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

UNIVERSITE ABOU-BEKR BELKAID - TLEMCEN

Laboratoire STIC

THÈSE

Présentée à :

FACULTE DES SCIENCES – DEPARTEMENT D'INFORMATIQUE

Pour l'obtention du diplôme de :

DOCTORAT EN SCIENCES

Spécialité : Informatique

Par :

Melle BELKADI KHADIDJA

Sur le thème

Un routage tolérant aux pannes économe en énergie à aspects préventif et curatif pour les réseaux de capteurs sans fil

---

Soutenue publiquement le 18 Septembre 2023 à Tlemcen devant le jury composé de :

Mr BENMAMMAR Badr	Professeur	Université de Tlemcen	Président
Mr LEHSAINI Mohamed	Professeur	Université de Tlemcen	Directeur de thèse
Mr BOUKLI HACENE Sofiane	Professeur	Université de Sidi Bel Abbes	Examinateur
Mr MERAD BOUDIA Omar Rafik	Maître de Conférences A	Université d'Oran 1	Examinateur
Mr DENNOUNI Nassim	Maître de Conférences A	Ecole Supérieure de Management Tlemcen	Examinateur
Mr HADJILA Mourad	Maître de Conférences A	Université de Tlemcen	Examinateur

Laboratoire Systèmes et Technologies de l'Information et de la Communication.
BP 119, 13000 Tlemcen - Algérie

Remerciements

Je tiens à remercier ALLAH TOUT PUISSANT de m'avoir donnée la force, le courage, la patience pour réaliser cette thèse.

Je tiens particulièrement à exprimer ma profonde gratitude à mon directeur de thèse, Mr LEHSAINI Mohamed, Professeur au département d'Informatique à l'université Abou Bekr Belkaid de Tlemcen pour son professionnalisme, sa générosité scientifique, sa disponibilité,sa ponctualité, ses remarques et conseils brefs et pertinents et ses efforts fournis qui m'ont permis de mener à bien ce travail de thèse .

Mes remerciements les plus sincères sont adressés au Professeur BENMAMMAR Badr de me faire l'honneur de s'intéresser à ce travail et d'avoir présidé le jury.

J'adresse tous mes remerciements à Mr BOUKLI HACENE Sofiane, Mr DENNOUNI Nassim, Mr MERAD BOUDIA Omar Rafik et Mr HADJILA Mourad qui m'ont fait l'honneur d'accepter d'être les rapporteurs de cette thèse.

Ce travail a été réalisé au sein du laboratoire Systèmes et Technologies de l'Information et de la Communication (STIC) de l'université de Tlemcen. Je tiens à remercier les membres de ce laboratoire et en tout premier lieu les responsables du laboratoire, le directeur Mr LEHSAINI, Mr FEHAM de m'avoir accueilli au sein de ce laboratoire. Á la secrétaire du laboratoire Madame Morso Nouria pour sa disponibilité et son aide. Enfin, à tout le personnel du laboratoire en souhaitant l'épanouissement de leurs recherches.

J'adresse mes remerciements : à mes parents qui m'ont fait croire arriver à ce que je réalise depuis toujours et qui n'ont jamais délaissé de m'encourager pour arriver à ce travail .

A mon très cher frère Bekhedda pour son encouragement, son soutien.

A mes très chères frères et soeurs .

A toute personne qui m'a aidé à réaliser ce travail d'une manière ou autre.

" le plus sûr avantage de la recherche schientifique , c'est le progrès du chercheur "

Dédicace

Je dédie ce travail À :

Ma force dans les moments de faiblesse ... à mon père .
La personne qui illumine ma vie par le Douâa ... à ma mère
Mes frères , mes soeurs , mes nieces et mes neveux .

Khadidja

Table des matières

Liste des figures

Liste des tableaux

Glossaire

Glossaire

3C-CNP Component-Cardinality-Constrained Critical Node Problem. 52

ACO Ant Colony Optimization. 26

ADC Analog to Digital Converter. 11

AODV Ad-hoc On-demand Distance Vector. 2

ASNs Alternatif Sensor Nodes. 29

BMR Block Movement Recovery. 39

CDS Connected Dominating Set. 41

CFTM Centralized Fault Tolerant Mechanism. 40

CH Cluster Head. 3

CIVA Centralized Immune-Voronoi deployment Algorithm. 32

CNDP Critical node detection problem. 52

CNP Critical Node Problem. 2

CSA-MGR Carrier Sense Aware Multipath Geographic Routing protocol. 74

DA Dragon fly. 74

DCR Distributed partitioning detection and Connectivity Restoration algorithm. 40

DD Directed Diffusion. 29

DECROP Distributed and Effective Cluster Routing Protocol. 29

DMRF Dynamical jumping real-time fault-tolerant routing protocol. 72

DSHA Distributed Self-Healing Approach. 38

DSP Dual Separate Paths. 28

DURA Distributed Underwater Recovery Algorithm. 39

EADC Energy-Aware Clustering Algorithm. 3

EADUC An energy-aware distributed unequal clustering protocol. 76

ECSOM Energy Clustering based on Self-Organizing Map. 74

EE-FT Energy-Efficient cluster-based Fault-Tolerant routing protocol for WSNs. 3

EE-FTR Energy-Efficient Fault-Tolerant Routing protocol for WSNs. 3

EFT-PMD Efficient Fault Tolerance Path graph flow Modelling with Marchenko–Pastur Distribution algorithm. 3

FCGW Fault-tolerant Clustering routing protocol based on Gaussian network for Wireless sensor network. 27

FD-AOMDV Fault-Tolerant Disjoint Multipath Distance Vector Routing Algorithm. 71

FF Firefly algorithm. 74

FMS Fault tolerant multilevel routing protocol with sleep scheduling. 71

FPU-DA FF replaced position update in DA. 74

GA-CNP Genetic Algorithm-Critical Node Problem. 2

GAs Genetic Algorithms. 2

GMFT Geographic Multipath routing protocol reinforced by Fault-Tolerant mechanism. 37

GPS Global Positioning System. 11

GSA-SSD Gravitational Search Algorithm with Social Ski-Driver. 30

GSTEB General Self-organizing Tree-based Energy Balance. 26

GWO Grey Wolf Optimizer. 26

HEED Hybrid Energy Efficient Distributed. 26

HSNs Homogeneous Sensor Nodes. 31

HSR High Availability Seamless Redundancy. 28

IACOSC Improved Ant Colony Optimization-based Sweep Coverage. 32

IEEMARP Improvised Energy Efficient Multipath ACO based Routing Protocol. 27

ILP Integer Linear Programming. 31

INLP Integer NonLinear Programming. 31

IoT Internet of Things. 46

LEACH Low-energy adaptive hiérarchie de clustering. 26

LeDiR Least-Disruptive topology Repair. 41

LP Linear Programming. 51

MIP Mixed-Integer Programming. 51

MRMS Multipath Routing in large scale sensor networks with Multiple Sink nodes. 29

MSN Mobile Sensor Nodes. 32

MWSNs Multimedia Wireless Sensor Networks. 32

NSGA-II Non-dominated Sorting GA. 31

PSO Particle Swarm Optimization. 26

QoS Qualité of Service. 28

RCSF Réseau de Capteurs Sans Fil. 1

RCSFs Réseaux de Capteurs Sans Fil. 1

REAR Reliable Energy Aware Routing. 28

RNFR Rotating Nodes based Failure Recovery. 39

Introduction Générale

Introduction Générale

Contexte

Les progrès technologiques dans les microsystèmes électromécaniques et les communications sans fil ont conduit à la production de dispositifs miniaturisés et moins coûteux appelés "noeuds capteurs" ou "motes", qui peuvent communiquer entre eux par ondes radio pour former un Réseau de Capteurs Sans Fil (RCSF).

Un RCSF se compose généralement d'un grand nombre de noeuds capteurs à faible coût, à faible puissance et alimentés par des batteries. Comme les noeuds de capteurs disposent de ressources énergétiques limitées et non rechargeables, l'énergie est considérée comme une ressource très précieuse dans ce type de réseaux. A cette fin, la consommation d'énergie doit être soigneusement gérée afin de prolonger la durée de vie des réseaux de capteurs.

Un RCSF est vu également comme une infrastructure composée de dispositifs de détection, de calcul et de communication qui permet à un centre de contrôle distant d'observer et de réagir à des événements et des phénomènes dans un environnement donné. Le centre de contrôle est généralement une organisation civile, gouvernementale, commerciale ou industrielle. L'environnement peut être le monde physique, un système biologique ou un cadre informatique. Les Réseaux de Capteurs Sans Fil (RCSFs) ont été largement déployés ces dernières années dans plusieurs domaines d'applications à savoir le domaine militaire, le domaine médical, le domaine environnemental, ..ect. Dans les RCSFs, outre la détection, on s'intéresse souvent au contrôle et à l'activation à l'aide d'actionneurs.

Dans les RCSFs, les noeuds capteurs permettent de capter les informations, de les traiter et de les transmettre à un centre de contrôle distant grâce à leurs composants : le microprocesseur, les capteurs, la mémoire, et l'unité de communication. Cependant, ces noeuds capteurs sont considérés comme des dispositifs fragiles et vulnérables aux pannes ; premièrement à cause de leur nature limitée en énergie du batterie qui est généralement non rechargeable et aussi de la nature des environnements hostiles dans lesquelles sont déployés. Ainsi, en assurant le fonctionnement des noeuds capteurs, ça nous permet de garantir le fonctionnement de l'ensemble du réseau. A cet effet, l'utilisation d'un mécanisme de tolérance aux pannes des noeuds capteurs s'avère indispensable. Dans ce contexte, plusieurs travaux ont été proposés dans la littérature pour surmonter le problème de l'épuisement de l'énergie de la batterie en un temps très court et des défaillances des noeuds capteurs dues à des événements naturels. Néanmoins, la majorité de ces propositions ne tiennent pas compte de l'importance des noeuds capteurs, ou bien elles utilisent des méthodes de détection des noeuds critiques, généralement basées sur des sommets coupés qui ne fragmentent pas réellement le réseau. En outre, les solutions proposées ne prennent pas non plus en compte les exigences des applications des RCSFs en termes de

manque de vue d'ensemble sur le réseau. Dans cette optique, nos travaux de recherche dans le cadre de cette thèse de doctorat proposent de nouvelles contributions qui prennent en considération les limites déjà citées. Ces contributions consistent en des protocoles de routage tolérants aux pannes à aspect préventif et curatif et se basent sur le concept de problème des noeuds critiques. Dans ces contributions, nous avons fait appel à l'approche de clustering qui est considérée comme une approche efficace en termes de consommation d'énergie dans les RCSFs. La valeur ajoutée de cette approche est d'assurer une longue durée de vie aux noeuds capteurs puisque l'épuisement de l'énergie est considéré comme la première cause de panne dans les RCSFs.

Motivations de recherche

Le but de cette thèse consiste à proposer des contributions à la résolution du problème de tolérance aux pannes dans les RCSFs. Il s'agira de suggérer des schémas de routage tolérants aux pannes pour les RCSFs. Ces schémas de routage doivent traiter l'aspect préventif et curatif de la tolérance aux pannes. Les objectifs spécifiques de cette thèse se résument à :

- Mener une recherche bibliographique sur les protocoles de routage tolérants aux pannes conçus pour les RCSFs et discuter de leurs performances et de leurs limitations.
- Proposer sur la base de cet état de l'art de nouveaux schémas de routage tolérants aux pannes, efficaces et économes en énergie pour les RCSFs.
- Évaluer nos propositions analytiquement et par des simulations et situer nos solutions par rapport aux solutions existantes dans la littérature.

Contributions

Pour atteindre nos objectifs de recherche, nous avons proposé trois contributions :

- Notre première contribution est une approche de tolérance aux pannes basée sur le problème des noeuds critiques (Critical Node Problem (CNP)) et les algorithmes génétiques (Genetic Algorithms (GAs)), appelée "Genetic Algorithm-Critical Node Problem (GA-CNP)" [5]. Dans cette contribution, nous avons proposé une nouvelle approche pour la tolérance aux pannes dans les RCSFs. Notre approche se compose de deux phases. La première phase sélectionne les noeuds critiques dans le réseau dont la défaillance pourra entraîner une dégradation significative des performances du réseau. La deuxième phase consiste à appliquer une méthode d'augmentation pour maintenir la connectivité du réseau en cas de défaillance d'un noeud critique.

  Les résultats de simulations ont montré que l'approche proposée GA-CNP permet de sélectionner les noeuds critiques dont la défaillance peut dégrader la durée de vie du réseau avec une grande efficacité. De plus, l'approche Aug-CNP appliquée au protocole "Ad-hoc On-demand Distance Vector (AODV)" apporte des améliorations en termes de durée de vie du réseau par rapport au protocole AODV traditionnel.

- La deuxième contribution consiste en un protocole de routage tolérant aux pannes à haut rendement énergétique, basé sur la méthode de clustering utilisée dans le protocole "Energy-Aware Clustering Algorithm (EADC)" [6], appelé "Energy-Efficient cluster-based Fault-Tolerant routing protocol for WSNs (EE-FT)" [7]. EE-FT permet à couvrir les défaillances avant qu'elles ne se produisent i.e. la tolérance aux pannes est à aspect préventif. Il choisit les chemins fiables les plus courts pour le routage des données à la station de base en utilisant la loi de Bernoulli pour la sélection des noeuds fiables. En outre, dans EE-FT, les chemins établis sont formés par les CHs qui ont plus d'énergie. Dans le protocole EE-FT, nous visons à améliorer l'équilibrage de charge entre les noeuds CHs où il serait plus approprié d'avoir des clusters qui ont à peu près la même taille, ce qui aurait pour effet de homogénéiser le nombre de tâches réalisées par les différents noeuds CHs. Cela permet donc d'avoir quasiment le même taux de perte d'énergie au niveau des clusters. Ainsi, la durée de vie globale du réseau sera maximisée et le risque de perdre des parties du réseau avant d'autres sera grandement minimisé. De plus, dans notre contribution nous ajoutons une phase de réaffiliation à la méthode de clustering proposée dans EADC pour éviter d'avoir des clusters avec un très petit nombre des membres.

  Nous avons évalué et comparé les performances du protocole EE-FT à celles du protocole "Efficient Fault Tolerance Path graph flow Modelling with Marchenko–Pastur Distribution algorithm (EFT-PMD)" [8] et au protocole EADC [6] en termes de délai moyen de livraison de paquets, de taux de livraison des données, d'énergie dissipée et de durée de vie du réseau.

- La troisième contribution est un protocole de routage tolérant aux pannes basé sur la méthode de clustering utilisée dans le protocole EADC et sur un protocole de routage proactif, appelé "Energy-Efficient Fault-Tolerant Routing protocol for WSNs (EE-FTR)" [9]. Le protocole proposé vise à tolérer les défaillances en remplaçant le "Cluster Head (CH)" principal défaillant par un autre CH appelé CH assistant. Il est également basé sur l'optimisation de la consommation d'énergie, ce qui améliore la tolérance aux pannes dans les RCSFs. Nous avons évalué et comparé les performances de cette contribution à celles du protocole EFT-PMD en termes de délai de livraison moyen, de débit de livraison des données, de l'énergie dissipée et de durée de vie du réseau.

Organisation de la thèse

Le manuscrit de la thèse est structuré en quatre chapitres encadrés par une introduction et une conclusion :

- Dans le premier chapitre, nous donnons dans la première partie de ce chapitre un aperçu général sur les réseaux de capteurs sans fil, leurs caractéristiques spécifiques, leurs types d'application, leurs défis et d'autres considérations pratiques. Dans la deuxième partie de ce chapitre, nous allons voir quelques notions fondamentales de la tolérance aux pannes dans les RCSFs : définition de tolérance aux pannes, les types de pannes, la procédure de tolérance aux pannes.

- Le deuxième chapitre est un état de l'art sur les protocoles de routage tolérants aux pannes dans les RCSFs. Dans la première partie de ce chapitre nous classifions les protocoles du routage selon les mécanismes de tolérance aux pannes et aussi selon l'importance des noeuds capteurs. Dans la deuxième partie, nous énumérons quelques protocoles proposés dans la littérature en basant sur le mécanisme de classification temporelle proposée dans la première partie de ce chapitre.

- Le troisième chapitre présente notre première contribution, qui consiste en une approche de tolérance aux pannes basée sur l'augmentation dans les RCSFs. Dans un premier temps, nous présentons quelques notions de base en théorie des graphes. Ensuite, un état de l'art sur les propositions pour la détection des nœuds critiques dans les RCSFs est présenté selon les paramètres de performance et des paramètres structurels des graphes comme il est d'usage dans la littérature. Puis, nous proposons notre contribution qui est une solution hybride : la première proposition vise à détecter les noeuds critiques et la deuxième a comme objectif d'augmenter le réseau pour pallier le problème de détection des noeuds critiques. Nous terminons ce chapitre par une évaluation des performances de notre contribution et une comparison de ces performances à d'autres protocoles présentés dans la literature.

- Le quatrième chapitre consiste en deux contributions. La première contribution présentée dans ce chapitre consiste en un protocole de routage tolérant aux pannes à aspect préventif et économe en énergie, basé sur la méthode de clustering utilisée dans le protocole EADC et la loi de Bernoulli pour la sélection de noeuds fiables dans le processus de routage. La deuxième contribution consiste en un protocole de routage tolérant aux pannes à aspect curatif qui est basé sur une architecture clusterisée dans laquelle les clusters contiennent deux noeuds CHs : un CH principal et un CH assistant. Dans cette contribution, le protocole proposé sélectionne le chemin le plus court en basant sur l'énergie et le nombre du sauts. Enfin, nous présentons les performances de chacune des contributions et leurs atouts par rapport à d'autres travaux existants.

Finalement, nous clôturons ce manuscrit par une conclusion générale qui résume nos contributions proposées tout au long de ce travail de thèse et leurs perspectives.

Chapitre 1

Généralités et tolérance aux pannes dans les RCSFs

Chapitre 1

Généralités et tolérance aux pannes dans les RCSFs

1.1 Introduction

Les réseaux de capteurs sans fil sont largement répandus où leur utilisation est généralisée dans différents domaines grâce à la variété de leurs applications.

Un réseau de capteurs sans fil est composé d'un ensemble de noeuds capteurs qui communiquent entre eux via une liaison sans fil. Ces noeuds capteurs surveillent, détectent et transmettent les données correspondantes à des phénomènes pertinents dans une zone d'intérêt à un point de collecte distant appelé station de base. Les noeuds capteurs composant un RCSF sont des dispositifs fragiles, dotés d'une batterie limitée en énergie qui est généralement non rechargeable. Par ailleurs, les caractéristiques des noeuds capteurs ainsi que les environnements hostiles dans lesquels sont déployés les rendent vulnérables aux pannes qui peuvent être causées notamment par l'épuisement d'énergie et les phénomènes naturelles. Ces pannes peuvent mener à l'arrêt total du système.

Dans ce chapitre, nous présentons les caractéristiques et les contraintes sous-jacentes aux RCSFs, en commençant par un rappel sur les terminologies de type de réseaux telles la notion de noeud capteur, de RCSF, leurs spécificités et leurs domaines d'application. Puis, nous présentons la tolérance aux pannes dans les réseaux de capteurs et les différentes causes de pannes qui peuvent perturber le fonctionnement d'un RCSF.

1.2 Les Réseaux de capteurs sans fil (RCSFs)

Un réseau de capteurs sans fil (RCSF) est un réseau ad hoc composé d'un grand nombre de noeuds capteurs déployés d'une façon aléatoire ou prédéfinie dans un espace géographique où chaque noeud peut collecter, traiter et transmettre les données d'une façon autonome. La figure 1.1 illustre un exemple de réseaux capteurs sans fil.

1.2.1 Anatomie d'un noeud capteur

Un noeud capteur comme le montre la figure 1.2 est un dispositif autonome, de taille réduite, limité en terme d'énergie, de mémoire et de calcul, capable de détecter, traiter et

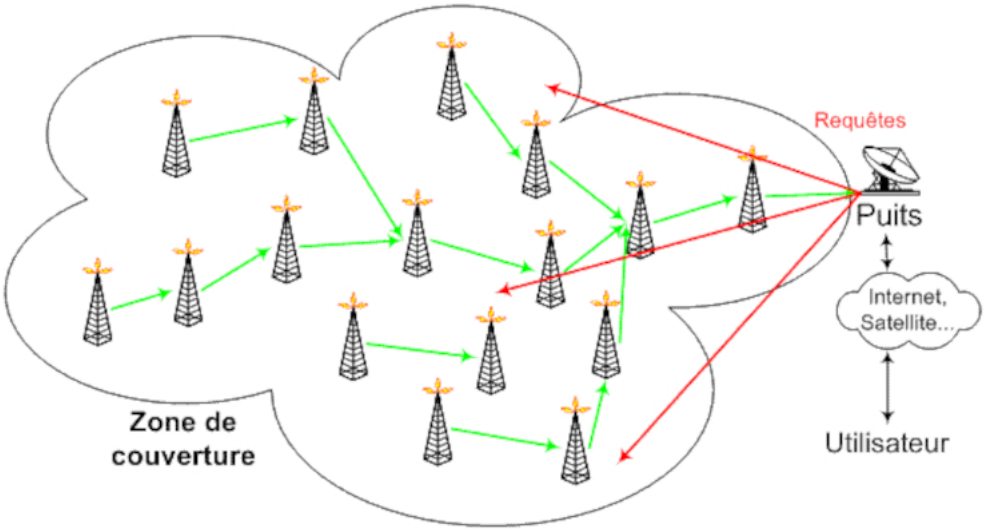


FIGURE 1.1 – Exemple de RCSFs [1]

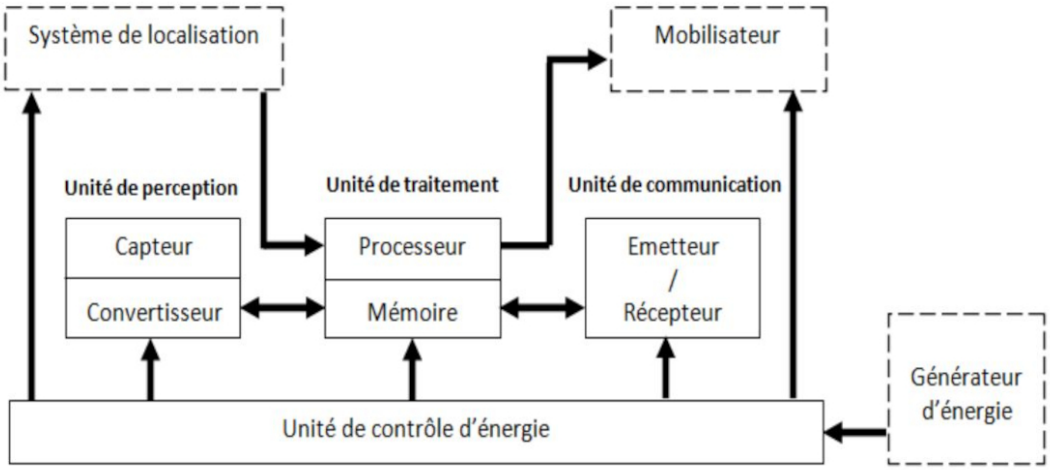


FIGURE 1.2 – Anatomie approchée d'un noeud capteur [2]

transmettre les données à un autre composant (capteur, unité de traitement, station de base ...).

Il existe plusieurs modèles de noeuds capteurs selon leurs domaines d'application, mais ces différents noeuds sont principalement composés d'unités de captage, de traitement, de stockage, de communication et d'énergie comme le montre la figure 1.2.

- Unité de traitement (Processeur) : L'unité de traitement dans un noeud capteur joue le rôle du contrôleur où elle envoie les données acquises par l'unité d'acquisition à l'unité de communication. Cette unité peut traiter les données et les agréger pour optimiser la consommation d'énergie.

- Unité du stockage (Mémoire) : L'unité de traitement utilise deux mémoires : mémoire de programme pour la sauvegarde des instructions exécutées par le processeur et la mémoire de données pour sauvegarder les données locales et celles requises de

l'unité d'acquisition.

- Unité de communication : L'unité de communication est responsable sur les émissions et les réceptions des données entre les noeuds capteurs via le support radio.
- Unité d'énergie (Batterie) : Un noeud capteur est doté d'une batterie comme source d'énergie qui est généralement non rechargeable ce qui rend l'optimisation de sa consommation une opération importante pour améliorer sa durée de vie et la durée de vie de tout le réseau. La consommation d'énergie est un enjeu primordial qui doit être pris en compte dans toutes les applications des RCSFs en raison des contraintes énergétiques des noeuds capteurs. Pour remédier au problème d'énergie, des efforts ont été déployés pour réaliser une unité d'alimentation électrique avec des panneaux solaires [10,11]. Néanmoins, le problème de l'économie d'énergie persiste, car il n'est pas toujours possible d'obtenir de l'énergie solaire par exemple dans les pays là où il y a moins de soleil durant l'année. C'est pourquoi, dans presque tous les travaux de recherche, la problématique concernée telle que la tolérance aux pannes dans les RCSFs est traitée conjointement avec celle de la consommation d'énergie.

De plus, selon les applications pour lesquelles les RCSFs sont élaborés, les noeuds capteurs peuvent également avoir besoin d'autres modules, comme une unité de localisation, pour identifier leur position géographique, ou un mobilisateur pour qu'ils puissent se déplacer [2]. Certaines applications peuvent également nécessiter des noeuds capteurs avec une mémoire externe pour stocker une grande quantité de données.

1.2.2 Caractéristiques d'un noeud capteur

Les noeuds capteurs ont des caractéristiques spécifiques, dont nous présentons les plus essentielles dans ce qui suit :

- **Énergie** : L'énergie est la contrainte la plus essentielle dans la plupart des applications des RCSFs vu que chaque noeud est équipé d'une batterie qui n'est généralement ni rechargeable ni remplaçable surtout lorsque le noeud capteur est déployé dans une zone hostile. Par conséquent, toute application conçue pour fonctionner sur un noeud capteur doit prendre en considération la contrainte énergétique pour qu'elle soit exploitée pour une longue durée. Ainsi, pour économiser l'énergie d'un noeud capteur, ce dernier ne doit passer en mode actif que lorsqu'il a des données à transmettre ou à recevoir et éviter les transmissions et réceptions redondantes. En outre, les communications dans les RCSFs sont les opérations les plus énergivores [12].
- **Portée de transmission** : La portée de transmission des nœuds de capteurs est liée à cinq paramètres : la puissance de transmission des paquets de données, la fréquence, la modulation, l'emplacement et les conditions météorologiques [13]. Elle peut aller de quelques mètres à des centaines de mètres. Par exemple, la portée de transmission de TelosB est de 75 à 100 mètres en extérieur (outdoor) et de 20 à 30 mètres en intérieur (indoor). Par conséquent, en fonction du déploiement des noeuds capteurs, ceux-ci ne seront pas toujours à portée radio de la station de base. Ils doivent donc coopérer les uns avec les autres pour acheminer les données collectées vers la station de base.

- **Puissance de calcul** : En raison de la taille réduite des noeuds capteurs, des microcontrôleurs sont généralement utilisés comme unité de calcul pour les noeuds capteurs. Par exemple, la plateforme TelosB de Crossbow est dotée d'un microcontrôleur MSP430 dont la puissance de calcul est 8 MHz. De ce fait, il est recommandé de concevoir des algorithmes legers en termes de calcul pour les RCSFs.
- **Capacité de stockage** : La capacité de stockage des microcontrôleurs est souvent limitée (elle peut aller de quelques koctets à des méga-octets de mètres) alors que les noeuds capteurs sont chargés d'effectuer plusieurs tâches telles que l'agrégation, la compression et parfois même des calculs très complexes comme dans le cas des applications de sécurité. Pour surmonter cette limitation, les noeuds capteurs doivent collaborer les uns avec les autres pour réaliser un objectif commun.

1.2.3 Architecture des RCSFs

Comme les RCSFs se caractérisent par l'absence d'une infrastructure prédéterminée, les noeuds apteurs coopèrent entre eux pour l'établir. De plus, les noeuds capteurs, comme tout autre composant de télécommunications, obéissent à une architecture protocolaire spécifique. Néanmoins, la mise en oeuvre de cette dernière doit tenir compte de la sévérité des contraintes dues aux limitations des ressources physiques des RCSFs. Par conséquent, la conception des protocoles de communication doit être réalisée de manière optimale.

a) Architecture de communication

Une fois les noeuds capteurs déployés dans une certaine zone d'intérêt, ils commencent par découvrir leurs voisins afin d'établir la topologie de communication. De cette façon, ils deviennent capables d'exécuter les tâches qui leur sont assignées. Dans un schéma de communication multi-sauts, les noeuds capteurs sont chargés de collecter des données, et de les acheminer vers la station de base qui à son tour, analyse ces données et les transmet à un centre de contrôle via Internet ou un satellite. Dans cette architecture, le RCSF est considéré comme un réseau d'acquisition de données, tandis que le réseau de distribution de données est composé des utilisateurs et du réseau de communication : Internet et les satellites.

b) Architecture protocolaire

Les techniques traditionnelles et les couches protocolaires utilisées dans les reseaux ad hoc ne répondent pas aux besoins des RCSFs vu qu'ils ne prennent pas en considération les spécificités des RCSFs notamment les limitations d'énergie et de mémoire des noeuds capteurs. Dans ce cadre, un standard de communication compatible avec les spécificités logicielles et matérielles des RCSFs est utilisé pour améliorer l'efficacité de ce type de réseaux.

Cette pile possède cinq (05) couches qui sont : la couche application, la couche transport, la couche réseau, la couche liaison de données et la couche physique, et trois (03) niveaux de gestion qui sont : le niveau de la gestion d'énergie, le niveau de la gestion des tâches et le niveau de la gestion de mobilité.

- **La couche application** : Elle assure l'interface avec les applications.

- **La couche transport** : Cette couche est chargée du transport des données, de leur découpage en paquets, du contrôle de flux, de la conservation de l'ordre des paquets et de la gestion des éventuelles erreurs de transmission.
- **La couche réseau** : La couche réseau est responsable de l'acheminement des données captées par les noeuds capteurs vers la station de base en optimisant la gestion soigneuse des ressources. Dans cette optique, plusieurs travaux ont été proposés dans la littérature pour améliorer le routage dans les RCSFs.
- **La couche liaison** : Cette couche définit l'échange des données entre les composants du réseau, le multiplexage des données, le contrôle d'erreurs, et l'accès au medium.
- **La couche physique** : Elle représente les caractéristiques matérielles, les fréquences porteuses, etc...
- **Plans de gestion** : Les plans de gestion d'énergie comme leur nom l'indique ont pour rôle de bien gérer le réseau en terme d'énergie, mobilité et distribution des tâches, ce qui permet à optimiser la consommation d'énergie dans le réseau, de garder la connectivité et organiser la collaboration dans la détection d'évènement entre les noeuds capteurs.
- **Plan de gestion d'énergie** : Il est responsable de la gestion d'énergie du noeud capteur (la batterie), par la gestion du récepteur où le noeud capteur éteint le récepteur pour éviter la duplication dans la réception des messages. Lors de l'extinction de la batterie par le noeud capteur, ce dernier prévient ses voisins qu'il ne participera pas dans le processus de routage de données à la station de base.
- **Plan de gestion de mobilité** : La possibilité de détecter le mouvement des noeuds capteurs voisins par un noeud capteur, cela permet à preserver la connectivité du réseau et optimiser la consommation d'énergie.
- **Plan de gestion de tâches** : La gestion des tâches de détection des noeuds capteurs où un noeud capteur peut avoir plus de tâches par rapport un autre noeud capteur dans une région bien précise selon son énergie.

1.2.4 Topologie des RCSFs

La topologie détermine l'organisation des noeuds capteurs dans une zone où les noeuds situés dans la même zone de couverture peuvent se communiquer entre eux. Les noeuds capteurs sont reliés avec une ou plusieurs stations de base qui ont comme objectif de récupérer les données détectées par les noeuds capteurs. Les principales topologies dans les protocoles de routage conçus pour les RCSFs sont :

a) Topologie plate

Dans cette topologie, tous les noeuds capteurs sont identiques en termes de fonctions à exécuter et de ressources. Ils peuvent transmettre les données vers la station de base selon deux schémas de transmission : mono-saut ou multi-sauts. Dans le schéma de transmission

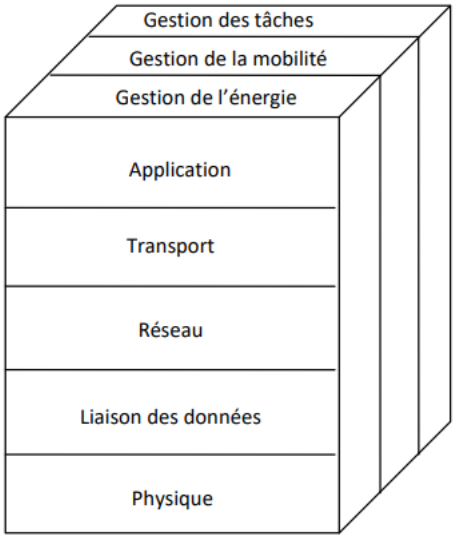


FIGURE 1.3 – Pile protocolaire [3]

mono-saut, tous les noeuds capteurs transmettent leurs données collectées directement à la station de base en utilisant une puissance de transmission élevée, ce qui peut entraîner un épuisement rapide de leurs batteries. En revanche, dans le second schéma de transmission, tous les noeuds capteurs coopèrent les uns avec les autres via un routage multi-sauts dans lequel chaque noeud capteur a le même rôle. Lorsqu'un noeud capteur souhaite communiquer avec une station de base située hors de sa portée de transmission, il fait appel à d'autres noeuds intermédiaires en tant que relais. De plus, lors de la transmission de données via un schéma de communication multi-sauts, d'autres noeuds capteurs participent au processus d'acheminement des données en plus du noeud capteur qui a capturé les données et donc chaque noeud capteur faisant partie du chemin de routage établi consommera une quantité de son énergie pour transférer ces données. Cela rend le passage à l'échelle une opération onéreuse en termes de consommation d'énergie.

La transmission de données dans une topologie plate présente certains avantages tels que l'absence de besoin de maintenir la topologie et fournit des liens de qualité entre les noeuds sources et la station de base. Cependant, la stratégie de cette topologie fait appel à un processus d'inondation pour établir les chemins entre les noeuds sources et la station de base et cette opération est très onéreuse en termes de consommation d'énergie. En outre, elle génère une consommation élevée de la bande passante en raison des messages redondants et une consommation d'énergie non uniforme entre les noeuds capteurs, car il y aura des noeuds capteurs sont sur-utilisés.

b) Topologie hiérarchique

Contrairement à la topologie plate, dans la topologie hiérarchique, les noeuds capteurs n'ont pas les mêmes rôles et peuvent ne pas disposer des mêmes ressources. Ces ressources concernent essentiellement le niveau d'énergie, la capacité de calcul et de stockage. Cette topologie est établie en divisant les noeuds du réseau en plusieurs niveaux. L'une des méthodes les plus utilisées pour la topologie hiérarchique est le clustering où le réseau est partitionné en clusters composés d'un chef du cluster (cluster-head) et ses membres.

Dans une approche hiérarchique, les noeuds capteurs sont regroupés en clusters et, en fonction de certains critères, un chef de cluster est sélectionné, qui sera responsable du routage des données. En outre, dans le rtopologie hiérarchique, une stratégie à deux couches est généralement adoptée, une couche étant chargée de détecter l'environnement physique et l'autre étant dédiée au routage de données vers la station de base. Les noeuds capteurs à faible énergie sont affectés à la détection, tandis que les noeuds capteurs à haute énergie sont souvent employés pour collecter, agréger et transmettre les données.

Dans la littérature, le clustering est utilisé pour optimiser la consommation d'énergie vu sa capacité de minimiser le nombre de noeuds capteurs participants à l'acheminement des données vers les collecteurs des données et de permettre le passage à l'échelle. Le principal inconvénient du clustering est la génération de clusters non uniformes en termes de nombre de membres, qui entraîne une forte dissipation d'énergie des noeuds CHs qui ont un grand nombre de membres, une plus grande consommation d'énergie totale et une connectivité réseau non garantie [14].

c) Topologie basée sur la localisation

Cette topologie est basée sur la localisation où chaque noeud capteur doit connaître la position des noeuds capteurs avec lesquels il échange les informations. La localisation des noeuds capteurs peuvent être réalisée à l'aide d'un système comme le système de positionnement mondial "Global Positioning System (GPS)", ou par le biais des protocoles de localisation moins gourmands en termes de consommation d'énergie.

Les protocoles basés sur la localisation sont nommés des protocoles de routage géographique.

1.2.5 Les différents aspects de conception des RCSFs

La conception des RCSFs doit prendre en considération plusieurs facteurs pour leur assurer un bon fonctionnement et parmi ces facteurs nous présentons les plus essentiels à savoir :

a) Contraintes matérielles et ressource énergétique limitée

Un noeud capteur est un dispositif fragile, vulnérable aux accidents, qui est doté d'une batterie généralement non rechargeable, notamment dans les réseaux à grande échelle et dans les zones de déploiement hostiles à cause de la difficulté de recharger ou de replacer la batterie après l'extinction de son énergie. Plusieurs protocoles de routage ont été conçus pour les RCSFs dans le but est d'optimiser la consommation d'énergie.

