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

N° d'ordre : .....

UNIVERSITE DE M'SILA

FACULTE DES MATHEMATIQUES ET DE L'INFORMATIQUE

Département d'Informatique

MEMOIRE de fin d'étude

Présenté pour l'obtention du diplôme de MASTER

Domaine : Mathématiques et Informatique
Filière : Informatique
Spécialité : Réseaux
Par: Chikouche Ali

SUJET

Simulation et évaluation des performances du protocole TinyOS beaconing « TOSB ».

Soutenu publiquement le : 25/ 06/2013 devant le jury composé de :

Nom et prénom Enseignant		
DEBBI	**Université de M'sila**	**Président**
ATTIR Azeddine	**Université de M'sila**	**Rapporteur**
HAMANI	**Université de M'sila**	**Examinateur**

Promotion : 2012 /2013

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

N° d'ordre : .....

UNIVERSITE DE M'SILA

FACULTE DES MATHEMATIQUES ET DE L'INFORMATIQUE

Département d'Informatique

MEMOIRE de fin d'étude

Présenté pour l'obtention du diplôme de MASTER

Domaine : Mathématiques et Informatique
Filière : Informatique
Spécialité : Réseaux

Par: Chikouche Ali

SUJET

Simulation et évaluation des performances du protocole TinyOS beaconing « TOSB ».

Soutenu publiquement le : / 06/2013 devant le jury composé de :

Nom et prénom Enseignant		
……	**Université de M'sila**	**Président**
Attir Azeddine	**Université de M'sila**	**Rapporteur**
……	**Université de M'sila**	**Examinateur**
……	**Université de M'sila**	**Examinateur**

Promotion : 2012 /2013

Dédicaces

A mon très cher Papa,

A ma très adorable Maman,

A toute ma famille,

A tous mes amis,

A toutes les personnes qui m'ont aidée
de près ou de loin, surtout Zakaria
ben halima ,kamal hadj hafsi .

Ali

Remerciements

Nous remercions Allah le tout puissant de nous avoir donné le courage jusqu'à l'achèvement de ce mémoire. Au terme de ce travail, nous adressons notre profonde gratitude à monsieur ATTIR Azeddine Nous vous remercions pour la gentillesse et spontanéité avec lesquelles vous avez bien dirigé ce travail. Nous avons eu le grand plaisir de travailler sous votre direction.

Un grande merci non moins reconnaissant à tous nos enseignants pour toutes les connaissances qu'ils nous ont inculquées.

Nos remerciements s'adressent également à tous les membres de jury l'immense également honneur de ce qu'ils nous font en acceptant d'évaluer ce modeste travail.

Nos remerciements s'adressent aussi à mes collègues du l'université de M'sila de la promotion de master informatique.

Encore merci à tous.

TABLE DES MATIERS

CHAPITRE 2:La tolérance aux pannes dans les RCSF

CHAPITRE 3:Le protocole de routage TinyOS Beaconing

Chapitre 4 : Solution proposée : T-TOSB

LISTE DES FIGURES

LISTE DES TABLES

INTRODUCTION GENERALE

A l'heure actuelle, le thème des réseaux de capteurs sans fil (RCSF) provoque un intérêt croissant. Ceci est dû essentiellement aux caractéristiques inhérentes de cette technologie, et qui la favorisent pour un large étendu d'applications dans plusieurs domaines. Parmi ces caractéristiques, on cite la possibilité de déploiement aléatoire du réseau dans des environnements hostiles tels que les champs de bataille, en plus de l'auto-organisation et le fonctionnement autonome des nœuds capteurs.

De plus, les nœuds capteurs collaborent pour accomplir des opérations de calcul simples et de ne transmettre par la suite que les données nécessaires partiellement traitées, au lieu d'envoyer toutes les données captées à des nœuds intermédiaires dédiés aux opérations de traitement. Cette caractéristique implique d'autres verrous et contraintes importantes qui guident la conception des protocoles de routage de l'information dans les RCSF. Cependant, on ne peut pas garantir un bon acheminement

Dans les réseaux sans fil, on donne plus de l'importance à l'acheminement de l'information qui est assuré par des algorithmes de routage. Ces algorithmes doivent prendre en considération les changements de la topologie du réseau, ainsi que d'autres caractéristiques comme la bande passante, le nombre de liens, la limitation d'énergie, etc. En particulier pour les réseaux de capteurs qui se caractérisent par des liens volatiles et des dispositifs fragiles, les protocoles de routage perdent leurs performances quand un lien est perdu ou un dispositif cesse de fonctionner. Dans ce contexte, plusieurs recherches ont été menées notamment pour garantir le routage de l'information de n'importe quel nœud vers la station de base.

L'objectif principal de notre travail est de s'initier au domaine des réseaux de capteurs sans fil, étudier et traiter le problème de tolérance aux pannes dans les réseaux de capteurs pour garantir un routage efficace, surtout ceux de taille importante. Le souci principal est d'assurer la livraison de données à la station de base tout en prolongeant la vie du système. Pour cela, nous avons tout d'abord étudié les performances du protocole TinyOSBeaconing (TOSB) dans un environnement qui n'est pas idéal. Les résultats ont montré que TOSB perd ses performances dans ce type d'environnement. Afin d'améliorer les performances de ce protocole, nous avons proposé une nouvelle version appelée T-TOSB pour *Tolérant-TOSB*, et avec des simulations nous avons démontré l'apport de T-TOSB à travers plusieurs métriques.

Notre mémoire s'articule autour de quatre chapitres :

Chapitre 1: décrit l'architecture d'un capteur et présente les principes et les caractéristiques des réseaux de capteurs aussi que ses domaines d'application et le routage.

Chapitre 2 : nous présentons la tolérance aux pannes dans les réseaux de capteurs et sa classification.

Chapitre 3 : présente le protocole TinyOS Beaconing sujet de notre mémoire, qui est un protocole de routage conçu pour réseaux de capteurs.

Chapitre 4: nous présenterons la conception de notre solution pour améliorer ce protocole de telle sorte qu'il soit tolérant aux pannes.

Nous concluons ce mémoire par des perspectives envisagées pour une amélioration future.

CHAPITRE 1

PRESENTATION DES RESEAUX DE CAPTEURS SANS FIL

1.1 Introduction

Les réseaux de capteurs sans fil (RCSF) représentent un domaine en forte expansion, avec des applications très importantes dans le domaine de l'instrumentation, des économies d'énergie et de la gestion de l'environnement. Le magazine Technology Review du MIT[1], précisait récemment que les réseau de capteurs sans fil est l'une des dix nouvelles technologies qui bouleverseront le monde et notre manière de vivre et de travailler.

Les avantages principaux des RCSF résident dans leur autonomie, leur capacité d'auto organisation et d'acheminement des données. Les RCSF ne cessent de progresser dans chacun de ces aspects. Les méthodes d'accès, le routage et l'économie d'énergie représentent donc des problématiques clés dans le domaine des réseaux de capteurs sans fil.

Dans ce chapitre, nous allons présenter un ensemble de généralités sur les réseaux de capteurs, leurs caractéristiques ainsi que leurs domaines d'applications. Nous discuterons les principaux facteurs et contraintes, leurs consommation d'énergie et sécurité, puis le routage dans les RCSF, et les principaux domaines de recherche dans les RCSF.

1.2 Qu'est-ce qu'un capteur sans fil

Un capteur sans fil est un petit dispositif électronique capable de mesurer une valeur physique environnementale (température, lumière, pression, etc.) et de la communiquer à un centre de contrôle via une station de base. Les progrès conjoints de la microélectronique, des technologies de transmission sans fil et des applications logicielles ont permis de produire à coût raisonnable des micro-capteurs de quelques millimètres cubes de volume, susceptibles de fonctionner en réseaux [1].

1.3 Architecture physique d'un capteur

Un capteur est composé de quatre composants de base: Unité de capture, unité de traitement, unité d'émission/réception, et une unité d'énergie (batterie) [2] [3]. Il se peut aussi qu'il existe d'autres composants additionnels dépendant de l'application [4] (voir la figure 1-1)

---

1)*Technology Review :* est un magazine américain publié par Technology Review, une société de média appartenant au Massachusetts Institute of Technology . Le magazine d'une bimensuel sur ce site Internet : www.technologyreview.com .

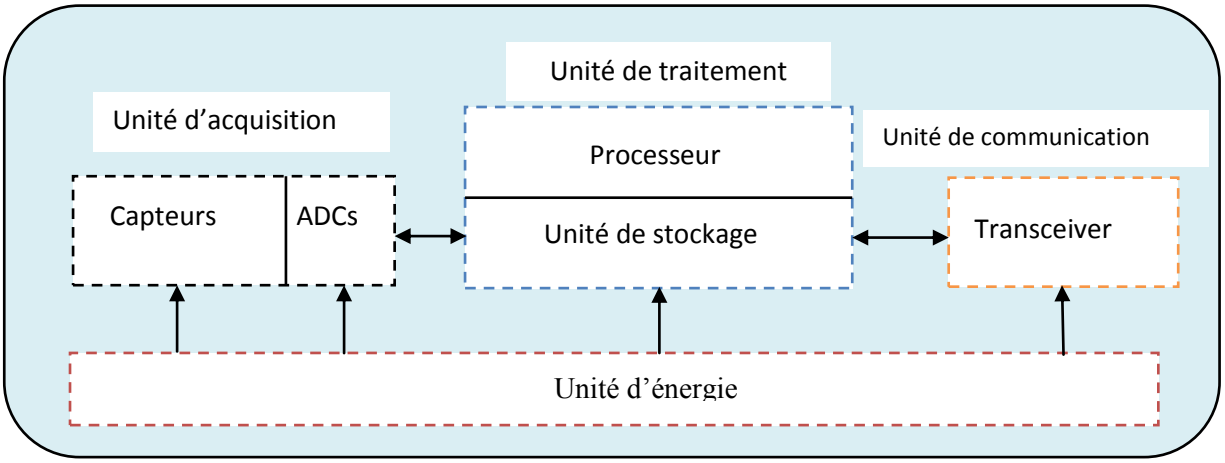


Figure 1.1 Architecture physique d'un capteur.

