightweight and Reliable Routing Approach for in-Network Aggregation in Wireless Sensor Networks, IEEE TRANSACTIONS ON COMPUTERS,2012,pp.1-14

[11] M . GAYE ,Etat de l'art sur les WSN Wireless Sensor Network,Universite Cheikh Anta DIOP de Dakar,juin 2014.

[12] M. Bouallegue , Protocoles de communication et optimisation de l'énergie dans les réseaux de capteurs sans fil, these doctorat, Université du Maine,2016 .

[13] M.BEKKAR, Née DJABER Dehbia, Stratégie de tolérance aux pannes dans les RCSF, mémoire master2, Université Mouloud Mammeri de Tizi-Ouzou, 2015.

[14] M.Kaur, Bhupinder Kaur, Review Paper on DRINA Protocol, Vol. 4, Issue 9, September 2015,pp.239-242.

[15] N.Ould Mohamedi, Tolérance aux pannes d'une station de base (SINK) dans un réseau de capteurs sans fil, mémoire magister, UNIVERSITE FERHAT ABBAS – SETIF UFAS (ALGERIE),

[16] S. Meenakshi Sundaram, Shilpa S G, Data Aggregation Techniques Over Wireless Sensor Network- A Review, International Journal of Engineering Research & Technology (IJERT), Volume 5, Issue 22, 2017,pp .1-6.

[17] S.Belkheyr, La Géo-localisation dans les Réseaux de Capteurs sans Fil, Université Abou Bakr Belkaid– Tlemcen,2011.

[18] S.LAHLOUH, OMOURI Sarah, L'agrégation de données dans un réseau de capteurs sans fil, Université Mouloud Mammeri de Tizi-Ouzou, mémoire master,2011.

[19] Y. Djebaili, UN PROTOCOLE DE ROUTAGE TOLERANT AUX PANNES POUR LES RCSF, these doctorat, Université de Batna 2 Faculté de Mathématiques et D'Informatique, 2018.

ملخص

سيتم نشر شبكات الاستشعار اللاسلكية الكثيفة واسعة النطاق (WSN) بشكل متزايد في فئات مختلفة من التطبيقات من أجل المراقبة الدقيقة. يعد فشل جهاز استشعار أو أكثر مشكلة تقلل من جودة خدمة شبكة المستشعرات اللاسلكية ، ومعالجة وكشف الأعطال اللازمة لاستمرارية وظائف الشبكة اللاسلكية ، وذلك بسبب الكثافة العالية للعقد في هذه الشبكات ، من المحتمل أن يتم الكشف عن البيانات الزائدة عن طريق العقد القريبة عند اكتشاف حدث (فشل جهاز الاستشعار). نظرًا لأن الحفاظ على الطاقة يمثل مشكلة رئيسية في شبكات WSN ، يجب استغلال دمج البيانات وتجميعها من أجل توفير الطاقة. في هذه الحالة ، يمكن تجميع البيانات الزائدة عن الحاجة في العقد الوسيطة لتقليل حجم وعدد الرسائل المتبادلة ، وبالتالي تقليل تكاليف الاتصال واستهلاك الطاقة. في هذا العمل ، نقترح توجيه بيانات جديدًا لتجميع الشبكة ، يسمى DRINA ، لمحاولة تقليل عدد الرسائل (تقارير الفشل).

الكلمات الرئيسية: شبكات الاستشعار اللاسلكية (RCSF) ، التوجيه ، معالجة الأخطاء ، إدارة الطاقة ، التكرار ، تجميع الشبكة، DRINA

Abstract

Large-scale dense wireless sensor networks (WSN) will increasingly be deployed in different classes of applications for accurate monitoring. the failure of one or more sensors is a problem that decreases the quality of service of the wireless sensor network, the processing and detection of failures necessary for the continuity of the functionality of the wireless network, Due to the high density of nodes in these networks, it is likely that redundant data will be detected by nearby nodes upon detection of an event (a sensor fails). Since energy conservation is a key issue in WSNs, data fusion and aggregation should be exploited in order to save energy. In this case, redundant data can be aggregated at intermediate nodes reducing the size and the number of messages exchanged and, thus, reducing communication costs and energy consumption. In this work, we propose a new data routing for network aggregation, called DRINA, to try to minimize the number of messages (failure reports) .

Keywords: wireless sensor networks (RCSF), routing, fault processing, energy management, redundancy, network aggregation, DRINA.

Résume

Les réseaux de capteurs sans fil denses à grande échelle (WSN) seront de plus en plus déployés dans différentes classes d'applications pour une surveillance précise. la panne d'un ou plusieurs capteurs est un problème qui diminue la qualité de service de réseau de capteur sans fils ,la traitement et détection des pannes nécessaire pour continuité la fonctionnalité de réseau sans fils , En raison de la forte densité de nœuds dans ces réseaux, il est probable que des données redondantes seront détectées par des nœuds proches lors de la détection d'un événement(un capteur tombe en panne). Étant donné que la conservation de l'énergie est un problème clé dans les WSN, la fusion et l'agrégation de données doivent être exploitées afin d'économiser de l'énergie. Dans ce cas, des données redondantes peuvent être agrégées au niveau de nœuds intermédiaires réduisant la taille et le nombre de messages échangés et, ainsi, diminuant les coûts de communication et la consommation d'énergie. Dans ce travail, nous proposons un nouveau routage de données pour l'agrégation en réseau, appelé DRINA, esseyer minimiser le nombre de messages (rapports d'échecs).

Mot clés : réseaux de capteurs sans fil (RCSF), routage, traitement de panne, gestion d'énergie, redondance, agrégation en réseaux, DRINA.