En plus des quatre unités qui composent un noeud capteur (unité de détection, unité de traitement, unité d'émetteur-récepteur, et unité d'énergie), ce dernier peut également inclure d'autres composants tels qu'un système de localisation GPS, un générateur d'énergie (cellule solaire) et un mobilisateur. L'unité de est composée de deux sous-unités : des capteurs et des convertisseurs analogique-numérique (Analog to Digital Converter (ADC)). Les signaux analogiques correspondants au phénomène observé sont convertis en signaux numériques par l'ADC, puis envoyés à l'unité de traitement. L'unité de traitement contient généralement une petite unité de stockage. Une unité d'émetteur-récepteur

permet de connecter le noeud capteur au réseau. L'unité d'énergie est l'un des composants les plus importants d'un noeud capteur. Elle peut être supportée par une unité de production d'énergie telle que les cellules solaires. Il existe également d'autres sous-unités, qui dépendent de l'application.

Dans les RCSFs, certains protocoles de routage ont besoin de connaître l'emplacement avec une grande précision pour faciliter l'intervention dans certaines applications. Ainsi, il est courant qu'un noeud capteur possède un système de localisation. En outre, un mobilisateur peut être nécessaire dans certaines applications pour déplacer les noeuds capteurs d'un endroit à un autre. En résumé, un noeud capteur doit répondre aux restrictions suivantes :

- minimiser la consommation d'énergie pour qu'il favorise une longue durée de vie pour le réseau,
- être autonome sans intervention humaine surtout lorsqu'il est déployé dans une zone hostile,
- être adaptatif avec l'environnement dans lequel il est déployé,
- préserver les mêmes capacités même dans les environnements denses.

b) Passage à l'échelle

Les RCSFs ont la possibilité de s'organiser à grande échelle et les protocoles utilisés pour ce type de réseaux doivent s'adapter avec la dimension des réseaux en termes de nombre de noeuds.

Le nombre de noeuds capteurs déployés pour surveiller un phénomène peut aller d'une dizaine à des millions selon l'application, la surface de la zone d'intérêt et le niveau de couverture. Dans les RCSFs, les protocoles doivent pouvoir fonctionner avec un grand nombre de noeuds capteurs et prendre en compte l'aspect haute densité des RCSFs sans dégrader leurs performances. Par exemple, dans les applications de surveillance de l'habitat, le nombre de noeuds capteurs peut varier de 25 à 100 par région [15]. De plus, une maison intelligente peut contenir un grand nombre d'appareils avec des noeuds capteurs et ce nombre peut augmenter si des noeuds capteurs sont intégrés dans des meubles et d'autres produits. La densité sera extrêmement élevée lorsqu'une personne contient des milliers, voire des millions de noeuds capteurs si ceux-ci sont à l'échelle nano comme les noeuds capteurs injectés dans le sang pour détecter certaines maladies à un stade précoce.

c) Consommation d'énergie

Un noeud capteur pourra consommer son énergie généralement dans la réalisation des trois principales opérations : l'acquisition, le traitement et la communication des données.

- **L'énergie d'acquisition** : cette énergie représente un pourcentage minimal de l'énergie totale du noeud capteur où elle est dissipée dans : l'échantillonnage, le traitement de signal, la conversion analogique/numérique et l'activation du capteur.
- **Énergie de traitement** : ce type d'énergie est composé de deux énergies. La première représente l'énergie dissipée dans l'alimentation et la commutation tandis que la deuxième est l'énergie de fuite quand le module ne réalise aucun traitement.

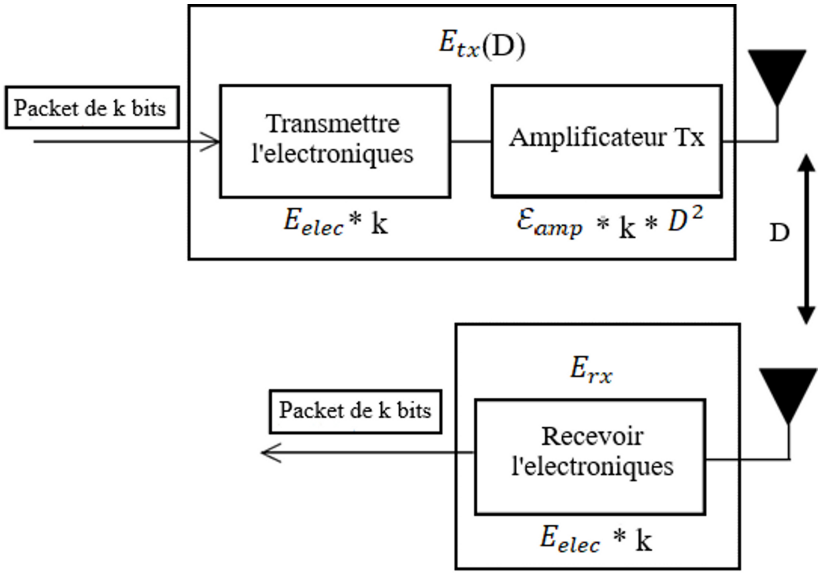


FIGURE 1.4 – Modèle radio de consommation d'énergie [4]

- **Énergie de communication** : Comme son nom l'indique, cette énergie représente l'énergie d'émission et de réception. Elle est définie en termes de quantité des données à échanger et la distance de transmission. Il faut noter que le taux d'énergie consommé est directement proportionnel avec la force du signal et la quantité de données communiquées. Le signal aura une grande portée quand la puissance d'émission est élevée.

La figure1.4 montre le modèle radio de consommation d'énergie le plus connu pour les RCSFs.

Les équations (1.1) et (1.2) représentent l'énergie d'émission $E_{Tx}(n, D)$ et l'énergie de réception des données $E_{Rx}(n)$.

$$E_{Tx}(n, D) = n * (E_{elec} + \epsilon_{amp} * D^2) \tag{1.1}$$

$$E_{Rx}(n) = n * E_{elec} \tag{1.2}$$

où :

- n : La taille du paquet,
- E_{elec} : L'énergie de transmission/réception électronique,
- ϵ_{amp} : L'énergie d'amplification,
- D : La distance entre l'émetteur et le récepteur.

d) La limite en puissance de calcul et en mémoire

Les noeuds capteurs sont limités en puissance de calcul et en mémoire ce qui rend impossible de gérer des algorithmes complexes. Généralement, les algorithmes proposés pour les RCSFs sont simples à être exécuter par un noeud capteur alors que les algorithmes gourmands en terme de puissance de calcul sont exécutés d'une manière centralisée (ils sont exécutés au niveau des stations de base).

e) La tolérance aux pannes

Dans les RCSFs, un noeud capteur peut tomber en panne en n'importe quel moment à cause de différentes raisons, ce qui peut avoir un effet négatif sur les performances du réseau. Pour assurer que le fonctionnement d'un RCSF soit maintenu, des mécanismes de détection et de tolérance aux pannes doivent être fournis pour ce RCSF [16].

La fiabilité d'un noeud capteur utilise la distribution de Poisson pour calculer la probabilité que ce noeud ne tombe pas en panne dans l'intervalle de temps $[0, t]$. Cette probabilité est représentée par l'équation 1.3.

$$R_k(t) = exp(-\lambda_k * t) \tag{1.3}$$

où λ_k est un paramètre qui exprime le taux de défaillance du noeud capteur k et t est la période de temps.

En outre, pendant le déploiement d'un réseau de capteurs ou après son déploiement, certains noeuds capteurs peuvent cesser de fonctionner en raison d'un manque d'énergie, de dommages physiques ou de conditions environnementales. Il faut donc prévoir que la défaillance des noeuds capteurs ne devrait pas affecter la tâche globale du réseau de capteurs mis en oeuvre.

Dans les RCSFs, les protocoles doivent être conçus pour répondre à un niveau satisfaisant de tolérance aux pannes, en particulier dans les applications très sensibles. Par exemple, si les noeuds capteurs sont déployés dans un champ de batailles pour la surveillance et la détection des ennemis, le niveau de tolérance aux pannes doit être élevé car les données détectées sont critiques et les noeuds capteurs peuvent être détruits intentionnellement par les ennemis. Par conséquent, le niveau de tolérance aux pannes doit dépendre de la nature de l'application, et les protocoles doivent tenir compte de ce paramètre dans les applications.

f) Supports de transmission

Dans les RCSFs, les noeuds capteurs communiquent entre eux via un support sans fil. Ainsi, pour favoriser l'"exploitation de ces réseaux, il est judicieux d'utiliser un support de transmission largement utilisé dans différents environnements.

Les liaisons radio dans les RCSFs utilisent des bandes industrielles, scientifiques et médicales (ISM), qui ne sont pas nocives pour la santé humaine et permettent des communications sans licence dans la plupart des pays. Pour les RCSFs, un petit émetteur-récepteur peu coûteux et à très faible puissance est requis. Selon les auteurs dans [17], certaines contraintes matérielles et le compromis entre efficacité de l'antenne et la consommation d'énergie limitent le choix d'une fréquence porteuse pour de tels émetteurs-récepteurs à la gamme des ultra-hautes fréquences. Ils proposent également l'utilisation des bandes ISM

433 MHz et ISM 915 MHz. En outre, les principaux avantages de l'utilisation des bandes ISM sont la radio gratuite, l'attribution massive du spectre et la disponibilité mondiale. De plus, ces bandes de fréquences ne sont pas liées à une norme particulière, ce qui donne plus de liberté pour la mise en oeuvre de stratégies d'économie d'énergie dans les RCSF.

Les exigences de certaines applications RCSF rendent plus difficile le choix des supports de transmission. Par exemple, les applications marines et souterraines peuvent nécessiter respectivement l'utilisation d'un milieu de transmission aqueux et d'un milieu de transmission du sol. Dans ce type de scénarios, on aimerait utiliser un rayonnement de grande longueur d'onde qui peut pénétrer la surface de l'eau et la surface du sol. De plus, une antenne dans un noeud capteur peut ne pas avoir la hauteur et la puissance de rayonnement d'autres dispositifs sans fil. Par conséquent, le choix du support de transmission doit être pris en charge par des schémas de modulation robustes qui tiennent compte de l'environnement de déploiement des RCSFs.

g) Sécurité

Les RCSFs sont vulnérables aux tentatives malveillantes ainsi que les attaques physiques à cause des circonstances environnementales. Ainsi, pour assurer le bon fonctionnement des RCSFs, un mécanisme de sécurité des noeuds capteurs et des liens entre eux doit être mis en place.

Ainsi, l'aspect sécurité doit être très bien pris en compte, l'attaquant peut cibler la disponibilité d'un RCSF en capturant ou en désactivant un ou plusieurs noeuds capteurs, ce qui peut provoquer des anomalies dans le fonctionnement du réseau mis en place. Par exemple, dans un réseau de capteurs corporels (WBAN), il existe des attaques qui peuvent causer la mort de patients. Dans ce type de réseaux, l'attaquant peut désactiver un noeud capteur de type EEG et envoyer de fausses informations au médecin traitant. Cela peut mener à une situation de danger de mort ou même causer la mort du patient. Un attaquant peut également utiliser le brouillage et l'altération. Le brouillage peut être utilisé par un attaquant sur quelques noeuds pour paralyser l'ensemble du réseau. Cette attaque ne peut pas perturber les grands réseaux, mais comme les réseaux corporels sans fil sont généralement de petits réseaux, elle peut les paralyser et même causer une perte de paquets de données. En fait, un altère parfois physiquement les données échangées dans les WBAN. Il peut également utiliser une technique d'inondation pour provoquer un déni de service et empêcher le système de fonctionner correctement.

La sécurité doit être traitée d'une manière particulière dans les RCSFs vu que ces derniers présentent des contraintes en termes de calcul, mémoire et énergie et ils ne peuvent pas supporter des solutions de sécurité faisant appel à des solutions cryptographiques nécessitant beaucoup de calculs et de mémoire.

1.2.6 Domaines d'application des RCSFs

La variété des types de capteurs (multimédia, sismique, thermique, aquatique et acoustique) qui peuvent composer les RCSF a élargi leurs domaines d'application. Dans ce qui suit, nous citons brièvement quelques domaines d'application des RCSF.

1. **Domaine militaire**
   Les RCSFs ont fait leur apparition dans le domaine militaire en raison de leurs

caractéristiques, à savoir l'utilisation de la communication sans fil au lieu du câblage, le faible coût de la communication et la capacité à répondre aux exigences du domaine en termes de tolérance aux pannes. Le système de surveillance sonore (SOSUS) est la première application des RCSFs. Son utilisation remonte à la guerre froide, au début des années 1950 du siècle précédent, pour détecter et suivre les sous-marins soviétiques à l'aide de capteurs acoustiques [18]. Par la suite, un programme de recherche a été lancé par la Defense Advanced Research Projects Agency (DARPA) du Département de la Défense américain, qui est responsable de la recherche et du développement de nouvelles technologies à usage militaire. Il existe plusieurs applications militaires utilisant les RCSFs, notamment :

- Surveillance des champs de batailles ou des frontières,
- Détection des attaques chimiques,
- Détection des radiations

Un exemple d'application est le système iWEDS [19], un système de détection d'explosifs utilisant des RCSF, conçu pour aider la police et les forces militaires en Inde. Un autre exemple est celui des mines intelligentes [20], qui sont des mines intégrées avec des capteurs sonores et des LED/buzzers.

2. **Surveillance environnementale**
La surveillance de l'environnement est l'une des applications les plus courantes des RCSFs, qui requiert généralement une longue durée de vie. Toutefois, la contrainte intrinsèque de l'énergie des noeuds capteurs complique considérablement l'obtention d'une durée de vie satisfaisante du réseau, ce qui peut devenir un handicap pour de telles applications. Les RCSFs sont une solution largement adoptée dans ce domaine, et peuvent être utilisés pour :

   - Le suivi des animaux,
   - La surveillance de désastre naturel,
   - La surveillance de pollution,
   - La surveillance et la détection des feux de forêt,

   La surveillance environnementale est un domaine dans lequel il est préférable d'appliquer les RCSFs. Un exemple de telles applications est celui présenté dans [21] où les auteurs ont conçu un réseau réactif et événementiel dédié à la surveillance environnementale de l'humidité du sol. Un autre exemple d'application des RCSFs dans le domaine environnemental est le système présenté dans [22]. Il s'agit d'un système qui effectue une surveillance micro-environnementale.

3. **Domaine médical**
Les progrès de la technologie des RCSFs ont permis de développer de nouveaux types d'applications dans le domaine de la santé, qui permettent d'observer les personnes malades ou âgées à domicile et de surveiller leurs fonctions vitales telles que le rythme cardiaque.

La surveillance à distance de la santé des patients, y compris des fonctions vitales, nécessite l'assurance de la détection et de la transmission des informations afin de permettre une intervention opportune des médecins traitants en cas de problèmes dans l'état du patient. Cette assurance requiert la mise en place d'un mécanisme de tolérance aux pannes pour éviter toute cause d'échec dans la détection du problème chez le patient ou dans son acheminement vers le centre de contrôle.

Parmi les applications existantes dans ce domaine, citons Sensatex [23], un dispositif portable de surveillance de la santé qui intègre un certain nombre de capteurs sur la carte mère portable de Georgia Tech. Un autre exemple est Lifeguard, un projet de l'université de Stanford qui est un système de surveillance physiologique composé de capteurs physiologiques (électrodes ECG/Respiration, tensiomètre, sonde de température), d'un dispositif portable avec accéléromètres intégrés (CPOD) et d'une station de base (Pocket PC). Le CPOD acquiert et enregistre les paramètres physiologiques mesurés par les capteurs.

4. **Domotique**
   Les maisons d'aujourd'hui sont de plus en plus numérisées et intelligentes. La mise en place des RCSFs permet de disposer d'une base d'informations utiles à la gestion de ces maisons. Par exemple, dans le domaine de la surveillance de l'habitat, on trouve des capteurs de détection de mouvement, des capteurs sonores, des caméras sans fil, etc., ou dans d'autres applications qui permettent la gestion des systèmes domotiques tels que le chauffage, la climatisation, l'éclairage, etc. Les noeuds capteurs créent ainsi un environnement intelligent qui fournit toutes les informations nécessaires aux applications de confort, de sécurité et de maintenance de la maison. Des exemples de telles applications sont :

   - **Contrôle de l'éclairage** : Les lumières peuvent être actionnées en réponse à une commande d'une télécommande ainsi qu'automatiquement lorsque les capteurs de détection de présence et de luminosité détectent que des personnes se trouvent dans une pièce peu éclairée.
   - **Sécurité** : Les systèmes de sécurité perfectionnés peuvent être basés sur plusieurs capteurs (par exemple, des détecteurs de fumée, des capteurs de brise-vitre et des capteurs de mouvement) pour détecter les éventuelles situations à haut risque et déclencher les interventions adéquates en réponse. Par exemple, les détecteurs de fumées peuvent activer des alarmes incendie et les capteurs de brise-vitre peuvent actionner des alarmes sonores.

5. **Domaine industriel**
   Le vieillissement des infrastructures des unités de production, entraînent les pannes des pannes des machines et par conséquent des arrêts imprévus. L'ARC (Advisory Group) estime que 5 % de la production en Amérique du Nord est perdue en raison des temps d'arrêt. Ainsi, l'intégration des RCSFs permet de surveiller l'état des machines et d'assurer un fonctionnement sûr de ces unités de production. Les pipelines et les réservoirs vieillissants sont devenus un problème dans l'industrie pétrolière et gazière. La surveillance de la corrosion à l'aide de processus manuels prend énormément de temps et n'est pas fiable. Un réseau de capteurs de corrosion sans fil peut

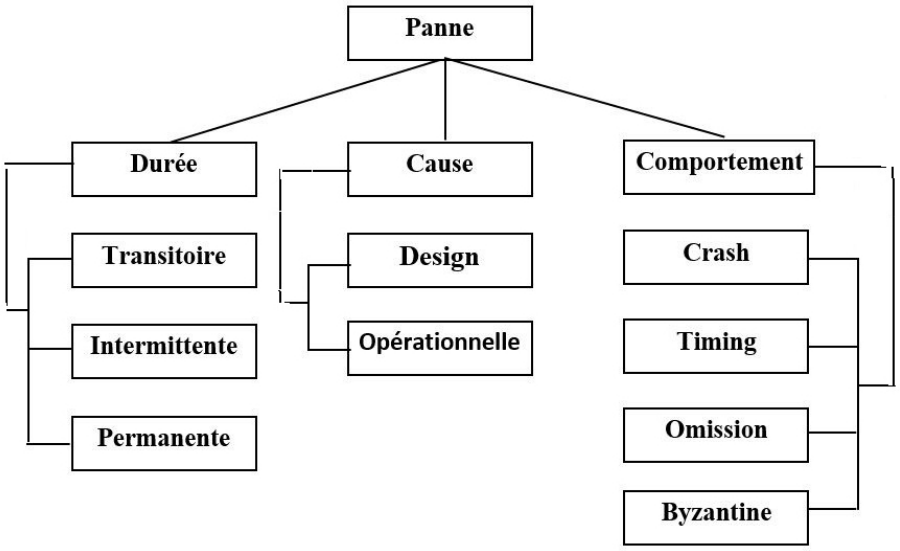


FIGURE 1.5 – Classification des pannes

être déployé de manière économique pour identifier de manière fiable les problèmes avant qu'ils ne deviennent des défaillances.

1.3 La tolérance aux pannes dans les RCSFs

un noeud capteur est un composant délicat et vulnérable aux pannes à cause d'une faible énergie, des interférences ou un dégât matériel causé d'une manière intentionnelle ou par des conditions environnementales. La panne d'un noeud capteur pourra avoir un impact négatif sur le bon fonctionnement d'un RCSF. Par conséquent, il est primordial d'instaurer des mécanismes de tolérances aux pannes pour assurer la continuité de service quand la panne d'un noeud ou plusieurs noeuds dans le RCSF survient.

1.3.1 Types de pannes

Un système est considéré en panne quand il ne fournit plus les fonctionnalités voulues. La panne est une conséquence d'une ou plusieurs erreurs où une erreur représente un état invalide du système à cause d'une faute.

1.3.2 Classification des pannes dans RCSFs

Généralement les pannes sont classifiées selon différents critères comme il est montré dans la figure 1.5. Dans ce qui suit, une classification des pannes selon trois critères est présentée :

a) Pannes selon la durée

Cette catégorie est basée sur la durée :

- **La panne transitoire** : c'est une panne temporaire qui peut disparaître sans aucune intervention.
- **La panne intermittente** : c'est un type de pannes occasionnel.
- **La panne permanente** : elle persiste et exige une intervention externe pour la surmonter. Il s'agit généralement d'un problème physique dans le composant matériel.

b) Pannes selon la cause

Dans cette catégorie, on trouve deux types de pannes :

- **Panne de conception** : Cette panne est due à une mauvaise structuration du réseau ou du composant en particulier. En pratique, ce genre de pannes ne devrait pas exister grâce aux tests et simulations avant la réalisation finale du réseau.
- **Panne opérationnelle** : Généralement, ce type de pannes se produit à cause des problèmes physiques qui sont :
  - **Énergie** : Un noeud capteur est doté d'une batterie dont son extinction cause son arrêt. Par ailleurs, l'arrêt d'un noeud capteur peut avoir de grave répercussions sur le fonctionnement du réseau.
  - **Sécurité** : Les RCSFs exigent l'existence de la sécurité pour protéger le réseau contre les attaques intentionnelles et des accidents environnementaux.
  - **Transmission** : Les transmissions radio sont vulnérables aux fautes à cause des interférences électriques et les obstacles existants dans les environnements où les RCSFs sont déployés.

c) Pannes selon le comportement résultant

Après l'occurrence d'une panne, nous distinguons quatre comportements différents possibles du composant concerné :

- **Panne accidentelle** : l'arrêt du composant peut être définitif ou récupérable.
- **Panne d'omission** : la panne du composant est irrécupérable.
- **Panne de synchronisation** : le composant réalise sa tâche mais les résulats sont fournis en retard.
- **Panne byzantine** : elle est le résultat des attaques qui visent à faire échouer le système.

1.3.3 La source des pannes dans les RCSFs

Selon la source, les pannes dans les RCSFs sont classifiées en deux classes : panne du noeud capteur et panne du système.

a) Pannes du noeud capteur

La panne d'un noeud capteur est due à une défaillance physique de l'un de ses composants tels que la mémoire, la batterie .. etc ou une défaillance logicielle telle que les problèmes survenus dans les applications.

Il faut noter que la défaillance matérielle d'un noeud capteur peut causer une défaillance logicielle. Si nous prenons l'exemple de la batterie quand l'énergie d'un noeud capteur diminue en dessous d'un seuil ce dernier commence à fournir des informations erronées.

b) Pannes du réseau

La nature des liaisons sans fil rend les RCSFs vulnérables aux pannes à cause des interférences et des collisions qui sont à l'origine de la perte de paquets et à la dégradation des performances du réseau en terme de délai de bout en bout, de débit et de la consommation d'énergie. Les mécanismes utilisés dans le routage des données vers le collecteur peuvent aussi influencer les performances du réseau. Ainsi, l'acheminement des données en utilisant le même chemin peut mener à l'extinction prématurée des batteries des noeuds faisant partie de ce chemin et par consequent, cela pourra causer une dégradation de la durée de vie du réseau. De ce fait, il faut également prendre en considération le type d'applications pour répondre à leurs exigences lors de la selection des chemins de routage.

1.3.4 Les étapes de la tolérance aux pannes

Dans la majorité des systèmes, la procédure de tolérance aux pannes passe par les étapes citées ci-dessous :

- **Détection d'erreur** : C'est la phase dans laquelle un évènement imprévisible se produit.
- **Détention de la panne** : Dans cette étape, une procédure de gestion de pannes est exécutée dans le but est de garder le reste du réseau fonctionnel.
- **Recouvrement d'erreur** : Cette étape permet de faire disparaître les conséquences des pannes à l'aide de l'information redondante pour remplacer l'information erronée ou en re-exécutant des parties du programme.
- **Traitement de panne** : C'est l'étape dans laquelle la réparation du composant défaillant s'exécute.

1.4 Le routage dans les RCSFs

Le routage est le mécanisme qui permet d'établir des chemins entre les noeuds afin d'acheminer les données détectées via plusieurs sauts pour les transmettre vers un point de collecte appelé station de base ou noeud puits.

L'optimisation de la consommation d'énergie dans les RCSFs est considérée parmi les exigences de l'efficacité des protocoles de routage dans ce type de réseaux vu que les

noeuds capteurs sont généralement déployés dans des zones hostiles où le remplacement des batteries ou leur rechargement sont des opérations quasiment difficile voire impossible. Les protocoles de routage peuvent être distingués selon la topologie des RCSFs utilisée.

Les noeuds capteurs sont sujets à des pannes et leur pannes pourra y avoir un impact sur le fonctionnement du réseau. A cet effet, il est judicieux que le protocole de routage conçu pour ce type de réseaux soit tolérant aux pannes. D'où, la mise en oeuvre de mécanismes de tolérance aux pannes avec les protocoles de routage permet le bon fonctionnement des RCSFs.

1.5 Conclusion

Ce chapitre a été consacré pour présenter des caractéristiques et les contraintes sous-jacentes aux RCSFs. Dans la première partie, nous avons présenté la notion des RCSFs et des noeuds capteurs, ensuite nous avons présenté les spécificités des RCSFs. Cette partie nous permet de connaître les contraintes intrinsèques associées aux RCSFs et par conséquent la proposition de toute solution pour ce type de réseaux doit prendre en considérations ces contraintes.

Dans la deuxième partie, nous avons présenté des notions de base sur les tolérances aux pannes, en commençant par la définition de la tolérance aux pannes, ensuite la définition des pannes, la classification des pannes, leurs sources et les procédures de les tolérer.

Le chapitre suivant sera consacré à l'un état de l'art sur la tolérance aux pannes dans les RCSFs et cet état de l'art nous permettra de connaître les lacunes des protocoles de routage tolérants aux pannes présentés dans la littérature et d'en proposer une solution tolérante aux pannes qui est plus efficace.

Chapitre 2

État de l'art sur les protocoles de routage tolérants aux pannes dans les RCSFs

Chapitre 2

État de l'art sur les protocoles de routage tolérants aux pannes dans les RCSFs

2.1 Introduction

La fragilité des noeuds capteurs et les environnements de leur déploiement qui sont généralement des endroits ouverts dans la nature rendent les noeuds capteurs vulnérables aux défaillances. A cet effet, la mise en place de mécanismes de tolérance aux pannes est devenue indispensable pour assurer le bon fonctionnement des RCSFs. Dans cette optique, plusieurs approches de tolérance aux pannes basées sur différents mécanismes ont été proposées dans la littérature.

Ce chapitre est un état de l'art qui porte sur les protocoles de routage tolérants aux pannes dans les RCSFs. Ainsi, avant de présenter cet état de l'art en détails, nous présentons une taxinomie de classification des mécanismes de tolérance aux pannes dans les RCSFs selon différentes techniques. Ensuite, nous détaillons l'état de l'art basé sur la classification temporelle tout en mettant l'accent sur les protocoles basés sur les noeuds critiques. Dans cette classification les protocoles de routage tolérants aux pannes sont scindés en deux classes : les protocoles tolérants aux pannes à aspect préventif et les protocoles de routage tolérants aux pannes à aspect curatif.

2.2 Classification des techniques de tolérance aux pannes

Les protocoles tolérants aux pannes sont répartis en plusieurs classes selon différents critères. Dans ce qui suit nous présentons quelques mécanismes de tolérance aux pannes basés sur différentes techniques :

2.2.1 Classification temporelle

Dans la classification temporelle, le critère de base pour catégoriser un mécanisme de tolérance aux pannes est le temps de début de son exécution si c'est avant ou après l'occurrence de la panne. Ainsi, selon ce critère le type de mécanismes est classé comme préventif ou curatif.

a) Aspect préventif

Ce type de mécanismes de tolérance aux pannes vise à garder le réseau fonctionnel le plus longtemps possible tout en tentant à retarder ou éviter l'occurrence des pannes. Dans ce type de mécanismes, nous optons à des stratégies qui permettent de garantir une longue durée de vie des noeuds notamment les stratégies d'optimisation de la consommation d'énergie de la batterie et la mise en oeuvre des chemins alternatifs.

b) Aspect curatif

Cette technique est basée sur une approche optimiste où le mécanisme de tolérance aux pannes n'est déclenché qu'après l'occurrence de la panne en tentant à reprendre le fonctionnement du réseau correctement. Parmi les mécanismes les plus connus est le recouvrement du chemin de routage et le remplacement du noeud défaillant par un autre noeud où sa sélection peut suivre différents critères.

Dans le deuxième état de l'art nous se concentrons sur une classification architecturale.

2.2.2 Classification architecturale

Dans cette classification, les mécanismes sont présentés en quatre classes principales :

a) Mécanismes de gestion de l'énergie

L'utilisation permanente d'un noeud capteur peut causer l'extinction prématurée de son énergie. Le mécanisme de gestion de l'énergie implique des méthodes d'équilibrage de charge qui permettent d'utiliser des noeuds alternatifs pour ne pas surcharger un seul noeud.

b) Mécanismes de gestion des flux

Cette technique est basée sur la sélection des chemins fiables entre les noeuds du réseau et la station de base. Cela permet de définir les meilleurs chemins de routage de données captées et de faciliter la récupération de la connectivité.

c) Mécanismes de gestion des données

L'optimisation de la consommation d'énergie est un mécanisme très important pour prolonger la durée de vie des RCSFs. L'un des facteurs influençant l'énergie des noeuds capteurs est la quantité de données transmises, en particulier les données redondantes. Le mécanisme de gestion des données réduit la quantité de données envoyées à la station de base grâce aux techniques de compression et d'agrégation.

d) Mécanismes de gestion de la couverture et de la connectivité

La couverture de la zone dans les RCSFs représente la qualité de la surveillance d'une zone d'intérêt. L'absence de couverture de certains points a un impact très important sur la surveillance de la zone d'intérêt et la connectivité est une mesure importante pour évaluer les performances du réseau, car elle garantit un acheminement fiable des données à

la station de base. Le mécanisme de la couverture et de la connectivité traite les problèmes de déploiement des noeuds capteurs.

2.2.3 Classification selon la taille du réseau

Les RCSFs à petite échelle sont de petits réseaux composés de dizaines de noeuds capteurs déployés sur une petite zone, utilisés dans diverses applications telles que les applications de santé et de sécurité domestique.

Dans un réseau de capteurs à petite échelle, la défaillance d'un noeud capteurs peut avoir un impact considérable sur le fonctionnement du réseau, car dans ce type de réseaux, un nombre minimal de capteurs est utilisé et chaque noeud capteur joue un rôle important dans la surveillance et l'acheminement des données d'une petite zone spécifique de la zone de déploiement. Ce type de réseaux requiert un type de mécanismes de tolérance aux pannes qui prend en considération l'importance de chaque noeud capteur dans le réseau. Par ailleurs, les RCSFs à grande échelle sont composés d'un grand nombre de noeuds capteurs dispersés sur une grande zone géographique avec une corrélation spatiale très grande qui permet de tolérer la panne d'un capteur où une zone précise peut être surveillée par plusieurs noeuds capteurs. Par conséquent, la défaillance d'un noeud capteur dans les RCSFs à grande échelle n'a pas la même influence par rapport aux RCSFs à petite échelle. Dans ce qui suit, nous présenterons les protocoles de routage tolérants aux pannes basés sur les noeuds critiques dans les RCSFs. Puis, nous présentons les différentes approches de tolérance aux pannes dans les RCSFs à aspect préventif et curatif.

2.2.4 Classification basée sur les noeuds critiques

Un noeud critique est un noeud capteur dont la défaillance entraîne une perte de connectivité et une division du réseau en plusieurs sous-réseaux non connectés. Dans la littérature, la notion de noeud critique diffère d'une approche à l'autre en fonction de différents paramètres. En général, un noeud critique est défini en fonction de l'impact de sa défaillance sur les performances du réseau auquel il appartient. Dans cet état de l'art, nous présentons des travaux qui proposent des méthodes permettant de tolérer la défaillance des noeuds critiques.

2.3 Tolérance aux pannes basée sur la classification temporelle

Dans la classification temporelle, le critère de base pour la classification de la technique de tolérance aux pannes est le moment du début de son exécution, qu'elle soit lancée avant ou après l'occurrence de la panne et selon ce critère, le type de technique est classé comme préventif ou curatif. La figure 2.1 illustre la classification temporelle.

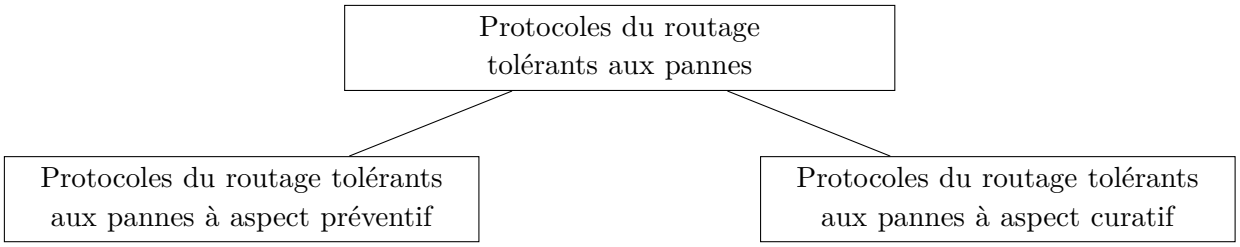


FIGURE 2.1 – Classification temporelle des protocoles du routage tolérants aux pannes

2.3.1 Approches à aspect préventif

Dans ce qui suit, une présentation des protocoles de routage tolérants aux pannes sera présentée selon les mécanismes de tolérance aux pannes suivants : gestion d'énergie et de données dans les RCSFs basée sur le clustering et l'agrégation et gestion préventive des flux basée sur le routage multi-chemins. La figure 2.2 illustre une classification des approches à aspect préventif.

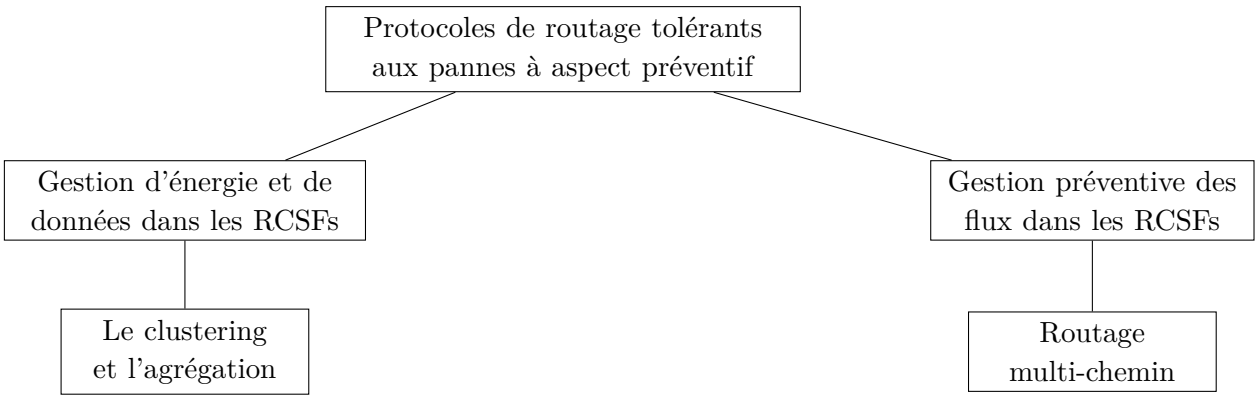


FIGURE 2.2 – Protocoles du routage tolérants aux pannes à aspect préventif

a) Gestion d'énergie et des données dans les RCSFs

Dans ces approches ont fait appel généralement à l'agrégation de données et au clustering. L'objectif de l'agrégation de données est de réduire la quantité de données envoyées à la station de base. Elle minimise la consommation d'énergie, en particulier dans les RCSFs à grande échelle où le chevauchement dans la détection des noeuds disjoints est intrinsèque. Dans la littérature, l'agrégation de données est utilisée avec la méthode de clustering, dont l'objectif principal est de minimiser la quantité de données traitées et transmises, optimisant ainsi la consommation d'énergie du réseau et prolongeant par conséquent sa durée de vie. En outre le clustering est considéré parmi les mécanismes préventifs de la tolérance aux pannes. Il est basé sur le regroupement des noeuds du réseau sous forme de clusters où chaque cluster a un chef du cluster(CH) qui gère le traitement et la transmission des mesures détectées par les noeuds capteurs membres du même cluster et l'agrégation des données se fait au niveau des CHs. Le clustering vise à équilibrer la

consommation d'énergie nodale dans les RCSFs. Dans ce qui suit, nous présentons les principaux travaux décrits dans la littérature qui utilisent des mécanismes de gestion de l'énergie et des données pour la tolérance aux pannes dans les RCSFs.

Dans [24], les auteurs ont proposé un protocole de routage tolérant aux pannes pour les RCSFs, appelé "General Self-organizing Tree-based Energy Balance (GSTEB)" dans le but est d'améliorer l'agrégation des données inter-cluster. Dans GSTEB, une amélioration de l'algorithme de colonies de fourmis (Ant Colony Optimization (ACO)) a été proposée pour sélectionner efficacement les noeuds CHs.

Daneshvar et al. [25] ont proposé un protocole tolérant aux pannes basé sur la méta-heuristique d'optimisation des loups gris (Grey Wolf Optimizer (GWO)) pour la sélection des noeuds CHs. La sélection des CHs est basée sur la consommation d'énergie prévue et l'énergie résiduelle actuelle de chaque noeud. Ainsi, pour améliorer la consommation d'énergie, le protocole proposé utilise le même clustering pour plusieurs rounds consécutifs contrairement à "Low-energy adaptive hiérarchie de clustering (LEACH)" [26].