- ***L'unité d'acquisition*** : elle est généralement composée de deux sous-unités qui sont les capteurs et les convertisseurs analogique-numérique ADCs (Analog-Digital Converter). Les capteurs obtiennent des mesures sur les paramètres environnementaux et les transforment en signaux analogiques. Les ADCs convertissent ces signaux analogiques en signaux numériques.
- ***L'unité de traitement*** *:* elle est composée de deux interfaces qui sont une interface avec l'unité d'acquisition et une autre avec le module de transmission. Elle contrôle les procédures permettant au nœud de collaborer avec les autres nœuds pour réaliser les tâches d'acquisition et stocker les données collectées.
- ***Un module de communication (Transceiver)*** *:* il est composé d'un émetteur/récepteur permettant la communication entre les différents nœuds du réseau via un support de communication radio.
- ***Batterie*** *:* elle alimente les unités que nous avons citées et elle n'est généralement ni rechargeable ni remplaçable. La capacité d'énergie limitée au niveau des capteurs représente la contrainte principale lors de conception de protocoles pour les réseaux de capteurs (1ou 2 joule).

Il peut contenir également, suivant son domaine d'application, des modules supplémentaires tels qu'un système de localisation (GPS), ou bien un système générateur d'énergie (cellule solaire). On peut même trouver des micro-capteurs, un peu plus volumineux, dotés d'un système mobilisateur chargé de déplacer le micro-capteur en cas de nécessité [4].

Il existe dans le monde plusieurs fabricants de capteurs. Nous citerons Crossbow, Cisco, Dalsa, EuroTherm, et Sens2B. Parmi ces capteurs, Les capteurs se déclinent en une multitude de modèles en relation avec l'application à laquelle il est destiné. Parmi les modèles les plus courants, on trouve par exemple le capteur "weC" de l'université de Berkeley pour capter la température et la luminosité [15]. La figure 1.2 montre les images de quelques capteurs.

Figure 1.2 Exemples de nœuds capteurs (Kmote 80$ et TelosB 100$) [5].

1.4 Caractéristiques des réseaux de capteurs

1.4.1 Architecture d'un réseau de capteurs sans fil

Les réseaux de capteurs sans fil (WSNs) sont un type particulier de réseau Ad-hoc[1], dans lesquels les nœuds sont des capteurs, Ils se composent généralement d'un grand nombre de capteurs communicants entre eux via des liens radio pour le partage d'information et le traitement coopératif [02].

Dans ce type de réseau, les capteurs échangent des informations par exemple sur l'environnement pour construire une vue globale de la région contrôlée, qui est rendue accessible à l'utilisateur externe par un ou plusieurs nœud(s). Les données collectées par ces capteurs sont acheminées directement ou via les autres capteurs de proche en proche à un « point de collecte », appelé station de base (ou puits, dite sink en anglais). Cette dernière peut être connectée à une machine puissante via internet ou par satellite.

1) Ad-hoc : Un réseau mobile Ad Hoc, appelé généralement MANET (Mobile Ad hoc NETwork)

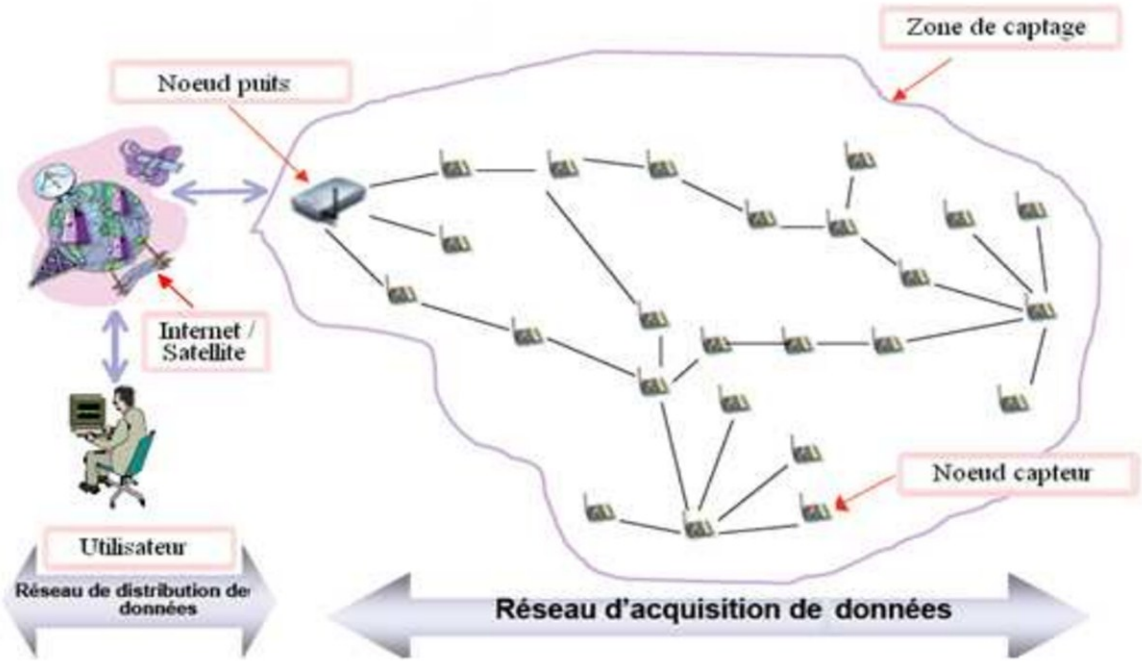


Figure 1.3 Architecture de communication RCSF. [06]

1.4.2 Comparaison entre le RCSF et réseaux Ad hoc

Les RCFS sont souvent comparés aux réseaux ad hoc traditionnels. Les réseaux mobiles ad hoc partagent beaucoup de points communs avec les réseaux de capteurs sans fil. Les points communs essentiels sont [41]:

- Tous les deux sont des réseaux ad hoc, c'est `a dire, ils fonctionnent sans avoir besoin d'une infrastructure pour la gestion des échanges. De ce fait, ils ont besoin d'être auto-configurable.
- Tous les deux sont des réseaux sans fil, ce qui fait que la portée des communications est limitée par la capacité de rayonnement des antennes utilisées et les puissances mises en jeu. Ainsi, les nœuds dans ces types de réseaux sont souvent dans des configurations multi-sauts ce qui induit la mise en place de protocoles de routage multi-sauts.
- Le m´médium utilisé pour ´échanger entre les nœuds est l'air. Ainsi, les protocoles d'accès au médium des réseaux MANET et des RCSF sont très proches et sont typiquement en mode half-duplex (les entités étant incapable de recevoir et d'émettre en même temps).
- Ces réseaux travaillent sur une bande de fréquences non propriétaire, ce qui rend leurs communications vulnérables aux problèmes d'interférences.

- Les entités de ces réseaux sont souvent alimentées par des batteries.

Malgré les points sur lesquels ces deux types de réseaux convergent, ils diffèrent sur plusieurs aspects. Comme illustre dans le tableau suivant :

	RCSF	**Ad hoc (MANET)**
Flot de communication	Tous vers un	Tous vers tout
Contrainte clé	Energie	Débit
Communication	Broadcast	Point à point
Relation entre les nœuds	Collaboration	Chaque nœud à son objectif
identification des nœuds	Très grand nombre de nœuds n'ayant pas tous une ID	Notion d'ID
Objective de réseaux	Objectif ciblé	Générique / communication

Table 1.1 Comparaison entre les RCSF et réseaux Ad hoc

1.4.3 Les Domaines d'application des RCSF

La miniaturisation des capteurs, le coût de plus en plus faible, la large gamme des types de capteurs disponibles ainsi que le support de communication sans fil utilisé, permettent aux réseaux de capteurs de se développer dans plusieurs domaines d'application Ils permettent aussi d'étendre les applications existantes. Les réseaux de capteurs peuvent se révéler très utiles dans de nombreuses applications lorsqu'il s'agit de collecter et de traiter des informations provenant de l'environnement. Parmi les domaines où ces réseaux peuvent offrir les meilleures contributions, nous citons les domaines : militaire, surveillance, environnemental, médical, domestique, commercial, etc. [11] [17].

- **Les applications militaires** : surveiller les activités des forces ennemies, détection d'agents chimiques.
- **La surveillance de l'environnement :** détection de feux de forêt, surveillance d'une centrale nucléaire.
- **La santé :** parmi ses applications, on peut citer la surveillance l'état des patients et le taux de médicaments qui leur ont été administrés, et l'aide à la localisation des médecins et des patients au sein d'un hôpital.
- **La maison intelligente** : réglage de l'éclairage en fonction de la position des habitants.
- **Les autres applications commerciales** : musées interactifs, gestion de stocke [1], La climatisation pourra être déclenchée seulement aux endroits où il y a des

personnes présentes et seulement si c'est nécessaire grasse à plusieurs micro-capteurs intégrés dans les tuiles du plancher et dans les meubles.

Les réseaux de capteurs auront un impact majeur sur la vie courante dans l'avenir, par exemple l'utilisation de ces réseaux dans les applications de sécurité du travail, le chauffage et la climatisation, etc. [17]

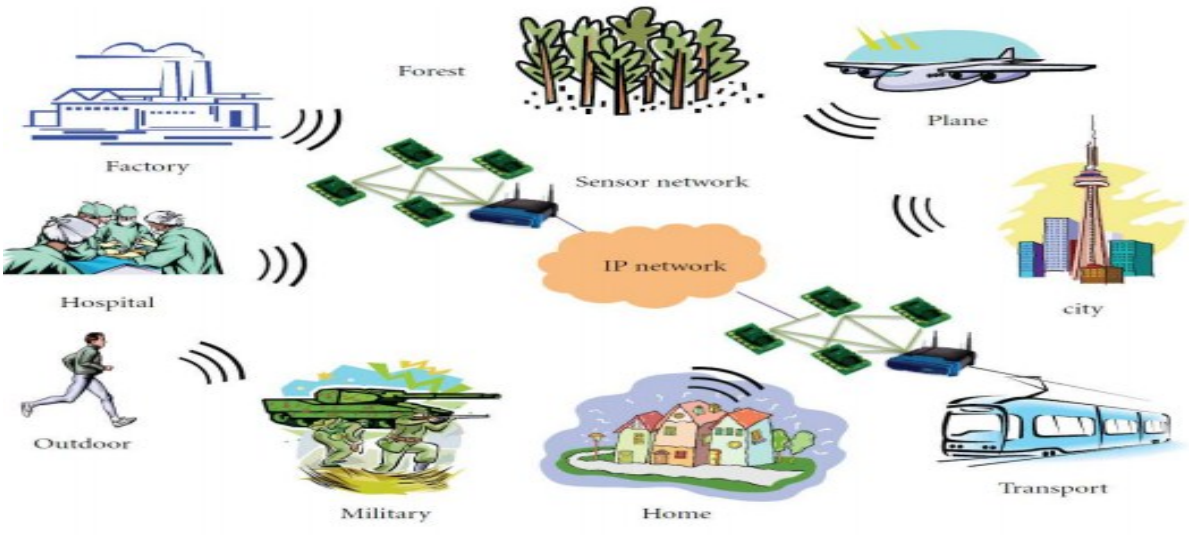


Figure 1.4 : Quelques domaines d'application pour les RCSFs [07].

1.4.4 Architecture protocolaire :

Dans le but d'un établissement efficace d'un RCSF, une architecture en couches est adoptée afin d'améliorer la robustesse du réseau. Une pile protocolaire de cinq couches est donc utilisée par les nœuds du réseau. Citons la couche application, la couche transport, la couche réseau, la couche liaison de données et la couche physique. De plus, cette pile possède trois plans (niveaux) de gestion : le plan de gestion des tâches qui permet de bien affecter les tâches aux nœuds capteurs, le plan de gestion de mobilité qui permet de garder une image sur la localisation des nœuds pendant la phase de routage, et, le plan de gestion de l'énergie qui permet de conserver le maximum d'énergie[02].

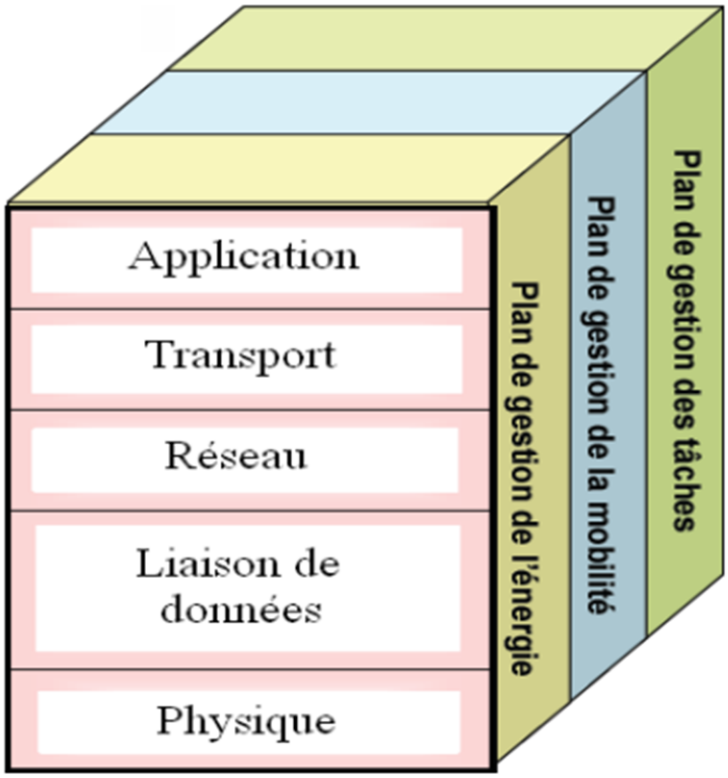


Figure 1.5 La pile protocolaire dans les réseaux de capteurs. [06]

- **Couche application** : Elle assure l'interface avec les applications. Il s'agit donc de la couche la plus proche des utilisateurs, gérée directement par les logiciels. Parmi les protocoles d'application, nous citons : SMP (Sensor Management Protocol) et TADAP (Task Assignement and Data Advertisement Protocol) [02].
- **Couche transport :** Cette couche est particulièrement nécessaire lorsque le système est prévu pour être accessible par le biais d'Internet ou d'autres réseaux externes en utilisant l'interface TCP-spliting pour vérifier la compatibilité entre ces deux réseaux communicants. Maintenir le flux de données en cas de nécessité. Généralement cette couche utilisé un protocole de transport plus proche du protocole UDP appelé UDP-Like (User Datagram Protocol Like) [08].
- **Couche réseau :** Elle s'occupe du routage de données fournies par la couche transport. Elle établit les routes entre les nœuds capteurs et le nœud puits et sélectionne le meilleur chemin en termes d'énergie, délai de transmission, débit, etc.
- **Couche liaison de données :** Elle est responsable de l'accès au media physique et la détection et la correction d'erreurs intervenues sur la couche physique. De plus, elle établit une communication saut-par-saut entre les nœuds. C'est-à-dire, elle détermine les liens de communication entre eux dans une distance d'un seul saut.

- **Couche physique :** Elle permet de moduler les données et les acheminer dans le media physique tout en choisissant les bonnes fréquences.

- **Le plan de gestion d'énergie :** Les fonctions intégrées à ce niveau consistent à gérer l'énergie consommée par les capteurs. Dès lors, un capteur peut par exemple éteindre son interface de réception dès qu'il reçoit un message d'un nœud voisin afin d'éviter la réception des messages dupliqués. De plus, quand un nœud possède un niveau d'énergie faible, il peut diffuser un message aux autres capteurs pour ne pas participer aux tâches de routage, et conserver l'énergie restante aux fonctionnalités de capture [02].
- **Le plan de gestion de mobilité :** Ce niveau détecte et enregistre tous les mouvements des nœuds capteurs, de manière à leur permettre de garder continuellement une route vers l'utilisateur final, et maintenir une image récente sur les nœuds voisins. Cette image est nécessaire pour pouvoir équilibrer l'exécution des tâches et la consommation d'énergie [02].
- **Le plan de gestion des tâches :** Lors d'une opération de capture dans une région donnée, les nœuds composant le réseau ne doivent pas obligatoirement travailler avec le même rythme. Cela dépend essentiellement de la nature du capteur, son niveau d'énergie et la région dans laquelle il a été déployé. Pour cela, le niveau de gestion des tâches assure l'équilibrage et la distribution des tâches sur les différents nœuds du réseau afin d'assurer un travail coopératif et efficace en matière de consommation d'énergie, et par conséquent, prolonger la durée de vie du réseau [02].

1.4.5 Facteurs et contraintes des RCSF

La conception et la réalisation des réseaux de capteurs sans fil sont influencées par plusieurs paramètres. Ces facteurs servent comme directives pour le développement des algorithmes et protocoles utilisés dans les RCSF.

- **Durée de vie du réseau :** C'est l'intervalle de temps qui sépare l'instant de déploiement du réseau de l'instant où l'énergie du premier nœud s'épuise [8]. Selon l'application, la durée de vie exigée pour un réseau peut varier entre quelques heures et plusieurs années [9].

- **Ressources limitées :** En plus de l'énergie, les nœuds capteurs ont aussi une capacité de traitement et de mémoire limitée. En effet, les industriels veulent mettre en œuvre des capteurs simples, petits et peu coûteux.
- **Bande passante limitée :** Afin de minimiser l'énergie consommée lors de transfert de données entre les capteurs, les capteurs opèrent à bas débit. Typiquement, le débit utilisé est de quelques dizaines de Kb/s. Un débit de transmission réduit n'est pas handicapant pour un réseau de capteurs où les fréquences de transmission ne sont pas importantes.
- **Facteur d'échelle (Scalability) :** Le nombre de nœuds déployés pour une application peut atteindre des milliers de nœuds. Dans ce cas, le réseau doit fonctionner avec des densités de capteurs très grandes. Un nombre aussi important de nœuds engendre beaucoup de transmissions entre les nœuds et nécessite que la station de base soit équipée de mémoire suffisante pour stocker les informations reçues [02].
- **Topologie dynamique :**La topologie des réseaux de capteurs peut changer au cours du temps pour les raisons suivantes[1] :

  • Les nœuds capteurs peuvent être déployés dans des environnements hostiles (champ de batail par exemple), la défaillance d'un nœud capteur est, donc très probable.

  • Un nœud capteur peut devenir non opérationnel à cause de l'expiration de son énergie.