Kaur et Kumar [27] ont proposé un protocole basé sur l'optimisation d'essaim de particules (Particle Swarm Optimization (PSO)) pour prolonger durée de vie du réseau tout assurant la tolérance aux pannes. L'approche PSO permet de minimiser la moyenne des distances de communication intra-cluster, et inter-cluster. Elle permet également de maximiser la somme d'énergie des noeuds CHs. Le protocole proposé introduit un algorithme de tolérance aux pannes en définissant le noeud substituant du noeud CH en cas de sa défaillance. Le noeud substituant est le membre du cluster le plus proche du CH avec un taux d'énergie suffisant pour accomplir ses tâches pour un round. Le processus de re-clustering est exécuté lorsque l'énergie de certains noeuds CHs diminue sous un seuil calculé qui est une valeur approximative de la quantité d'énergie nécessaire pour fonctionner pendant un round.

Dans [28], les auteurs ont proposé un protocole de routage tolérant aux pannes pour les RCSFs. Ce protocole utilise une méthode de clustering économe en énergie basée sur l'algorithme "Hybrid Energy Efficient Distributed (HEED)" [29]. Les noeuds CHs sont sélectionnés en fonction de l'énergie résiduelle et la distance avec leurs voisins. Le protocole utilise un noeud de sauvegarde pour tolérer la panne des CHs. Dans ce protocole, la méthode veille/sommeil a été adaptée pour réduire la consommation d'énergie.

Dans [30], le protocole de clustering proposé est basé sur l'algorithme de clustering HEED. Dans ce protocole, un noeud de sauvegarde est utilisé pour tolérer la panne du noeud CH. Ce noeud de sauvegarde est un noeud voisin du noeud CH. En outre, la méthode veille/réveil est utilisée pour les membres du cluster afin d'améliorer la consommation d'énergie.

Sahoo et al. [31] ont proposé un protocole basé sur le comportement robuste des algorithmes génétiques afin d'optimiser la sélection des CHs. Dans la sélection des noeuds CHs l'algorithme génétique prend en considération plusieurs facteurs tels que l'énergie résiduelle des noeuds, le niveau du noeud, l'énergie moyenne et le taux de consommation d'énergie. Ces facteurs ont été utilisés comme paramètres de la fonction de fitness de l'algorithme génétique.

Dans [32], les auteurs ont conçu un protocole de tolérance aux pannes hybride qui combine les concepts des algorithmes libellule et luciole (dragon fly and firefly algorithms) dans le processus de sélection des noeuds CHs. Ce protocole vise à améliorer l'efficacité énergétique, le retard et de probabilité de risque.

Pandiyaraju et al. [33] ont proposé un protocole qui fonctionne en trois phases à savoir : la phase de formation des champs, la phase d'élection des chefs de champs et la phase de routage. Dans la première phase, la surface qui est une terre agricole est divisée en petites zones ayant la même superficie appelées champs. Dans la deuxième phase, les chefs de champs sont choisis à l'aide des règles de logique floue faisant intervenir la distance entre les noeuds capteur et la station de base et l'énergie résiduelle des noeuds capteurs. Dans ce protocole, la transmission des données d'une source à la station de base se fait à l'aide des chefs des champs qui jouent le rôle de relais. La sélection des chefs des champs participants dans le routage des données est basée sur l'énergie résiduelle des chefs des champs, leur degré et la distance entre le chef du champ et la station de base.

Dans [34], les auteurs ont proposé un protocole de routage de clustering hybride tolérant aux pannes basé sur un réseau gaussien pour les RCSFs (Fault-tolerant Clustering routing protocol based on Gaussian network for Wireless sensor network (FCGW)). L'objectif de FCGW est d'améliorer la tolérance aux pannes, d'augmenter la fiabilité des données et de réduire la consommation d'énergie des RCSFs. FCGW divise la zone du réseau en petites grilles carrées dans lesquelles le chef du cluster de chaque grille est représenté par un entier gaussien. Ces chefs des clusters sont reliés entre eux pour créer un réseau gaussien. Pour tolérer la panne des CHs, chaque CH échange ses informations avec les CHs voisins. Si un CH ne reçoit pas les informations de son voisin il le considère comme défaillant et il sélectionne un autre CH pour le saut suivant.

Bhat et Santhosh [35] ont proposé un protocole tolérant aux pannes économe en énergie. Ce protocole sélectionne les noeuds défaillants en utilisant les méthodes de regroupement K-means et de vote majoritaire. Les performances de ce protocole ont été comparées à celles d'autres protocoles basés sur la localisation. Le protocole présenté montre une meilleure précision de localisation et une performance plus stable dans des conditions de défaillance.

b) Gestion préventive des flux dans les RCSFs

La gestion des flux permet de définir les mécanismes de gestion de l'acheminement des données pour différentes couches : comme le routage dans la couche réseau et la sélection des canaux de transmission dans la couche MAC. Elle utilise généralement un routage multi-chemins pour assurer la tolérance aux pannes dans les RCSFs. Ce schéma de routage fournit une tolérance aux pannes préemptive en établissant plusieurs chemins de routage entre chaque noeud capteur et la station de base. Cela garantit la disponibilité des chemins alternatifs pour le transfert de données en cas de défaillance du premier chemin sélectionné. Dans ce qui suit, nous présentons les principaux travaux qui font appel à ce mécanisme de tolérance aux pannes dans les RCSFs.

Dans [36], Nayyar et Singh ont présenté un nouveau protocole de routage multi-chemin et économe en énergie basé sur la métaheuristique de colonie de fourmis (ACO) pour les RCSFs, appelé "Improvised Energy Efficient Multipath ACO based Routing Protocol (IEEMARP)". Le protocole proposé se déroule en trois phases : la phase de découverte des voisins par la connaissance des liens, la phase de transmission des paquets basée sur la méthode de la moyenne mobile pondérée et la phase de livraison des paquets avec acquittement (ACK) pour assurer une livraison fiable de bout en bout. IEEMARP implique la métaheuristique ACO pour résoudre le problème d'optimisation combinatoire à fin de sélectionner le plus court chemin. Les résultats de simulation ont montré que ce

protocole fournit de meilleures performances par rapport à plusieurs protocoles tels que DSDV, DSR, et un protocole basé sur la version originale de la métaheuristique ACO.

Bouatit et al. [37] ont proposé un protocole de routage multi-chemin non interférant pour optimiser la qualité de service (Qualité of Service (QoS)) dans les RCSFs. Pendant la phase de construction des chemins, le protocole proposé tente de trouver le maximum de chemins disjoints entre les noeuds en minimisant autant que possible les interférences entre ces chemins adjacents. h Dans [38], les auteurs ont tenu compte du fait que l'utilisation systématique des chemins les moins énergivores peut ne pas être optimale en termes de durée de vie du réseau et de connectivité à long terme. Pour optimiser ces critères de performances, ils ont proposé un nouveau schéma de routage appelé "energy aware routing" qui utilise occasionnellement des chemins sous-optimaux pour obtenir des gains substantiels. Les résultats de simulations ont montré une amélioration de la durée de vie du réseau allant jusqu'à 40% par rapport à d'autres schémas de routage tels que le schéma de routage par diffusion dirigée (Directed Diffusion) [39]. En outre, dans le protocole proposé les noeuds consomment l'énergie de manière plus équitable dans le réseau.

Tien et al. [40] ont proposé un nouvel algorithme basé sur la redondance des chemins, appelé "Dual Separate Paths (DSP)", qui fournit une communication tolérante aux pannes avec l'amélioration des performances du trafic réseau pour les applications WSN. L'algorithme DSP proposé établit deux chemins séparés entre une source et une destination dans un réseau basé sur les informations de topologie du réseau. Ces chemins sont des chemins noeuds-disjoints et ont des distances de chemin optimales entre la source et la destination. Les trames unicast sont délivrées de la source à la destination dans le réseau à travers deux chemins, ce qui permet une communication tolérante aux pannes et réduit le trafic unicast redondant pour le réseau. L'algorithme DSP peut être appliqué aux réseaux câblés et sans fil, tels que les RCSFs, afin de fournir une communication transparente et tolérante aux pannes pour les applications critiques et vitales telles que les CPS tolérants aux pannes. Les résultats de simulation ont montré que l'approche basée sur le DSP fournit non seulement une communication tolérante aux pannes, mais améliore également les performances du trafic réseau. En outre, le protocole basé sur DSP a été appliqué aux réseaux "High Availability Seamless Redundancy (HSR)" et les résultats fournis ont montré que ce dernier a réduit le trafic réseau de 80 à 88 % par rapport au protocole HSR standard, améliorant ainsi les performances du trafic réseau.

Hassanein et Luo [41] ont présenté une nouvelle approche de la fiabilité dans les RCSFs. Il s'agit d'un protocole de routage distribué, à la demande et réactif, qui vise à fournir un environnement de transmission fiable pour la livraison paquets de données, appelé "Reliable Energy Aware Routing (REAR)". Le protocole proposé permet la sélection de noeuds locaux, la réservation de chemin et le délai de diffusion des demandes de chemin pour fournir un environnement de transmission fiable afin de réduire retransmissions causées par des chemins instables. Le schéma de routage adopté utilise efficacement l'énergie limitée et les ressources de mémoire disponibles des noeuds de capteurs. REAR tente de prendre précaution contre les erreurs, au lieu de trouver une solution après avoir rencontré les erreurs. Les simulations ont montré que REAR surpasse les schémas de routage traditionnels en établissant un chemin économe en énergie de la source à la station de base, et aussi en distribuant la charge du trafic de manière plus uniforme dans le réseau. L'inconvénient de ce protocole est que les ressources réservées au niveau des noeuds capteurs pour la route de secours peuvent n'être jamais utilisées si la route primaire reste

fonctionnelle ce qui mène à un gaspillage inutile de ressources.

Le protocole présenté dans [42] utilise les mêmes techniques que le protocole "Directed Diffusion (DD)" [39], sauf qu'en phase de renforcement, deux messages sont transmis au lieu d'un. Le premier message renforce le meilleur voisin et le deuxième message renforce le deuxième meilleur voisin. Ce processus est répété au niveau de chaque noeud, vise à trouver plusieurs chemins partiellement disjoints ce qui permet de se remettre d'une panne rapidement.

Dans [43], les auteurs ont proposé un protocole appelé "Multipath Routing in large scale sensor networks with Multiple Sink nodes (MRMS)" qui incorpore des noeuds puits multiples, une nouvelle métrique du coût du chemin pour améliorer la sélection du chemin, la maintenance dynamique des clusters et le changement de chemin pour une meilleure efficacité énergétique. En cas de panne d'un noeud CH, MRMS sélectionne un nouveau noeud CH pour remplacer le noeud défaillant ou sélectionner un autre chemin. Le protocole MRMS utilise une méthode d'agrégation et fournit une approche tolérante aux pannes des noeuds capteurs et les stations de base en sélectionnant différents chemins entre les noeuds capteurs et les stations de base. Les résultats de simulation ont montré que MRMS augmente considérablement la durée de vie des noeuds de capteurs par rapport à d'autres protocoles. Cependant, la sauvegarde de tous les chemins alternatifs nécessite une utilisation importante des ressources du réseau ce qui rend la solution proposée dans MRMS très coûteuse et peu exploitable.

Chen et al. [44] ont présenté le protocole du routage appelé "Distributed and Effective Cluster Routing Protocol (DECROP)", qui est basé sur le clustering dans lequel les CHs ont la capacité du traitement et d'agrégation des mesures captées par les membres des clusters. DECROP comporte trois processus : l'initialisation, la formation de clusters distribués, la transmission de données et la maintenance des routes. Dans DECROP, les chemins sont sélectionnés dans la phase d'initialisation ce qui minimise le nombre des messages de contrôle échangés et réduit la consommation d'énergie et le délai de bout en bout. Il permet également de sélectionner un autre chemin en cas de panne du chemin principal. Les résultats de simulations ont montré que DECROP a moins de messages de contrôle, un délai de bout en bout plus court dans les applications de transmission de données à la station de base par rapport au protocole AODV et l'énergie résiduelle est proche de celle du protocole AODV. DECROP est particulièrement adapté aux RCSFs à grande échelle avec des capteurs homogènes. Néanmoins, l'inconvénient dans ce protocole revient à la taille des clusters où le grand nombre de membres dans les clusters augmente la consommation énergétique des CHs.

Dans [45], Lu et al. ont étudié tout d'abord les problèmes de routage pour les RCSFs et ont proposé un nouvel algorithme de routage économe en énergie basé sur les clusters pour les RCSFs hiérarchiques, dans lequel ils ont hiérarchisé les noeuds de capteurs en différents niveaux en utilisant le nombre de sauts de transmission vers la station de base. Les CHs sont sélectionnés de manière autonome et transmettent des données à la station de base en utilisant des transmissions multi-sauts, tandis que les noeuds membres communiquent directement avec les noeuds CHs. Le protocole propose la possibilité d'utiliser des noeuds capteurs alternatifs (Alternatif Sensor Nodes (ASNs)) pour les chemins de routage des données. Un noeud capteur alternatif est un noeud dans la plage de transmission (R) avec un noeud appartient au chemin principal, son énergie résiduelle est supérieure à celle du noeud principal et la distance entre eux est inférieure à $R/2$. Le protocole garde la

connectivité en utilisant le noeud alternatif où dans le cas de défaillance d'un noeud relais, un noeud peut envoyer les données immédiatement au noeud alternatif. Les résultats de la simulation ont montré que, pour les RCSFs à grande échelle, l'algorithme proposé est plus performant en termes de durée de vie du réseau. De plus, l'algorithme atténue l'effet du trou noir auto-induit et équilibre l'utilisation de l'énergie dans le réseau en impliquant des noeuds de capteurs alternatifs dans le processus de routage. Cependant, la construction des clusters à chaque itération dégrade les performances du réseau en terme d'énergie.

c) Gestion préventive de la couverture et de la connectivité

Dans cette sous-section, nous présentons les principaux protocoles qui se basent sur la gestion préventive de la couverture et de la connectivité pour garantir la tolérance aux pannes dans les RCSFs.

Le protocole [46] propose une solution pour les problèmes de couverture et de connectivité dans les RCSFs. L'objectif principal de ce protocole est de fournir un déploiement permettant d'assurer la couverture séquentiellement en utilisant un nombre minimal de noeuds capteurs sur une grille. Pour atteindre cet objectif le protocole fait appel à une approche hybride basée sur trois algorithmes. Le premier algorithme déploie les noeuds capteurs de manière à ce que toutes les zones cibles soient couvertes. Le deuxième algorithme réduit le nombre de noeuds de capteurs en supprimant les noeuds capteurs redondants, tandis que le troisième algorithme sélectionne les chemins optimaux reliant les noeuds capteurs à la station de base à l'aide d'un algorithme basé sur les algorithmes génétiques.

Dans [47], les auteurs ont proposé un algorithme hybride de recherche gravitationnelle avec un modèle basé sur un conducteur de ski social (Gravitational Search Algorithm with Social Ski-Driver (GSA-SSD)). GSA-SSD vise à optimiser les exigences de couverture et de connectivité dans les RCSFs. Ainsi, en adaptant le comportement dynamique de l'algorithme SSD, la performance de GSA est améliorée. Les performances relatives du modèle d'optimisation hybride GSA-SSD proposé ont été validées et comparées à d'autres algorithmes d'optimisation en termes de taux de surface non couverte, de nombre de capteurs actifs sélectionnés, de consommation d'énergie, de connectivité et de durée de vie du réseau.

Dans [48], une nouvelle méthode d'ordonnancement des trajectoires basée sur le taux de couverture de plusieurs stations de base mobiles (TSCR-M : Trajectory Scheduling method based on Coverage Rate for Multiple mobile sinks) est présentée, en particulier pour les RCSFs à grande échelle. Cette méthode est basée sur une optimisation par essaims de particules (PSO) améliorée et combinée à un opérateur de mutation pour rechercher les positions de stationnement avec un taux de couverture optimal. Ensuite, un algorithme basé sur les AGs est adopté pour planifier la trajectoire de déplacement de plusieurs stations de base mobiles. Des simulations approfondies ont été réalisées pour valider les performances de la méthode proposée. Les résultats obtenus ont montré que TSCR-M optimise la consommation d'énergie et prolonge la durée de vie du réseau par rapport à d'autres protocoles.

Dans [49], l'approche proposée vise à renforcer les exigences de couverture à l'aide d'algorithme basé sur les AGs en fournissant une surveillance continue des zones cibles spécifiées pendant la durée la plus longue possible. L'approche permet aussi de garder la connectivité en permettant aux noeuds capteurs de se déplacer vers des positions appro-

priées à des vitesses variables pour détecter des mesures sur l'environnement. L'approche assure la connectivité du réseau et prolonge sa durée de vie.

Harizan et Kuila [50] ont proposé un protocole basé sur "Non-dominated Sorting GA (NSGA-II)" qui est l'un des algorithmes évolutionnaires multi-objectifs les plus populaires. NSGA-II vise à optimiser plusieurs objectifs simultanément (multi-objectif), sans être affecté par aucune autre solution. Dans ce travail, un NSGA-II avec dominance modifiée a été proposé pour le problème d'ordonnancement. Plusieurs paramètres tels que la couverture, la connectivité et l'énergie résiduelle des noeuds capteurs sont pris en compte. Les noeuds capteurs ayant un niveau d'énergie relativement élevé sont préférés pour être sélectionnés dans un tour afin qu'ils puissent servir un maximum de tours. Les auteurs ont également formulé le problème traité sous la forme d'une programmation linéaire (LP). Les chromosomes sont conçus efficacement et il est démontré que la validité des chromosomes est préservée après les opérations de croisement et de mutation. Les quatre objectifs conflictuels multiples sont dérivés pour évaluer les chromosomes. La procédure de domination est modifiée pour améliorer les performances de l'algorithme. L'algorithme proposé fait l'objet d'une simulation approfondie et les résultats ont démontré sa supériorité par rapport aux algorithmes connexes existants dans la littérature.

Le travail présenté dans [51] est une étude qui considère une application hybride de couverture de points et de barrières pour les réseaux de capteurs hétérogènes (Homogeneous Sensor Nodes (HSNs)). Dans cette application, un décideur cherche à localiser des noeuds capteurs le long d'une région frontière bidimensionnelle en forme de ceinture pour deux buts : (i) protéger les installations critiques situées à l'intérieur de la région de frontière, et (ii) empêcher le franchissement illégal des frontières. En utilisant ce cadre multi-objectif, cette étude incorpore les facteurs suivants : plusieurs types de capteurs, intrus et installations critiques, modèle de couverture des capteurs, allocation de couverture coopérative, et contraintes techniques. Pour résoudre le problème défini, l'auteur a développé d'abord une formulation multi-objectif de programmation non linéaire en nombres entiers (Integer NonLinear Programming (INLP)). Comme le modèle INLP est non-convexe, il peut ne pas produire de solutions globalement optimales. C'est pourquoi, à l'aide d'une technique de mappage spéciale, il a reformulé le problème sous la forme de programmation linéaire en nombres entiers (Integer Linear Programming (ILP)) multi-objectif. Ensuite, il a utilisé une métaheuristique basée sur les algorithmes génétiques pour résoudre le problème. Des simulations ont été réalisées pour mesurer et comparer les performances des solutions INLP, ILP et GA proposées. Les résultats obtenus ont montré que, bien que la solution basée sur ILP soit efficace pour les problèmes de petite taille, elle nécessite des temps de calcul plus longs pour fournir des solutions globalement optimales. En revanche, les solutions basées sur INLP et les AGs ont permis de fournir un équilibre entre la qualité de la solution et le temps de calcul pour les problèmes de plus grande taille. Cependant, la contribution ne prend pas en compte les contraintes de connectivité et d'interférences.

Dans [52], les auteurs ont proposé une solution basée sur une amélioration de l'algorithme de colonies de fourmis afin d'assurer un déploiement efficace des noeuds capteurs dans les RCSFs pour garantir la couverture d'une zone d'intérêt et la connectivité en utilisant un nombre minimum de noeuds capteurs. La solution proposée permet la détection d'obstacles et l'optimisation du nombre de sauts pour acheminer les données vers la station de base.

Dans [53] un protocole de couverture par balayage basé sur l'optimisation de la méta-heuristique ACO (Improved Ant Colony Optimization-based Sweep Coverage (IACOSC)) a été proposé dans le but d'assurer une collecte de données régulière et efficace à partir des noeuds capteurs. L'objectif du protocole IACOSC est d'impliquer un nombre minimal de noeuds capteurs mobiles pour garantir la couverture de la zone d'intérêt et de la connectivité pour la livraison des données à la station de base. Dans IACOSC, les fourmis artificielles ont été utilisées pour créer les routes de couverture initiales pour les points d'intérêt. Ensuite, une nouvelle métrique appelée efficacité de la couverture des routes a été utilisée pour évaluer ces routes. Enfin, un algorithme de recherche locale basé sur la suppression de routes et l'insertion de noeuds a été utilisé pour optimiser ces routes. Les résultats de simulations ont montré que, par rapport aux approches existantes de couverture par balayage qui prennent en compte la livraison des données, IACOSC réduit considérablement la complexité du calcul et diminue le temps de calcul de 50 % tout en minimisant le nombre de capteurs mobiles de 16,73 % dans les mêmes scénarios de réseau.

Abo-Zahhad et al. [54] ont proposé un algorithme immunitaire centralisé de déploiement basé sur le diagramme de Voronoï (Centralized Immune-Voronoi deployment Algorithm (CIVA)) pour maximiser la couverture d'une zone d'intérêt. CIVA utilise l'algorithme immunitaire multi-objectif qui implique les propriétés du diagramme de Voronoï pour fournir un meilleur compromis entre la couverture et la consommation d'énergie. L'algorithme CIVA se compose de deux phases pour améliorer la durée de vie et la couverture des réseaux de capteurs sans fil multimédias (Multimedia Wireless Sensor Networks (MWSNs)). Dans la première phase, CIVA contrôle les positions et les portées de détection des noeuds capteurs mobiles (Mobile Sensor Nodes (MSN)) en fonction de la maximisation de la couverture et de la minimisation de l'énergie dissipée dans la mobilité et la détection. La deuxième phase de CIVA ajuste la radio (sommeil/actif) des MSNs pour minimiser le nombre de capteurs actifs en se basant sur la minimisation de la consommation d'énergie dans la détection et la couverture redondante et en préservant la couverture à un niveau élevé. Les performances de CIVA ont été comparées à des algorithmes existants dans la littérature pour différentes configurations de réseau avec et sans obstacles. Les résultats de simulations ont montré que l'algorithme CIVA surpasse d'autres algorithmes en termes de couverture et d'énergie dissipée pour différentes configurations de réseaux.

TABLE 2.1 – Récapitulatif sur les protocoles de routage tolérants aux pannes à aspect préventif le clustering et l'agrégation

Protocole	**Proposition**	**Approche**	**Avantages**	**Inconvénients**
GSTEB [24]	Clustering et agrégation : la métaheuristique ACO est utilisée pour sélectionner les CHs	Centralisée	Amélioration de l'agrégation des données et optimisation de la consommation d'énergie	Temps de convergence élevé
Daneshvar et al. [25]	Clustering et agrégation : la métaheuristique GWO est utilisée pour sélectionner les CHs	Centralisée	Optimisation de la consommation d'énergie	L'optimisation de l'énergie a été faite au détriment des autres paramètres de QoS
Kaur et Kumar [27]	Clustering et agrégation : la métaheuristique PSO est utilisée pour sélectionner les CHs	Centralisée	Prolongation de la durée de vie du réseau	Plus de messages de contrôle
FTEC [30]	Clustering et agrégation : l'algorithme de HEED est utilisée pour sélectionner les CHs	Distribuée	Prolongation de la durée de vie du réseau	L'optimisation de la consommation d'énergie n'est pas minimale
GAPSO-H [31]	Clustering et agrégation : les AGs et l'algorithme PSO sont utilisés pour sélectionner les CHs	Centralisée	Optimisation de la sélection des CHs	- Durée de vie du réseau n'est pas optimale -Temps de calcul élevé
PU-DA [32]	Clustering et agrégation : Une hybridation des algorithmes dragonfly et firefly pour sélectionner les CHs	Centralisée	Amélioration de l'efficacité énergétique	Nombre d'itérations et temps de convergence ne sont pas optimisés
Pandiyaraju et al. [33]	Clustering et agrégation : Sélection des chefs des champs à l'aide de la logique floue	Distribuée	prolongation de la durée de vie du réseau	L'amélioration des autres performances n'est pas optimale
FCGW [34]	Clustering et agrégation : La zone de déploiement est divisée en petites zones et les CHs de chaque grille sont représentés par un entier gaussien	Centralisée	Tolérance aux pannes des CHs	L'optimisation de la consommation d'énergie n'est pas prise en considération
Bhat et Santhosh [35]	Clustering et agrégation : Utilisation de K-means et la méthode de vote majoritaire pour former et élire les CHs	Centralisée	Le nombre de clusters est fixé auparavant	La sélection des CHs est faite après le clustering

IEEMARP [36]	Routage multi-chemin : la métaheuristique ACO est utilisée pour la sélection du plus court chemin	Centralisée	Optimisation de la consommation d'énergie	Le temps de calcul augmente lors du passage à l'échelle
Bouatit et al. [37]	Routage multi-chemin : Utilise des chemins disjoints alternatifs non interférants	Centralisée	Amélioration de débit de livraison	Le protocole n'assure pas une optimisation de consommation d'énergie
Shah et Rabaey [38]	Routage multi-chemin : Utilise différents chemins basés sur la métrique d'énergie et évite l'utilisation permanente de la route la plus économe en énergie	Distribuée	L'utilisation des différents chemins évite l'épuisement prématuré de l'énergie d'un chemin par rapport aux autres	L'utilisation de chemins alternatifs pourra atténuer d'autres performances telles que le délai
Tien et al. [40]	Routage multi-chemin : Utilisation de différents chemins	Distribuée	Optimisation de la consommation d'énergie et une bonne tolérance aux pannes des noeuds capteurs	Plus de messages de contrôle
Hassanein et Luo [41]	Routage multi-chemin : Utilise deux chemins (un chemin de service qui est le chemin primaire et un chemin de secours qui va être utilisé en cas de panne du chemin de service)	Distribuée	La solution tolère la panne d'un chemin	Un gaspillage inutile des ressources
Ganesan et al. [42]	Routage multi-chemin : Utilise le principe du protocole "Directed Diffusion" et de deux messages pour le renforcement : le premier message renforce le meilleur voisin et le deuxième message renforce le deuxième meilleur voisin	Centralisée	La solution permet de trouver plusieurs chemins partiellement disjoints ce qui permet de recouvrir une panne rapidement	Les chemins alternatifs partiellement disjoints sont aussi vulnérables aux pannes parce qu'ils sont proches du chemin principal
Y. Chen et al. [43]	Routage multi-chemin : Utilise une méthode de changement de chemin en cas de panne d'un noeud relais	Centralisée	Optimisation de la consommation d'énergie grâce aux algorithmes de clustering et de la tolérance aux pannes	Solution coûteuse à cause de la sauvegarde de tous les chemins alternatifs

J. Chen et al. [44]	Routage multi-chemin : Sélection des chemins durant la phase d'initialisation et d'un autre chemin en cas de panne du chemin principal	Distribuée	Tolérance aux pannes et optimisation d'énergie	Le grand nombre des membres des clusters augmente la consommation énergétique des CHs
Lu et al. [45]	Routage multi-chemin : Utilise une méthode de changement de chemin en cas de panne d'un noeud relais	Centralisée	Optimisation de la consommation d'énergie	Solution coûteuse à cause de la sauvegarde de tous les chemins alternatifs
Njoya et al. [46]	Couverture et Connectivité : Le premier algorithme déploie les noeuds capteurs de façon à ce que la zone soit couverte. Le deuxième algorithme réduit le nombre de capteurs redondants. Le troisième algorithme implique les AGs pour sélectionner les chemins optimaux entre les noeuds capteurs avec la station de base	Centralisée	Assure la couverture et la connectivité	Temps de calcul élevé
GSA-SSD [47]	Couverture et connectivité : Algorithme de recherche gravitationnelle "Social Ski-Driver"	Centralisée	Amélioration de la durée de vie. Assurance de connectivité et couverture	Une amélioration dans le temps de calcul reste limitée
TSCR-M [48]	Couverture et connectivité : Utilise la technique PSO pour augmenter la couverture et minimiser le taux d'interférences et un algorithme génétique pour obtenir un mouvement de trajectoire efficace pour plusieurs stations de base	Centralisée	Amélioration de la couverture	La solution ne prend pas en considération les autres performances
Elhoseny et al. [49]	Couverture et connectivité : Approche basée sur les AGs	Centralisée	Une couverture continue des zones d'intérêt, une assurance de connectivité et prolongation de la durée de vie du réseau	Temps de calcul élevé

Harizan et Kuila [50]	Couverture et connectivité : Utilise une version améliorée de NSGA (Non-dominated Sorting GA)	Centralisée	La solution évite les trous dans la connectivité, garde la couverture et prolonge la durée de vie	Solution coûteuse en terme de calcul
Karatas's protocol [51]	Couverture et connectivité : Développe des modèles d'optimisation et d'analyse basés sur les AGs	Centralisée	La solution fournit une bonne couverture	La proposition ne prend pas en compte les contraintes de connectivité et d'interférence
EasiDesign [52]	Couverture et connectivité : Utilise une version améliorée de la métaheuristique ACO	Centralisée	Garantir la couverture et la connectivité en utilisant un nombre minimum de noeuds et des chemins optimaux en termes de sauts	La solution ne prend pas en considération la consommation d'énergie
IACOSC [53]	Couverture et connectivité : Utilise une version améliorée de la métaheuristique ACO	Centralisée	Un nombre minimum des noeuds capteurs mobiles pour garantir la couverture	La solution ne prend pas en considération l'atténuation des autres performances
CIVA [54]	Couverture et connectivité : Utilise l'algorithme de déploiement immunitaire de Voronoi	Centralisée	Assurer la couverture en optimisant la consommation d'énergie	Temps de calcul assez grand

2.3.2 Approches à aspect curatif

Dans cette partie, les protocoles de routage tolérants aux pannes à aspect curatif seront classifiés selon deux classes : la première représente l'ensemble de protocoles qui tolèrent la panne des noeuds critiques et la deuxième présente les protocoles qui gèrent de façon curative les flux dans les RCSFs, basés sur le routage multi-chemin. La figure 2.3 illustre une classification des approches de tolérance aux pannes à aspect curatif.

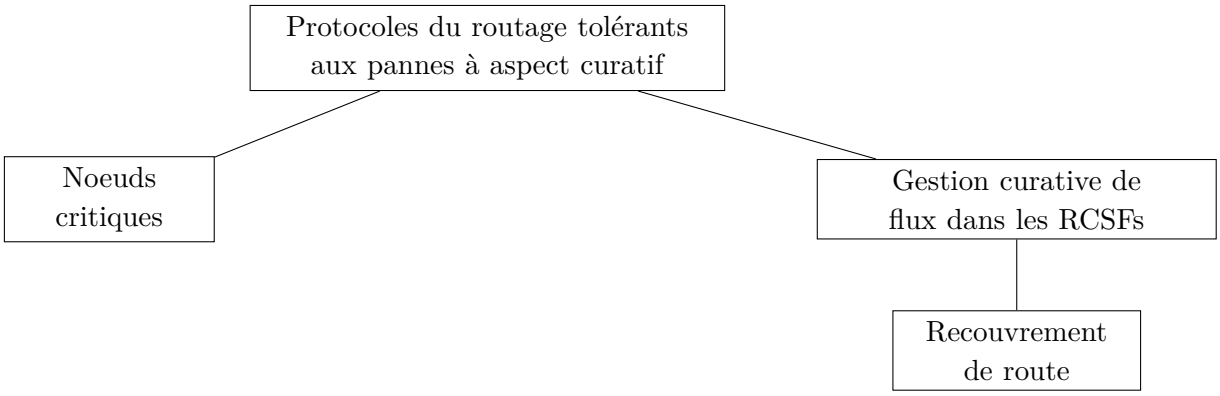


FIGURE 2.3 – Protocoles de routage tolérants aux pannes à aspect curatif

a) Gestion curative des flux dans les RCSFs

Dans cette section, nous présentons les principaux protocoles de routage tolérants aux pannes qui font appel à une gestion curative des flux dans les RCSFs. Ces protocoles permettent le recouvrement des chemins après leur défaillance.

Chouikhi et al. [55] ont proposé une solution distribuée économe en énergie pour l'allocation de plusieurs canaux. Cette solution met en oeuvre un mécanisme de tolérance aux pannes pour reconnecter le réseau après une défaillance d'un noeud d'articulation. La tâche principale de l'approche proposée est de minimiser le nombre d'interférences lors de l'allocation du nombre limité de canaux disponibles. En second lieu, l'approche minimise la consommation d'énergie en utilisant une stratégie de sommeil/activité. Le mécanisme de recouvrement après défaillance vise à rétablir la connectivité du réseau et à réallouer les canaux sans affecter l'ensemble du RCSF. Les performances de la solution proposée sont évaluées par simulation et ont montré de grands gains par rapport à d'autres solutions décrites dans la littérature.

Dans [56], les auteurs ont considéré conjointement la transmission à travers plusieurs chemins, l'équilibrage de charge et la tolérance aux pannes, afin d'améliorer la fiabilité des données transmises dans les réseaux de capteurs multimédias. Ils ont proposé un protocole de routage géographique multi-chemin renforcé par un mécanisme de tolérance aux pannes (Geographic Multipath routing protocol reinforced by Fault-Tolerant mechanism (GMFT)). GMFT utilise un mécanisme de tolérance aux pannes curatif où si un noeud constate l'absence successif des accusés de réception de son successeur, il suppose qu'il est défaillant et réagit en envoyant un message de blocage au noeud source pour éviter

la perte de paquets et augmenter le taux de livraison de données. Dès la réception d'un message de blocage, le noeud source bloque immédiatement le chemin défectueux pour choisir un autre chemin opérationnel pour router les données et assurer la connectivité. Le noeud source initie une phase de réparation locale sans avoir besoin de reconstruire un nouveau chemin reliant la source à la station de base. La réparation locale se fait en cherchant un noeud de jonction appartenant au chemin défaillant initial, et qu'il soit plus proche de la station de base par rapport au noeud défaillant. Cela permet à restaurer la connectivité sans avoir besoin de sélectionner un nouveau chemin à partir de source à la station de base. Par conséquent, le coût de recouvrement ne sera pas consistant par rapport à une solution de recouvrement de la source à la station de base. Les résultats théoriques et ceux obtenus à partir d'une étude de simulation et d'expériences sur un banc d'essai réel (testbed) ont montré la validité et l'efficacité du protocole proposé, et ont illustré qu'il est hautement conseillé pour la transmission multimédia et la stabilité des réseaux vu qu'il réduit le nombre de retransmissions inutiles et restaure la connectivité immédiatement après la panne d'un noeud.

Dans le protocole [57], les noeuds relais ont été utilisés comme noeuds d'ancrage pour les noeuds de capteurs déployés. Une heuristique a été proposée pour le placement des noeuds relais, parce que trouver le nombre minimum de noeuds relais requis pour couvrir un réseau est considéré comme un problème NP-difficile. Le protocole proposé se déroule en deux phases : la phase intra-partition et la phase inter-partitions. Dans la phase intra-partition, le protocole augmente la couverture de chaque partition vers les régions non couvertes du réseau en déplaçant les noeuds redondants vers la limite des partitions. Les noeuds sont déplacés par itérations jusqu'à la zone représentative des noeuds relais. Dans la phase inter-partitions, une approche basée sur la théorie des jeux est proposée pour restaurer la connectivité entre les partitions obtenues lors de la phase intra-partition. Dans le cas des réseaux denses l'approche utilise un noeud relais commun entre deux partitions. Le protocole proposé est analysé expérimentalement et évalué par simulation. Les résultats obtenus ont montré qu'il est plus performant que d'autres protocoles existants en termes de fiabilité et de durée de vie. Néanmoins, il ne permet d'assurer la couverture qu'au sein d'une partition et non sur l'ensemble du réseau.

Elsayed et al. [58] ont présenté une approche distribuée d'auto-recouvrement, appelée "Distributed Self-Healing Approach (DSHA)". Dans DSHA, la tolérance aux pannes concerne les noeuds capteurs membres et les CHs. Au niveau des noeuds membres, les pannes de la batterie, des capteurs et du récepteur peuvent être diagnostiqués, tandis qu'au niveau des CHs, les noeuds émetteurs et mal fonctionnels peuvent être détectés et récupérés. Comparé à d'autres protocoles, DSHA tolère jusqu'à 67,3 % des différentes défaillances matérielles au niveau des noeuds. En outre, il a atteint une précision de détection de 76,9 % pour les pannes de circuits des capteurs, 52 % pour les pannes de batteries et 71,96 % pour les pannes des récepteurs. Au niveau des CHs, 75,7 % des pannes de l'émetteur et 60 % des pannes du microcontrôleur sont réalisés. Par conséquent, le protocole permet d'augmenter la durée de vie du réseau d'une façon remarquable.