  • Dans certaines applications, les nœuds capteurs et les stations de base sont mobiles.

- **Agrégation de donnée :**
  Dans les réseaux de capteurs, les données produites par les nœuds capteurs voisins sont très corrélées spatialement et temporellement. Ceci peut engendrer la réception par la station de base d'informations redondantes. Réduire la quantité d'informations redondantes transmises par les capteurs permet de réduire la consommation d'énergie dans le réseau et ainsi d'améliorer sa durée de vie. L'une des techniques utilisée pour réduire la transmission d'informations redondantes est l'agrégation des données. Avec cette technique, les nœuds intermédiaires agrègent l'information reçue de plusieurs sources. Cette technique est connue aussi sous le nom de fusion de données.

- **Tolérance aux pannes :** Les nœuds peuvent être sujets à des pannes dues à leur fabrication (ce sont des produits de série bon marché, il peut donc y avoir des capteurs défectueux) ou plus fréquemment à un manque d'énergie. Les interactions externes (chocs, interférences) peuvent aussi être la cause des dysfonctionnements. Afin que les pannes n'affectent pas la tâche première du réseau il faut évaluer la capacité du réseau à fonctionner sans interruption [1].

1.5 La Consommation d'énergie dans les RCSF

L'énergie consommée par un nœud capteur est due essentiellement aux opérations suivantes : la capture, le traitement et la communication de données [12]. Peut-être classer selon l'ordre décroissant suivant [13] : La communication (émission et réception), traitement de données, et acquisition ou capture.

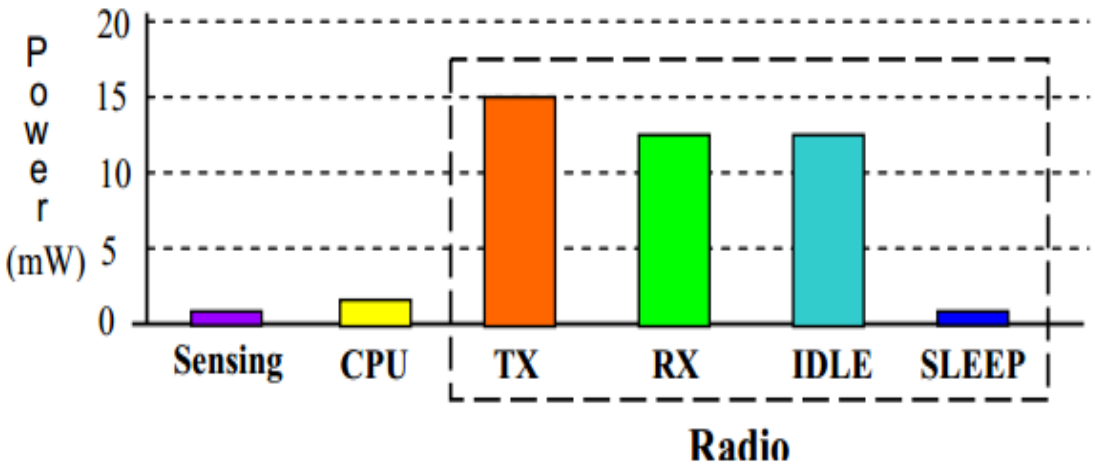


Figure 1.6 Énergie consommée par les sous-systèmes d'un nœud de capteur [06].

Où RX signifie énergie pour réception, TX pour transmission, IDLE en écoute de canal, SLEEP est l'état sommeil.

1.5.1 Energie de capture

L'énergie de capture est dissipée pour accomplir les tâches suivantes : échantillonnage, traitement de signal, conversion analogique/numérique et activation de la sonde du capture. En général, l'énergie de capture représente un faible pourcentage de l'énergie totale consommé par un nœud [11].

1.5.2 Energie de traitement

L'énergie de traitement se divise en deux parties : l'énergie de commutation et l'énergie de fuite. L'énergie de commutation est déterminée par la tension d'alimentation et la capacité totale commutée au niveau logiciel (en exécutant un logiciel). Par contre l'énergie de fuite correspond à l'énergie consommée lorsque l'unité de calcul n'effectue aucun traitement. En général, l'énergie de traitement est faible par rapport à celle nécessaire pour la communication [11].

1.5.3 Energie de communication

L'énergie de communication se décline en deux parties : l'énergie de réception et l'énergie de l'émission. Cette énergie est déterminée par la quantité des données à communiquer et la distance de transmission, ainsi que par les propriétés physiques du module radio. L'émission d'un signal est caractérisée par sa puissance. Quand la puissance d'émission est élevée, le signal aura une grande portée et l'énergie consommée sera plus élevée. Notons que l'énergie de communication représente la portion la plus grande de l'énergie consommée par un nœud capteur [11].

1.6 La Sécurité dans les réseaux de capteurs

Les RCSFs sont déployés, la plupart du temps, dans des zones accessibles ; ce qui engendre plus de risques d'attaques physiques (ex. capture d'un nœud). De plus, les capteurs qui les constituent sont limités en termes d'énergie, de puissance de calcul et de capacité de communication. Par conséquent, les techniques de sécurité utilisées dans les réseaux traditionnels sont inadaptables aux RCSFs ; ce qui oblige les spécialistes à développer de nouvelles solutions de sécurité adéquates à ces derniers.

1.6.1 Objectifs de la sécurité

Les objectifs de la sécurité sont [18]:

1. **Authentification:** action de vérifier qu'un nœud correspond bien à ce qu'il prétend et/ou qu'une donnée provient d'où elle est censée provenir.

2. **Intégrité :** une donnée ne doit subir aucune modification au cours de son acheminement vers le puits.

3. **Confidentialité :** une donnée ne doit être accessible qu'aux seuls nœuds autorisés.

4. **Disponibilité :** une donnée n'est présente et n'est utilisable qu'au moment où l'on a besoin.

5. **Non-rejeu :** un message ne doit être transmis qu'une seule fois.

6. Non-répudiation: s'assurer qu'un nœud ne pourra pas répudier ses actes (ex. réception et émission).

1.6.2 Objectifs des attaques

Les capteurs peuvent être objets de plusieurs types d'attaques, suivant leur fonctionnement et leurs localités dans le réseau. Dans la littérature, ces différentes attaques ont été classifiées de diverses manières [19] [20]. On cite ci-dessous leurs principaux objectifs:

1. **Espionnage:** l'attaquant cherche à obtenir les données du réseau dont l'accès n'est pas autorisé. L'espionnage peut s'effectuer par une écoute passive ou en envoyant des requêtes aux nœuds capteurs, aux agrégateurs ou par la capture des nœuds pour avoir plus d'informations.

2. **Perturbation :** le but de l'attaquant est de perturber le fonctionnement du réseau par injection des données erronées, altération des messages de données ou par manipulation directe de l'environnement en générant des fausses alertes.

3. **Détournement :** dans ce cas, l'attaquant cherche à détourner les applications des capteurs de leurs bons fonctionnements, par l'obtention du contrôle d'un ou d'un ensemble de capteurs. L'obtention du contrôle peut se faire, par exemple, par la compromission ou la capture d'un nœud.

1.6.3 Classification des attaques dans les RCSFs [21] [22]

Une attaque est un ensemble de techniques informatiques, visant à causer des dommages à un réseau, en exploitant les failles de celui-ci.

Une variété d'attaques contre les RCSFs est rapportée dans la littérature. Pour faire face à ces attaques, diverses contre-mesures ont été proposées. Nous présentons dans la suite les principaux types d'attaques, classifiées selon leurs affectations aux couches concernées de la pile protocolaire dans les RCSFs [23].

- **Attaques de la couche physique** : Brouillage (jamming), Attaque physique d'un nœud.

- **Attaques de la couche liaison :** Attaques de collision, Exhaustion, Privation de mise en veille.
- **Attaque de la couche réseaux :** Les réseaux utilisent une communication multi sauts pour router les paquets vers la destination et les attaques dans cette couche peuvent êtres**:** Select forwarding , Sink Hole , Sybil attack , Attaque par inondation "HELLO" , Wormholes , Blackhole Attack ,comme illustre dans la figure suivant 1.7 .

Dans notre travail s'intéresse aux attaques de cette couche , on explique quelque type attaque dans la chapitre 3 .

- **Attaques de la couche application :** Si les couches liaison de données et réseau sont sécurisées, la couche transport peut être sûre que les paquets qu'elle reçoit de la couche réseau sont confidentiels et authentifiés [48].

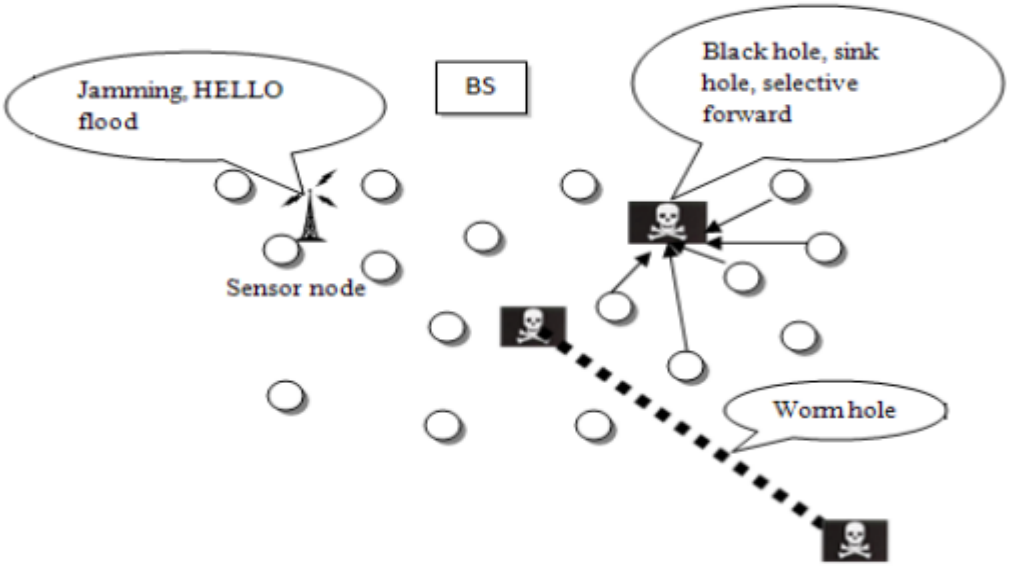


Figure 1.7 Attaques dans la couche réseaux dans un RCSF [48].