Le travail présenté dans [59] vise à concevoir un protocole de routage tolérant aux pannes à plusieurs niveaux qui prolonge la durée de vie du réseau. Il est également cohérent dans la transmission des données même lorsqu'un noeud manque d'énergie, ce qui maintient la connectivité du réseau. Dans le protocole proposé, lorsqu'un noeud capteur manque d'énergie il tente de trouver un chemin alternatif adéquat vers la station de base

en établissant dynamiquement une nouvelle connexion avec les noeuds à sa portée. Le chemin alternatif augmente la précision de la transmission des données entre les noeuds sources et leurs noeuds puits respectifs. Les simulations sur le protocole proposé ont été réalisées à l'aide du simulateur Castalia et ses performances ont été comparées à celles des protocoles flooding et de la diffusion dirigée. Les résultats de simulation ont montré que le protocole proposé fournit une consommation d'énergie et un délai de livraison des paquets de données plus faibles et un taux de livraison plus élevé par rapport aux protocoles auxquels ses performances ont été comparées. Cependant, la limitation de ce protocole est que le temps pris pour trouver un nouveau noeud voisin affecte la durée de livraison de données.

Dans [60], les auteurs ont proposé une nouvelle approche curative centralisée, appelée "Rotating Nodes based Failure Recovery (RNFR)", dédiée à la restauration de la connectivité dans les RCSFs multicanaux. La solution proposée vise la défaillance de noeuds particuliers désignés comme noeuds d'articulation, ce qui conduit à la partition du RCSF en de nombreux segments isolés les uns des autres et entraîne une perte de connectivité. Par conséquent, les principales tâches de RNFR sont la restauration de la connectivité après la défaillance d'un noeud d'articulation en utilisant la réorganisation et la réaffectation des canaux. De plus, la solution utilise une technique de rotation des noeuds pour communiquer les informations de rétablissement à toutes les parties disjointes du réseau. L'approche proposée s'est avérée intéressante en donnant des résultats motivants lors de son évaluation par simulation.

Uzun et al. [61] ont présenté deux algorithmes : "Block Movement Recovery (BMR)" et "Distributed Underwater Recovery Algorithm (DURA)". Ces deux algorithmes peuvent détecter le partitionnement du réseau dû à de telles défaillances de noeuds et rétablir la connectivité du réseau par un ajustement en profondeur contrôlé des noeuds de manière distribuée. L'idée est d'identifier d'abord si la défaillance de chaque noeud causera un partitionnement ou non en se basant sur des informations locales. Si un partitionnement doit se produire suite à la défaillance éventuelle d'un noeud particulier, BMR et DURA désignent des noeuds de secours pour gérer la récupération à l'avenir. Alors que DURA vise à localiser le processus de récupération et à minimiser la charge de mouvement sur les noeuds, BMR se charge de réduire le temps de récupération au détriment de l'augmentation de la charge de mouvement en employant un mouvement de bloc à deux phases. Les performances des approches proposées sont validées par des simulations approfondies. Les résultats ont illustré que DURA peut fournir des économies d'énergie aussi importantes qu'une approche exhaustive centralisée, tandis que BMR fournit le temps de récupération le plus rapide.

Dans [62], les auteurs ont proposé une extension de l'architecture cellulaire présentée dans [63] pour la détection et le recouvrement des pannes. Ils ont développé un nouveau mécanisme de gestion des pannes pour détecter les noeuds défaillants et rétablir la connectivité dans les RCSFs. Dans cette nouvelle version, ils ont proposé un nouveau modèle de connaissance des défaillances pour aider les noeuds capteurs à répondre aux défaillances du réseau. En outre, ils ont examiné l'efficacité de l'architecture cellulaire proposée pour la détection et la récupération des pannes. Dans l'architecture cellulaire qu'ils ont proposée, le réseau entier est une grille virtuelle de cellules. Un gestionnaire de cellules est choisi dans chaque cellule pour effectuer les tâches de gestion. Ces cellules se combinent pour former différents groupes et chaque groupe choisit l'un de ses gestionnaires de cellules

comme gestionnaire de groupe. Ils ont utilisé une structure de gestion hiérarchique pour garantir que la capacité d'autogestion est respectivement distribuée. Le cadre de gestion hiérarchique et le rôle de gestion des noeuds sont auto-adaptables dynamiquement aux changements survenant dans le réseau. Par exemple, le remplacement du gestionnaire de cellule défaillant, le transfert d'une partie de la charge de travail des noeuds capteurs dont l'état des ressources résiduelles est à un niveau critique. Les noeuds capteurs défaillants sont détectés et récupérés dans leurs cellules respectives sans affecter la structure globale du réseau. Les résultats de simulation ont prouvé l'efficacité de l'architecture cellulaire conçue.

b) Approches basées sur les noeuds capteurs critiques

Dans cette sous-section, nous présentons les principaux protocoles de routage tolérants aux pannes qui se basent sur les noeuds critiques.

Dans [64], les auteurs proposent une nouvelle mesure de centralité pour définir les noeuds importants. L'indice de centralité calcule l'importance d'un noeud en fonction de l'influence de sa suppression sur la connectivité et l'allongement du chemin le plus court entre les autres noeuds et les stations de base, ce qui a un impact sur le délai de l'acheminement des données. L'algorithme proposé détermine les noeuds capteurs qui ont un indice de centralité élevé.

Dans les protocoles de routage basés sur le clustering le noeud CH est considéré comme un noeud important vu ses tâches de collecte, d'agrégation et d'acheminement des données des membres de son cluster vers le collecteur des données. Ainsi, la tolérance aux pannes des CHs est indispensable pour assurer le bon fonctionnement du réseau où leur défaillance provoque la déconnexion du réseau et atténue ses performances. Plusieurs approches sont proposées dans le cadre de la tolérance de la panne des CHs. Dans [65], les auteurs ont proposé un mécanisme centralisé de tolérance aux pannes (Centralized Fault Tolerant Mechanism (CFTM)) pour surmonter la panne des noeuds CHs quelle que soit sa nature : permanente ou transitoire. Le mécanisme proposé est capable de maintenir la continuité de service du réseau malgré les défaillances du noeud CH en sélectionnant le meilleur membre du même cluster en terme d'énergie comme un nouveau CH. La detection de la panne se fait grâce à un compteur qui est mis à jour à chaque fois où le noeud CH ne répond pas sur le message de présence, la valeur du compteur est mise à 0 si la station de base reçoit des données du noeud CH ou une réponse sur le message de présence avant que sa valeur soit 4 sinon le noeud CH est considéré comme défaillant et la station de base lance l'opération de la sélection du nouevau CH comme présenté auparavant.

Dans [66], les auteurs proposent une méthode de tolérance aux pannes essentiellement pour garder la connectivité du réseau. En premier lieu, l'algorithme "Distributed partitioning detection and Connectivity Restoration algorithm (DCR)" détermine les noeuds critiques en se basant sur des informations topologiques locales et sur cette base, les sauvegardes appropriées pour chaque noeud sont sélectionnées. La version améliorée de DCR, appelée RAM permet de gérer la défaillance de plusieurs noeuds critiques adjacents au même temps. Après la détection de la panne d'un noeud critique par le noeud de sauvegarde, ce dernier se déplace pour remplacer le noeud défaillant. L'approche utilisée cherche des sauvegardes de manière recursive en prenant en considération la panne du noeud et sa sauvegarde.

Dans [67], les auteurs considèrent le problème de couverture minimale par noeud

pour déterminer l'ensemble des noeuds dont la défaillance diminue la valeur k de la k-connectivité. La défaillance de k noeuds déconnecte le graphe. Ainsi, pour restaurer la k-connectivité, l'approche déplace le noeud non critique le plus proche vers l'emplacement du noeud défaillant. L'augmentation de la valeur de k accroît le nombre de chemins disjoints entre les noeuds, créant ainsi des chemins alternatifs pour améliorer les performances du réseau telles que le débit, le délai de transmission et la tolérance aux pannes.

Dans [68], les auteurs proposent une approche de tolérance aux pannes des noeuds critiques dont leur défaillance partitionne le réseau, appelée NORAS. Dans NORAS, la détermination des noeuds critiques est basée sur l'identification des sommets coupés (cut vertex) où leur défaillance fragmente le réseau en partitions disjointes. Pour tolérer la panne de ces noeuds, NORAS propose de sélectionner des noeuds de sauvegarde en fonction du degré du noeud et la redondance dans la couverture. Ainsi, lors de la détection de la défaillance d'un noeud critique, le réseau est reconfiguré pour restaurer la connectivité.

Dans [69], le protocole de tolérance aux pannes est basé sur l'algorithme de détection et de récupération des partitions (PADRA) pour surmonter la défaillance d'un noeud de type cut-vertex dont sa défaillance partitionne le réseau en sous-réseaux disjoints. Ce protocole implique l'ensemble dominant connecté (Connected Dominating Set (CDS)) pour définir si un noeud est un sommet coupé ou non d'une manière proactive. Après la panne du sommet coupé, l'algorithme lance l'opération de la récupération de la panne en cherchant le noeud dominant le plus proche du noeud défaillant afin de le remplacer.

Afin de ne pas dégrader les performance du réseau dans la récupération de connectivité en cas de panne, les auteurs ont proposé une approche tolérante aux pannes appelée "Least-Disruptive topology Repair (LeDiR)" [70]. Cette approche est moins gourmande en terme de frais de restauration de connectivité. LeDiR permet de partitionner le réseau en zones en utilisant le diagramme de décomposition de Voronoï [71] en cas de panne d'un noeud critique et le noeud qui appartient à la zone disjointe la plus petite en terme de nombre de noeuds se déplace pour restaurer la connectivité.

TABLE 2.2 – Récapitulatif sur les protocoles tolérants aux pannes à aspect curatif dans les RCSFs

Protocole	Proposition	Approche	Avantages	Inconvénients
Chouikhi et al. [55]	Recouvrement de route : Un mécanisme pour reconnecter le réseau après la défaillance d'un noeud d'articulation	Distribuée	Économe en énergie et permet de restaurer la connectivité	Les solutions de tolérance aux pannes ne sont pas optimisées
GMFT [56]	Recouvrement de route : Routage géographique multi-chemin renforcé par un mécanisme de tolérance aux pannes	Distribuée	Optimisation de la consommation d'énergie et maintenance de la connectivité	La solution prend un temps pour l'exploration du nouveau chemin après la panne
Jha et al. [57]	Recouvrement de route : Utilise une heuristique pour trouver le nombre minimum de noeuds relais pour assurer la couverture dans le réseau	Centralisée	Le protocole rend le système fiable et efficace, et augmente la durée de vie du réseau	Le protocole proposé assure la couverture seulement au sein d'une partition et non sur l'ensemble du réseau
DSHA [58]	Recouvrement de route : Utilise une approche d'auto-recouvrement distribuée pour la détection, le diagnostic et la réparation des pannes des noeuds membres et des CHs	Distribuée	Amélioration de la tolérance des pannes et prolongation de la durée de vie du réseau	Le protocole ne prend pas en considération la couverture et le temps de livraison
Ajay et al. [59]	Recouvrement de route : Exploitation d'un chemin alternatif pour établir une nouvelle connexion quand un noeud capteur est sur le point d'épuiser son énergie avec ses noeuds voisins	Distribuée	Fournit une tolérance aux pannes des noeuds qui épuisent leurs batteries	Le temps pris pour trouver un nouveau noeud voisin affecte la durée de livraison de données

RNFR [60]	Couverture et connectivité : Utilisation de la coloration des graphes et le problèmes d'arbre de Steiner pour détecter et récupérer la défaillance d'un noeud d'articulation	Centralisée	Restauration de la connectivité après une défaillance	La solution n'améliore pas la durée de vie du réseau
BMR et DURA [61]	Couverture et connectivité : Utilise deux algorithmes pour détecter le partitionnement du réseau à cause de la défaillance des noeuds et rétablir la connectivité du réseau	Distribuée	Assurer la connectivité du réseau	Le protocole ne prend pas en considération la consommation d'énergie
Asim et al. [62]	Couverture et connectivité : Utilise une grille virtuelle de cellules pour la détection et la récupération des défaillances	Distribuée	La détection de pannes et la récupération de la connectivité se fait d'une façon rapide	Le protocole est basé sur l'échange des messages de contrôle ce qui influe sur l'énergie du réseau
PINC [67]	Noeuds critiques : Cut-vertex [72] où un noeud non critique avec un coût de déplacement minimum	Centralisée	Mouvements optimaux des noeuds de sauvegarde	Détermination des noeuds critiques demande un temps éleve
LeDIR [70]	Noeuds critiques : Cut-vertex où le noeud appartenant à la plus petite partition disjointe du noeud défaillant	Distribuée	Moins gourmand	Le chemin le plus court n'est pas étendu par rapport à son état de pré-échec
RAM [65]	Noeuds critiques : Cut-vertex [73] où le noeud le plus proche du noeud défaillant remplace ce dernier	Distribuée	Possibilité de gestion de plusieurs noeuds critiques	Coût plus ou moins élevé
Sitanayah [64]	Noeuds critiques : Le noeud voisin ayant le degré de centralité élevé	Centralisée	Amélioration de la robustesse du réseau	Coût plus ou moins élevé
CFTM [66]	Noeuds critiques : Le nouveau noeud CH est le meilleur membre du même cluster en terme d'énergie	Centralisée	Garde le bon fonctionnement du réseau sans atténuer ses performances	Coût plus ou moins élevé pour déterminer le nouveau CH

NORAS [68]	Noeuds critiques : Cut-vertex [74] où le nouveau CH est sélectionné en fonction du degré de noeud et la redondance dans la couverture	Distribuée	Grade la connectivité du réseau	Coût plus ou moins élevé pour sélectionner le nouveau CH
PADRA [69]	Noeuds critiques : Cut-vertex basé sur CDS où le noeud dominant le plus proche du noeud défaillant est élu comme noeud CH	Distribuée	Solution optimale en terme de distance parcourue tout en minimisant la complexité des messages	Coût plus ou moins élevé pour sélectionner le nouveau CH

2.4 Conclusion

Dans ce chapitre, une classification des protocoles tolérants aux pannes pour les RCSFs a été suggérée. Au debut, les mécanismes de tolérance aux pannes ont été classifiés selon différents critères comme il est coutumier dans la littérature. Ensuite, certains protocoles décrits dans la littérature sont classifiés sur la base de l'architecture temporelle en précisant le mécanisme de tolérance aux pannes utilisé.

Dans l'architecture temporelle, les protocoles de routage tolérants aux pannes sont classifiés selon le temps de déclenchement de l'opération de la tolérance aux pannes si elle est exécutée avant ou après la panne. Ces protocoles sont classés selon deux aspects : aspect préventif et aspect curatif. D'autre part, certains protocoles basés sur la tolérance aux pannes des noeuds critiques sont exposés.

En mettant l'accent sur les protocoles cités dans l'état de l'art, nous sommes arrivés à nos contributions dans le cadre de tolérance aux pannes dans les RCSFs. Ces contributions avec les simulations et les discussions de résultats vont être présentées dans les chapitres suivants.

Chapitre 3

Une approche de tolérance aux pannes basée sur l'augmentation dans les RCSFs

Chapitre 3

Une approche de tolérance aux pannes basée sur l'augmentation dans les RCSFs

3.1 Introduction

Un réseau de capteurs sans fil (RCSF) est généralement composé d'un grand nombre de micro-dispositifs appelés capteurs, capables de détecter, collecter et transmettre de manière autonome des données à une station de base distante. Les données collectées par les noeuds capteurs sont généralement relayées à la station de base à l'aide d'un système de routage multi-sauts puisque le rayon de communication des noeuds capteurs est restreint et il y a des obstacles possibles dans la région de déploiement.

Les RCSFs et l'Internet des objets (Internet of Things (IoT)) envahissent progressivement divers domaines à travers de nombreuses applications, notamment les applications militaires, commerciales, médicales et de surveillance environnementale. Cependant, dans les RCSFs, des défaillances peuvent se produire en raison de l'épuisement de l'énergie des noeuds capteurs, des risques environnementaux, des défaillances matérielles, des erreurs de liaison de communication, etc. Ces défaillances peuvent les empêcher d'accomplir leurs tâches. De plus, dans les applications critiques, ces défaillances peuvent entraîner un désastre. Ainsi, il est nécessaire d'établir un schéma efficace de tolérance aux pannes dans ce type de réseaux pour garantir la livraison des données à la station de base lorsque certains noeuds cessent de fonctionner correctement. En outre, les approches de routage dédiées à ce type de réseaux devraient fournir de meilleures performances en tolérance aux pannes et qualité de service (QoS) pour les nouvelles applications et surtout les applications critiques qui nécessitent une fiabilité de détection et de routage.

De plus, en raison de la fragilité des noeuds de capteurs et les environnements hostiles dans lesquels ils sont déployés.Ces deux paramètres les rendent très vulnérables aux pannes. A cet effet, il est primordial de fournir des propriétés telles que la tolérance aux pannes et la conservation de l'énergie pour assurer leur bon fonctionnement pour une longue durée. Dans cette optique, plusieurs approches et travaux ont été proposés dans la littérature pour surmonter ces défis.

Dans la littérature, il existe plusieurs approches qui ont traité le problème de la tolérance aux pannes dans les RCSFs à savoir les approches qui sont basées sur l'utilisation

de plus d'un chemin vers la station de base [38, 39, 41, 75], les approches qui offrent une double couverture de n'importe quel point de la zone de déploiement des capteurs [76], les approches qui se basent sur la stratégie des noeuds et/ou liens disjoints [40, 42], les solutions de routage basées sur le clustering qui permettent une tolérance préventive aux pannes [4, 6, 77, 78]. Comme il existe des solutions qui se basent sur les noeuds critiques pour mettre en oeuvre des mécanismes de tolérance aux pannes dans les RCSFs [67, 79–82].

Dans ce chapitre, nous nous concentrons sur les solutions basées sur l'impact de la détection des noeuds critiques pour améliorer les performances des RCSFs. Nous proposons une approche de tolérance aux pannes dans les RCSFs [5]. Cette approche est basée sur le problème d'augmentation après la détection des noeuds critiques dans le réseau de capteurs considéré. Le principe de cette approche est d'ajouter des liens inexistants pour préserver la connectivité du réseau en cas de panne des noeuds critiques. Cette opération est équivalente à ajouter des arêtes inexistantes dans un graphe, mais dans les RCSFs, il s'agit d'ajouter des liens radios en ajustant leur niveau de puissance de transmission pour pouvoir envoyer des données à des noeuds de capteurs qui n'étaient pas dans leur portée de transmission initialement. Néanmoins, le réglage du niveau de puissance nécessite une consommation d'énergie supplémentaire, ce qui nous amène à faire un ajustement très précis pour ne pas augmenter la consommation d'énergie dans le réseau considéré.

En outre, l'approche proposée permet à un protocole de routage de tolérer la défaillance des noeuds critiques. Elle est exécutée en deux phases. Dans la première phase, un algorithme génétique hybride avec une heuristique de recherche locale appelée GA-CNP (Genetic Algorithm-Critical Node Problem) est utilisé pour sélectionner les noeuds critiques et dans la deuxième phase, un algorithme appelé Aug-CNP est impliqué pour traiter le problème d'augmentation en déployant des liens sans fil supplémentaires pour préserver la connectivité du réseau en cas de défaillance d'un noeud critique. Notre contribution a été développée à l'aide du simulateur OMNET++ [83] et le framework Castalia [84], évaluée et comparée au protocole AODV (Ad-hoc On-demand Distance Vector) [85]. Les résultats de simulations ont montré que l'algorithme GA-CNP sélectionne les noeuds critiques dont leur défaillance peut dégrader la durée de vie du réseau avec un taux de 40 %. De plus, l'algorithme Aug-CNP appliqué au protocole AODV apporte des améliorations en termes de durée de vie du réseau de l'ordre de 22% par rapport au protocole AODV traditionnel.

3.2 Contexte

Nous présentons d'abord quelques notions de la théorie des graphes qui sont nécessaires à la compréhension de notre contribution. Tous les graphes présentés dans ce travail sont finis, c'est-à-dire que le nombre de sommets est fini.

Soit le graphe $G=(V,E)$ où V est l'ensemble des sommets (noeuds) et E représente l'ensemble des arêtes (liens). Soit A un sous-ensemble de V ($A \subseteq V$). Nous notons $G[S]=(A,E(S))$ le sous-graphe de G induit par S comme c'est présenté dans l'équation (3.1). Le sous-graphe induit par $V \setminus S$ est étiqueté $G[V \setminus S]$. Si G est un graphe orienté, le lien (u,v) est un arc dirigé à partir du noeud u au noeud v.

$$E(S) = \{(u, v) \in E \mid \quad u, v \in S\} \tag{3.1}$$

Un chemin dans G est une suite ordonnée de noeuds $(v_1,\ v_2,\ \cdots,\ v_k)$ où chaque paire de noeuds qui se suivent dans le chemin (v_i, v_{i+1}) est une arête dans E. Deux noeuds sont dits connectés si chacun peut atteindre l'autre directement ou via d'autres noeuds intermédiaires.

Un sous-ensemble A de V $A \subseteq V$ est appelé un ensemble de sommets coupés (cut vertex set) de G ; si la suppression de tous les sommets de A de G déconnecte G.

Un ensemble indépendant de G est un sous-ensemble de sommets $S \subseteq V$, où deux sommets de S ne sont pas adjacents. Cet ensemble indépendant est dit maximal si aucun ensemble indépendant ne le contient correctement. Un ensemble indépendant de cardinalité maximale est appelé un ensemble indépendant maximal.

Dans les réseaux complexes, les sommets ont des degrés d'importance variables. Dans la littérature, ces sommets (noeuds) sont apparus sous différents noms, tels que : noeuds les plus influents [86], noeuds les plus vitaux [87, 88], noeuds de centralité [89], noeuds d'acteurs clés (key-player nodes) [90]... etc. Ces types de noeuds ont été largement étudiés dans les réseaux sociaux. Récemment, un nouveau concept d'évaluation des noeuds importants a été introduit, appelé noeuds critiques, où un noeud est considéré comme un noeud critique si sa défaillance affecte substantiellement les performances du réseau. Ainsi, une fois que les noeuds critiques sont identifiés, ils peuvent être surveillés de manière défensive pour un ajustement positif ou tentés de manière offensive pour un ajustement négatif.

L'objectif du problème de noeuds critiques est de détecter les noeuds où leur suppression a un impact négatif sur le niveau de connectivité du réseau. Ce niveau de connectivité est modélisé comme une métrique à satisfaire. De nombreuses métriques de connectivité ont été proposées dans la littérature : maximiser le nombre de composants connectés [91,92], réduire la connectivité par paires [93], limiter la taille du plus grand composant à une valeur donnée [94].

Nous illustrons cette taxonomie à travers l'exemple suivant. En considérant le graphe de la Figure 3.1, nous supposons que seulement deux noeuds critiques doivent être détectés. Pour optimiser le nombre de composants, la meilleure solution consiste à supprimer les noeuds v_{11} et v_{10}, ce qui donne sept composants. Pour réduire la taille maximale du composant, la meilleure solution consiste à supprimer les noeuds v_{10} et v_{13}, ce qui donne un composant plus grand avec cinq noeuds. Pour augmenter le nombre de paires perturbées, la solution idéale consiste à supprimer le noeud v_{11}, ce qui perturbe la communication entre v_4 et 12 paires de noeuds. Ces problèmes d'optimisation ne sont donc pas équivalents.

3.3 Travaux connexes

La tolérance aux pannes dans les RCSFs est un problème qui a été abordé par plusieurs chercheurs en proposant différentes approches. Dans ce contexte, il existe des solutions qui sont basées sur l'implication de plusieurs chemins dans le processus de routage de données entre les noeuds sources et la station de base [38, 39, 41, 75]. Ces solutions visent à garantir la fiabilité de routage de données dans les RCSFs en permettant de trouver très rapidement un chemin alternatif lorsque le chemin principal échoue. Cependant, ces solutions sont coûteuses en termes de consommation d'énergie et de temps de recherche des différents chemins qui relient un noeud source à la station de base.

D'autres solutions offrent une double couverture de n'importe quel point de la zone

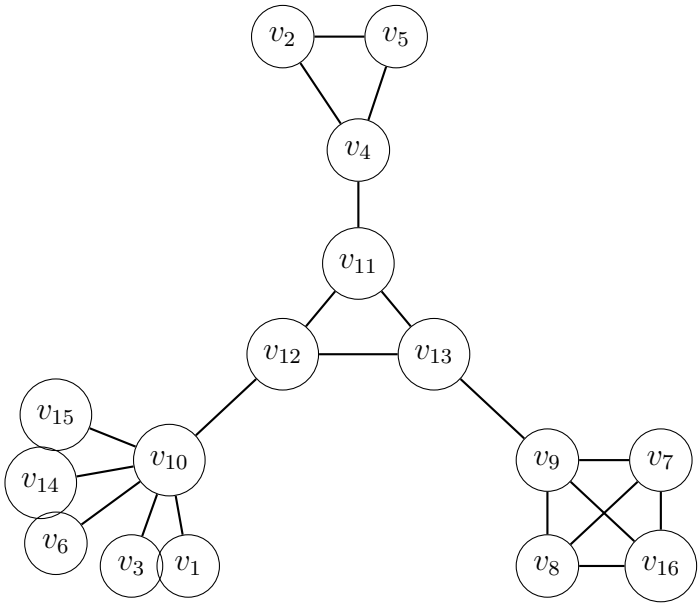


FIGURE 3.1 – Exemple illustratif de CNP (Critical Node Problem)

d'intérêt, comme celle présentée dans [76]. D'autres solutions se basent sur la stratégie des noeuds et/ou liens disjoints [40,42]. Dans [40], la solution proposée utilise le meilleur chemin de la source à la destination avec des noeuds n'appartenant à aucun autre chemin et dans [42], Ganesan et al. ont proposé une solution de tolérance aux pannes basée sur plusieurs chemins partiellement disjoints. Comme il existe des solutions de routage basées sur le clustering qui permettent d'assurer une tolérance préventive aux pannes vu que le clustering améliore la durée de vie du réseau en minimisant les échanges de messages [4,6,77,78,95–97]. Dans [77], le protocole proposé vise à préserver la couverture du réseau, où en cas de défaillance d'un noeud CH, chaque membre de son cluster rejoint le CH actif le plus proche. Dans [95], les auteurs proposent une architecture clusterisée basée sur la technique PSO pour la tolérance aux pannes dans les RCSFs. L'architecture proposée tolère la défaillance du noeud CH en le remplaçant par un noeud de substitution. Le noeud CH informe le noeud de substitution avant que son énergie ne soit épuisée et ce dernier informe les membres du cluster qu'il est le nouveau CH du cluster. Dans [96], le protocole proposé offre une tolérance aux pannes en minimisant l'énergie de la recherche de chemins à l'aide d'un algorithme Q-learning basé sur l'apprentissage par renforcement. Il permet de tolérer la défaillance du noeud CH en sélectionnant un nouveau noeud qui a le maximum d'énergie résiduelle en tant que noeud CH. Dans [97], les noeuds sont classés en quatre catégories : noeud normal, noeud de trafic, noeud final et noeud mort. Le noeud normal est soit un noeud CH soit un membre du cluster. Si l'énergie du noeud CH diminue au dessous d'un certain seuil, son rôle est changé en noeud de trafic. Un noeud de trafic peut retrouver son rôle de noeud CH, si le noeud CH consomme son énergie de manière significative. Si le circuit récepteur d'un noeud tombe en panne, ce dernier ne participe pas dans le processus de routage et son rôle est transféré à un noeud final. La notion de noeuds critiques ou de noeuds importants est utilisée dans plusieurs travaux pour améliorer la tolérance aux pannes dans les RCSFs et pour augmenter leurs performances. La bonne détermination des noeuds critiques du réseau et la prévention des défaillances

de ces noeuds aident à maintenir la connectivité du réseau et améliorer sa durée de vie. En outre, l'identification des noeuds critiques dans les RCSFs dépend de la connectivité du réseau et de certaines mesures de performances (durée de vie, latence, énergie) que nous recherchons après la suppression des noeuds.

L'identification des noeuds les plus critiques est très utile dans de nombreuses applications dans un certain nombre de domaines tels que la gestion des risques des réseaux [98], l'évaluation de la vulnérabilité des réseaux [99], les études de molécules biologiques [100, 101], l'immunisation des réseaux [102] et les communications dans les réseaux [82].

Dans la littérature, la définition des noeuds critiques dans les RCSFs varie en fonction des paramètres de performances à optimiser dans le réseau tels que : la latence, la durée de vie, la transmission des données, et des paramètres de graphe structurels tels que la connectivité et la centralité (voir la Figure 3.2 pour plus de détails). Dans ce contexte, plusieurs approches basées sur les noeuds critiques pour assurer la tolérance aux pannes dans les RCSFs ont été proposées à cette fin [67, 79–82].

Dans [67], Akram et al. utilisent l'algorithme du minimum de sommets (minimum vertex algorithm) pour définir les noeuds critiques dans le réseau où leur défaillance décrémente la valeur k qui représente le niveau de connectivité dans le réseau (k-connectivité). Pour préserver la k-connectivité dans le réseau, l'approche déplace le noeud non critique le plus proche vers l'emplacement du noeud critique défaillant. Les auteurs ont considéré un graphe k-connecté i.e un graphe G dont la coupe minimale de sommets a au moins k sommets. La réduction de la valeur de k peut avoir un impact significatif sur les performances du réseau. Les auteurs ont défini les noeuds critiques comme l'union de toutes les coupes minimales des sommets où $(V \backslash C)$ représente l'ensemble des noeuds non critiques. Il est clair qu'une défaillance de tout noeud critique $v \in C$ réduit la connectivité k de 1 et affaiblit la tolérance aux pannes du réseau. Pour surmonter cette anomalie, ils ont proposé un algorithme de restauration de connectivité qui déplace un noeud non critique avec un coût de déplacement minimal vers la position du noeud critique défaillant. D'autres travaux pour cette mesure peuvent être trouvés dans [103–105].

Dans [79], la suppression des noeuds critiques est utilisé pour optimiser la latence. La méthode proposée est basée sur le modèle MIP (Mixed-Integer Programming). Cependant, l'inconvénient de ce modèle est que la suppression des noeuds critiques se fait de manière itérative les uns après les autres, ce qui augmente le temps de calcul. Yildiz et al. [80] ont appliqué le même principe qu'en [79] dans le but d'améliorer la durée de vie du réseau. Dans [81], les auteurs déterminent l'état d'un noeud (critique ou non critique) à l'aide d'algorithmes distribués. Ils ont proposé deux algorithmes pour traiter le problème du noeud critique. Le premier algorithme basé sur l'ensemble dominant connexe (CDS) et permet de sélectionner les noeuds dominants les plus critiques et non critiques. Le deuxième algorithme est basé sur le premier, son principe est de trouver le statut de tous les noeuds en appliquant un algorithme de recherche distribué dans les régions non reconnues du réseau. Ce protocole n'est pas énergivore puisqu'il détermine l'état des noeuds avec moins d'énergie. Hoffmann et Wanke [82] ont proposé une solution pour résoudre le problème d'augmentation de voisinage de noeud en ajoutant un nombre minimum d'arêtes, ce qui fournit un sous-graphe connexe du graphe de communication. Cette solution permet de tolérer la défaillance d'un noeud en diffusant le message dans son voisinage.

Dans [106], les auteurs ont défini les noeuds critiques comme un ensemble de noeuds dont la suppression aura le plus d'impact sur la latence du réseau. Ils ont proposé une approche basée sur le modèle "Mixed-Integer Programming (MIP)" pour évaluer l'impact de ces noeuds en termes de latence. Dans le même contexte, Yuksel et al. [79] ont proposé une approche basée sur le modèle "Linear Programming (LP)" pour évaluer l'impact de la suppression des noeuds les plus critiques sur la durée de vie dans les RCSFs. Bien que les modèles MIP et LP fournissent des résultats exacts. Ils présentent certains inconvénients en raison du temps d'exécution élevé et de la complexité. Pour dépasser ces limites, Sembroiz et al. [107] ont proposé deux métaheuristiques de recherche adaptatif randomisé pour identifier les noeuds critiques lorsque les métriques de performances sont respectivement la latence et la durée de vie.

Liu et al. [108] ont proposé une approche pour déterminer les noeuds critiques en tenant compte de la consommation d'énergie et de la durée de vie nodale. En outre, dans [109], les auteurs ont introduit une méthode basée sur un modèle de champ d'énergie dans les RCSFs qui évalue l'importance des noeuds à l'aide de la transmission de données. Néanmoins, le principal inconvénient des noeuds critiques basés sur les métriques de performances est que la suppression des noeuds critiques se fait de manière itérative les uns après les autres, ce qui augmente le temps de calcul.

Pour la métrique de connectivité, les noeuds de capteurs peuvent cesser de fonctionner pour plusieurs raisons et le réseau peut se diviser en deux ou plusieurs partitions déconnectées. En théorie des graphes, nous les appelons sommets coupés (cut vertex). La détection des sommets coupés est un domaine de recherche important pour diverses applications dans les RCSFs [107, 110]. Les algorithmes de détection de sommets coupés disponibles dans la littérature peuvent être divisés en deux catégories : algorithmes distribués [81, 111–113] et algorithmes centralisés [107, 110].

Certains concepts utilisés dans l'analyse des réseaux sociaux, tels que les indices de centralité [114], jouent un rôle clé dans les RCSFs car ils permettent de déterminer l'importance d'un noeud dans un réseau. Pour mesurer ce type de paramètres, plusieurs indices ont été proposés dans la littérature, tels que le degré, la proximité et la centralité intermédiaire. Dans [64], Sitanayah a introduit un nouvel indice de centralité appelé centralité des défaillances, qui est une combinaison entre la connectivité et la longueur du chemin le plus court pour le reste du réseau. Elle a utilisé cette centralité des défaillances pour identifier les noeuds critiques qui ont besoin de noeuds de sauvegarde afin de maintenir le système global fonctionnel. Dans [115], les noeuds critiques sont identifiés à l'aide d'une nouvelle mesure de centralité appelée connectivité et centralité de réacheminement à contrainte de longueur (l-CRC). Cette mesure est basée sur l'idée que la défaillance d'un noeud critique peut faire perdre à d'autres noeuds leurs chemins d'accès vers les noeuds puits.

Yin et al. [116] ont proposé une nouvelle évaluation de l'importance des noeuds, appelée *MADME*, qui combine certaines métriques de performances des RCSFs avec des paramètres de graphe structurel. Ils ont considéré quatre indicateurs : degré de centralité, nombre d'arbres couvrants, délai et la consommation d'énergie du réseau. Néanmoins, le principal inconvénient des problèmes de noeuds critiques basés sur des paramètres de graphe structurel est que ces approches ne prennent pas en compte le degré de fragmentation du réseau.

La première définition de CNP (problème des noeuds critiques) a été introduite par Arulselvan et al. [93]. Cette définition a été inspirée de l'étude menée par Borgatti sur

les key-players [117]. Arulselvan et al. ont présenté deux variantes du problème de détection des noeuds critiques : le problème CNP [93] et le problème des noeuds critiques contraint par la cardinalité (CC-CNP) [118]. Ils ont déduit des formulations mathématiques et proposé des approches heuristiques pour les résoudre dans des graphes généraux. Dans [94], Lalou et al. ont introduit un nouveau type de CNP, qui est le problème des noeuds critiques sous contraintes de cardinalité des composantes (Component-Cardinality-Constrained Critical Node Problem (3C-CNP)). Dans 3C-CNP, ils cherchent à trouver un ensemble minimal de sommets, délimitant la cardinalité de chaque composante connexe dans le graphe induit. Ils essaient de déterminer un ensemble minimal de sommets, délimitant la cardinalité de chaque composante connexe dans le graphe induit. Ils ont démontré la NP-hardness du problème 3C-CNP sur un graphe de degré maximum $\triangle = 4$.

Dans les réseaux sans fil, la détection des noeuds critiques peut être effectuée par deux approches : défensive et offensive. En fait, ce sont ces noeuds qui doivent soit être supprimés pour désactiver la capacité de communication du réseau, soit conservés pour empêcher toute tentative de dégradation de la connectivité du réseau. Dans [119], les auteurs ont étudié le problème d'interférences dans les réseaux sans fil. Cette étude vise à définir les emplacements des dispositifs d'interférences afin de les désactiver dans les réseaux sans fil. Diverses définitions de programmation mathématique basées sur la couverture des noeuds et la limitation de l'indice de connectivité des noeuds ont été proposées. L'objectif principal de ce travail est de minimiser le coût total des interférences de sorte que l'indice de connectivité de chaque noeud ne dépasse pas la valeur seuil.

Dans [93], les auteurs considèrent la variante de "Critical node detection problem (CNDP)" telle que présentée dans l'équation (3.2) avec les entrées suivantes : Graphe G=(V,E) et l'entier k,

$$A = argmin \sum_{i,j \in A} u_{ij}(G(V \setminus A)) : |A| \leq k \tag{3.2}$$

où

$$u_{ij} = \begin{cases} 1 & \text{Si i et j sont dans la même composante de } G(V \setminus A) \\ 0 & \text{Sinon} \end{cases}$$

L'objectif dans cette variante de CNDP est de trouver un sous-ensemble $S \subseteq V$ contenant au moins k sommets, dont la suppression minimise le nombre de paires de noeuds connectés (connectivité par paires) parmi les sommets dans le graphe résiduel. Il a été prouvé que ce problème est NP-complet [93].