1.7 Le Routage dans les RCSF

En général, le routage est une méthode d'acheminement des informations à la bonne destination à travers un réseau de connexion donné. Le problème de routage consiste à déterminer un acheminement optimal des paquets à travers le réseau.

1.7.1 Taxonomie des protocoles de routage

Récemment, les protocoles de routage conçus pour les RCSF ont été largement étudiés. Les méthodes employées peuvent être classifiées suivant plusieurs critères qui sont illustrés dans le tableau suivant :

Type de classification	Classes
Paradigme de communication	Centré-nœuds
	Centré-données
	Basé-localisation
	Basé-QoS
Topologie du réseau	Hiérarchiques
	Plates
Méthode d'établissement de routes	Proactive
	Réactive
	Hybrides

Table 1.2 Taxonomie des protocoles de routage. [11]

1.7.1.1 Classification selon les paradigmes de communication

Le paradigme de communication est déterminé par les contraintes sous lesquelles les nœuds du réseau sont interrogés. Dans les RCSF, il peut être classé comme étant centré-nœuds, centré-données, basés-localisation. Il existe également quelques protocoles basés sur la qualité de service (Basé-QoS), qui tentent de garantir certaines exigences des applications au moment du routage [24].

1. Centré-nœuds

Ce modèle est utilisé dans les réseaux conventionnels où il est important de connaître les nœuds communicants. Cependant, ce paradigme ne reflète pas la vision des RCSF quant à leurs applications où la donnée transmise est plus importante que l'émetteur. Néanmoins, le paradigme centré-nœuds n'est pas totalement écarté, car certaines applications nécessitent une interrogation individuelle des nœuds [25].

2. Centré-données

Ce modèle est utilisé dans les réseaux où il n'existe pas un système d'identification global, et cela dans presque toutes les applications des RCSF. En effet, il n'est généralement pas possible d'attribuer les identificateurs globaux (comme les adresses IP) pour chaque nœud à cause de nombre élevé de capteurs déployés. Ainsi, l'identité de chaque nœud n'est pas aussi importante que les données qui lui sont associées. Ce manque d'identification, avec le déploiement aléatoire des nœuds, font qu'il est difficile de sélectionner un ensemble

de nœuds pour être interrogé. Par conséquent, les données sont généralement transmises de chaque nœud avec un taux important de redondances à l'intérieur de la région de déploiement. Ainsi, des protocoles de routage centrés-données ont été proposés pour être en mesure de sélectionner un bon ensemble de nœuds demandés, sans l'utilisation d'identifiants globaux. Ils visent également à utiliser l'agrégation de données pour éviter le gaspillage d'énergie dû aux redondances de données [26].

3. Basé-localisation

Ce paradigme est utilisé dans les applications où il est plus intéressant d'interroger le système en se basant sur la localisation des nœuds, et où on peut tirer profit des positions des nœuds pour prendre des décisions qui minimisent le nombre de messages transmis pendant le routage. Avant d'envoyer ses données à un nœud destination, le nœud source utilise un mécanisme pour déterminer sa localisation. Il est donc nécessaire de se pencher sur une solution de localisation géographique dont le degré de précision dépend de l'application visée. [27][28] Il existe deux techniques de localisation : absolue où on peut utiliser un système GPS (Global Positioning System)[29], ou, relative où les nœuds sont localisés approximativement suivant la direction ou la durée lors d'une transmission [30].

4. Basé-QoS

Les protocoles de routage basés-QoS sont utilisés dans les applications qui ont des exigences temps-réel. Par exemple, dans le domaine de la sécurité, la détection d'intrusion doit être acheminée au plus bref délai vers la sink. Ce type de protocoles essaye de répondre à quelques exigences de qualité de service (délais de transmission ou niveau de fiabilité) et doit faire l'équilibre avec la consommation d'énergie [31].

1.7.1.2 Classification selon la topologie du réseau

La topologie détermine l'organisation logique adaptée par les protocoles de routage afin d'exécuter les différentes opérations de découverte de routes et de transmission de données. Elle joue un rôle significatif dans le fonctionnement d'un protocole. La topologie peut être hiérarchique ou plate [32].

1. Topologie plate

Dans cette topologie tous les nœuds sont considéré homogènes et communiquent entre eux sans aucun intermédiaire, et seul la sink est chargé de la collecte de données issues des différents nœuds capteurs afin de les transmettre vers le centre de traitement (ex :

utilisateur). Au cas où la destination (D) ne fait pas partie du voisinage de la source (S), les données seront transmises en utilisant des sauts multiples comme l'illustre la figure 1.8.

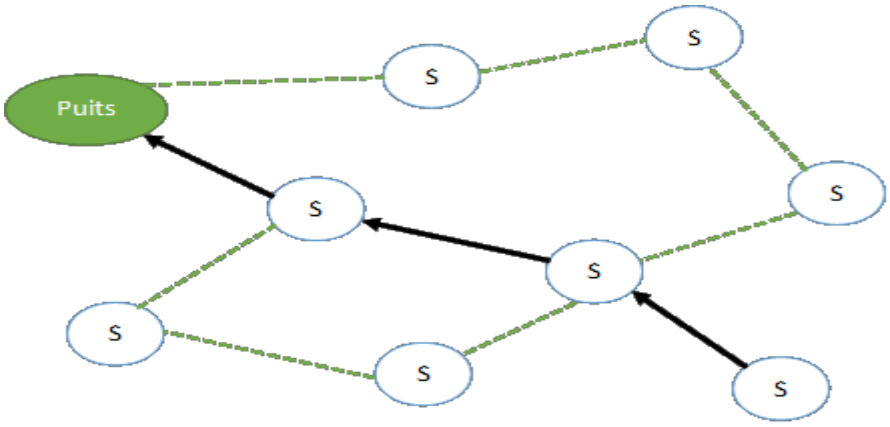


Figure 1.8 Topologie plate. [33]

Les topologies plates sont caractérisées par la simplicité des algorithmes exécutés par les protocoles de routage. Et comme les RCSF souffrent des changements brusques de la topologie, une organisation plate permet la possibilité de construire différents chemins des sources vers le nœud puits. Cependant plusieurs protocoles rentrent dans cette catégorie comme: Directed Diffusion [26].

2. Topologie hiérarchique

Les réseaux hiérarchiques associent des rôles différents aux nœuds du réseau. Ils supposent des nœuds spéciaux plus puissants que les autres qui sont chargés d'effectuer les tâches les plus coûteuses en termes d'énergie afin d'alléger la charge sur les nœuds plus contraints en ressources énergétiques qui se consacrent uniquement au captage. De ce fait, des ensembles de ces derniers sont construits et gérés par les nœuds spéciaux appelés chefs d'ensembles ,(Cluster Head en anglais). Dans ce cas, le routage devient plus simple, puisqu'il s'agit de passer par les chefs pour atteindre le nœud puits qui leur sont directement attachés.

Comme le montre la figure 1.9, il existe deux configurations possibles pour les ensembles construits. Dans la première configuration, les membres d'un ensemble ne communiquent qu'avec leurs chefs de groupes, en obtenant ainsi un modèle basé sur les groupes. Dans la seconde, ils construisent des listes et les membres d'un ensemble utilisent d'autres nœuds comme passerelles appelés Leaders pour transmettre leurs données à leurs chefs en obtenant ainsi un modèle basé sur les listes (chaînes).

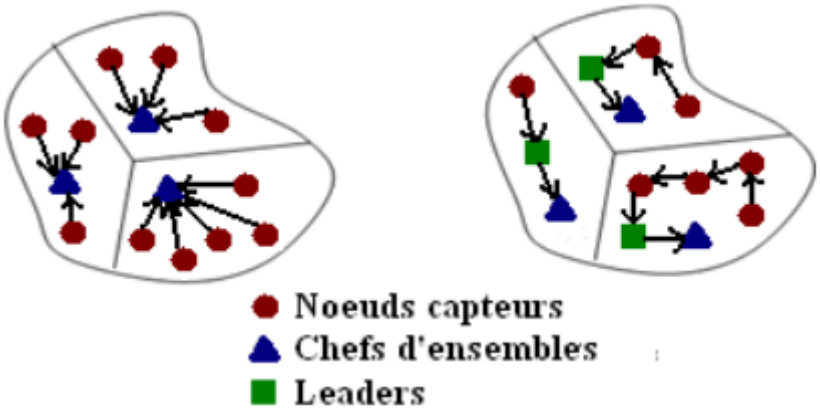


Figure 1.9 Configurations pour les RCSF découpés en ensembles.