Considérons l'exemple présenté dans la Figure 3.2. Il est clair que le noeud v_6 possède la meilleure centralité, incluant les mesures de degré, de proximité et d'intermédiarité (betweenness), mais sa suppression ne fragmente pas le réseau. En revanche, si nous sélectionnons les sommets coupés de taille 1 comme noeuds critiques, nous obtenons trois cas possibles : v_1, v_8 et v_{13}. La suppression de v_8 ou de v_{13} permet d'isoler un seul sommet. Cependant, la suppression du noeud v_1 divise également le graphe en deux composantes, mais davantage de paires de sommets (connectivité par paires) seraient séparées les unes des autres. Nous pouvons constater que la taille des composantes créées par la suppression d'un sommet coupé n'est pas prise en compte dans cette mesure. Néanmoins, la variante du CNDP définie dans l'équation 3.2 renvoie uniquement le noeud v_1 comme noeud critique. Il est prouvé dans [93] que l'optimisation de la fonction objectif de CDNP maximise non

seulement la connectivité par paires entre les noeuds restants, mais minimise également la variance des cardinalités des composantes.

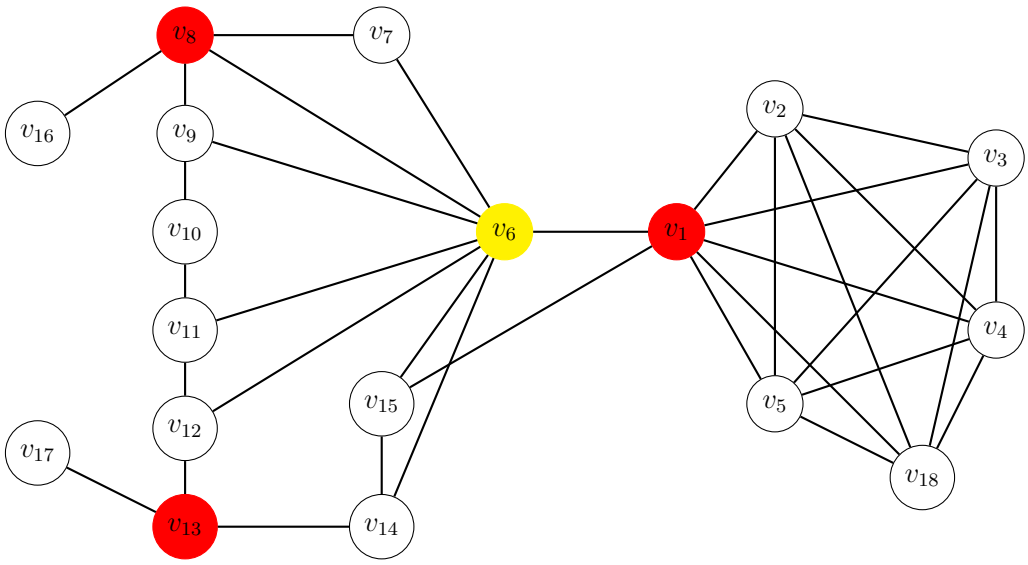


FIGURE 3.2 – Solutions optimales pour différentes variantes de noeuds critiques où un seul noeud est supprimé : degré de centralité

La figure 3.3 résume des variantes des noeuds critiques décrites dans les différentes approches de tolérance aux pannes dans les RCSFs.

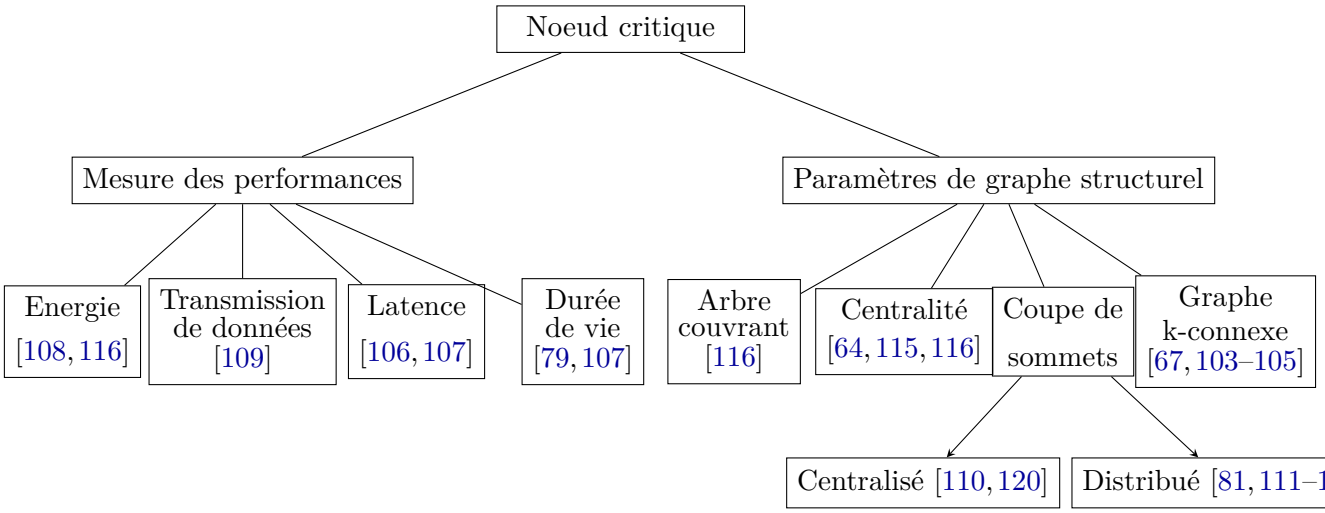


FIGURE 3.3 – Classification des variantes des noeuds critiques dans les RCSFs

Pour évaluer et détecter les noeuds critiques dans les RCSFs, les recherches précédentes se sont concentrées sur le problème de la coupe des sommets, ce qui est inadéquat puisque les informations dynamiques affectent également le résultat de l'évaluation. Dans la section

suivante, nous proposons une nouvelle approche basée sur les algorithmes génétiques pour résoudre le problème 3C-CNP dans les RCSFs. L'approche proposée réduit de manière significative les coûts de communication et la vitesse de détection des noeuds critiques, et s'adapte aux changements de topologie dans les RCSFs.

3.4 Contribution

La contribution proposée est divisée comme suit : tout d'abord, nous modélisons le réseau de capteurs comme un graphe non orienté G=(V,E). Ensuite, nous proposons un algorithme génétique hybride avec une approche de recherche locale pour résoudre le CNDP sur le graphe $G = (V, E)$. Nous obtenons ainsi un ensemble de noeuds critiques S. Ensuite, nous étudions l'impact de la suppression des noeuds critiques sur le graphe $G[V \setminus S]$. Enfin, nous définissons un nouveau problème d'augmentation des arêtes pour réduire l'impact des noeuds critiques sur le graphe G. Les étapes d'exécution de notre contribution sont représentées comme le montre la Figure 3.4.

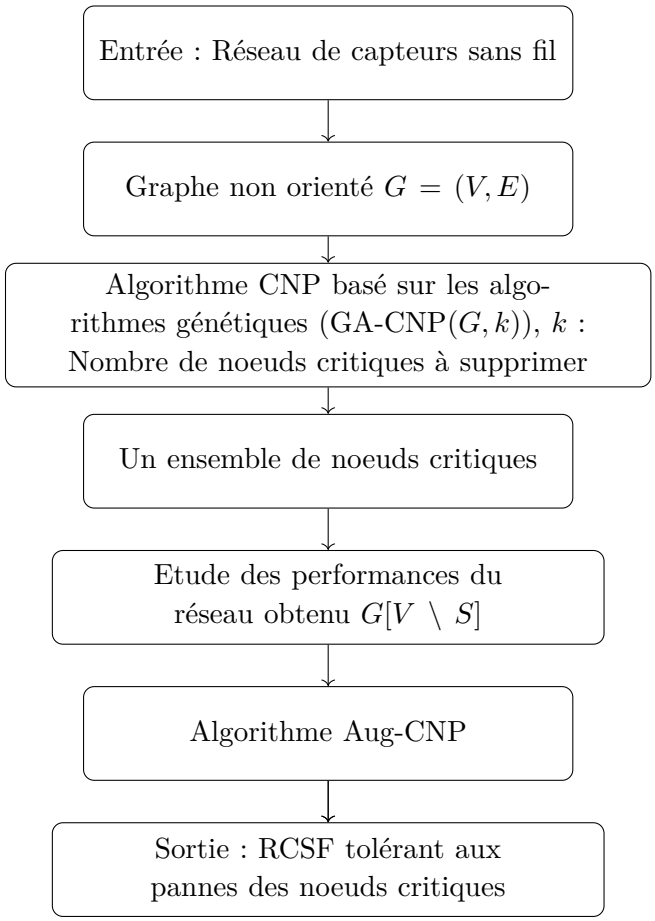


FIGURE 3.4 – Organigramme de notre contribution

3.4.1 CNP basé sur l'algorithmes génétique (GA-CNP)

Les algorithmes génétiques (AGs) sont largement utilisés dans la littérature pour résoudre les problèmes d'optimisation dans les RCSFs, tels que le routage [109, 121], la localisation [122, 123], la tolérance aux pannes [124, 125]. Dans la contribution proposée, nous proposons d'abord un algorithme génétique pour résoudre le problème de la variante CNDP décrit dans l'équation 3.2. Le résultat de cet algorithme est un ensemble de noeuds critiques qui maximise la connectivité par paire dans le graphe $G = (V, E)$.

Dans cette section, nous proposons une approche CNP basée sur les algorithmes génétiques pour résoudre le problème des noeuds critiques. Les performances de l'approche proposée dépendent principalement de la fonction de fitness. La solution GA-CNP proposée est décrite dans l'algorithme suivant (Algorithme 1).

Algorithm 1 GA-CNP

1: **Begin**
Input : Graphe *G=(V,E)*, k : Nombre de sommets à supprimer, P : Taille de la population et T : Nombre de générations
Output : $A = argmin\ \sum_{i,j \in A} u_{ij}(G(V \backslash A)) : |A| \leq k$, comme présenté dans l'équation (3.2)
2: Générer aléatoirement une population initiale de taille P en supprimant k sommets de G pour chaque chromosome individuel.
3: Calculer la valeur de fitness de chaque chromosome à l'aide de la fonction objectif définie dans l'équation (3.3).
4: Appliquer la stratégie de sélection $\mu + \lambda$ pour éliminer la solution la moins optimale.
5: Les opérateurs de croisement et de mutation sont appliqués à un nombre λ de chromosomes pour produire la prochaine génération.
6: Répéter les étapes 3 à 5 pour un nombre de générations égal à T.
7: Soit S la solution du graphe ayant la valeur de fitness la plus élevée.
8: S^* = localSearch(S)
9: Retourner la meilleure solution S^*
10: **End**

a) Représentation des chromosomes

Le codage des chromosomes joue un rôle important dans les algorithmes génétiques. Dans la solution proposée, un modèle de codage binaire est employé pour chaque solution, de sorte que chaque chromosome est représenté comme un tableau A de n sommets, où n est l'ordre du graphe d'entrée G. Lorsqu'un sommet v est choisi pour être supprimé, le gène correspondant dans le chromosome est mis à 0, sinon il est mis à 1. La Figure 3.5 montre la représentation d'une solution candidate. Dans cette figure, deux sommets sont supprimés dans G.

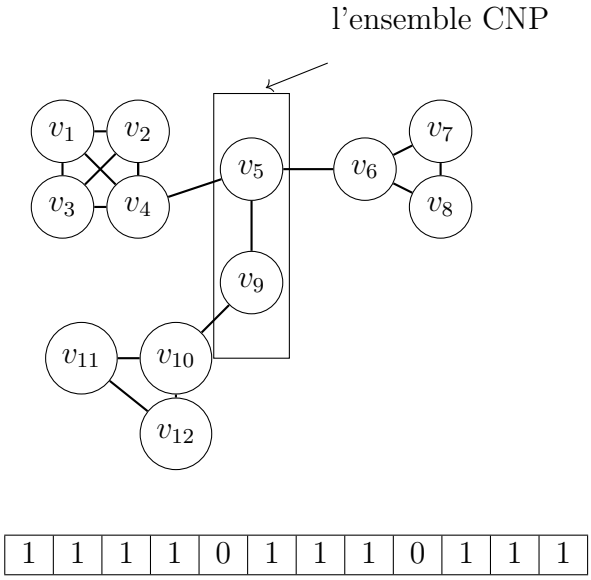


FIGURE 3.5 – Un exemple de représentation d'un chromosome

b) Population initiale et fonction de fitness

La vitesse de convergence des algorithmes génétiques dépend fortement de la qualité de la population initiale. Les chromosomes sont générés aléatoirement à la première génération. La taille de la population initiale *(P)* a été fixée en fonction de l'ordre du graphe G. Puisque les chromosomes sont produits aléatoirement après les opérations de croisement et de mutation, la plupart d'entre eux peuvent ne pas être en mesure de fournir une bonne solution pour CNP. Par conséquent, les solutions candidates appropriées doivent être choisies en fonction de la valeur de fitness déterminée par la connectivité par paires dans le graphe restant après avoir supprimé k sommets. Rappelons que $\sum_{i,j \in V} u_{ij}$ est une mesure de la connectivité totale par paires du graphe. Nous remarquons que puisque u_{ij} est binaire et égal à 1 si et seulement si i et j sont dans la même composante dans la solution optimale, la fonction de fitness peut être exprimée selon l'équation 3.3.

$$\sum_{K \in M} \frac{\sigma_h(\sigma_h - 1)}{2} \tag{3.3}$$

où M est l'ensemble de toutes les composantes connectées maximales et σ_h est la taille de la $h^{ième}$ composante, qui peut être facilement identifiée par des algorithmes rapides tels que les algorithmes de recherche de type breadth-first ou depth-first dont la complexité en temps est $O(|E|)$ en utilisant une représentation de liste d'adjacence du réseau [93].

c) Sélection

Dans cette étape, nous attribuons d'abord un rang à chaque solution individuelle en fonction de sa valeur de fitness. La valeur de fitness de chaque solution (individu) est calculée sur la base de la fonction objectif définie dans la section précédente. Dans notre approche, nous utilisons la stratégie $\mu + \lambda$ pour sélectionner les chromosomes de la prochaine génération où la moitié supérieure des individus ayant une meilleure valeur de fitness est sélectionnée.

d) Opérateur de croisement (crossover)

Dans cette étape, notre algorithme combine les caractéristiques des deux chromosomes pour générer de nouveaux chromosomes afin d'obtenir une solution optimale. Pour l'opération de croisement, nous utilisons un croisement à point unique qui peut garantir une fragmentation maximale du graphe chez l'individu enfant. Étant donné deux individus parents arbitraires et un tableau binaire aléatoire est créé comme indiqué sur la Figure 3.6. Le nombre de chromosomes qui subissent l'opération de croisement est déterminé par un paramètre appelé probabilité de croisement.

Chromosome 1	11011	00100110110
Chromosome 2	00100	11100011110
Offspring 1	11011	11100011110
Offspring 2	00100	00100110110

FIGURE 3.6 – Opération de croisement

e) Mutation

La mutation est un processus qui augmente l'exploration de l'espace de recherche en introduisant des variations aléatoires dans la population. Dans notre travail, nous sélectionnons aléatoirement deux gènes tels qu'ils ne sont pas identiques dans les positions correspondantes du tableau A et n'ont pas la même valeur binaire, et nous les échangeons.

f) Recherche locale

La dernière étape de notre contribution consiste à faire apple à une stratégie de recherche locale itérative dans le but est d'améliorer la solution actuelle. Cette stratégie est exécutée selon l'algorithme 2. L'idée de cet algorithme est inspirée de l'algorithme de recherche locale proposé dans [93].

D'après les résultats expérimentaux, nous avons observé que l'algorithme GA-CNP converge très rapidement vers la solution optimale pour les graphes à faible et moyenne densité, et ne nécessite pas beaucoup de temps pour converger vers la meilleure solution dans les graphes denses.

Algorithm 2 LocalSearch(Chromosome S)

```
1: Begin
2: S* = S ;
3: bol=true ;
4: while bol==true do
5:    bol=false
6:    for 1 ≤ i ≤ n do
7:       for i + 1 ≤ j ≤ n − 1 do
8:          if (S[i] == 0 and S[j] == 1) or (S[i] == 1 and S[j] == 0)  then
9:             swap(S[i],S[j])
10:            if f(S) ≤ f(S*) then
11:               S* = S
12:               bol=true ;
13:            end if
14:         else
15:            swap(S[i],S[j]) ;
16:         end if
17:      end for
18:   end for
19: end while
20: return S*
```

3.4.2 Tolérance aux pannes basée sur l'augmentation du graphe

D'après la comparaison des résultats expérimentaux de la section précédente, nous pouvons constater que l'élimination des noeuds critiques affecte considérablement la durée de vie du réseau. Pour surmonter ce problème, nous étudions le problème de l'ajout de liens sans fil supplémentaires pour augmenter la connectivité d'un RCSF.

En théorie des graphes, le problème de l'augmentation consiste à ajouter un nombre minimal d'arêtes à un graphe donné G de sorte que le graphe résultant ait la propriété P. Ce problème a été largement étudié en tant que sujet important dans la conception des réseaux, et de nombreux paramètres ont été développés jusqu'à présent.

Dans [82], Hoffmann et Wanke ont considéré un nouveau problème d'augmentation des arêtes appelé *"Locally Connected Augmentation Problem (LCAP)"*. Soit $G = (V, E)$ un graphe non orienté, $LCAP$ requiert un ensemble minimal E' d'arêtes supplémentaires tel que les voisinages définis par G induisent des sous-graphes connectés du graphe augmenté $G' = (V, E \cup E')$. Ce problème peut être formulé comme suit

> **Input :** Un graphe non orienté $G = (V, E)$. **Output :** Un ensemble de nouvelles arêtes E' de cardinalité minimale tel que pour chaque sommet $v \in V$, le voisinage *NG(v)* induit un sous-graphe connecté de $(V, E \cup E')$.

La NP-hardness de $LCAP$ a été prouvée par Hoffmann et Wanke [82] en utilisant une réduction en temps polynomial du problème de satisfaisabilité.

Theorem 1 ([82]). *Le problème d'augmentation pour obtenir un graphe localement connecté est un problème NP-complet*

Ce type de problèmes est très utile pour les RCSFs car il décrit la capacité des réseaux à réparer de manière réactive les chemins de routage dans une zone locale après la défaillance d'un noeud. Dans un réseau localement connecté, un chemin de routage peut être récupéré après la défaillance d'un noeud en diffusant simplement le message à travers le sous-graphe induit par le voisinage du noeud défaillant.

Nous présentons maintenant quelques notations utilisées dans la section suivante. Soit *G=(V,E)* un graphe simple non orienté ayant n sommets. Nous associons un poids w_{ij} à chaque arête $(ij \in E)$. Le poids du lien *(ij)* est calculé en fonction de la distance entre les noeuds i et j et de leurs énergies comme le montre l'équation 3.4.

$$w_{ij} = \frac{2 * dist_{ij}}{resEnergy(i) + resEnergy(j)} \tag{3.4}$$

où $dist_{ij}$ est la distance euclidienne entre les noeuds i et j, et *resEnergy(x)* représente l'énergie résiduelle du noeud x dans le réseau.

Notre objectif dans cette contribution est de trouver les arêtes de l'ensemble de poids minimum (minimum-weight) dont l'ajout à G donne un graphe avec une condition de connectivité par paire donnée. À cette fin, nous procédons comme suit :

Problème Aug-CNP

Entrée : *G=(V,E)* : un graphe dont l'ordre est n, S : un ensemble de noeuds critiques dont la taille est k, et un poids non négatif w_{ij} pour chaque paire $(i, j) \in V$.

Sortie : Un ensemble de poids minimum de nouvelles arêtes *E'* tel que dans le graphe augmenté $H = (V, E \cup E')$, nous obtenons :

$$f(H \setminus S) = \frac{|V \setminus S| * (|V \setminus S| - 1)}{2} \tag{3.5}$$

Dans l'équation 3.5, Aug-CNP garantit que le graphe G reste connecté même après avoir supprimé l'ensemble des noeuds critiques S. L'exemple présenté dans la Figure 3.7 illustre cette propriété après avoir retiré l'ensemble de noeuds $S = \{v_4, v_9, v_{10}\}$ du graphe.

Motivés par le résultat de complexité de [82] (Theorem 1), nous proposons la conjecture suivante :

Conjecture 1. *Le problème des noeuds critiques d'augmentation est NP-complet.*

Nous présentons maintenant un algorithme glouton (Algorithme 3) pour le problème Aug-CNP qui présente un intérêt pratique, notamment dans les réseaux de capteurs sensibles aux pannes.

La Figure 3.8 présente un exemple d'augmentation de graphe où la Figure 3.8b montre la décomposition du graphe présenté dans la Figure 3.8a en 7 composantes après avoir supprimé le sommet v_5. Dans la Figure 3.8c, nous appliquons Aug-CNP, qui cherche à ajouter un nombre minimum d'arêtes pour que l'ensemble du graphe soit connecté. Dans cet exemple, Aug-CNP ajoute 7 arêtes comme présenté dans l'équation 3.6.

$$E' = \{(v_4, v_1),\ (v_4, v_2),\ (v_4, v_3),\ (v_4, v_0),\ (v_4, v_9),\ (v_9, v_6),\ (v_9, v_8)\} \tag{3.6}$$

Algorithm 3 Aug-CNP Algorithm

1: **Input** : Graphe *G=(V,E)* d'ordre n, S un ensemble de noeuds critiques de taille k, et un poids non négatif w_{ij} pour chaque couple $(i, j) \in V$.
2: **Output** : Ensemble de poids minimum des nouvelles arêtes *E'* tel que l'équation (3.5) soit satisfaite dans l'augmentation du graphe $G' = (V, E \cup E')$
3: **Begin**
4: Soit H le sous-graphe induit par l'ensemble des sommets $V \setminus S$.
5: Nous définissons $M(H) = \{h_1, h_1, \ldots, h_k\}$ comme l'ensemble des composantes connexes de H.
6: $W = \emptyset$
7: $E' = \emptyset$
8: **for** Chaque paire de sommets non connectés *(i,j)* **do**
9: $W = W \cup \{w_{ij}\}$
10: **end for**
11: **while** H n'est pas connecté **do**
12: Soit w_{ij} est le poids minimum dans l'ensemble W.
13: $E' = E' \cup \{(i, j)\}$
14: $W = W \setminus \{w_{i,j}\}$
15: **end while**
16: $G' = (V, E \cup E')$
17: **end**

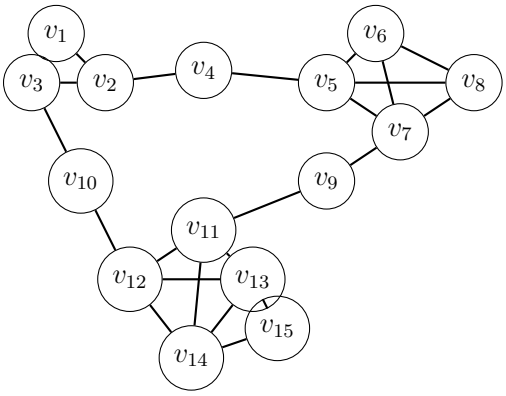
L'ajout d'arêtes est basé sur une matrice de poids M (Equation 3.7). Comme expliqué précédemment, les arêtes ajoutées sont les arêtes de poids minimum w_{ij} qui peuvent connecter l'ensemble du réseau. Cette opération nécessite d'ajuster la puissance de transmission des noeuds impliqués dans l'augmentation afin qu'ils puissent se connecter entre eux.

$$M = \begin{pmatrix} 0 & 2.09 & 0.88 & 1.23 & 2.08 & 2.71 & 3.63 & 3.98 & 4.84 & 5.56 \\ 2.09 & 0 & 0.61 & 0.42 & 0.21 & 0.31 & 0.76 & 0.94 & 1.37 & 1.74 \\ 0.88 & 0.61 & 0 & 0.19 & 0.59 & 0.92 & 1.37 & 1.54 & 1.98 & 2.34 \\ 1.23 & 0.42 & 0.19 & 0 & 0.44 & 0.73 & 1.19 & 1.37 & 1.80 & 2.16 \\ 2.08 & 0.21 & 0.59 & 0.44 & 0 & 0.40 & 0.83 & 0.98 & 1.42 & 1.77 \\ 2.71 & 0.31 & 0.92 & 0.73 & 0.40 & 0 & 0.45 & 0.64 & 1.06 & 1.43 \\ 3.63 & 0.76 & 1.37 & 1.19 & 0.83 & 0.45 & 0 & 0.21 & 0.60 & 0.98 \\ 3.98 & 0.94 & 1.54 & 1.37 & 0.98 & 0.46 & 0.21 & 0 & 0.45 & 0.79 \\ 4.84 & 1.37 & 1.98 & 1.80 & 1.42 & 1.06 & 0.60 & 0.45 & 0 & 0.40 \\ 5.56 & 1.74 & 2.34 & 2.16 & 1.77 & 1.43 & 0.98 & 0.79 & 0.40 & 0 \end{pmatrix} \quad (3.7)$$

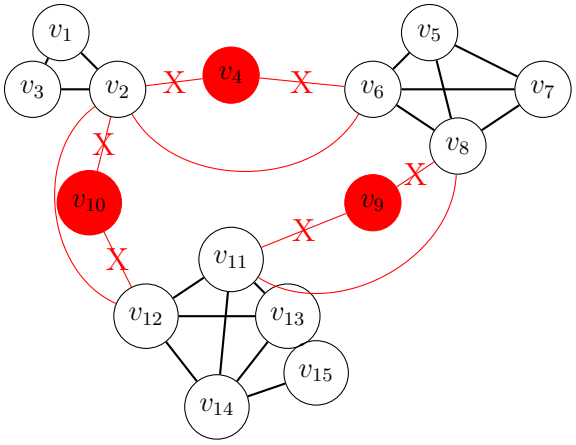
Le théorème suivant donne la complexité de notre heuristique utilisée.

Theorem 2. *L'algorithme (3) s'exécute avec une complexité d'ordre* $O(n^2)$.

Démonstration. Tout d'abord, l'étape 4 de l'algorithme (3) peut être calculée par un algorithme basé sur DFS (Depth-first search). La complexité temporelle est de $O(n + m)$ où n et m sont respectivement le nombre de noeuds et d'arêtes. La boucle *FOR* (lignes



(a) Set of critical nodes $S = \{v_4, v_9, v_{10}\}$



(b) Graphe après la suppression des noeuds critiques

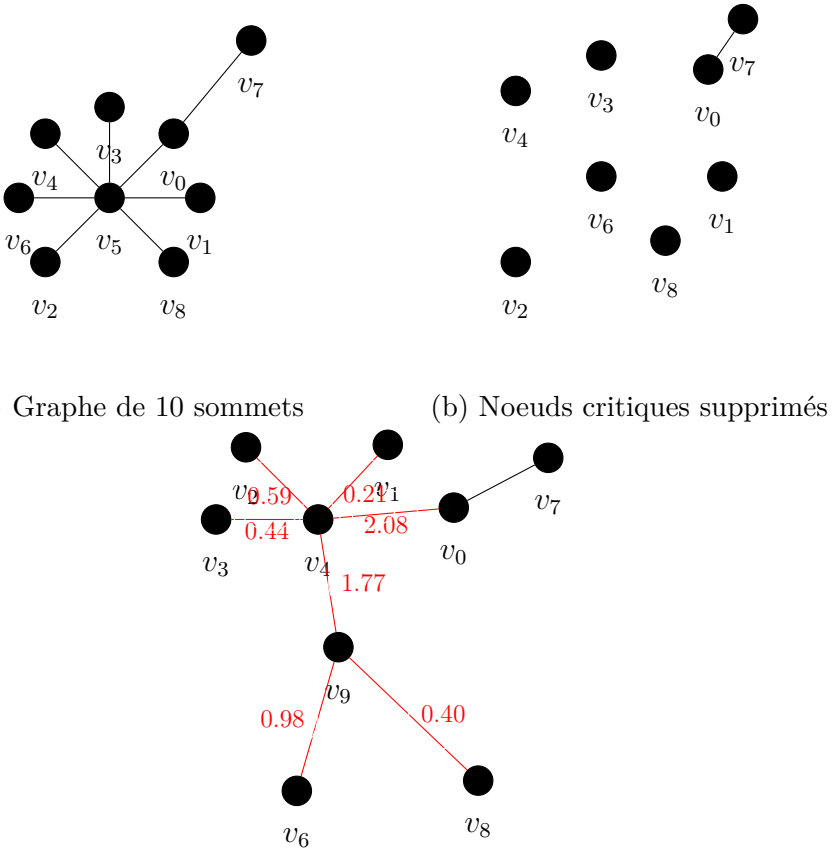
FIGURE 3.7 – Un exemple de problème d'augmentation

9-10) s'exécute en $O(n^2)$. Dans la dernière boucle *WHILE* (ligne 11-15), il est clair que le nombre d'itérations pour obtenir une composante connectée H est $|M(h) - 1|$. Dans le pire des cas, toutes les composantes connectées sont des sommets isolés. Cette boucle s'exécute avec une complexité d'ordre $O(n)$. □

3.5 Évaluation des performances et discussion

3.5.1 Environnement de travail

Les simulations ont été réalisées en utilsant le simulateur OMNET++ [83] et le framework Castalia [84] sur le protocole AODV [85]. Chaque résultat de simulation est associé à un scénario dans lequel le nombre de noeuds est compris entre 50 et 200 et ces noeuds sont déployés de manière non uniforme. Nous avons utilisé une topologie de réseau à disque unitaire avec une portée de transmission de *150 m*. La simulation a duré 250 secondes et les autres paramètres de simulation sont résumés dans le tableau 3.1. Nous avons effectué une grande série de mesures dans lesquelles nous faisons varier le nombre de noeuds de



(a) Graphe de 10 sommets (b) Noeuds critiques supprimés

(c) Augmentation de graphe

FIGURE 3.8 – Un example du problème d'augmentation

50 à 200.

Pour la couche MAC, nous avons utilisé le protocole S-MAC [126] prédéfini dans le simulateur Castalia. Ce protocole est considéré comme l'un des meilleurs protocoles éco-énergétiques grâce à l'utilisation d'un cycle de service basé sur le mécanisme de "veille/réveil" où un noeud en mode veille consomme moins d'énergie par rapport au mode "écoute permanente" [127]. S-MAC utilise l'écoute synchrone des canaux en échangeant des paquets de synchronisation entre les noeuds voisins qui permet aux noeuds de connaître l'état des noeuds voisins s'ils sont inactifs ou en mode veille. Le processus de synchronisation entre les noeuds évite le problème de la perte de données et de retransmissions, qui peut exister dans les protocoles asynchrones.

3.5.2 Métriques de performances

Pour évaluer l'approche proposée, nous avons effectué plusieurs simulations dans lesquelles nous avons mesuré la fonction de fitness et le taux de dégradation de la durée de vie. Ces mesures ont été évaluées en fonction du nombre de noeuds critiques et du nombre de noeuds lorsqu'un seul noeud critique est bloqué.

TABLE 3.1 – Paramètres de simulation (Aug-CNP)

Paramètre	Valeur
Simulateur utilisé	OMNET++/Castalia
Environnement radio	UDGM (Unit Disk Graph Medium)
Surface de déploiement	1000m x 1000m
Nombre de noeuds	50-200
Portée de transmission	150 (m)
Taille du paquet	250 bytes
Temps de simulation	250 sec
Nombre de répétitions des simulations	200

a) Fonction de fitness

Les Figures 3.9 et 3.10 montrent la valeur de la fonction objectif (connectivité par paires) et la cardinalité de la plus grande composante de connectivité en fonction du nombre de noeuds critiques supprimés dans les réseaux denses. Pour illustrer les performances de notre contribution, nous avons comparé GA-CNP avec d'autres approches d'évaluation des noeuds critiques proposées dans la littérature : MADME [116], IE-Matrix [128], Betweenness [129]. Les résultats obtenus ont prouvé que GA-CNP minimise la connectivité par paire entre les noeuds restants et la variance des cardinalités des composantes.

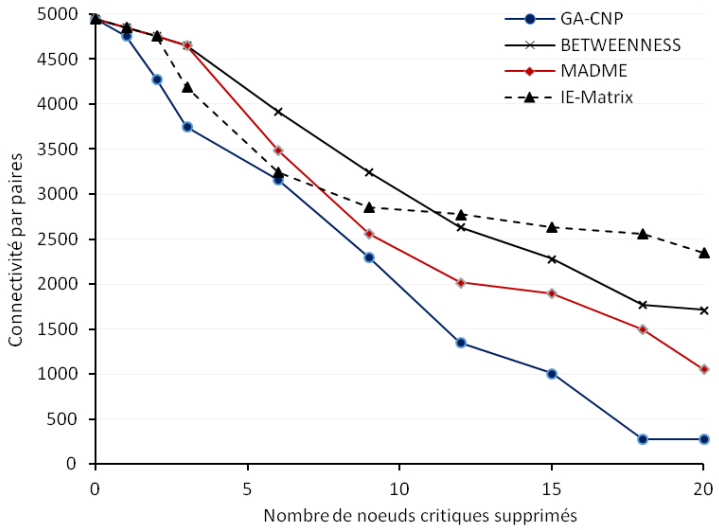


FIGURE 3.9 – Connectivité par paires vs. Nombre de noeuds critiques supprimés

b) Durée de vie du réseau en fonction du nombre de noeuds critiques

Dans cette sous-section, nous étudions l'impact de la suppression de noeuds critiques sélectionnés par GA-CNP sur la durée de vie du réseau.

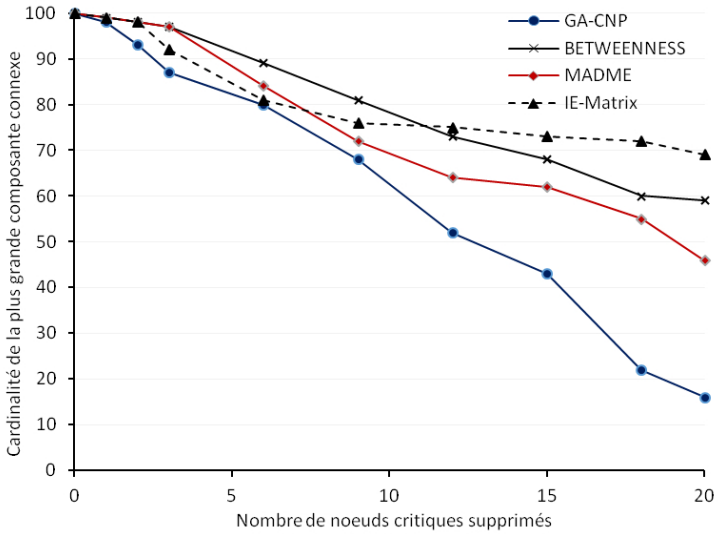


FIGURE 3.10 – Cardinalité de la plus grande composante connexe vs. Nombre de noeuds critiques supprimés

La Figure 3.11 montre la variation de la durée de vie du réseau en fonction du nombre de noeuds critiques bloqués. Les résultats obtenus expliquent l'importance des noeuds sélectionnés comme critiques par notre approche, compte tenu du taux de dégradation de la durée de vie du réseau. Par conséquent, notre approche sélectionne les meilleurs noeuds critiques qui fragmentent le mieux le réseau.

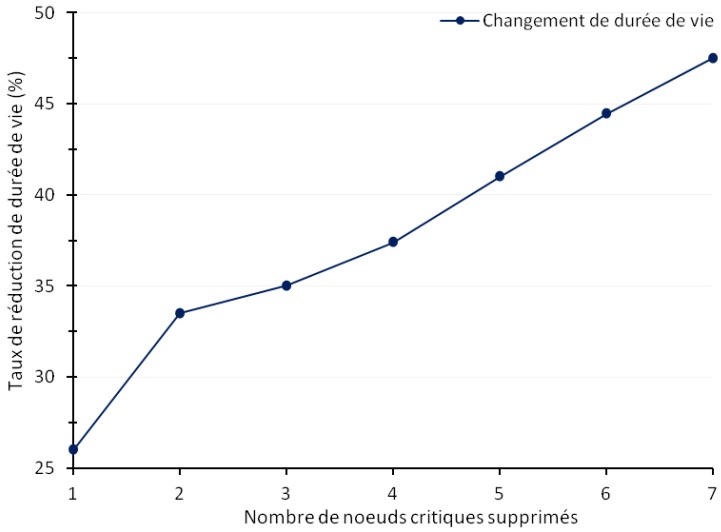


FIGURE 3.11 – Durée de vie du réseau vs. Nombre de noeuds critiques supprimés

c) Durée de vie du réseau en fonction du nombre de noeuds

La Figure 3.12 montre le taux de dégradation de la durée de vie du réseau lorsqu'un seul noeud critique est bloqué dans différentes topologies : 50, 100, 150 et 200 noeuds. Le blocage d'un seul noeud critique donne de meilleurs résultats dans les réseaux moins

denses (exemple d'un réseau de 50 noeuds) comme le montre la Figure 3.12. De plus, en augmentant le nombre de noeuds critiques, la dégradation de la durée de vie du réseau augmente.