L'avantage du routage hiérarchique est que les données d'un ensemble vont être combinées par le chef d'ensemble avant leur arrivée au nœud puits ce qui allège le travail de ce dernier, ainsi que celui des nœuds qui l'entourent. De plus, contrairement aux réseaux plats, un réseau hiérarchique possède une forte scalabilité. En effet, l'ajout des nœuds ne dégrade pas les performances du réseau car le réseau peut gérer seulement les nouveaux nœuds (par exemple, en les groupant et les associant à un chef d'ensemble) sans qu'il affecte tous les nœuds restants du réseau.

Cependant, les nœuds élus comme chefs d'ensembles consomment plus d'énergie que les autres nœuds. S'ils jouent toujours le rôle d'un chef d'ensemble, ils vont être épuisés à un moment donné. Par conséquent, le réseau va être divisé ce qui implique le découpage du réseau en secteurs inaccessibles. Parmi les protocoles qui utilisent cette topologie: LEACH (Low-Energy Adaptive Clustering Hierarchy)[13].

1.7.1.3 Classification selon la méthode d'établissement de routes

Suivant la manière de création et de maintenance de routes lors de l'acheminement des données, les protocoles de routage peuvent être séparés en catégories : protocoles proactifs, réactifs ou hybrides [34].

1. Protocoles proactifs

Les protocoles de routage proactifs établissent au préalable les meilleures routes pour chaque nœud vers toutes les destinations possibles. Ces protocoles maintiennent en permanence une vision globale de l'état du réseau grâce à une gestion périodique des tables de routage et l'échange des messages de contrôle. Ceci induit un contrôle excessif d'autant

plus qu'ils sont particulièrement utilisés pour les réseaux denses. De plus, ils présentent un autre inconvénient dû à la sauvegarde des routes même si elles ne sont pas utilisées.

2. Protocoles réactifs

Les protocoles de routage réactifs calculent des routes à la demande. Lorsque le réseau a besoin d'une route, une procédure de découverte est lancée. Une fois la route n'est plus utilisée, elle sera immédiatement détruite ce qui permet une conservation d'énergie. Cependant, le routage à la demande induit une lenteur à cause de la durée nécessaire à rechercher les chemins, ce qui peut dégrader les performances des applications interactives.

3. Protocoles hybrides

Les protocoles hybrides combinant entre les deux techniques précédentes utilisent des méthodes proactives pour l'établissement de la route dans le proche voisinage (par exemple le voisinage à deux ou trois sauts) et des méthodes réactives au-delà de la zone de voisinage.

1.7.2 Les Métriques de routage

Cette section étudie les métriques communes utilisées pour mesurer l'efficacité des protocoles de routage. Un calcul de métrique est un algorithme qui traite un coût associé à un certain chemin de routage. Les protocoles de routage permettent aux nœuds de comparer les métriques calculées afin de déterminer les routes optimales à emprunter. Plus la métrique n'est optimale, plus le protocole de routage considère que la probabilité d'atteindre le nœud puits à travers ce nœud intermédiaire est grande. Plusieurs métriques peuvent affecter le routage en termes d'énergie, délai, longueur du chemin, etc. De plus, elles peuvent être considérées seules ou combinées (hybrides) [36].

1.7.2.1 Métriques pour la consommation énergétique

Les protocoles de routage utilisent cet ensemble de métriques pour minimiser la consommation d'énergie pendant le routage [37]. L'idée est de calculer l'énergie disponible (ED) pour chaque nœud du réseau et l'énergie nécessaire (EN) pour les transmissions des paquets entre une paire de nœuds.

Les routes entre les nœuds et la station de base (La puits) sont établies et chacune d'elles est caractérisée par la somme des ED des nœuds qui la constituent et par la somme des EN des liaisons qui la construisent. La consommation d'énergie suit plusieurs approches dont on peut citer :

- Par considération de puissance La route choisie est celle caractérisée par la somme des ED la plus élevée.
- Par considération du coût La route choisie est celle caractérisée par la plus petite somme des EN.
- Par considération de puissance et du coût Cette métrique est la combinaison des deux métriques précédentes. La route choisie est celle caractérisée par la plus petite somme des EN et la plus grande somme des ED.

1.7.2.2 Nombre de sauts

Les protocoles de routage utilisent cette métrique pour minimiser le nombre de sauts pendant le routage. L'idée est de calculer le nombre de nœuds intermédiaires pouvant être traversés lors d'une transmission d'un paquet du nœud source vers le nœud sink. La route choisie est celle qui contient un nombre minimum de nœuds (minimum de sauts) [37].

1.7.2.3 Perte de paquets

Les protocoles de routage utilisent cette métrique dans le but de minimiser le nombre de paquets de données perdus lors du transfert depuis une source vers une destination pendant le routage [38]. L'idée est de calculer le rapport des paquets perdus et des paquets émis transitant dans le réseau. Autrement dit, on calcule le nombre de paquets perdus sur le nombre de paquets transmis lors d'une transmission. Dans le cas où le taux de perte de paquets est élevé, il est nécessaire de mettre en place des mécanismes qui permettent de minimiser les collisions.

1.7.2.4 Délai de bout-en-bout EED

L'EED (End-to-End Delay) est le temps moyen nécessaire pour qu'un paquet de données soit acheminé à partir de la source vers la destination [38]. Cette technique est parmi les métriques les plus connues dans les réseaux sans fil. Les protocoles de routage l'utilisent pour minimiser le temps de propagation des paquets de données échangés pendant le routage.

1.8 Les principaux domaines de recherche

Dans la littérature, plusieurs travaux de recherche visent à proposer des solutions optimales et efficaces à un ou plusieurs problèmes des RCSF illustrés précédemment. Les principaux domaines de recherche abordés dans les RCSF sont les suivants [18]:

- **Efficacité énergétique:** en raison de la ressource énergétique limitée, plusieurs solutions, à la fois du matériel et des logiciels, ont été proposées afin d'optimiser l'utilisation de l'énergie;
- **Localisation** : vu le très grand nombre des nœuds capteurs sur un RCSF et leur déploiement d'une manière ad hoc, de nombreux systèmes de coordonnées spatiales et virtuelles ont été proposés, auxquels les nœuds capteurs peuvent s'identifier pour se localiser dans le RCSF;
- **Routage** : plusieurs protocoles de routage ont été proposés pour les RCSF pour minimiser les coûts de communication, afin de réduire la consommation énergétique ;
- **Sécurité :** les applications utilisant les RCSF ont souvent besoin d'un niveau de sécurité élevé. Or, de par leurs caractéristiques (cités dans la section 1.6), la sécurisation des RCSF est à la source de beaucoup de travaux scientifiques et techniques proposant des solutions de sécurité efficaces.
- **La Tolérance aux pannes** : La tolérance aux pannes est définie par l'aptitude du protocole de routage à maintenir ses fonctionnalités, en cas de panne de quelques nœuds. Le but de la tolérance aux pannes est d'éviter la faille totale du système malgré la présence de fautes dans un sous ensemble de ses composants élémentaires. Les pannes sont tolérées puisqu'elles sont plus fréquentes à cause de l'épuisement rapide d'énergie et à la nature contraignante de l'environnement qui expose les nœuds à des endommagements physiques. Pour cela, les protocoles de routage conçus doivent atteindre le niveau de tolérance aux pannes requis selon l'application. A cet effet, les protocoles de routage doivent, en cas de défaillance de liens de communication, procéder à la formation de nouvelles routes entre les nœuds [40].
- **Clustering :** Le clustering consiste à découper le réseau en groupes de nœuds appelés Cluster. Pour chaque cluster un nœud maître appelé Cluster-Head est élu selon l'état courant du réseau afin d'accomplir des tâches spécifiques.
- **Agrégation de données** : L'une des caractéristiques des réseaux de capteurs est la possibilité de réduire la quantité de données circulant dans le réseau, afin de conserver

de l'énergie, en fusionnant les données par des nœuds particulier du réseau. Ce processus est appelé agrégation de données.

1.9 Conclusion

Dans ce premier chapitre nous avons procédé à l'étude des réseaux de capteurs sans fil. Nous avons posé les briques de base et fédéré quelques concepts nécessaires à la compréhension de nos problématiques dans la suite de ce manuscrit. Nous avons présenté en premier lieu quelques généralités sur les RCSF, à savoir la description d'un RCSF, leurs caractéristiques intrinsèques, les paramètres influençant leur conception, La Consommation d'énergie et leurs exigences de sécurité. Puis, nous avons présenté un état de l'art sur les protocoles de routage dédiés aux RCSF. Enfin, nous avons remarqué que plusieurs facteurs et contraintes compliquent la gestion de ce type de réseaux. En effet, les réseaux de capteurs se caractérisent par une capacité énergétique limitée rendant l'optimisation de la consommation d'énergie dans des réseaux pareils une tâche critique pour prolonger la durée de vie du réseau.

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

Le chapitre suivant est consacré pour détailler la notion de tolérance aux pannes dans les réseaux de capteurs sans fil et son utilité.

CHAPITRE 2

LA TOLERANCE AUX PANNES DANS LES RCSF

2.1 Introduction

La limitation d'énergie dans les capteurs sans fil, et les environnements hostiles dans lesquels ils pourraient être déployés, sont des facteurs qui rendent ce type de réseaux très vulnérables. Ainsi la perte de connexions sans fil peut être due à une extinction d'un capteur suite à un épuisement de sa batterie, ou tout simplement à une destruction physique accidentelle ou intentionnelle par un ennemi.

Par ailleurs, l'absence de sécurité physique pour ce type de capteurs, et la nature vulnérable des communications radios sont des caractéristiques qui augmentent les risques de pannes sur ce type de réseau. Etant donné que les réseaux de capteurs reposent sur des protocoles de communication ad hoc, il est donc nécessaire de considérer la tolérance aux pannes comme critères indispensable dans la conception de ces protocoles.