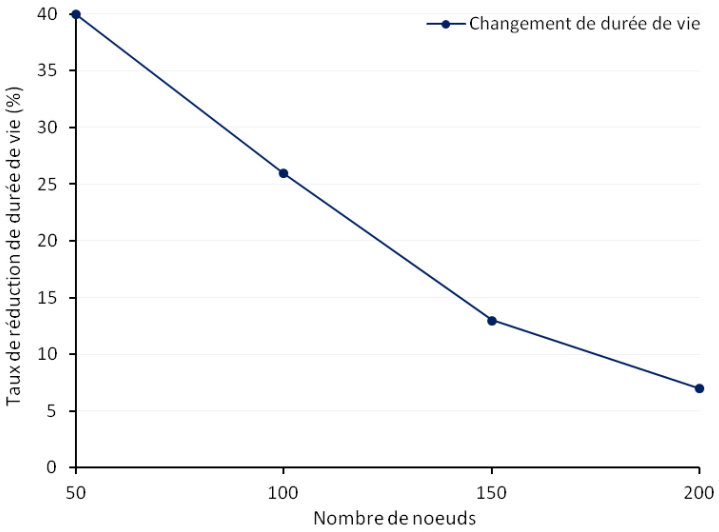


FIGURE 3.12 – Durée de vie du réseau vs. Taille du réseau

d) Performances de la contribution Aug-CNP

Dans cette phase, nous prenons l'exemple d'un réseau de 100 noeuds avec une topologie de réseau en forme de disque unitaire avec une portée de transmission de 150 m pour étudier les performances du réseau entre le protocole AODV traditionnel [85] et le protocole AODV avec notre méthode d'augmentation Aug-CNP. L'algorithme Aug-CNP proposé nécessite l'ajout des arêtes en ajustant la radio des noeuds impliqués dans l'augmentation afin qu'ils puissent se connecter et donc la connectivité du réseau reste préservée. En outre, Aug-CNP montre que la topologie utilisée contient trois noeuds critiques et qu'en augmentant le nombre de noeuds critiques la durée de vie du réseau diminue.

La Figure 3.13 montre que notre approche Aug-CNP améliore les performances du réseau en termes de durée de vie. Notre proposition augmente la durée de vie du réseau de 22% par rapport au protocole AODV traditionnel. Dans ce scénario, la surcharge des noeuds importants peut rapidement épuiser leur énergie. De plus, Aug-CNP fournit un aspect de tolérance aux pannes au protocole de routage concerné en lui permettant de trouver un chemin alternatif en cas de défaillance des noeuds critiques avec un poids minimal. En conséquence, la consommation d'énergie dans le réseau sera optimisée.

La Figure 3.14 illustre que le protocole AODV avec Aug-CNP diminue le taux de perte de paquets par rapport au protocole AODV traditionnel puisque notre approche donne la possibilité aux noeuds voisins d'un noeud critique de trouver un chemin alternatif en cas de congestion ou de défaillance du noeud critique. Par conséquent, notre solution maintient la connectivité du réseau loin du noeud critique.

En outre, s'il y a un problème dans un chemin, le protocole AODV-Aug-CNP essaie de réparer la connectivité localement pour trouver un chemin dans le voisinage. Cette opération est répétée jusqu'à ce qu'un chemin soit trouvé. Dans le cas de noeuds critiques,

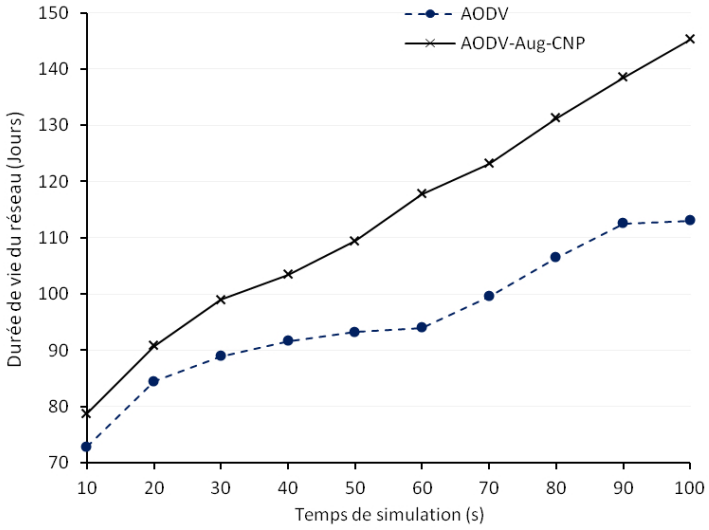


FIGURE 3.13 – Durée de vie du réseau vs. Temps de simulation

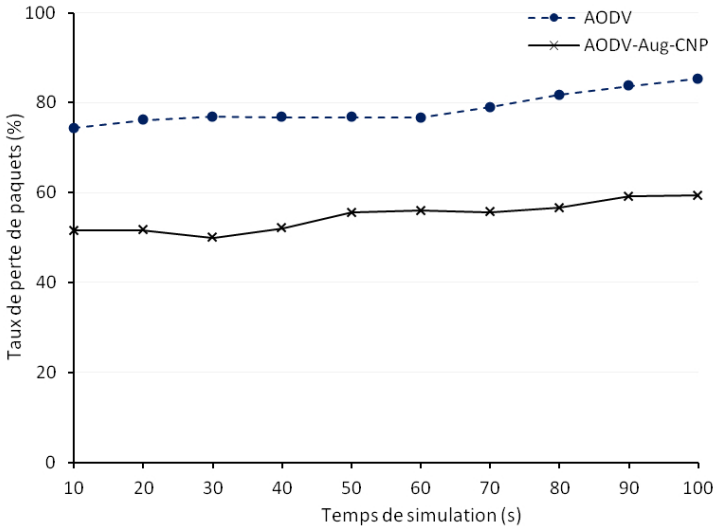


FIGURE 3.14 – Taux de perte de paquets en fonction du temps de simulation

cette opération est inévitable en raison de la congestion causée par leur saturation ou leur défaillance, elle peut donc être répétée plusieurs fois jusqu'à la fin de la congestion si aucun autre chemin n'est trouvé. Cette opération dans le protocole AODV traditionnel augmente le délai de bout en bout et même le taux de perte de paquets, alors que dans le protocole AODV-Aug-CNP, il fournit de meilleurs résultats en termes de délai par rapport au protocole AODV traditionnel, comme le montre la Figure 3.15, grâce à l'algorithme Aug-CNP qui permet au protocole AODV-Aug-CNP de trouver un chemin alternatif en cas de défaillance des noeuds critiques.

La Figure 3.16 montre la consommation d'énergie en fonction de la portée de transmission. Nous constatons que l'augmentation de la portée de transmission augmente le nombre de voisins des noeuds, ce qui permet de réduire le nombre de noeuds impliqués dans le routage des paquets vers la station de base et donc la consommation d'énergie sera réduite. Cependant, l'augmentation de la portée de transmission accroît l'utilisation

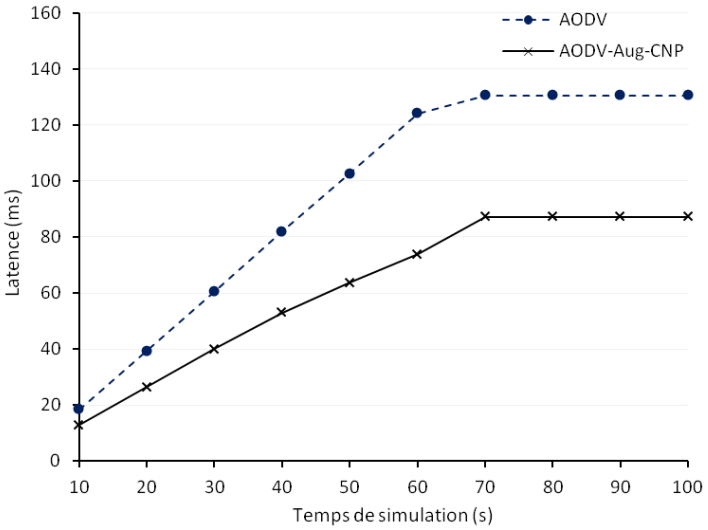


FIGURE 3.15 – Latence en fonction du temps de simulation

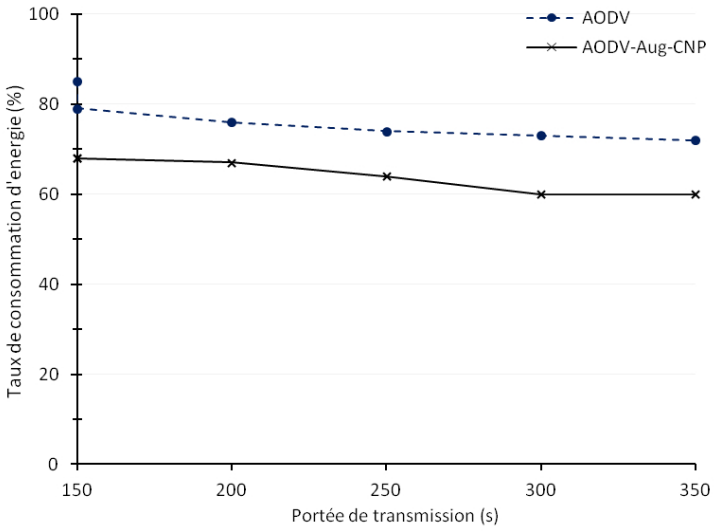


FIGURE 3.16 – Taux de consommation d'énergie en fonction de la portée de transmission

de la batterie et la probabilité de collision et d'interférences, ce qui augmente la consommation d'énergie. Par conséquent, la différence entre le taux de consommation d'énergie avec différentes portées de transmission n'est pas significative. Notre approche améliore la consommation d'énergie du protocole AODV pour différentes portées de transmission avec presque le même taux car elle sélectionne le meilleur saut alternatif en cas de défaillance d'un noeud critique. En outre, AODV-Aug-CNP minimise la consommation d'énergie des retransmissions inutiles et recherche des chemins alternatifs.

La Figure 3.17 montre la variation du débit en fonction de la portée de transmission. La valeur du débit augmente proportionnellement à la portée de transmission. Nous constatons que le protocole AODV-Aug-CNP améliore le débit pour les différentes portées de transmission et fournit une meilleure connectivité car il sélectionne le meilleur chemin alternatif en cas de défaillance des noeuds critiques. D'où, le nombre de paquets envoyés par unité de temps dans AODV-Aug-CNP est augmenté par rapport au protocole AODV

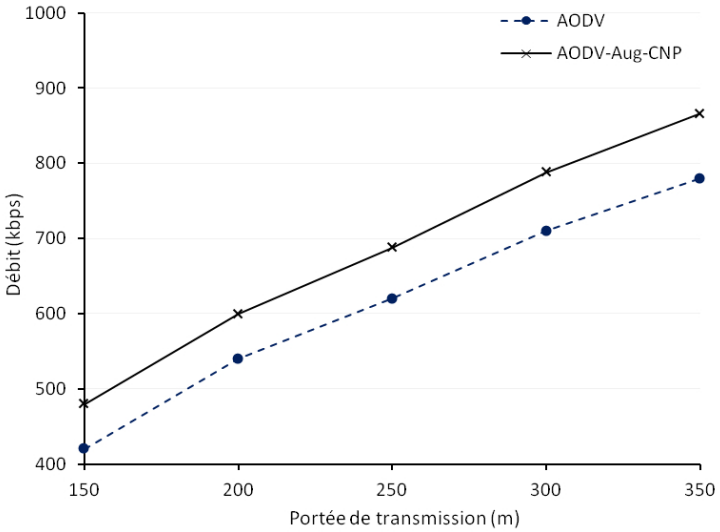


FIGURE 3.17 – Débit en fonction de la portée de transmission

traditionnel.

3.6 Conclusion

La contrainte énergétique des noeuds capteurs rend les réseaux de capteurs vulnérables aux pannes où l'épuisement de la batterie d'un noeud peut réduire la durée de vie du réseau. En outre, la dégradation de la durée de vie du réseau varie en fonction de l'importance du noeud où l'épuisement de la batterie d'un noeud critique peut dégrader considérablement la durée de vie du réseau, voire même entraîner son arrêt.

Dans ce chapitre, nous avons proposé une nouvelle approche pour la tolérance aux pannes dans les RCSFs. Cette approche se compose de deux phases. La première phase sélectionne les noeuds critiques dans le réseau dont la défaillance entraîne une dégradation significative des performances du réseau et la seconde phase applique une méthode d'augmentation pour maintenir la connectivité du réseau en cas de défaillance de l'un des noeuds critiques.

Les résultats de simulation ont montré que l'approche GA-CNP proposée, qui est basée sur des algorithmes génétiques, peut sélectionner les noeuds critiques dont la défaillance peut dégrader la durée de vie du réseau. De plus, l'approche Aug-CNP appliquée au protocole AODV apporte des améliorations en termes de durée de vie du réseau par rapport au protocole AODV traditionnel.

Dans le chapitre suivant, nous proposons deux protocoles tolérants aux pannes économes en énergie, basés sur le clustering et la sélection des meilleurs chemins pour le routage de données. Le premier est à aspect préventif et le deuxième est à aspect curatif. Par ailleurs, l'optimisation de la consommation d'énergie est considérée comme un moyen de tolérance préventif aux pannes car la plupart des pannes qui surviennent dans les RCSFs sont causées par le manque d'énergie de certains noeuds de capteurs.

Chapitre 4

Un Routage tolérant aux pannes et économe en énergie pour les RCSFs

Chapitre 4

Un Routage tolérant aux pannes et économe en énergie pour les RCSFs

4.1 Introduction

Les RCSFs sont devenus de plus en plus très répandus ; ils sont utilisés dans divers domaines. Leurs candidatures sont de plus en plus nombreuses et diverses. Ils peuvent être classés principalement dans les domaines : militaire, environnemental, médical et commercial [130] qui leur permettent de réaliser diverses tâches telles que la surveillance, la détection d'événements et la collecte d'informations. Ces tâches ne peuvent être exécutées correctement que si les RCSFs présentent des propriétés telles que la tolérance aux pannes, la conservation d'énergie. Cependant, la nature des noeuds de capteurs et les environnements hostiles dans lesquels ils sont déployés les rendent vulnérables aux défaillances pour diverses raisons telles que le manque d'énergie des noeuds de capteurs, les dommages intentionnels des équipements ou à cause de leur écrasement par des animaux, ou les conditions environnementales, ce qui ne permet pas aux RCSFs d'assurer leur bon fonctionnement. Plusieurs protocoles ont été proposés dans la littérature pour faire face à ces défis tout en tenant compte des limitations des RCSFs.

Les RCSFs sont devenus très répandus en raison de la variété de leurs applications qui visent à effectuer différentes tâches telles que la surveillance, la détection d'événements et le traitement de l'information. Les applications des RCSFs ne peuvent pas toujours être réalisées correctement du fait de l'existence de noeuds capteurs très fragiles et très sensibles aux pannes. De plus, leur déploiement dans des environnements hostiles augmente la probabilité de leur défaillance. Ces défaillances peuvent être causées intentionnellement ou par des phénomènes naturels. Pour résoudre ce problème et s'assurer que le réseau fonctionne correctement même en cas de panne de certains noeuds capteurs, il est recommandé de mettre en oeuvre un processus de routage tolérant aux pannes de manière préventive et/ou curative.

En outre, la défaillance des noeuds capteurs ne doit pas avoir un effet sur le bon fonctionnement du réseau. C'est le but de la recherche basée sur la tolérance aux pannes dans les RCSFs qui vise à préserver le fonctionnement du réseau sans interruption en empêchant les pannes et/ou les restaurer. Dans ce contexte, nous avons orienté nos recherches sur la conservation de l'énergie, ce qui améliore la propriété de tolérance aux pannes préventive dans les RCSFs.

Dans une architecture clusterisée, outre la nature des noeuds capteurs et les environnements hostiles dans lesquels ils sont déployés, et en raison des tâches de gestion et de routage des données vers la station de base par les noeuds CHs, ces derniers sont sujets à des pannes. De ce fait, afin d'atteindre la tolérance aux pannes et ne pas perdre la connectivité dans le réseau, il serait plus approprié de trouver un CH alternatif du CH défaillant.

Dans ce chapitre, nous proposons deux contributions. La première contribution consiste en un protocole de routage tolérant aux pannes à haut rendement énergétique, basé sur la méthode de clustering utilisée dans le protocole EEADC (Energy Efficient Data Aggregation in Clustered WSN) [131], appelé EE-FT (Energy-Efficient cluster-based Fault-Tolerant routing protocol for WSNs) [7]. EE-FT permet à couvrir les défaillances avant qu'elles ne se produisent i.e. la tolérance aux pannes est à aspect préventif. Il choisit les chemins fiables les plus courts pour le routage des données à la station de base en utilisant la loi de Bernoulli pour la sélection des noeuds fiables. En outre, dans EE-FT, les chemins établis sont formés par les CHs qui ont plus d'énergie. Nous avons évalué et comparé les performances du protocole EE-FT à celles du protocole EFT-PMD (Efficient Fault Tolerance Path graph flow Modelling with Marchenko–Pastur Distribution algorithm) [8] en termes de délai moyen de livraison de paquets, de taux de livraison des données, d'énergie dissipée et de durée de vie du réseau.

La deuxième contribution est un protocole de routage tolérant aux pannes basé sur la méthode de clustering utilisée dans le protocole EADC (energy-aware clustering algorithm) [6] et sur un protocole de routage proactif, appelé EE-FTR (Energy-Efficient Fault-Tolerant Routing protocol for WSNs) [9]. Le protocole proposé vise à tolérer les défaillances en remplaçant le CH principal défaillant par un autre CH appelé CH assistant. Il est également basé sur l'optimisation de la consommation d'énergie, ce qui améliore la tolérance aux pannes dans les RCSFs. Nous avons évalué et comparé les performances de cette deuxième contribution à celles du protocole EFT-PMD en termes de délai de livraison moyen, de débit de livraison des données, de l'énergie dissipée et de durée de vie du réseau.

4.2 Contexte

La propriété de tolérance aux pannes est définie par la capacité du réseau pour maintenir sa fonctionnalité sans interruption lors de la défaillance des noeuds capteurs. Dans RCSFs, les noeuds de capteurs sont sujets à des pannes dues à diverses causes : épuisement d'énergie, dommages dus aux conditions naturelles ou aux animaux, etc. De plus, dans les RCSFs, les pannes causées par l'épuisement de batteries des noeuds capteurs sont les plus prédominantes. A cet effet, la conservation de l'énergie des noeuds de capteurs permet d'éviter l'extinction prématurée de leurs batteries et augmente la durée de vie des noeuds capteurs. Pour assurer la propriété de tolérance aux pannes dans ce type de réseaux, les protocoles tolérants aux pannes utilisent des algorithmes de recouvrement des pannes. Ce mécanisme est considéré comme une approche optimiste où elle n'est exécutée qu'après la détection des pannes. En outre, il existe également des protocoles tolérants aux pannes qui fournissent des stratégies qui tentent de retarder ou d'éviter tout type de pannes afin de maintenir le fonctionnement du réseau aussi longtemps que possible. Dans ce contexte, nous proposons un protocole de routage tolérant aux pannes économe en énergie, basé sur

le clustering pour les RCSFs. Ce protocole permet de couvrir les pannes avant qu'elles ne surviennent, appelé protocole EE-FT [7].

Le protocole EE-FT choisit les chemins fiables les plus courts pour acheminer les données vers la station de base. Il utilise une approche de clustering basée sur la loi de Bernoulli pour sélectionner les noeuds fiables. Dans EE-FT, les chemins de routage de données sont formés par des noeuds CHs qui ont plus d'énergie parmi tous les noeuds CHs. L'évaluation de EE-FT a permis de montrer que ce dernier fournit de meilleures performances en termes de durée de vie du réseau, de délai de bout en bout et de taux de perte de paquets par rapport à d'autres protocoles.

Le clustering sous contraintes des utilisateurs pour les RCSFs est considéré comme un défi à relever en tenant compte de la nature des noeuds capteurs et l' objectif de clustering. Dans ce contexte, de nombreux travaux ont été proposés dans la littérature pour étendre les algorithmes classiques en prenant en compte des contraintes des utilisateurs pour les réseaux de capteurs. Néanmoins ces travaux n'ont pas pu relever le défi totalement et fournir de très bons résultats. Par exemple, les protocoles basés sur le clustering qui impliquent l'approche K-means [132] dont les résultats dépendent du nombre de clusters "K" initialement fixé et de les positions des centres de cluster (centroides) qui sont choisis aléatoirement. Aussi, pour les solutions basées sur des graphes, il faut avoir une connaissance préalable de l'architecture du réseau où chaque noeud doit connaître la position des autres noeuds, ce qui n'est pas toujours possible et dans les meilleurs des cas ça va être très coûteux. Dans ce contexte, nous proposons un protocole de routage tolérant aux pannes basé sur le clustering qui implique un CH assistant pour tolérer la panne du CH principal dans un cluster et qui vise également l'optimisation de la consommation d'énergie [9].

Dans les deux contributions, notre objectif est d'améliorer la durée de vie du réseau en proposant des protocoles simples et peu gourmands en termes d'énergie et de puissance de calcul, et adaptés aux systèmes à ressources limitées tels que les RCSFs.

4.3 Travaux connexes

La tolérance aux pannes est considérée comme une problématique clé dans les RCSFs. C'est la raison pour laquelle, plusieurs approches de tolérance aux pannes ont été proposées dans littérature à savoir les approches présentées dans [8, 32, 133–139]. Dans ce qui suit, nous présentons les principaux protocoles pour améliorer la consommation d'énergie et la tolérance aux pannes dans les RCSFs.

Le protocole "Fault-Tolerant Disjoint Multipath Distance Vector Routing Algorithm (FD-AOMDV)" [134] permet de trouver des chemins disjoints tout en minimisant considérablement la surcharge de routage. Le protocole proposé fournit des meilleurs résultats par rapport au protocole AOMDV [140] en termes de réduction de la surcharge de routage et du taux de livraison des paquets ainsi que de délai de bout en bout.

Ajay et al. [137] ont proposé un protocole de routage multiniveau (Fault tolerant multilevel routing protocol with sleep scheduling (FMS)) tolérant aux pannes qui maintient la connectivité du réseau en cas de défaillance d'un noeud. Ce protocole est basé sur un processus d'ordonnancement périodique de veille et de transmission de données. Si l'énergie résiduelle d'un noeud descend en dessous d'une valeur seuil, il en informe les noeuds fils afin qu'ils puissent trouver de nouveaux parents. En conséquence, des chemins alternatifs

sont établis et la connectivité est maintenue. Les résultats de simulation ont montré que le protocole proposé a une consommation d'énergie et un délai de livraison des paquets de données plus faibles, et un taux de livraison plus élevé, comparé aux protocoles flooding et diffusion directe (directed diffusion) [39].

Kulothungan et al. [138] ont proposé un protocole de routage adaptatif tolérant aux pannes avec rapport d'erreur (RERP : Routing with Error Reporting Protocol) pour les RCSFs. Il s'agit d'un protocole de routage proactif piloté par table qui utilise l'énergie et les performances passées du lien comme métrique pour sélectionner le meilleur chemin. Les fonctions du rapport d'erreur utilisent deux types de messages : les messages de rapport d'erreur et les messages de requête/réponse. Les messages de rapport d'erreur sont générés lorsqu'une condition d'erreur se produit pendant la transmission d'un paquet et sont envoyés à la source du paquet de données correspondant. Un message de requête/réponse est un message dans lequel un noeud de capteurs expéditeur envoie un paquet de requête au noeud de capteurs destinataire et attend un paquet de réponse. Il est utilisé à des fins de diagnostic. Afin de surmonter les défaillances des noeuds ou des chemins, un chemin de secours est maintenu par chaque noeud du réseau. Chaque fois qu'un noeud de capteurs rejette un paquet de données en raison de la défaillance d'un autre noeud de capteurs ou de la non-disponibilité du chemin de livraison des paquets, il passe au chemin de secours, ce qui assure la tolérance aux pannes et augmente la fiabilité et la disponibilité du système.

Dans [139], Wu et al. ont présenté un protocole de routage dynamique de saut en temps réel tolérant aux pannes (Dynamical jumping real-time fault-tolerant routing protocol (DMRF)). Dans le protocole proposé, chaque noeud utilise le temps de transmission restant des paquets de données et l'état de l'ensemble des noeuds candidats à l'acheminement pour choisir dynamiquement le prochain saut. En cas de défaillance d'un noeud, de congestion du réseau ou de région vide, le mode de transmission passe en mode de transmission par saut, ce qui permet de réduire le délai de transmission et de garantir l'envoi des paquets de données au noeud de destination dans le délai spécifié. En utilisant un mécanisme de rétroaction, chaque noeud ajuste dynamiquement les probabilités de saut pour augmenter le taux de transmission réussie. Les résultats de simulation ont montré que le protocole DMRF peut non seulement réduire efficacement les effets des noeuds défaillants, de la congestion et de la région vide, mais aussi produire un taux plus élevé de transmissions réussies, un délai de transmission plus faible et un nombre réduit de paquets de contrôle.

Dans [133], les auteurs ont proposé une solution efficace en énergie et tolérante aux pannes. Cette solution permet de détecter la défaillance des noeuds CHs et non-CHs.Les noeuds non-CHs sont notifiés uniquement lorsqu'un événement de l'intérêt se produit. En outre, un ensemble de nombre minimal de noeuds sont sélectionnés comme actifs dans chaque cluster. Cela réduit la consommation énergétique dans le réseau. Cependant, dans ce protocole, le mécanisme utilisé pour le clustering ne prend pas en compte l'homogénéité des clusters en termes de taille, ce qui peut affecter l'uniformité de la consommation d'énergie dans le réseau comme dans le protocole LEACH [4] et certaines de ses variantes.

Dans [38], les auteurs ont proposé un protocole de routage multi-chemins qui utilise des chemins différents en fonction de la métrique énergétique tout en évitant l'utilisation permanente du chemin le plus économe en énergie qui peut provoquer l'épuisement de l'énergie des noeuds sur ce chemin. Le protocole proposé a amélioré les performances des réseaux en termes de durée de vie et de taux de livraison des paquets. Cependant, les frais

généraux étaient très élevés en raison de la mise en place de plusieurs chemins.

Le protocole proposé dans [76] offre une double couverture de chaque point de la zone de déploiement. De plus, il vise à maximiser la durée de vie du réseau en considérant les noeuds relais avec un minimum d'énergie nécessaire pour signaler l'événement à la station de base. Cependant, le coût de la couverture de la zone cible est élevé car chaque point de la zone nécessite au moins deux noeuds capteurs pour fournir une couverture.

Dans [40], Tien et al. ont proposé un protocole de routage pour les RCSFs qui permet une communication tolérante aux pannes en envoyant des trames unicast d'une source à une destination via des chemins à noeuds disjoints avec la meilleure distance possible entre la source et la destination. Le protocole proposé a un surcoût très élevé.

Le protocole présenté dans [41] permet une tolérance aux pannes en sélectionnant deux chemins : un chemin de service qui est le chemin principal et un chemin de secours qui sera utilisé en cas d'échec du chemin de service. L'inconvénient de ce protocole est que les ressources réservées au niveau des noeuds capteurs pour le chemin de sauvegarde ne peuvent jamais être utilisées si le chemin principal reste fonctionnel, ce qui conduit à un gaspillage inutile de ressources.

Dans [39], la station de base explore tous les chemins possibles à partir de la source pour sélectionner le chemin ayant le délai de livraison de paquets le plus petit pour la transmission entre la source et la station de base. Si la station de base constate un problème sur le chemin principal, cette dernière sélectionne un autre chemin ou initie la phase d'exploration de chemins.

Le protocole proposé dans [42] utilise la même technique que le protocole de diffusion directe [39] à la différence que dans la phase de renforcement, deux messages sont transmis au lieu d'un seul. Le premier message renforce le meilleur voisin et le deuxième message renforce le deuxième meilleur voisin. Ce processus est répété par chaque noeud pour trouver plusieurs chemins partiellement disjoints, ce qui permet de récupérer un échec d'envoi très rapidement. Néanmoins, le surcoût est très élevé pour faire un grand nombre d'explorations de chemins entre les noeuds et la station de base.

Dans [6], Yu et al. ont proposé un protocole de routage basé sur le clustering pour les RCSFs avec une distribution non uniforme des noeuds. Le protocole proposé comprend un algorithme de mise en clusters sensible à l'énergie (EADC) et un algorithme de routage basé sur le clustering. EADC utilise le rayon de transmission pour construire des clusters de taille égale. Néanmoins, la non-uniformité de la répartition des noeuds ne permet pas d'équilibrer le nombre de noeuds dans les clusters et donc la consommation d'énergie entre les noeuds CHs. Pour dépasser cette limite, un algorithme de routage est utilisé qui augmente les tâches d'acheminement des noeuds dans les zones peu couvertes en forçant les noeuds CHs à choisir des noeuds avec une énergie plus élevée et moins de noeuds membres comme prochains sauts. Ce schéma de routage permet un équilibrage de charge entre les noeuds CHs. L'analyse théorique et les résultats de simulations ont montré que le protocole proposé équilibre la consommation d'énergie entre les noeuds et augmente considérablement la durée de vie du réseau. Cependant, le principal inconvénient de ce protocole est qu'il ne tient pas compte de la longueur des chemins, et par conséquent plusieurs CHs peuvent participer au routage de données vers la station de base, ce qui peut provoquer la perte d'énergie dans plusieurs noeuds.

Le protocole proposé dans [33] consiste en trois phases à savoir : phase de formation des clusters, phase d'élection des noeuds CHs et phase de routage. Dans la première phase,

les terres agricoles sont divisées en petites zones de taille égale appelée champ. Dans la deuxième phase, dans chaque zone, un noeud CH est choisi en utilisant des règles floues qui impliquent la distance jusqu'à la station de base et l'énergie restante des noeuds dans le processus d'élection des noeuds CHs. La transmission des données de la source à la station de base est faite par les CHs qui agissent comme des noeuds relais. Le noeud relais est choisi en fonction de l'énergie restante, de la distance à la station de base et le degré du noeud.

Dans [141], le protocole proposé optimise la consommation d'énergie dans les RCSFs sur la base des paramètres et des règles exécutés de manière distribuée dans le réseau. Les auteurs ont proposé un ensemble de règles de gestion qui sont exécutées par chaque noeud capteur dans réseau. Ces règles s'adaptent aux noeuds capteurs en fonction de leur état énergétique et de l'énergie du réseau. Chaque noeud capteur calcule ses règles après chaque période et décide comment se comporter (passer en mode dormi pendant une longue période ou non). Une expérimentation de ces règles a été mise en place sur l'ensemble du réseau et il a été constaté que l'utilisation de ces règles permet d'augmenter la durée de vie énergétique moyenne jusqu'à 20 %.

Dans [142], Bennis et al. ont proposé un protocole de routage multi-chemin tolérant aux fautes appelé "Carrier Sense Aware Multipath Geographic Routing protocol (CSA-MGR)". CSA-MGR crée plusieurs chemins tout en évitant les interférences en utilisant un processus distribué et un dynamique. En outre, CSA-MGR utilise une nouvelle métrique appelée le nombre de voisins communs pour garantir une construction de chemin plus rapide et efficace. Les simulations effectuées sur le simulateur NS-2 ont montré des résultats prometteurs en termes de délai, de taux de livraison de paquets et de surcharge de routage dans CSA-MGR comparé à d'autres protocoles.

Les auteurs de [135] ont proposé un protocole tolérant aux pannes basé sur une variante de l'algorithme Firefly pour maximiser l'efficacité énergétique du réseau et la durée de vie des noeuds en sélectionnant les noeuds CHs de manière optimale. Dans ce travail, l'algorithme Firefly avec randomisation cyclique est proposé pour sélectionner les meilleurs noeuds CHs. Les performances du réseau sont améliorées par cet algorithme comparativement aux autres algorithmes conventionnels.

Le protocole "FF replaced position update in DA (FPU-DA)" [32] est une hybridation des algorithmes "Dragon fly (DA)" et "Firefly algorithm (FF)" pour la sélection du noeud CH dans chaque cluster. FPU-DA propose un nouveau modèle de clustering avec une sélection optimale des noeuds CHs en considérant quatre critères majeurs comme l'énergie, le délai, la distance et la sécurité. Les performances de FPU-DA surpassent celles retournées par d'autres modèles conventionnels en termes de nombre de noeuds vivants, d'énergie du réseau, de délai et de probabilité de risque.

Dans [136], Shafiabadi et al. ont proposé un protocole de routage pour les RCSFs en utilisant le clustering énergétique basé sur une carte auto-organisée (Energy Clustering based on Self-Organizing Map (ECSOM)). Dans le processus de clustering qui est basé sur un réseau neuronal un plan auto-organisateur est utilisé. Le réseau neural utilise trois dimensions les coordonnées spatiales du noeud (X et Y) et son énergie restante E pour déterminer les noeuds énergétiques, ce qui permet de générer des clusters dans lesquels il y a un noeud à haute énergie et des noeuds à faible énergie. Par conséquent, tous les clusters formés ont presque le même niveau d'énergie. Dans ce protocole, la sélection des noeuds CHs est effectuée après chaque transfert de données vers la station de base. Les résultats

de simulations ont montré que le protocole proposé fournit de bonnes performances en termes du taux de livraison des paquets. Cependant, les frais généraux sont élevés en raison du grand nombre d'opérations de sélection des noeuds CHs.

Dans [8], les auteurs ont proposé un protocole de routage tolérant aux pannes basé sur le clustering et à chemins disjoints entre le noeud source et la station de base. La solution proposée améliore les performances en termes de débit, taux de livraison de paquets, latence et consommation d'énergie. Cependant, il génère des frais généraux élevés.

La plupart de ces travaux se sont concentrés seulement sur le routage tolérant aux pannes. Cependant, il est recommandé de tenir compte en même temps de l'efficacité énergétique dans ce type de réseaux, car il s'agit de réseaux présentant un problème énergétique majeur qui pourra être la cause principale de leur dysfonctionnement. Dans notre contribution, nous proposons de viser la tolérance aux pannes conjointement avec l'optimisation de la consommation d'énergie.

4.4 EE-FT : Routage tolérant aux pannes et économe en énergie à aspect préventif

L'inconvénient du routage multi-sauts dans les RCSFs est l'échange fréquent de messages pour l'établissement des chemins valides, ce qui nécessite une énergie supplémentaire pour la transmission et retransmission. Cependant, l'approche de clustering fournit de meilleurs résultats en termes d'économies d'énergie. En effet, l'épuisement de la batterie est considéré comme l'une des principales causes de l'échec des noeuds de capteurs. Ainsi, l'optimisation de la consommation d'énergie est essentielle pour améliorer la durée de vie d'un noeud capteur, et donc d'améliorer la durée de vie global du réseau. Dans ce contexte, notre contribution consiste à adopter un protocole de routage basé sur le clustering pour surmonter cette limitation.

Le clustering sous les contraintes de l'utilisateur pour les RCSFs est considéré comme un défi à relever compte tenu de la nature des noeuds capteurs et l'objectif de clustering. De nombreux travaux sont proposés pour étendre les protocoles classiques en prenant en compte les contraintes des utilisateurs pour les RCSFs de capteurs, mais cela ne donne pas toujours de bons résultats. Comme le cas des travaux dont le clustering est basé sur la méthode K-means [132]. Dans ces travaux, la qualité des résultats est en fonction du nombre de clusters "K" initialement fixé et les positions des centroides qui sont choisis aléatoirement. Aussi pour les solutions basées sur des graphes, il faut au préalable connaître l'architecture du réseau où chaque noeud doit connaître la position des autres noeuds, ce qui n'est pas toujours possible.

Dans cette contribution, nous visons à améliorer la durée de vie du réseau tout en garantissant la tolérance aux pannes. Notre proposition consiste en un protocole de routage tolérant aux pannes basé sur le clustering qui n'est pas très gourmand en énergie et en puissance de calcul, adapté à la conception des RCSFs dont l'énergie et la mémoire sont limitées.

4.4.1 Méthode de clustering proposée

Dans cette solution, nous proposons d'améliorer la méthode du clustering utilisée dans le protocole EADC [6] où le processus de formation des clusters se compose de deux phases : formation de clusters selon la méthode de clustering EADC et la phase de réaffiliation.

a) Formation de clusters selon la méthode de clustering EADC

Le protocole EADC utilise une méthode de clustering pour améliorer la durée de vie du réseau. Les performances de cette méthode ont été comparées à celles des méthodes de clustering utilisées dans les protocoles "An energy-aware distributed unequal clustering protocol (EADUC)" [143] et LEACH [4] dans un environnement non uniforme. La méthode de clustering utilisée dans [6] est réalisée comme suit :

- Le processus d'élection des noeuds CHs est basé sur le taux de la moyenne de l'énergie résiduelle des nœuds voisins et l'énergie résiduelle du noeud lui-même. Cette méthode d'élection des noeuds CHs garantit que chaque cluster contient un noeud CH avec une quantité d'énergie suffisante pour accomplir ses tâches. Contrairement aux autres méthodes de clustering où le choix des noeuds CHs se fait après la formation des clusters et le noeud CH est sélectionné parmi les membres formants le cluster, dans ce cas nous pouvons avoir des clusters où tous les membres ont peu d'énergie.

- Les noeuds CHs diffusent leurs principaux messages en utilisant la même portée de transmission pour construire des clusters de même taille. Ainsi, la consommation d'énergie des membres du cluster peut être bien équilibrée. Cependant, cette solution peut pénaliser les noeuds CHs se trouvant dans les zones denses en terme de consommation d'énergie à cause de la distribution non uniforme des noeuds dans la zone de déploiement. Les noeuds CHs des zones denses ont plus de noeuds membres, et par conséquent ils ont une consommation d'énergie intra-cluster élevée.

Le critère de densité est donc essentiel pour homogénéiser le nombre de noeuds dans les clusters, en conséquence la consommation d'énergie au niveau des CHs et du réseau en général sera équilibrée.

b) Phase de formation des clusters

Dans le protocole EE-FT, nous visons à améliorer l'équilibrage de charge entre les noeuds CHs. Il serait plus approprié d'avoir des clusters qui ont à peu près de la même taille, ce qui aurait pour effet de homogénéiser le nombre de tâches réalisées par les différents noeuds CHs. Cela permet donc d'avoir quasiment le même taux de perte d'énergie au niveau des clusters. Ainsi, la durée de vie globale du réseau sera maximisée et le risque de perdre des parties du réseau avant d'autres sera grandement minimisé. De plus, dans notre contribution nous ajoutons une phase de réaffiliation à la méthode de clustering proposée dans EADC pour éviter d'avoir des clusters avec un très petit nombre des membres.

c) Phase de réaffiliation

Après la première phase de clustering mentionné ci-dessus, les noeuds CHs diffusent le nombre de membres de la même manière que la première phase selon la portée radio RC (Communication radius). Le noeud qui reçoit le nombre de membres de tous les CHs de sa table, calcule la pondération F selon l'équation (4.1) pour chaque CH, et envoie un message de jointure au CH dont le poids est minimal.

$$F = \alpha * energy + \beta * density \tag{4.1}$$

où $\alpha = 1$ et $\beta = 1 - \alpha$

Les résultats de simulations ont montré que la valeur de pondération 0.5 associée à α et β donne de meilleurs résultats.

4.4.2 Processus de routage

Dans le protocole EE-FT, l'optimisation de la consommation d'énergie est appliquée au niveau des clusters (intra-cluster) et entre les noeuds CHs (inter-cluster) pour router les données détectées vers la station de base. Ainsi, pour minimiser la consommation d'énergie dans le réseau, nous minimisons le nombre de noeuds CHs impliqués dans l'acheminement des données entre les noeuds CHs et la station de base. Pour cela, nous proposons d'établir le chemin le plus court entre les noeuds CHs et la station de base.

Plusieurs solutions heuristiques ont été proposées dont l'objectif est de trouver le chemin le plus court, mais ces solutions nécessitent beaucoup de puissance de calcul ainsi que beaucoup de mémoire et généralement elles sont basées sur des graphes ce qui nécessite une connaissance de l'architecture du réseau où les noeuds doivent connaître la position des autres noeuds. Ainsi, pour garder la même philosophie utilisée dans la phase de clustering, nous préservons le même principe de simplicité en proposant un protocole de routage économe en énergie qui ne nécessite pas beaucoup de puissance de traitement et de mémoire. Le processus de routage proposé dans le protocole EE-FT se déroule comme suit :

- La station de base envoie le message de découverte de route aux noeuds CHs à un saut qui contient : ID et le nombre de sauts par rapport à la station de base (pour la station de base le nombre de sauts est égal à 0).

- Lorsque le noeud CH reçoit le message, il ajoute l'ID du CH source avec le nombre de sauts dans sa table de routage, ensuite il augmente le nombre de sauts et rediffuse le message de découverte de route, et ainsi de suite.

- Lors de l'envoi des données détectées à la station de base, le noeud CH source sélectionne le CH avec le nombre minimum de sauts comme saut suivant. Si un CH ne reçoit pas un message d'acquittement dans un délai "t", il considère que le paquet est perdu et il sélectionne un autre CH avec un nombre minimum de sauts, et ainsi de suite. Chaque CH conserve une copie du paquet envoyé jusqu'à ce qu'il reçoive un message d'accusé de réception (un message ACK).

Afin d'assurer une couverture maximale de la surveillance de la zone d'intérêt, Le rayon de communication R_C entre les noeuds de capteurs est égale à deux fois le rayon de détection (couverture) R_S i.e $R_C = 2 * R_S$.

Dans le protocole EE-FT, nous choisissons le CH avec un minimum de nombre de sauts vers la station de base comme saut suivant, en supposant que les CHs sont les meilleurs noeuds en termes de ressources, de sorte que les données sont envoyées régulièrement, et après chaque envoi des données, le clustering est restauré. De plus, dans cette contribution, afin d'assurer que le CH sur le chemin le plus court vers la station de base n'est pas épuisé, nous appliquons une loi de probabilité pour choisir les CHs les plus fiables et ainsi éviter les pannes.

4.4.3 Modélisation de la fiabilité du protocole EE-FT

La probabilité qu'un noeud tombe en panne est basée sur plusieurs paramètres. Dans ce travail, nous prenons en considération seulement la défaillance causée par l'épuisement d'énergie.

Soit k le nombre de noeuds dans le RCSF considéré où ces noeuds sont identiques et fonctionnent indépendamment les uns des autres. Soit E_{init} l'énergie initiale d'un noeud N_i à l'instant t_0, avec $i = 1, 2, ..., k$. Après une période $\Delta t > 0$ de fonctionnement du RCSF, le noeud N_i est :

- Soit en un bon état, si son niveau d'énergie est supérieur à une valeur r de son énergie initiale E_{init}, avec r est comprise entre 0 et 1.
- Soit il est déclaré en panne si son énergie est inférieure à r_γ. Considérons X_i la variable aléatoire qui représente l'état du noeud au temps $t > t_0$:

$$X_i = \begin{cases} 1, & \text{si le noeud est en bon état} \\ 0, & \text{si le noeud est défaillant} \end{cases} \tag{4.2}$$

X_i est une variable aléatoire de Bernoulli dont la loi de probabilité est donnée par :

$$F_{X_i}(x) = \mathbb{P}(X_i \leq x) = p^x(1-p)^{1-x} \tag{4.3}$$

avec : $x \in \{0, 1\}$ and $p = r_\gamma$

Dans l'étude de simulation, nous fixons r_γ à 3 joules et r à $0,25$.

4.5 Évaluation des performances et discussion

Dans cette section, nous présentons l'environnement de simulations et les performances du protocole proposé ainsi qu'une comparaison avec d'autres protocoles pour illustrer les gains apportés par notre contribution.

4.5.1 Environnement de travail

Pour évaluer les performances du protocole proposé, un ensemble de simulations a été réalisé en utilisant le simulateur OMNeT++. Nous avons évalué les métriques suivantes : durée de vie du réseau, délai de bout en bout, taux de livraison des paquets et consommation d'énergie. Les résultats obtenus sont comparés à ceux fournis par d'autres protocoles dans le même environnement de simulation que celui présenté dans [6]. Chaque résultat de simulation présenté dans ce chapitre est la moyenne de 200 expériences indépendantes. Le nombre de noeuds varie de 50 à 300 qui sont déployés de manière non uniforme sur un champ de $200m \times 200m$. Les paramètres des simulations sont présentés dans le tableau 4.1.

TABLE 4.1 – Paramètres de simulation (EE-FT)

Paramètres	Valeurs
Simulateur utilisé	OMNET++/Castalia
Environnement radio	UDGM (Unit Disk Graph Medium)
Surface de déploiement	$200m \times 200m$
Nombre de noeuds	100
Localisation de la station de base	(250,100)
Taille du paquet	500 bytes
E_{elec}	$50nJ/bit$
ϵ_{fs}	$10\ pJ/(bit\,m^2)$
ϵ_{mp}	$0.0013\ pJ/(bit\,m^4)$
E_{sen}	$0J/bit$
E_{com}	$5nJ/(bit\,signal)$

4.5.2 Résultats de Simulation

Dans cette section, nous présentons les résultats obtenus après simulations et nous les comparons à ceux des protocoles EADC [6] et EFT-PMD [8].

a) Durée de vie du réseau

La figure 4.1 montre que la durée de vie du réseau dans les protocoles EE-FT, EADC et EFT-PMD dans un réseau contenant 100 noeuds de capteurs. Cette figure illustre que le protocole EE-FT dépasse ceux des protocoles EADC et EFT-PMD. Ceci est dû d'une part que le protocole EE-FT optimise la consommation d'énergie du réseau et d'autre part qu'il permet l'équilibrage de charge entre les clusters efficacement par rapport aux deux protocoles puisqu'il implique un processus de réaffiliation lors de l'opération de clustering. Cette méthode de réaffiliation permet aux noeuds appartenant à des clusters qui contiennent un grand nombre de membres de rejoindre des clusters contenant un petit nombre de noeuds. En outre, dans le protocole EE-FT, la méthode de clustering utilisée ne nécessite pas l'intervention de la station de base, ce qui évite l'échange de messages

entre les noeuds et la station de base. En conséquence, il y aurait moins d'énergie dissipée ce qui se répercute sur la durée de vie du réseau. De plus, le choix du plus court chemin réduit le nombre des noeuds participants dans le chemin de routage des données vers la station de base, ce qui minimise la consommation d'énergie dans le réseau. Dans EE-FT, la probabilité de demande de retransmissions de paquets à la station de base est quasiment nulle grâce à l'implication des CHs qui ont suffisamment d'énergie dans le processus de routage de données à la station de base. Ces noeuds CHs sont choisis à l'aide de la méthode de prévention des pannes qui est basée sur la probabilité de Bernoulli.

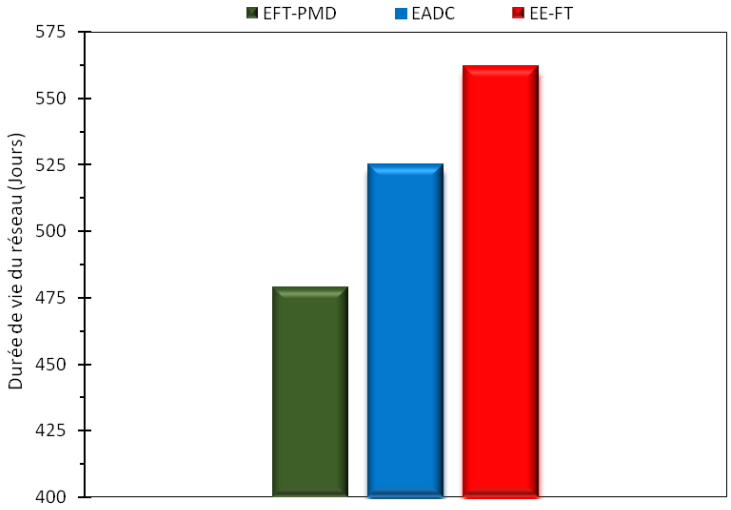


FIGURE 4.1 – Durée de vie du réseau vs Nombre de noeuds

b) Taux de perte de paquets

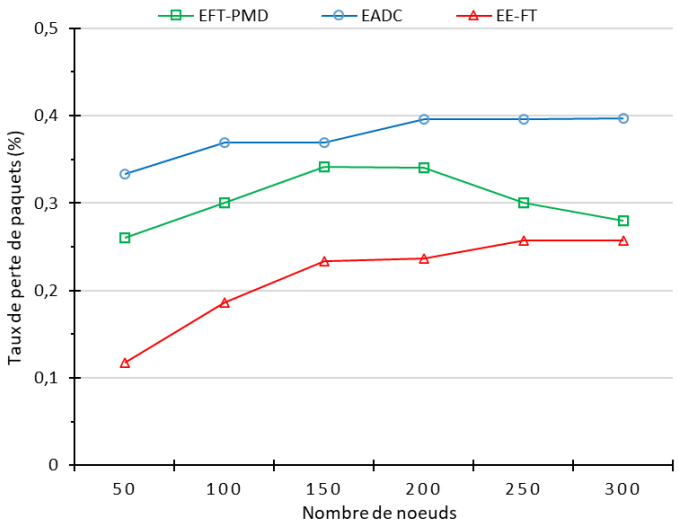


FIGURE 4.2 – Taux de perte de paquets vs Nombre de noeuds

La figure 4.2 illustre le taux de perte de paquets dans les trois protocoles : EFT-PMD , EADC et EE-FT. Comme le montre cette figure, le protocole EE-FT fournit des meilleures

performances par rapport aux deux autres protocoles grâce à l'utilisation de la méthode d'évitement de pannes dans laquelle le processus de routage des données évite les noeuds CHs avec une faible probabilité de fiabilité selon la loi de Bernouli. De plus, le protocole EE-FT implique les CHs qui ont plus d'énergie dans le processus de routage. Le protocole EE-FT surpasse EFT-PMD en termes de taux de perte des paquets qui prouve que la tolérance aux pannes avec un aspect préventif utilisé dans EE-FT donne des meilleurs résultats que le routage tolérant aux pannes avec un aspect curatif basé sur la méthode des chemins disjoints utilisée dans EFT-PMD.

c) Délai de bout en bout

La figure 4.3 montre le délai moyen de bout en bout dans les protocoles EE-FT, EADC et EFT-PMD. Le protocole EE-FT surpasse le protocole EFT-PMD en termes de délai moyen de bout en bout, ce qui prouve que la tolérance aux pannes avec aspect préventif utilisée dans notre protocole fournit de meilleurs résultats que la tolérance aux pannes avec aspect curatif basée sur la stratégie de chemins disjoints utilisée dans le protocole EFT-PMD. L'aspect préventif de notre solution permet de prédire les défaillances dans le réseau et donc d'éviter les noeuds moins fiables lors du routage des données, ce qui permet d'éviter les retransmissions et donc de réduire le délai moyen de bout en bout. De plus, le délai moyen réduit dans le protocole EE-FT par rapport à ceux des protocoles EADC et EFT-PMD est obtenu grâce à la méthode d'amélioration de la durée de vie du réseau dans EE-FT qui est basée sur le clustering et l'équilibrage de charge entre les noeuds CHs. Par conséquent, la probabilité que des CHs défaillants participent au processus de routage est presque nulle, ce qui évite les retransmissions de paquets perdus et minimise le délai de bout en bout.

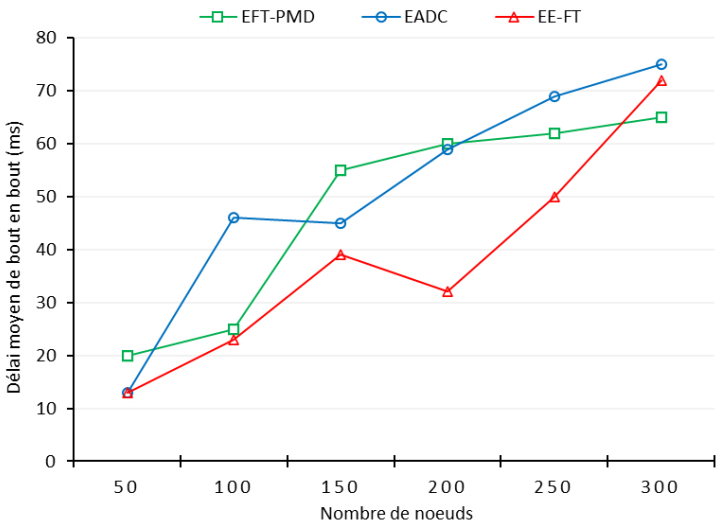


FIGURE 4.3 – Délai moyen de bout en bout vs Nombre de noeuds

4.6 EE-FTR : Routage tolérant aux pannes et économe en énergie à aspect curatif

Dans cette section, nous présentons notre contribution qui consiste en un protocole de routage tolérant aux pannes et économe en énergie, appelé EE-FTR.

4.6.1 Éléments du protocole EE-FTR

Dans ce qui suit, nous décrivons les éléments du protocole EE-FTR.

a) Tolérance aux pannes

Après la sélection des CHs de la même manière que dans [6]. Dans chaque cluster, le noeud ayant l'énergie maximale parmi les noeuds membres du cluster est sélectionné comme CH assistant (secondaire) et peut prendre le rôle du CH principal en cas de défaillance de ce dernier.

b) Le rôle de l'assistant CH

Le CH assistant est le seul noeud qui est notifié de la part du CH principal après avoir envoyé les données détectées. S'il ne reçoit pas l'accusé de réception ou s'il ne reçoit pas l'attribution d'un créneau horaire au début d'une nouvelle frame, il suppose que le CH principal est défaillant. Pour s'assurer de la défaillance du CH principal, il déclenche un temporisateur et envoie un message "Hello". S'il ne reçoit pas de réponse, il considère que le CH est vraiment défaillant et il se déclare comme nouveau CH principal. Ensuite, il change sa position pour celle du CH défaillant afin de garder la connectivité avec les noeuds du cluster et les autres CHs, et envoie aux noeuds membres de son cluster le début d'une frame dans laquelle à chaque noeud membre une tranche de temps (slot) lui a été affectée. Puis, le CH assistant envoie aux CH voisins un paquet qui contient son identifiant "ID" et celui du CH défaillant. Les CHs choisissent une route qui ne contient pas le noeud défaillant. Les noeuds du cluster (membres du cluster) conservent les données détectées pendant une période T et s'ils ne reçoivent pas de demande de retour de données, ils les suppriment. La sélection du CH assistant s'effectue selon l'algorithme 4.

c) Processus de routage

Le processus d'établissement des chemins entre les CHs et la station de base (BS) comme c'est présenté dans l'algorithme 5. La station de base envoie le message de découverte de routes ($Route\_Msg$) aux CHs qui se trouvent à un saut d'elle. Le message contient les informations suivantes : L'identifiant (ID), l'énergie et le nombre de sauts vers la station de base. L'énergie est initialisée à zéro et le nombre de sauts également. De plus, lorsqu'un CH reçoit le message de découverte de chemins, il ajoute son énergie résiduelle à l'énergie reçue selon l'équation 4.4, ajoute l'ID de la source avec l'énergie moyenne à la station de base dans sa table de routage où l'énergie moyenne est donnée par l'équation 4.5.

$$Energie = Energie_{Res} + Energie_{Rec} \tag{4.4}$$

Algorithm 4 :Sélection du CH assistant

1: **Begin**
Input : Ensemble des membres du cluster
Output : Le noeud avec l'énergie la plus élevée parmi les membres du cluster (CH Assistant)
2: $Nb = Size(C_i)$;
- Nb est le nombre de membres dans le cluster C_i
3: $EM = N[1]$;
4: **for** $j = 2$ **to** $j = Nb$ **do**
5: **if** $((EM \neq CH) \wedge (Energy(N[j]) > Energy(EM)))$ **then**
6: $EM \leftarrow N[j]$
7: **end if**
8: **end for**
9: **End**

où $Energie_{Res}$ et $Energie_{Rec}$ représentent respectivement l'énergie résiduelle du noeud et l'énergie reçue.

$$Taux_{Energie} = \frac{Energy}{Nombre_{Sauts-To-BS}} \tag{4.5}$$

où $Nombre_{Sauts-To-BS}$ représente le nombre de sauts de la station de base jusqu'au noeud qui a reçu le message de découverte de routes.

Algorithm 5 : Processus du routage basé sur le clustering

1: **Begin**
2: SB : Envoie le message de découverte de routes $Route\_Msg$ aux CHs qui sont à un saut ;
- $Route\_Msg$ contient l'identifiant de la station de base (BS),
le nombre de sauts ($Nombe_{Sauts-To-BS} = 0$) et l'énergie ($Energie = 0$) ;
3: CHs : Envoie $Route\_Msg$ aux CHs dans leur rayon de transmission (R_c)
4: CHs : Reçoit $Route\_Msg$: chaque CH met à jour sa table de routage en ajoutant des CHs émetteurs et l'énergie moyenne :
$Taux_{Energie} = \frac{Energy}{Nombre_{Sauts-To-BS}}$;
5: **End**

Le noeud CH augmente le nombre de sauts et ajoute son énergie au message de découverte de routes $Route\_Msg$ et répond à la station de base, et ainsi de suite. Lorsqu'il envoie les données détectées à la station de base, le CH sélectionne le chemin avec la moyenne d'énergie maximale. Si un CH ne reçoit pas de message d'accusé de réception (un message ACK) dans le temps "t", il considère que le paquet est perdu, et il sélectionne le deuxième chemin avec la valeur la plus élevée dans sa table de routage, et ainsi de suite comme indiqué dans l'algorithme 6. Chaque CH conserve une copie du paquet jusqu'à ce qu'il reçoive un message d'accusé de réception. La table de routage est mise à jour après chaque phase de découverte de routes.

Pour garantir une couverture maximale de la zone de surveillance, le rayon de communication du noeud (R_c) est supposé être deux fois plus grand que la zone de couverture

Algorithm 6 : Envoie des données

1: **Begin**
2: Trier la table de routage en fonction de l'énergie moyenne maximale ;
3: Choisir le chemin en fonction de l'énergie moyenne maximale) ;
4: **if** CH ne reçoit pas de message ACK **then**
5: Choisir un autre chemin ;
6: **end if**
7: **End**

(R_s) ($R_c = 2R_s$).

Le protocole EE-FTR se déroule comme s'est illustré par l'organigramme de la figure 4.4.

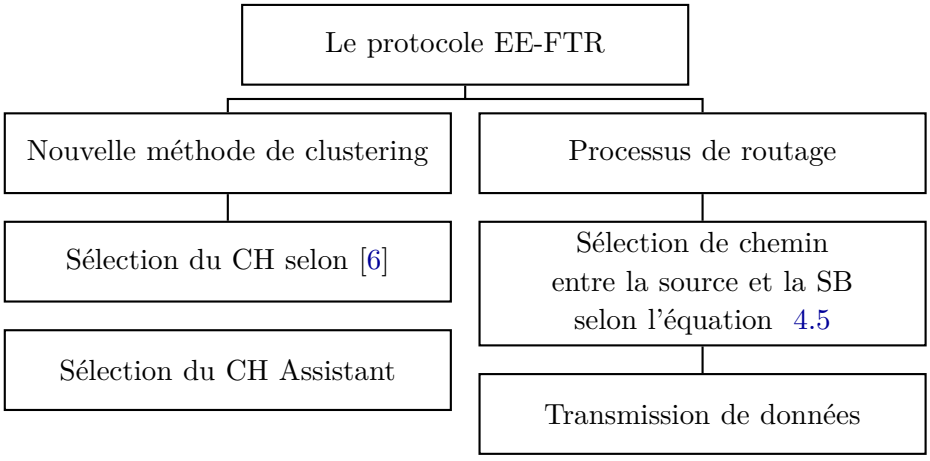


FIGURE 4.4 – Un organigramme illustrant le fonctionnement du protocole EE-FTR

4.7 Évaluation des performances et discussion

Dans cette section, nous évaluons les performances du protocole EE-FTR et nous les comparons à celle du protocole EFT-PMD [8].

4.7.1 Environnement de travail

Pour évaluer les performances de notre contribution, nous avons effectué plusieurs simulations sur OMNET++ et le framework Castalia. Chaque résultat de simulation présenté dans ce chapitre est la moyenne de 100 expériences indépendantes. Le nombre de noeuds est entre 100 et 500 qui sont déployés de manière uniforme sur un champ de $1000m \times 1000m$. Les paramètres des simulations sont présentés dans le tableau 4.2.

TABLE 4.2 – Paramètres de simulation (EE-FTR)

Paramètres	Valeurs
Simulateur réseau	OMNET++/Castalia
Environnement radio	UDGM (Unit Disk Graph Medium)
Surface de déploiement	$1000m \times 1000m$
Nombre de noeuds	$100 - 500$
Localisation de BS	$(1000, 500)$
Taille du paquet	500 bytes
E_{elec}	$50nJ/bit$
ε_{fs}	$10pJ/(bit\,m^2)$
ε_{mp}	$0.0013pJ/(bit\,m^4)$
E_{Sen}	$0J/bit$
E_{Com}	$5nJ/(bit\,signal)$
Énergie initiale des noeuds	3J

4.7.2 Analyse des performances

Pour illustrer les performances du protocole proposé, un ensemble de simulations a été effectué sur le simulateur OMNeT++. Nous évaluons les mesures suivantes : durée de vie du réseau, délai de bout en bout, taux de livraison des paquets et consommation d'énergie. Les résultats obtenus sont comparés à ceux fournis par le protocole EFT-PMD dans le même environnement de simulation.

a) Durée de vie du réseau

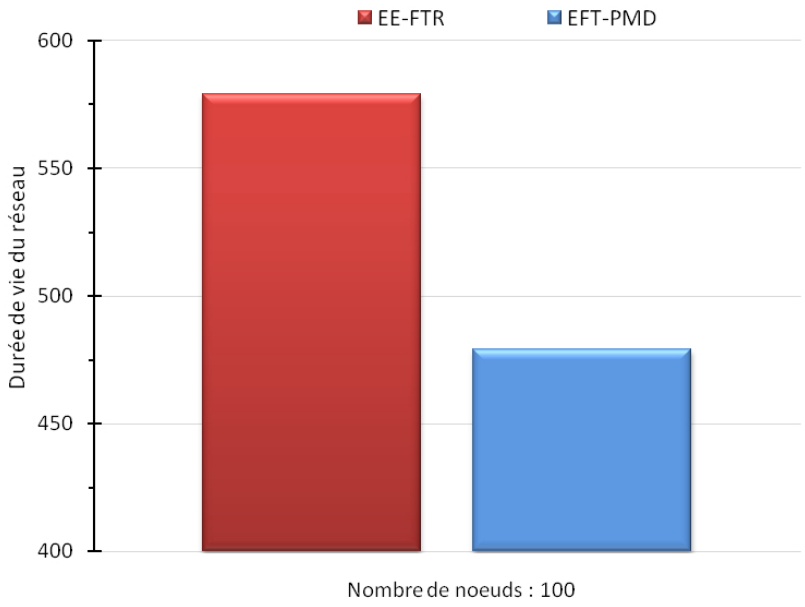


FIGURE 4.5 – Durée de vie pour un RCSF de 100 noeuds

La notion de durée de vie du réseau varie d'un contexte à un autre. Dans certains contexte, la durée de vie est définie comme étant le temps écoulé entre le déploiement du réseau et la mort du dernier noeud dans le réseau ou un certain pourcentage de noeuds. Dans ce contexte, nous supposons que la durée de vie du réseau est le temps écoulé entre le déploiement du réseau et la mort du premier noeud.

La figure 4.5 montre que la durée de vie du réseau obtenue par les protocoles : EE-FTR et EFT-PMD [8] à travers la simulation pour un réseau dont la taille est 100 noeuds où chaque noeud a une énergie initiale de $3J$. Les résultats obtenus montrent que la durée de vie du réseau fournie par notre protocole dépasse celle du protocole EFT-PMD. Notre protocole optimise la consommation d'énergie du réseau grâce à la méthode de clustering utilisée et au processus de routage adopté.

b) Délai moyen de livraison de paquets

Le délai moyen de livraison de paquets est le temps pris par un paquet de données envoyé par un noeud source à la station de base. La figure 4.6 montre le temps nécessaire pour transmettre un paquet de données d'un noeud source à la station de base dans les deux protocoles (EE-FTR et EFT-PMD). Ce temps est estimé en fonction de la taille du réseau afin d'illustrer la robustesse des protocoles lorsque le nombre de noeuds dans le réseau augmente (passage à l'échelle).

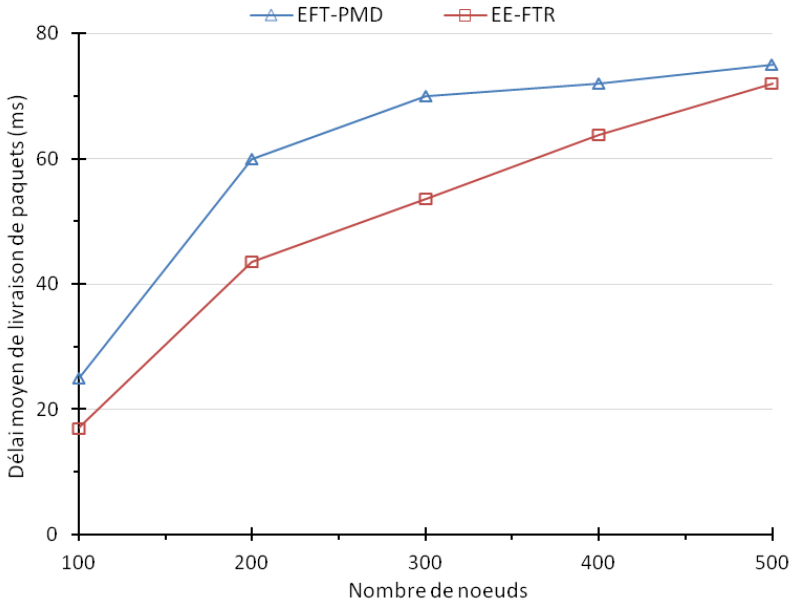


FIGURE 4.6 – Délai moyen de livraison de paquets vs Nombre de noeuds

Comme le montre la figure 4.6, le délai moyen de livraison de paquets est faible dans le protocole EE-FTR par rapport à celui dans le protocole EFT-PMD grâce à la diminution du nombre de retransmissions due à la méthode de clustering utilisée et au choix du meilleur chemin en termes d'énergie et de nombre de sauts.

c) Taux de livraison des paquets (PDR)

Le taux de livraison de paquets (PDR : Packet Delivery Ratio) est le rapport entre le nombre de paquets reçus à la station de base et le nombre de paquets envoyés depuis les noeuds sources. La figure 4.7 montre le taux de livraison des paquets en fonction de la taille du réseau dans les deux protocoles (EE-FTR et EFT-PMD). Comme le montre la figure 4.7, le taux de livraison de paquets augmente en fonction du nombre de noeuds dans le réseau car à mesure que le nombre de noeuds augmente, les zones avec des trous de routage seront remplies. De plus, le protocole EE-FTR fournit un PDR plus élevé que le protocole EFT-PMD en raison du choix de meilleurs chemins et de l'implication du CH assistant dans le processus de routage lorsque le CH principal cesse de fonctionner dans le protocole EE-FTR.

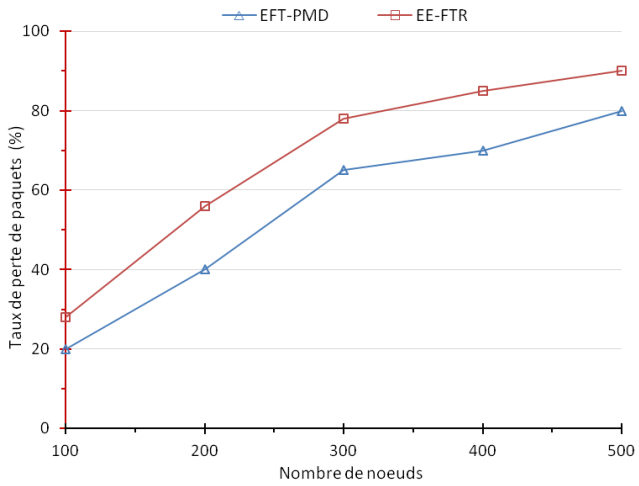


FIGURE 4.7 – Taux de livraison de paquets vs Nombre de noeuds

d) Consommation d'énergie

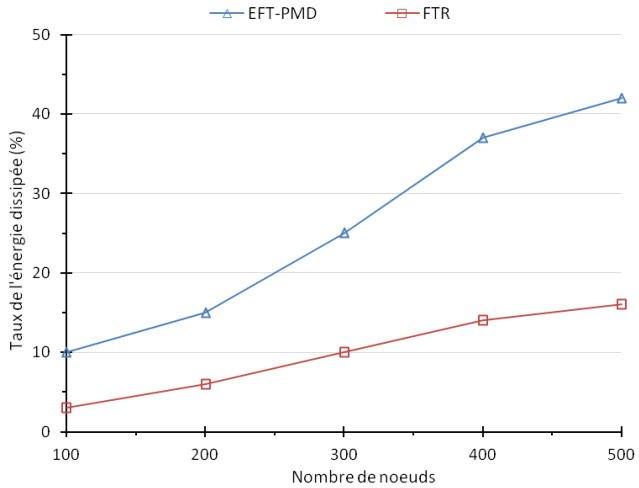


FIGURE 4.8 – Consommation d'énergie vs Nombre de noeuds

La figure 4.8 montre que l'énergie dissipée moyenne dans notre protocole est faible par rapport à celle du protocole EFT-PMD. Ce résultat s'explique par l'utilisation de la méthode de clustering, qui implique des CHs assistants dans les clusters lorsque les CHs principaux cessent de fonctionner, et en minimisant le nombre de retransmissions grâce au choix des chemins fiables qui permettent également la tolérance aux pannes. Les résultats de simulation montrent que le protocole EE-FTR fournit de meilleurs résultats en termes de consommation d'énergie quelle que soit la taille du réseau (dense ou moins dense) par rapport au protocole EFT-PMD.

4.8 Conclusion

Dans ce chapitre, nous avons proposé deux contributions qui assurent la tolérance aux pannes dans les RCSFs tout en optimisant la consommation d'énergie. Ces deux contributions sont basées sur une approche de clustering inspirée de la méthode EADC. Cette technique de clustering utilisée permet de homogénéiser le nombre de noeuds dans les clusters où le processus de clustering implique une phase de réaffiliation durant laquelle les noeuds appartenant à des clusters denses migrent vers des clusters moins denses. Cette stratégie permet alors de minimiser la consommation d'énergie intra-clusters et d'équilibrer la charge entre les différents CHs. De plus, pour améliorer la consommation d'énergie inter-clusters, les paquets agrégés passent par le chemin le plus court vers la station de base afin d'optimiser la consommation d'énergie dans le réseau.

Dans la première contribution, le protocole proposé est un protocole de routage tolérant aux pannes à aspect préventif. Il implique une méthode d'évitement des défaillances basée sur la probabilité de Bernoulli où chaque CH retire les CHs de sa table de routage ayant la plus grande probabilité de défaillance. Cette probabilité de défaillance est calculée en fonction de l'énergie résiduelle du CH.

Les résultats de simulations ont montré que le protocole EE-FT offre de meilleures performances par rapport aux protocoles EADC et EFT-PMD en termes de durée de vie du réseau, de délai moyen de bout en bout et de taux de perte de paquets.

La deuxième contribution consiste en un protocole de routage tolérant aux pannes économe en énergie à aspect curatif. Dans ce protocole, la méthode de clustering est basée sur la sélection d'un noeud CH alternatif appelé CH assistant en cas de défaillance du CH principal dans un cluster où le noeud avec la plus grande quantité d'énergie parmi les membres du cluster est élu comme CH assistant.

Les résultats de simulations ont montré que le protocole EE-FTR proposé offre de meilleures performances par rapport au protocole EFT-PMD en termes de délai moyen de livraison de paquets, de débit de livraison des paquets, de dissipation d'énergie et de durée de vie du réseau. Le protocole EE-FTR fournit des bons résultats grâce à la méthode de clustering utilisée qui offre de meilleures performances dans un environnement uniforme, ainsi que la méthode de routage des paquets agrégés utilisée, en choisissant le meilleur chemin en termes d'énergie et de nombre de sauts.

Conclusion Générale

Conclusion Générale

Les spécificités des noeuds capteurs leur permettent de participer dans diverses applications importantes et critiques. Cependant, ces dispositifs sont vulnérables aux pannes qui affectent les performances des RCSF. La vulnérabilité des noeuds capteurs est due à leurs limitations notamment en termes d'énergie et aux environnements hostiles dans lesquels ils sont déployés, ce qui peut provoquer leur défaillance. Par conséquent, il est primordial de faire appel à des mécanismes de tolérance aux pannes permettant de surmonter ces limitations. Ainsi, notre travail de thèse est axé sur la tolérance aux pannes dans les RCSFs avec des aspects préventifs et curatifs où nous avons proposé trois (03) contributions.

Après un premier chapitre consacré aux généralités sur les RCSFs et la tolérance aux pannes pour connaître leurs caractéristiques et leurs contraintes, une étude bibliographique sur le sujet a fait l'objet du deuxième chapitre de cette thèse pour décortiquer les atouts et les limitations des travaux existants. Cette étude nous a permis de proposer trois contributions :

- La première contribution est une approche de tolérance aux pannes pour les RCSFs. Cette approche est scindée en deux phases. Dans la première phase de cette approche, nous avons proposé une méthode de détection des noeuds critiques dont la défaillance dégrade la durée de vie du réseau en utilisant des algorithmes génétiques avec une heuristique de recherche locale. La deuxième phase consiste à appliquer une méthode d'augmentation en ajoutant des liens sans fil pour maintenir la connectivité du réseau en cas de défaillance de l'un des noeuds critiques.

- La deuxième contribution consiste en un protocole de routage tolérant aux pannes pour les RCSFs. L'approche améliore l'optimisation de la consommation d'énergie en utilisant une méthode de clustering qui homogénéise le nombre de noeuds dans les clusters pour équilibrer la charge entre les noeuds CHs. Elle propose également une méthode d'évitement des pannes basée sur la méthode de Bernoulli qui consiste à éviter d'impliquer les noeuds CHs dont la probabilité qu'ils cessent de fonctionner en raison de leur manque d'énergie est élevée.

- La troisième contribution est une approche pour la tolérance aux pannes des noeuds CHs qui sont considérés comme des noeuds importants avec le recours à des CHs alternatifs qui sont les noeuds ayant la plus grande quantité d'énergie dans leurs clusters. L'approche propose également une méthode de sélection du chemin le plus court basée sur l'énergie résiduelle des noeuds et la distance qui les sépare de la station de base.

Les trois contributions ont été évaluées et comparées à d'autres travaux existants et les résultats obtenus à travers des simulations intensives ont montré que les contributions proposées ont fourni de meilleures performances par rapport à ces travaux.

En perspectives, dans la première contribution, au lieu de se focaliser uniquement sur le paramètre de durée de vie dans la sélection des noeuds critiques, nous proposons d'ajouter d'autres paramètres dans la sélection des noeuds critiques et l'approche d'augmentation. Dans la deuxième contribution, nous envisageons une amélioration de notre proposition afin qu'elle puisse fournir une tolérance aux pannes avec les deux aspects préventifs et curatifs alors que dans la troisième contribution, nous prévoyons d'utiliser un protocole à chemins disjoints basé sur le protocole AOMDV en gardant la même méthode de clustering pour fournir un protocole de routage tolérant aux pannes très efficace.

Références Bibliographiques

Bibliographie

[1] T. Rault, *Energy-efficiency in wireless sensor networks*. PhD thesis, Université de Technologie de Compilègne, October 2015.