Ce chapitre s'articulera sur la notion de tolérance aux pannes dans les réseaux de capteurs où nous commencerons par sa définition. Après une classification des pannes dans les systèmes distribués .Par la suite, une classification des protocoles tolérants aux pannes sera présentée selon différents critères. En fin présenter une synthèse sur quelques protocoles de routage tolérants à pannes, proposées dans la littérature.

2.2 Définition de la tolérance aux pannes

Afin d'assurer la communication entre le nœud collecteur et les autres nœuds d'un réseau de capteurs, les protocoles de routage sont basés sur la communication multi-sauts. Chaque nœud joue alors, en plus du rôle de source de données, le rôle d'un routeur. Toutefois, ces nœuds sont sujets à de nombreuses pannes, dues principalement à l'épuisement des batteries et aux destructions physiques (par exemple, suite à un écrasement par des animaux). Ainsi, la panne de nœuds entraîne la perte des liens de communication et donc un changement significatif dans la topologie globale du réseau.

Ceci peut affecter d'une façon considérable la connectivité du réseau et diminuer, en conséquence, sa durée de vie.

La propriété de tolérance aux pannes est définie par l'aptitude du réseau à maintenir ses fonctionnalités, en cas de panne de certains de ses nœuds. Elle vise donc à minimiser l'influence de ces pannes sur la tâche globale du réseau [02].

2.3 Procédure générale de tolérance aux pannes [35]

La conception d'une procédure pour la tolérance aux pannes dépend de l'architecture et des fonctionnalités du système. Cependant, certaines étapes générales sont exécutées dans la plupart des systèmes [61] comme s'est illustré dans la figure 2-1

Figure 2.1 Procédure générale de tolérance aux pannes.

2.3.1 Détection d'erreurs

C'est la première phase dans chaque schéma de tolérance aux pannes, dans laquelle on reconnaît qu'un événement inattendu s'est produit. Les techniques de détection de pannes sont généralement classifiées en deux catégories : en ligne et autonome (offline).

La détection offline est souvent réalisée à l'aide de programmes de diagnostic qui s'exécutent quand le système est inactif. La détection en ligne vise l'identification de pannes en temps réel et est effectuée simultanément avec l'activité du système.

2.3.2 Détention de la panne

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

2.3.3 Recouvrement d'erreur

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

2.3.4 Traitement de pannes

Dans cette phase, la réparation du composant en panne isolé est effectuée.

La procédure de réparation dépend du type de la panne. Les pannes permanentes exigent une substitution du composant avec un autre composant fonctionnel. Le système doit contenir un ensemble d'éléments redondants (ou en état standby) qui servent à remplacer les nœuds en panne.

2.4 Classification des protocoles de tolérance aux pannes [35]

Les protocoles tolérants aux pannes peuvent être vus de plusieurs angles différents. De ce fait, un ensemble de critères est défini pour les classifier. Nous citons, entre autre, deux principales catégories ; à savoir les classifications temporelles et architecturales.

2.4.1 Classification temporelle

Dans la classification temporelle, nous divisons l'ensemble des algorithmes en deux catégories, et cela selon la phase de traitement. Si le traitement est effectué avant la panne ; on parle donc d'algorithmes préventifs. Sinon, les algorithmes sont dits curatifs.

- **Algorithme préventif:** implémente des techniques tolérantes aux pannes qui tentent de retarder ou éviter tout type d'erreur afin de garder le réseau fonctionnel le plus longtemps possible. La conservation d'énergie à titre d'exemple, permet de consommer moins d'énergie et évite donc une extinction prématurée de la batterie ce qui augmente la durée de vie des nœuds.
- **Algorithme curatif:** utilise une approche optimiste, où le mécanisme de tolérance aux pannes implémenté n'est exécuté qu'après la détection de pannes. Pour cela, plusieurs algorithmes de recouvrement après pannes sont proposés dans la littérature, par exemple : le recouvrement du chemin de routage, l'élection d'un nouvel agrégateur, etc.

2.4.2 Classification architecturale

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

2.4.2.1Gestion de la batterie

Cette catégorie est considérée comme une approche préventive, où les protocoles définissent une distribution uniforme pour la dissipation d'énergie entre les différents nœuds capteurs ; afin de mieux gérer la consommation d'énergie et augmenter ainsi la durée de vie de tout le réseau. En outre, le mécanisme de mise en veille est une technique de gestion de batterie. En effet, les protocoles déterminent des délais de mise en veille des nœuds capteurs inactifs pour une meilleure conservation d'énergie ;

2.4.2.2 Gestion de flux

Cette catégorie regroupe les techniques qui définissent des protocoles de gestion de transfert des données (routage, sélection de canal de transmission, etc.). Nous pouvons trouver des approches préventives ou curatives sur les différentes couches (réseau, liaison de données, etc.) telles que :

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

2.4.2.3 Gestion des données

Les protocoles classés dans cette catégorie offrent une meilleure gestion de données et de leur traitement. Deux principales sous-catégories sont déterminées :

- **Agrégation:** considérée comme approche préventive, l'opération d'agrégation effectue un traitement supplémentaire sur les données brutes captées depuis l'environnement. Un nœud agrégateur combine les données provenant de plusieurs nœuds en une information significative. Ce qui réduit considérablement la quantité de données transmises en consommant moins d'énergie pour leur dissémination. Ceci permet donc d'augmenter la durée de vie du réseau.
- **Clustering:** une des importantes approches pour traiter la structure d'un réseau de capteurs est le clustering. Il permet la formation d'un backbone virtuel qui améliore l'utilisation des ressources rares telles que la bande passante et l'énergie. Par ailleurs, le clustering aide à réaliser du multiplexage entre différents clusters. En outre, il améliore les performances des algorithmes de routage. Plusieurs protocoles utilisent cette approche préventive et parfois elle est considérée comme une approche curative.

2.5 Les protocoles de routage tolérants aux pannes dans les RCSF

La tolérance aux pannes pour assurer une fiabilité de délivrance de paquets à la station de base est traitée au niveau de la couche réseau. Dans ce qui suit, nous présentons les fonctionnalités de certains protocoles de routage tolérants aux pannes et nous discutons leurs limites:

2.5.1 RERP est un protocole de routage adaptatif tolérant aux pannes pour les RCSF

Un RCSF est formé d'un grand nombre de capteurs qui sont déployés aléatoirement dans une zone d'intérêt. Dans RERP [62], il est supposé que chaque nœud a au moins deux voisins dans la direction vers la station de base. De ce fait, il aura au moins deux chemins alternatifs pour acheminer les données vers la station de base. Les nœuds qui sont loin de la station de base n'empêchent pas la formation de la boucle. La capacité d'un nœud tolérant aux pannes dépend du nombre des nœuds voisins actifs, c'est-à-dire si un nœud a N voisin, il peut tolérer N-1 nœuds en panne.

Le protocole RERP est protocole de routage proactif et sa conception comporte deux tâches:

Mise en place de RERP : cette tâche s'exécute en cinq phases:

- **Phase de publicité:**

  Dans cette phase, la station de base diffuse un paquet de publicité à ses nœuds voisins pour indiquer qu'elle peut recevoir des paquets de données. Les nœuds qui reçoivent le

paquet de publicité établissent une table de routage pour indiquer le chemin vers la station de base.

- **Phase d'initialisation:**

Dans cette phase, les nœuds qui n'ont pas de chemin direct vers la station de base diffusent une requête de découverte de routes (RREQ) vers la station de base. Quand un concentrateur reçoit le paquet (RREQ), il diffuse une réponse (RREP). De même si ce nœud a déjà reçu la requête (RREQ) il diffuse un paquet (RREP) s'il existe un chemin entre lui et le concentrateur, sinon le paquet (RREQ) sera ignoré.

- **Route de sélection:**

Une table de routage est utilisée pour construire et entretenir les routes. Le choix de l'itinéraire des nœuds relais est basé sur l'énergie restante des nœuds.

- **Phase de transfert de données :**

Les nœuds capteurs génèrent des paquets de données à chaque fois qu'ils détectent toute nouvelle information. Cette information est transmise à la station de base dans un mode multi-sauts.

- **Table de sauvegarde:**

En plus du chemin principal, un chemin alternatif est prévu pour tous les nœuds du réseau. Chaque fois qu'un nœud reçoit un paquet RREP, si il ne dispose pas de chemin direct vers la station de base, il stocke le chemin dans la table de routage, et il stocke les paquets (RREP) dans une table de sauvegarde. La table de routage de secours dispose de deux champs, l'identifiant du nœud ID et son énergie.

- **Rapport d'erreurs:**

Les fonctions pour reporter les erreurs sont incorporées dans ce protocole de routage dont lesquelles figurent les types de messages suivants:

1. Echec des liens: le message d'échec de liens est généré dans les deux cas. Le premier se produit quand un RTS est envoyé mais aucune CTS correspondant n'est reçu et le nombre maximal de tentatives est dépassé. Le second se passe quand un paquet de données a été transmis, mais il n'a jamais reçu un ACK de réception et le nombre maximal de tentatives est dépassé.
2. Message de batterie critique: Ce message est généré lorsque le niveau de la batterie d'un nœud est inférieur à une valeur seuil dite critique. Ce message est envoyé au nœud source qui a envoyé les données et également aux voisins de ce nœud. Quand les autres nœuds reçoivent ce message ils suppriment l'identifiant du nœud défaillant de leurs tables de routage ou de leur table de voisins.