[2] G. Anastasi, M. Conti, M. Di Francesco, and A. Passarella, "Energy conservation in wireless sensor networks : A survey," *Ad Hoc Networks*, vol. 7, no. 3, pp. 537–568, 2009.

[3] H. Huo, Y. Xu, H. Yan, S. Mubeen, and H. Zhang, "An elderly health care system using wireless sensor networks at home," in *Proceedings of the Third International Conference on Sensor Technologies and Applications*, (Athens, Greece), pp. 158–163, IEEE, 2009.

[4] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences*, vol. 2, (Maui, HI, USA), pp. 1–10, IEEE, January 2000.

[5] K. Belkadi, M. Lehsaini, and M. A. Tahraoui, "Fault-tolerance based on augmenting approach in wireless sensor networks," *Concurrency and Computation : Practice and Experience*, vol. 34, no. 28, p. e7359, 2022.

[6] Y. Jiguo, Q. Yingying, W. Guanghui, and G. Xin, "A cluster-based routing protocol for wireless sensor networks with nonuniform node distribution," *AEU - International Journal of Electronics and Communications*, vol. 66, no. 1, pp. 54–61, 2012.

[7] K. Belkadi and M. Lehsaini, "Energy-efficient fault-tolerant routing for wireless sensor networks," in *Proceedings of the Second International Workshop on Human-Centric Smart Environments for Health and Well-being (IHSH)*, (Boumerdes, Algeria), pp. 131–136, IEEE, 2021.

[8] S. Sivakumar and P. Vivekanandan, "Efficient fault-tolerant routing in IoT wireless sensor networks based on path graph flow modeling with Marchenko–Pastur distribution (EFT-PMD)," *Wireless networks*, vol. 26, no. 6, pp. 4543–4555, 2020.

[9] K. Belkadi and M. Lehsaini, "EE-FTR : An Energy-Efficient Fault-Tolerant Routing Protocol for Wireless Sensor Networks," in *Proceedings of the 4th International Conference on Networking, Information Systems & Security*, (Kenitra, Morocco), pp. 1–5, ACM, 2021.

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

[11] T. Voigt, H. Ritter, and J. Schiller, "Utilizing solar power in wireless sensor networks," in *Proceedings of the28th Annual IEEE International Conference on Local Computer Networks*, (Bonn/Konigswinter, Germany), pp. 416–422, IEEE, 2003.

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

[13] C. A. Boano, J. Brown, Z. He, U. Roedig, and T. Voigt, "Low-Power Radio Communication in Industrial Outdoor Deployments : The Impact of Weather Conditions and ATEX-Compliance," in *Proceedings of International Conference on Sensor Applications, Experimentation, and Logistics* (N. Komninos, ed.), (Berlin, Heidelberg), pp. 159–176, Springer, 2010.

[14] V. Raghunathan, C. Schurgers, P. Sung, and M. B. Srivastava, "A Qualitative comparison of different logical topologies for wireless sensor networks," *Sensors (Basel)*, vol. 12, no. 11, p. 14887–14913, 2002.

[15] A. Cerpa, J. Elson, D. Estrin, L. Girod, M. Hamilton, and J. Zhao, "Habitat monitoring : Application driver for wireless communications technology," *ACM SIGCOMM Computer Communication Review*, vol. 31, no. 2, p. 20–41, 2001.

[16] G. Hoblos, M. Staroswiecki, and A. Aitouche, "Optimal design of fault tolerant sensor networks," in *Proceedings of IEEE International Conference on Control Applications*, (Anchorage, AK, USA), pp. 467–472, IEEE, September 2000.

[17] A.-S. Porret, T. Melly, C. Enz, and E. Vittoz, "A low-power low-voltage transceiver architecture suitable for wireless distributed sensors network," in *Proceedings of International Symposium on Circuits and Systems (ISCAS)*, vol. 1, (Geneva, Switzerland), pp. 56–59 vol.1, IEEE, 2000.

[18] H. Deng and R. Xu, "Acoustic threatening sound detection and recognition using wireless sensor networks," in *Proceedings of SPIE - The International Society for Optical Engineering*, pp. 73050S–73050S, 01 2009.

[19] B. Hariharan and A. Sasidharan, "iWEDS-An Intelligent Explosive Detection and Terrorist Tracking System Using Wireless Sensor Network," *International Journal of Computer Science Issues*, vol. 8, pp. 550–554, 07 2011.

[20] N. Shimoi, Y. Takita, K. Nonami, and K. Wasaki, "Smart sensing for mine detection studies with ir cameras," in *Proceedings of International Symposium on Computational Intelligence in Robotics and Automation (Cat. No.01EX515)*, (Banff, AB, Canada), pp. 356–361, IEEE, 2001.

[21] R. Cardell-Oliver, K. Smettem, M. Kranz, and K. Mayer, "Field testing a wireless sensor network for reactive environmental monitoring [soil moisture measurement]," in *Proceedings of International Conference on Intelligent Sensors, Sensor Networks and Information Processing Conference, 2004.*, (Melbourne, VIC, Australia), pp. 7–12, IEEE, 2004.

[22] X. Cao, J. Chen, Y. Zhang, and Y. Sun, "Development of an integrated wireless sensor network micro-environmental monitoring system," *ISA Transactions*, vol. 47, no. 3, pp. 247–255, 2008.

[23] A. Cakir, "Smart clothing – technology and applications," *Behaviour & Information Technology*, vol. 30, no. 2, pp. 287–288, 2011.

[24] S. Kaur and R. Mahajan, "Energy efficient clustering protocol for wireless sensor networks," *Modern Physics Letters B*, vol. 32, no. 32, p. 1850400 (12 pages), 2018.

[25] S. M. M. H. Daneshvar, P. Alikhah Ahari Mohajer, and S. M. Mazinani, "Energy-Efficient Routing in WSN : A Centralized Cluster-Based Approach via Grey Wolf Optimizer," *IEEE Access*, vol. 7, pp. 170019–170031, 2019.

[26] K. Agarwal, K. Agarwal, and K. Muruganandam, "Low Energy Adaptive Clustering Hierarchy (LEACH) Protocol : Simulation and Analysis using MATLAB," in *Proceedings of International Conference on Computing, Power and Communication Technologies (GUCON)*, (Greater Noida, India), pp. 60–64, IEEE, 2018.

[27] T. Kaur and D. Kumar, "Particle swarm optimization-based unequal and fault tolerant clustering protocol for wireless sensor networks," *IEEE Sensors Journal*, vol. 18, no. 11, pp. 4614–4622, 2018.

[28] E. Moridi, M. Haghparast, M. Hosseinzadeh, and S. Jafarali Jassbi, "Novel fault-tolerant clustering-based multipath algorithm (FTCM) for wireless sensor networks," *Telecommunication Systems*, vol. 74, no. 4, pp. 411–424, 2020.

[29] O. Younis and S. Fahmy, "HEED : a Hybrid, Energy-Efficient, Distributed clustering approach for ad hoc sensor networks," *IEEE Transactions on mobile computing*, vol. 3, no. 4, pp. 366–379, 2004.

[30] S. Jafarali Jassbi and E. Moridi, "Fault tolerance and energy efficient clustering algorithm in wireless sensor networks : FTEC," *Wireless Personal Communications*, vol. 107, no. 1, pp. 373–391, 2019.

[31] B. M. Sahoo, H. M. Pandey, and T. Amgoth, "GAPSO-H : A hybrid approach towards optimizing the cluster based routing in wireless sensor network," *Swarm and Evolutionary Computation*, vol. 60, p. 100772, 2021.

[32] T. A. Alghamdi, "Energy efficient protocol in wireless sensor network : optimized cluster head selection model," *Telecommunication Systems*, vol. 74, no. 3, pp. 331–345, 2020.

[33] V. Pandiyaraju, R. Logambigai, S. Ganapathy, and A. Kannan, "An energy efficient routing algorithm for WSNs using intelligent fuzzy rules in precision agriculture," *Wireless Personal Communications*, vol. 112, no. 1, pp. 243–259, 2020.

[34] D. N. Quoc, N. Liu, and D. Guo, "A hybrid fault-tolerant routing based on Gaussian network for wireless sensor network," *Journal of Communications and Networks*, vol. 24, no. 1, pp. 37–46, 2021.

[35] S. J. Bhat and K. V. Santhosh, "Fault tolerant localization based on k-means clustering in wireless sensor networks," in *Proceedings of International Conference on Electronics, Computing and Communication Technologies (CONECCT)*, (Bangalore, India), pp. 1–5, IEEE, 2020.

[36] A. Nayyar and R. Singh, "IEEMARP-a novel energy efficient multipath routing protocol based on ant Colony optimization (ACO) for dynamic sensor networks," *Multimedia Tools and Applications*, vol. 79, no. 47, pp. 35221–35252, 2020.

[37] M. N. Bouatit, S. Boumerdassi, and R. H. Milocco, "Non-interfering multipath mechanism for media stream transmission in wireless sensor networks," in *Proceedings of International Conference on Mobile, Secure, and Programmable Networking*, (Paris, France), pp. 311–321, Springer, 2018.

[38] R. C. Shah and J. M. Rabaey, "Energy aware routing for low energy ad hoc sensor networks," in *Proceedings of International Conference on Wireless Communications and Networking*, (Orlando, FL, USA), pp. 350–355, IEEE, 2002.

[39] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed Diffusion : a scalable and robust communication paradigm for sensor networks," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom'00)*, (Boston, Massachusetts, USA), p. 56–67, ACM, August 2000.

[40] N. X. Tien, S. Kim, J. M. Rhee, and S. Y. Park, "A novel dual separate paths (DSP) algorithm providing fault-tolerant communication for wireless sensor networks," *Sensors*, vol. 17, no. 8, p. 1699, 2017.

[41] H. Hassanein and J. Luo, "Reliable energy aware routing in wireless sensor networks," in *Proceedings of the second IEEE workshop on dependability and security in sensor networks and systems*, (Columbia, MD, USA), pp. 54–64, IEEE, 2006.

[42] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly-resilient, energy-efficient multipath routing in wireless sensor networks," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 5, no. 4, pp. 11–25, 2001.

[43] Y. Chen, E. Chan, and S. Han, "Energy efficient multipath routing in large scale sensor networks with multiple sink nodes," in *Proceedings of International Workshop on Advanced Parallel Processing Technologies*, (Hong Kong, China), pp. 390–399, Springer, 2005.

[44] J. Chen, Z. Yin, D. Li, and T. Sun, "A distributed and effective cluster routing protocol of sensor networks," in *Proceedings of the First International Conference on*

Intelligent Networks and Intelligent Systems, (Wuhan, China), pp. 271–275, IEEE, 2008.

[45] H. Lu, J. Li, and G. Wang, "A novel energy efficient routing algorithm for hierarchically clustered wireless sensor networks," in *Proceedings of the Fourth International Conference on Frontier of Computer Science and Technology*, (Shanghai, China), pp. 565–570, IEEE, 2009.

[46] A. N. Njoya, A. A. A. Ari, M. N. Awa, C. Titouna, N. Labraoui, J. Y. Effa, W. Abdou, and A. Gueroui, "Hybrid wireless sensors deployment scheme with connectivity and coverage maintaining in wireless sensor networks," *Wireless Personal Communications*, vol. 112, no. 3, p. 1893–1917, 2022.

[47] C. Shivalingegowda and P. V. Y. Jayasree, "Hybrid gravitational search algorithm based model for optimizing coverage and connectivity in wireless sensor networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 2, pp. 2835–2848, 2021.

[48] J. Wang, Y. Gao, C. Zhou, S. Sherratt, and L. Wang, "Optimal coverage multi-path scheduling scheme with multiple mobile sinks for WSNs," *Computers, Materials & Continua*, vol. 62, no. 2, pp. 695–711, 2020.

[49] M. Elhoseny, A. Tharwat, X. Yuan, and A. E. Hassanien, "Optimizing K-coverage of mobile WSNs," *Expert Systems with Applications*, vol. 92, pp. 142–153, 2018.

[50] S. Harizan and P. Kuila, "A novel NSGA-II for coverage and connectivity aware sensor node scheduling in industrial wireless sensor networks," *Digital Signal Processing*, vol. 105, p. 102753, 2020.

[51] M. Karatas, "Optimal deployment of heterogeneous sensor networks for a hybrid point and barrier coverage application," *Computer Networks*, vol. 132, pp. 129–144, 2018.

[52] D. Li, W. Liu, and L. Cui, "Easidesign : an improved ant colony algorithm for sensor deployment in real sensor network system," in *Proceedings of Global Telecommunications Conference (GLOBECOM'2010)*, (Miami, FL, USA), pp. 1–5, IEEE, 2010.

[53] P. Huang, F. Lin, L. J. Xu, Z. L. Kang, J. Zhou, and J. S. Yu, "Improved ACO-based sweep coverage scheme considering data delivery," *International Journal of Simulation Modelling*, vol. 16, no. 2, pp. 289–301, 2017.

[54] M. Abo-Zahhad, N. Sabor, S. Sasaki, and S. M. Ahmed, "A centralized immune-Voronoi deployment algorithm for coverage maximization and energy conservation in mobile wireless sensor networks," *Information Fusion*, vol. 30, pp. 36–51, 2016.

[55] S. Chouikhi, I. El Korbi, Y. Ghamri-Doudane, and L. A. Saidane, "Routing-based multi-channel allocation with fault recovery for wireless sensor networks," in *Proceddings of IEEE International Conference on Communications (ICC)*, (London, UK), pp. 6424–6430, IEEE, 2015.

[56] M. N. Bouatit, S. Boumerdassi, P. Minet, and A. Djama, "Fault-tolerant mechanism for multimedia transmission in wireless sensor networks," in *Proceedings of the 84th Vehicular Technology Conference (VTC-Fall)*, (Montreal, QC, Canada), IEEE, 2017.

[57] V. Jha, N. Prakash, and A. K. Mohapatra, "Energy efficient model for recovery from multiple nodes failure in wireless sensor networks," *Wireless Personal Communications*, vol. 108, no. 3, pp. 1459–1479, 2019.

[58] W. Elsayed, M. Elhoseny, S. Sabbeh, and A. Riad, "Self-maintenance model for wireless sensor networks," *Computers & Electrical Engineering*, vol. 70, pp. 799–812, 2018.

[59] A. Ajay, N. Tarasia, S. Dash, S. Ray, and A. R. Swain, "A dynamic fault tolerant routing protocol for prolonging the lifetime of wireless sensor networks,"

[60] S. Chouikhi, I. El Korbi, Y. Ghamri-Doudane, and L. A. Saidane, "Articulation node failure recovery for multi-channel wireless sensor networks," in *Proceedings of IEEE Global Communications Conference (GLOBECOM)*, (San Diego, CA, USA), pp. 1–7, IEEE, 2015.

[61] E. Uzun, F. Senel, K. Akkaya, and A. Yazici, "Distributed connectivity restoration in underwater acoustic sensor networks via depth adjustment," in *Proceedings of International Conference on Communications (ICC)*, (London, UK), pp. 6357–6362, IEEE, 2015.

[62] M. Asim, H. Mokhtar, and M. Merabti, "A self-managing fault management mechanism for wireless sensor networks," *International Journal of Wireless & Mobile Networks (IJWMN)*, vol. 2, no. 4, pp. 184–197, 2010.

[63] M. Asim, H. Mokhtar, and M. Merabti, "A cellular approach to fault detection and recovery in wireless sensor networks," in *Proceedings of the Third International Conference on Sensor Technologies and Applications*, (Athens, Greece), pp. 352–357, IEEE, 2009.

[64] L. Sitanayah, "Robust sensor network deployment with priority based on failure centrality," in *Proceeding of the 10th International Conference on Information Technology and Electrical Engineering (ICITEE)*, (Bali, Indonesia), pp. 175–180, IEEE, 2018.

[65] N. Moussa, Z. Hamidi-Alaoui, and A. E. B. El Alaoui, "CFTM : A centralized fault tolerant mechanism for wireless sensor networks," in *Proceedings of the 5th International Conference on Optimization and Applications (ICOA)*, (Kenitra, Morocco), pp. 1–6, IEEE, 2019.

[66] M. Imran, M. Younis, A. M. Said, and H. Hasbullah, "Localized motion-based connectivity restoration algorithms for wireless sensor and actor networks," *Journal of Network and Computer Applications*, vol. 35, no. 2, pp. 844–856, 2012.

[67] V. K. Akram, Z. A. Dagdeviren, O. Dagdeviren, and M. Challenger, "PINC : Pickup Non-Critical Node Based k-Connectivity Restoration in Wireless Sensor Networks," *Sensors*, vol. 21, no. 19, p. 6418, 2021.

[68] K. Vaidya and M. Younis, "Efficient failure recovery in wireless sensor networks through active, spare designation," in *Proceedings of the 6th IEEE International Conference on Distributed Computing in Sensor Systems Workshops (DCOSSW)*, (Santa Barbara, CA, USA), pp. 1–6, IEEE, 2010.

[69] K. Akkaya, F. Senel, A. Thimmapuram, and S. Uludag, "Distributed recovery from network partitioning in movable sensor/actor networks via controlled mobility," *IEEE Transactions on Computers*, vol. 59, no. 2, pp. 258–271, 2009.

[70] X. Wang, L. Xu, and S. Zhou, "Restoration strategy based on optimal relay node placement in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 11, no. 7, p. 409085, 2015.

[71] G. Albers, L. J. Guibas, J. S. B. Mitchell, and T. Roos, "Voronoi diagrams of moving points," *International Journal of Computational Geometry & Applications*, vol. 8, no. 3, pp. 533–541, 1998.

[72] A. Kanevsky, "Finding all minimum size separating vertex sets in a graph," *Networks*, vol. 23, no. 6, pp. 533–541, 1993.

[73] M. Jorgic, M. Hauspie, D. Simplot-Ryl, and I. Stojmenovic, "Localized algorithms for detection of critical nodes and links for connectivity in ad hoc networks," in *Proceedings of the Third Annual Mediterranean Ad Hoc Networking Workshop*, (Bodrum,Turkey), p. 12 pages, IFIP, 2004.

[74] X. Liu, L. Xiao, A. Kreling, and Y. Liu, "Optimizing overlay topology by reducing cut vertices," in *Proceedings of International Workshop on Network and operating systems support for digital audio and video*, (Newport, Rhode Island), pp. 1–6, ACM, 2006.

[75] S. Loganathan, J. Arumugam, and V. Chinnababu, "An energy-efficient clustering algorithm with self-diagnosis data fault detection and prediction for wireless sensor networks," *Concurrency and Computation : Practice and Experience*, vol. 33, no. 17, p. e6288, 2021.

[76] S. Henna, "Energy Efficient Fault Tolerant Coverage in Wireless Sensor Networks," *Journal of Sensors*, vol. Volume 2017, p. Article ID 7090782, 2017.

[77] N. Mazumdar, A. Nag, and S. Nandi, "HDDS : Hierarchical Data Dissemination Strategy for energy optimization in dynamic wireless sensor network under harsh environments," *Ad Hoc Networks*, vol. 111, p. 102348, 2021.

[78] X. Liu, J. Yu, W. Zhang, and H. Tian, "Low-energy dynamic clustering scheme for multi-layer wireless sensor networks," *Computers & Electrical Engineering*, vol. 91, p. 107093, 2021.

[79] B. O. Kahjogh, I. Demirkol, D. Careglio, and J. D. Pascual, "The impact of critical node elimination on the latency of wireless sensor networks," in *Proceedings of the 9th International Conference on Ubiquitous and Future Networks (ICUFN)*, (Milan, Italy), pp. 182–187, IEEE, 2017.

[80] H. U. Yildiz, B. Tavli, B. O. Kahjogh, and E. Dogdu, "The Impact of Incapacitation of Multiple Critical Sensor Nodes on Wireless Sensor Network Lifetime," *IEEE Wireless Communications Letters*, vol. 6, no. 3, pp. 306–309, 2017.

[81] O. Dagdeviren, V. K. Akram, and B. Tavli, "Design and evaluation of algorithms for energy efficient and complete determination of critical nodes for wireless sensor network reliability," *IEEE Transactions on Reliability*, vol. 68, no. 1, pp. 280–290, 2019.

[82] S. Hoffmann and E. Wanke, "Generic Route Repair : Augmenting Wireless Ad Hoc Sensor Networks for Local Connectivity," in *Proceedings of the 15th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*, (Vienna, Austria), pp. 1–10, IEEE, 2016.

[83] A. Varga and R. Hornig, "An Overview of the OMNeT++ Simulation Environment," in *Proceedings of the First International Conference on Simulation tools and techniques for communications, networks and systems & workshops*, (Marseille, France), pp. 1–10, ACM, 2008.

[84] A. Boulis, "Castalia : Simulator for wireless sensor networks and body area networks user manual online," tech. rep., National Information and Communications Technology Australia Ltd (NICTA), 2011.

[85] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Proceedings of the 2nd Workshop on Mobile Computing Systems and Applications*, (New Orleans, LA, USA), pp. 90–100, IEEE, 1999.

[86] C. Duanbing, L. Linyuan, S. Ming-Sheng, Z. Yi-Cheng, and Z. Tao, "Identifying influential nodes in complex networks," *Physica A : Statistical Mechanics and its Applications*, vol. 391, no. 4, pp. 1777–1787, 2012.

[87] H. D. Ratliff, G. T. Sicilia, and S. H. Lubore, "Finding the n most vital links in flow networks," *Management Science*, vol. 21, no. 5, pp. 531–539, 1975.

[88] H. W. Corley and D. Y. Sha, "Most vital links and nodes in weighted networks," *Operations Research Letters*, vol. 1, no. 4, pp. 157–160, 1982.

[89] K. You, R. Tempo, and L. Qiu, "Distributed Algorithms for Computation of Centrality Measures in Complex Networks," *IEEE Transactions on Automatic Control*, vol. 62, no. 5, pp. 2080–2094, 2017.

[90] S. P. Borgatti, "Identifying sets of key players in a social network," *Computational and Mathematical Organization Theory*, vol. 12, p. 21–34, 2006.

[91] S. Shen and J. C. Smith, "Polynomial-time algorithms for solving a class of critical node problems on trees and series-parallel graphs," *Networks*, vol. 60, no. 2, pp. 103–119, 2012.

[92] S. Shen, J. C. Smith, and R. Goli, "Exact interdiction models and algorithms for disconnecting networks via node deletions," *Discrete Optimization*, vol. 9, no. 3, pp. 172–188, 2012.

[93] A. Arulselvan, C. W. Commander, L. Elefteriadou, and P. M. Pardalos, "Detecting critical nodes in sparse graphs," *Computers & Operations Research*, vol. 36, no. 7, pp. 2193–2200, 2009.

[94] M. Lalou, M. A. Tahraoui, and H. Kheddouci, "Component-Cardinality-Constrained Critical Node Problem in Graphs," *Discrete Applied Mathematics*, vol. 210, no. C, p. 150–163, 2016.

[95] W. Kiran, S. Smys, and V. Bindhu, "Clustering of WSN Based on PSO with Fault Tolerance and Efficient Multidirectional Routing," *Wireless Personal Communications*, vol. 121, pp. 31–47, 2021.

[96] T. Mahmood, J. Li, Y. Pei, F. Akhtar, S. A. Butt, A. Ditta, and S. Qureshi, "An intelligent fault detection approach based on reinforcement learning system in wireless sensor network," *The Journal of Supercomputing*, vol. 2021, pp. 1–30, 2021.

[97] P. Chanak, I. Banerjee, and S. Bose, "An intelligent fault-tolerant routing scheme for internet of things-enabled wireless sensor networks," *International Journal of Communication Systems*, vol. 34, no. 17, p. e4970, 2021.

[98] A. Arulselvan, C. W. Commander, P. M. Pardalos, and O. Shylo, "Managing network risk via critical node identification," tech. rep., Air Force Research Laboratory, Springer, 2007. Risk Management in Telecommunication Networks, B. Rustem and N. Gulpinar (editors).

[99] Y. Shen and M. T. Thai, "Network vulnerability assessment under cascading failures," in *Proceedings of International Conference on Global Communications Conference (GLOBECOM)*, (Atlanta, USA), pp. 1526–1531, IEEE, 2013.

[100] V. Boginski and C. W. Commander, "Identifying critical nodes in protein-protein interaction networks," *Clustering Challenges in Biological Networks*, pp. 153–167, 2009.

[101] V. Tomaino, A. Arulselvan, P. Veltri, and P. M. Pardalos, "Studying connectivity properties in human protein–protein interaction network in cancer pathway," in *Data Mining for Biomarker Discovery, Springer Optimization and Its Applications* (Z. M. e. Pardalos P., Xanthopoulos P., ed.), ch. 8, pp. 187–197, Springer, 2012.

[102] R. Cohen, S. Havlin, and D. Ben-Avraham, "Efficient Immunization Strategies for Computer Networks and Populations," *Physical review letters*, vol. 91, p. 247901 (4 pages), Dec 2003.

[103] P. Szczytowski, A. Khelil, and N. Suri, "DKM : Distributed k-connectivity maintenance in wireless sensor networks," in *Proceedings of the 9th Annual Conference on Wireless On-Demand Network Systems and Services (WONS)*, (Courmayeur, Italy), pp. 83–90, IEEE, 2012.

[104] H. Sheikhi, M. Hoseini, and M. Sabaei, "k-connected relay node deployment in heterogeneous wireless sensor networks," *Wireless Personal Communications*, 2021.

[105] S. Lee, M. Younis, and M. Lee, "Connectivity restoration in a partitioned wireless sensor network with assured fault tolerance," *Ad Hoc Networks*, vol. 24, pp. 1–19, 2015.

[106] A. Yuksel, E. Uzun, and B. Tavli, "The impact of elimination of the most critical node on wireless sensor network lifetime," in *Proceedings of IEEE Sensors Applications Symposium (SAS)*, (Zadar, Croatia), pp. 1–5, IEEE, 2015.

[107] O. B. C. D. Sembroiz, D. and Ricciardi, "A grasp metaheuristic for evaluating the latency and lifetime impact of critical nodes in large wireless sensor networks," *Applied Sciences*, vol. 21, no. 9, p. 4564, 2019.

[108] B. Liu, W. Wang, Y. Li, R.-r. Yin, and T. Han, "Crucial node decision algorithm based on energy in WSN," *Journal of Electronics and Information Technology*, vol. 36, no. 7, pp. 1728–1734, 2014.

[109] Q. D. Sun, Y. M. Qiao, J. M. Wang, and S. Shen, "Node importance evaluation method in wireless sensor network based on energy field model," *EURASIP Journal on Wireless Communications and Networking*, vol. 2016, p. 199, 2016.

[110] O. Dagdeviren, V. K. Akram, B. Tavli, H. U. Yildiz, and C. Atilgan, "Distributed detection of critical nodes in wireless sensor networks using connected dominating set," in *Proceedings of International Conference on SENSORS*, (Orlando, FL, USA), pp. 1–3, IEEE, 2016.

[111] P. Barooah, H. Chenji, R. Stoleru, and T. Kalmar-Nagy, "Cut detection in wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 3, pp. 483–490, 2012.

[112] M. Won and R. Stoleru, "Destination-based cut detection in wireless sensor networks," in *Proceedings of the 9th International Conference on Embedded and Ubiquitous Computing*, (Melbourne, VIC, Australia), pp. 55–62, IFIP, 2011.

[113] S. Xiong and J. Li, "An efficient algorithm for cut vertex detection in wireless sensor networks," in *Proceedings of the 30th International Conference on Distributed Computing Systems*, (Genoa, Italy), pp. 368–377, IEEE, 2010.

[114] L. C. Freeman, "Centrality in social networks conceptual clarification," *Social networks*, vol. 1, no. 3, pp. 215–239.

[115] L. Sitanayah, K. N. Brown, and C. J. Sreenan, "Fault-tolerant relay deployment based on length-constrained connectivity and rerouting centrality in wireless sensor

networks," in *Proceedings of European Conference on Wireless Sensor Networks*, (Trento, Italy), pp. 115–130, Springer, 2012.

[116] R. Yin, X. Yin, M. Cui, and Y. Xu, "Node importance evaluation method based on multi-attribute decision-making model in wireless sensor networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, pp. 1–14, 2019.

[117] S. P. Borgatti, "Identifying sets of key players in a social network," *Computational and Mathematical Organization Theory*, vol. 12, p. 21–34, 2006.

[118] A. Arulselvan, C. W. Commander, O. Shylo, and P. M. Pardalos, "Cardinality-constrained critical node detection problem," No. 4, pp. 79–91.

[119] C. W. Commander, P. M. Pardalos, V. Ryabchenko, S. Uryasev, and G. Zrazhevsky, "The wireless network jamming problem," *Journal of Combinatorial Optimization*, vol. 14, p. 481–498, 2007.

[120] O. Dagdeviren and V. K. Akram, "An energy-efficient distributed cut vertex detection algorithm for wireless sensor networks," *The Computer Journal*, vol. 57, no. 12, pp. 1852–1869, 2014.

[121] L. Kong, J.-S. Pan, V. Snasel, T. P. W., and T. W. Sung, "An energy-aware routing protocol for wireless sensor network based on genetic algorithm," *Telecommunication Systems*, vol. 67, no. 3, pp. 451–463, 2018.

[122] B. Peng and L. Li, "An improved localization algorithm based on genetic algorithm in wireless sensor networks," vol. 9, pp. 249–256, 2015.

[123] A. Ouyang, Y. Lu, Y. Liu, M. Wu, and X. Peng, "An improved adaptive genetic algorithm based on dv-hop for locating nodes in wireless sensor networks," *Neurocomputing*, vol. 458, pp. 500–510, 2021.

[124] K. Rajeswari and S. Neduncheliyan, "Cluster based fault tolerance using genetic algorithm in wireless sensor network," in *Proceedings of International Conference on Information Communication and Embedded Systems (ICICES)*, (Chennai, India), pp. 1–4, IEEE, 2016.

[125] A. Ghaffari and S. Nobahary, "FDMG : Fault detection method by using genetic algorithm in clustered wireless sensor networks," *Journal of AI and Data Mining*, vol. 3, no. 1, pp. 47–57, 2015.

[126] W. Ye, J. Heidemann, and D. Estrin, "An energy-efficient MAC protocol for wireless sensor networks," in *Proceedings of the Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies*, vol. 3, (New York, NY, USA), pp. 1567–1576 vol.3, IEEE, 2002.

[127] B. Marques and M. Ricardo, "Synchronization of application-driven WSN," *EURASIP Journal on Wireless Communications and Networking*, vol. 2017, p. 37 (22 pages), 2017.

[128] Z. Xuan, Z. Feng-Ming, L. Ke-Wu, H. Xiao-Bin, and W. Hu-Sheng, "Finding vital node by node importance evaluation matrix in complex networks," *Acta Physica Sinica*, vol. 61, no. 5, p. 050201, 2012.

[129] A. Dorfman, N. Kumar, and J.-i. Hahm, "Highly sensitive biomolecular fluorescence detection using nanoscale ZnO platforms," *Langmuir*, vol. 22, no. 11, pp. 4890–4895, 2006.

[130] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–114, 2002.

[131] N. R. Roy and P. Chandra, "EEDAC-WSN : Energy Efficient Data Aggregation in Clustered WSN," in *Proceedings of International Conference on Automation, Computational and Technology Management (ICACTM)*, (London, UK), pp. 586–592, IEEE, 2019.

[132] J. MacQueen, "Some methods for classification and analysis of multivariate observations," in *Proceedings of the Fifth Berkeley Symposium on Mathematical Statistics and Probability*, (California, USA), pp. 281–297, Berkeley, 1967.

[133] L. Karim, N. Nasser, and T. Sheltami, "A fault-tolerant energy-efficient clustering protocol of a wireless sensor network," *Wireless Communications and Mobile Computing*, vol. 14, no. 2, pp. 175–185.

[134] Y. H. Robinson, E. G. . Julie, K. Saravanan, R. Kumar, and L. H. Son, "FD-AOMDV : fault-tolerant disjoint ad-hoc on-demand multipath distance vector routing algorithm in mobile ad-hoc networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, pp. 4455–4472, 2019.

[135] A. Sarkar and T. Senthil Murugan, "Cluster head selection for energy efficient and delay-less routing in wireless sensor network," *Wireless Networks*, vol. 25, no. 1, pp. 303–320, 2019.

[136] M. H. Shafiabadi, A. K. Ghafi, D. D. Manshady, and N. Nouri, "New method to improve energy savings in wireless sensor networks by using som neural network," *Journal of Service Science Research*, vol. 11, no. 1, pp. 1–16, 2019.

[137] A. Ajay, N. Tarasia, S. Dash, S. Ray, and A. R. Swain, "Fault-tolerant multilevel routing protocol with sleep scheduling (fms) for wireless sensor networks," *European Journal of Scientific Research*, vol. 55, no. 1, pp. 97–108, 2011.

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

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

[140] B. Mathur and A. Jain, "AOMDV Protocol : A Literature Review," *International Journal of New Technology and Research*, vol. 4, pp. 27–30, 7 2018.

[141] H. Fouchal, Y. Francillette, P. Hunel, and N. Vidot, "A distributed power management optimisation in wireless sensors networks," in *Proceedings of the 34th Conference on Local Computer Networks*, (Zurich, Switzerland), pp. 763–769, IEEE, 2009.

[142] I. Bennis, H. Fouchal, O. Zytoune, and D. Aboutajdine, "Carrier sense aware multipath geographic routing protocol," *Wireless Communications and Mobile Computing*, vol. 16, no. 9, pp. 1109–1123, 2016.

[143] J. Yu, Y. Qi, G. Wang, Q. Guo, and X. Gu, "An energy-aware distributed unequal clustering protocol for wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 7, no. 1, p. 202145, 2011.

Résumé

La tolérance aux pannes est un mécanisme primordial dans les réseaux de capteurs sans fil (RCSFs) pour garder le système fonctionnel quand certains cessent de fonctionner. Dans cette thèse, nous proposons trois contributions pour la tolérance aux pannes dans les RCSFs. La première contribution est basée sur le problème des nœuds critiques (CNP) et s'exécute en deux phases. La première phase consiste à sélectionner les nœuds critiques dont la défaillance fragmente le réseau et la deuxième phase fait appel au concept d'augmentation qui permet d'ajouter des liens sans fil pour tolérer la panne des nœuds critiques définis lors de la première phase. La deuxième contribution consiste en un protocole de routage tolérant aux pannes à aspect préventif basé sur le clustering. Dans ce schéma de routage les nœuds les plus fiables sont impliques dans le processus de routage et la probabilité de fiabilité des nœuds est calculée selon la loi de Bernoulli. La troisième contribution est un protocole de routage tolérant aux pannes à aspect curatif basé sur le concept de clustering. Dans ce protocole chaque cluster contient un CH principal et un CH assistant qui remplace le CH principal en cas de sa défaillance.

Les résultats obtenus après évaluation de ces contributions ont montré leurs performances par rapport à certains travaux existants.

Mots clés

Réseaux de capteurs sans fil, Tolérance aux pannes, Approche préventive, Approche curative, Nœuds critiques.

Abstract

Fault tolerance is an important mechanism in wireless sensor networks (WSNs) to keep the system functional when some of them stop working. In this thesis, we propose three contributions for fault tolerance in WSNs. The first contribution is based on the critical node problem (CNP) and is performed in two phases. The first phase consists in selecting the critical nodes whose failure fragments the network and the second phase uses the augmentation concept that allows adding wireless links to tolerate the failure of the critical nodes defined in the first phase. The second contribution is a fault-tolerant routing protocol with a preventive aspect based on clustering. In this routing scheme the most reliable nodes are involved in the routing process and the reliability probability of the nodes is calculated according to Bernoulli's law. The third contribution is a fault tolerant routing protocol with a curative aspect based on the concept of clustering. In this protocol each cluster contains a main CH and an assistant CH that replaces the main CH in case of its failure.

The results obtained after evaluation of these contributions showed their performance compared to some existing works.

Keywords

Wireless sensor networks, Fault tolerance, Preventive approach, Curative approach, Critical nodes.

خلاصة

يعتبر تحمل الأعطال آلية أساسية في شبكات الاستشعار اللاسلكية (WSNs) للحفاظ على عمل النظام عندما تتوقف بعض العقد عن العمل . في هذه الأطروحة نقترح ثلاث مساهمات للتسامح مع الخطأ في WSNs. تعتمد المساهمة الأولى على مشكلة العقد الحرجة (CNP) وتعمل على مرحلتين. تتكون المرحلة الأولى من اختيار العقد الحرجة التي يؤدي عطبها إلى تفتيت الشبكة وتستخدم المرحلة الثانية مفهوم الزيادة التي تجعل من الممكن إضافة روابط لاسلكية لتحمل عطب العقد الحرجة المحددة خلال المرحلة الأولى. تتكون المساهمة الثانية من بروتوكول توجيه متسامح مع الخطأ مع جانب وقائي و يعتمد على التجميع. في مخطط التوجيه هذا ، تشارك العقد الأكثر موثوقية في عملية التوجيه ويتم حساب احتمال موثوقية العقد وفقًا لقانون برنولي. المساهمة الثالثة هي بروتوكول توجيه متسامح مع الأخطاء يعتمد على مفهوم التجميع حيث تحتوي كل مجموعة على CH رئيسي و CH مساعد الذي يحل محل الرئيسي في حالة عطبه.

الكلمات المفتاحية

شبكات الاستشعار اللاسلكية، التسامح مع الأخطاء، النهج الوقائي، النهج العلاجي، العقد الحرجة