3. Message de destination inaccessible: Ce message est généré lorsque le paquet de données est mis au rebut sans être transmis au nœud de destination en raison de l'indisponibilité du chemin vers la station de base.
4. Sélection du chemin de secours: Chaque nœud possède une table de routage de secours dans laquelle il stocke un chemin de secours vers la destination. Quand un nœud échoue dans la transmission de paquet de donnée, alors son voisin consulte la table de secours pour trouver le chemin alternatif afin qu'il puisse transmettre le paquet de données.

Dans RERP la communication entre les nœuds est réalisée par des messages Requête/Réponse où le nœud expéditeur envoie une requête « Hello » au nœud de destination. Ce type de messages est utilisé pour vérifier si le voisin est accessible et pour calculer le temps de parcours.

RERP présente certaines limitations telles que la consommation d'énergie qui est assez grande lors de la diffusion des rapports d'erreurs.et aussi le paquet de données sera perdu lorsque le chemin vers la station de base n'est pas disponible à partir d'un nœud.

2.5.2 Protocole de routage temps réel tolérant aux pannes (DMRF)

DMRF [63] fonctionne en deux modes de transmission de données: saut-à-saut et le mode de transmission «Jumping». Chaque nœud utilise le temps restant pour transmettre un paquet à la station de base et l'ensemble des nœuds de transfert FCS (Set candidat Forwarding) pour choisir dynamiquement le prochain saut. Quand un nœud présente une défaillance, alors la congestion du réseau ou d'une région vide se produit. Le mode de transmission sera passé en mode« Jumping », ce qui peut réduire le délai de transmission, et assure la fiabilité de la livraison des paquets de données envoyés à la station de base dans un délai spécifié. Il est théoriquement prouvé que DMRF peut répondre en temps réel aux exigences de tolérance aux pannes.

Dans DMPF, le processus de transmission est divisé en cinq étapes:

- **Phase d'initialisation:**

  Dans cette phase, DMRF initialise la liste de voisinage des nœuds, la liste de l'état du réseau (information sur la congestion d'un nœud, les zones vides, …), liste des candidats FCS, table des probabilités de transition, et la voie de transmission initiale.

- **Phase de transmission des données:**

Dans cette phase, DMRF détecte la défaillance d'un nœud, la congestion du réseau et des régions vides. Le temps restant pour acheminer un paquet de données jusqu'à la station de base sera contrôlé. A partir de ce temps, le paquet sera transmis en mode « Jumping » ou non. Si aucune des conditions ci-dessus ne se produit, DMRF sélectionne dynamiquement un membre du FCS comme nœud relais en se basant sur le taux de transmission de données et des informations locales. Une fois les nœuds défaillants sont détectés, ou le temps restant est inférieur à un certain seuil, le mode de transmission « Jumping » sera utilisé.

- **Phase de transmission « Jumping »:**

Au cours de cette phase, chaque nœud ajuste dynamiquement le contenu de FCS et calcule la probabilité pour transiter à chacun de ces nœuds. Dans ce mode, le paquet de données peut un saut d'une grande portée pour éviter les nœuds défaillants. Cependant, il ne peutpas garantir le succès de la transmission. Donc la phase d'ajustement de probabilités de transitions est effectué après chaque transmission « Jumping ».

- **La phase de probabilité d'ajustement :**

Dans cette phase, DMRF ajuste la probabilité de saut en fonction du résultat de la transmission « Jumping » (succès ou l'échec) et renvoie l'information à son nœud en amont. Lorsque le paquet de données arrive au nœud récepteur, on considère que la transmission est terminée.

Dans DMRF, le nœud peut transmettre directement des données à la station de base ou en passant par des nœuds relais en fonction de la probabilité de transition vers ces nœuds. Si la transmission de données échoue, la probabilité de transition sera mise à jour via un mécanisme de rétroaction, qui peut non seulement éviter l'effet causé par la défaillance des nœuds, mais aussi d'améliorer le taux de transmission. Ceci permet de réduire la consommation d'énergie.

DMRF présente certaines limitations en particulier dans le mode « Jumping » qui ne garantit la fiabilité de livraison de données et qui consomme plus d'énergie quand il utilise une grande portée.

2.5.3 Amélioration du protocole de routage tolérant aux pannes AODV (ENFAT-AODV)

AODV (ENFAT-AODV) [64] est un protocole de routage permet la tolérance de pannes, l'auto-démarrage du routage multi-sauts entre les nœuds participants qui souhaitent créer et maintenir un réseau de capteurs sans fil. ENFAT-AODV offre une mise en place d'itinéraire rapide et efficace entre les nœuds de communication désirants.

En outre, ENFAT-AODV permet aux nœuds sur une voie principale de transmettre des données pour obtenir un chemin de secours, qui est utilisé lorsque leur chemins principal seront perdu, pour répondre à établir un lien entre les ruptures des nœuds dans les meilleurs délais. Le nombre de sauts long d'un trajet est utilisé en tant que métrique d'une sélection de chemin. Si des multiples RREP avec le numéro de destination on la même séquence sont reçus par la source, le chemin le plus court avec le comptage dehoublon est choisi. Ce qui fait que les demandes RREQs et les réponses RREP du même type sont acheminées. Tels qu'elles sont définis par AODV.

Toutefois, pour ENFAT-AODV, certains champs sont ajoutés dans les paquets de contrôle tels que "BACKUP" drapeau (en RREQ et RREP), "UPDATE" drapeau (en RREQ) et "Distance pour Dest" de terrain (dans RREQ). En outre, ENFAT-AODV nécessite que certains messages (par exemple, RREQ) doivent être largement diffusés, peut-être à travers le réseau. La zone de diffusion de ces RREQs est indiquée par le TTL dans l'en-tête IP.

En outre, ENFAT-AODV réduit également une certaine complexité de mise en œuvre par l'élimination d'un ensemble d'éléments du cahier des charges, les messages sont supprimés afin de réduire les paquets de contrôle inutiles dans le réseau. Ensuite, le fonctionnement local de réparation n'est pas inclus dans ENFAT-AODV.

- **Découverte de la route principale:**

  Quand un chemin principal de livraison des données vers la station de base est nécessaire, le nœud source coulera un message (découverte d'une route principal), un processus diffus un paquet de demande principale (principale RREQ) a la station de base. À chaque nœud intermédiaire, lorsqu'un RREQ principale est reçu, un chemin inverse à la source est créé. Si le nœud de réception n'a jamais reçu ce RREQ principal avant, et si le nœud ne connaît pas la route principale menant à la destination, il transmet le RREQ principale à ses voisins. Si le nœud de réception est la destination

ou bien s'il connaît la route principale menant à la destination, il va générer un itinéraire principal Réponse (principale RREP). Ensuite, le RREP principal est uni coulé par saut à la source. Comme le RREP principale est renvoyé à la source, chaque nœud intermédiaire qui traite le RREP principale crée un chemin principal vers la station de base. Lorsque la source reçoit le RREP principal, elle enregistre la route principale menant à la destination dans sa table de routage principale.

- **La construction la route de sauvegarde:**

Au cours de la phase de croisière réponse principale, les nœuds d'un chemin principal qui reçoivent un RREP principale créent un chemin de sauvegarde vers la station de base en diffusant un paquet de sauvegarde RREQ. Après la diffusion du RREQ sauvegarde, le nœud attend un paquet RREP sauvegarde de la destination elle-même ou un nœud intermédiaire qui peut satisfaire les conditions spécifiées comme suit:

- Il dispose d'une entrée de sauvegarde active du chemin principal vers la station de base,
- Il n'est pas un nœud sur le chemin principal,
- Et le nombre de sauts du chemin de sauvegarde active à partir du nœud intermédiaire à la destination est inférieur au domaine de la sauvegarde RREQ, pour garantir qu'il fournira un chemin de sauvegarde court.

- **Entretien de la route:**

Pendant la période de livraison de paquets de données, lorsque le chemin principal n'est pas valide ou reçoit un paquet de données destiné au nœud de destination pour laquelle il ne dispose pas d'un chemin actif principal, le nœud utilise immédiatement sa route de sauvegarde pour livrer les prochains paquets de donnée qui viennent, sans interruption. Par la suite, le nœud sur le nouveau chemin principal, qui utilise une route de secours, dirige un processus "Découverte de route de secours" visant à trouver une voie nouvelle. Par conséquence, il augmente de plus la fiabilité et la disponibilité par rapport à l'original du protocole AODV routage.

La limitation de ce protocole repose sur la consommation de l'énergie à cause de l'inondation des messages de contrôle.

2.5.4 FaT2D: Diffusion par tolérance aux pannes Réalisé pour les RCSF

FaT2D [65] est un protocole de tolérance aux pannes basée sur la diffusion. Ce dernier a l'avantage de fournir une forte tolérance contre les défaillances de nœuds grâce à sa construction des trajets multiples et l'exploration périodique des routes. FaT2D définit une nouvelle technique qui permet de détecter rapidement une panne et la recouvrir quand il y a une collision entre les nœuds et des changements de topologie. Il s'exécute selon la démarche qui suit:

- **Détection de panne:**

Un nouveau délai d'attente de détection de pannes, noté TFD, est défini afin de réduire le temps de recouvrement de la panne et par conséquent la réparation des nœuds et le chemin local se font rapidement, tout en tolérant les pannes intermittentes dues aux pertes de paquets. Si TFD s'épuise, FaT2D transmet immédiatement un nouveau message appelé Explore-Request pour notifier l'événement de détection de la panne et demande une nouvelle exploration pour trouver un autre chemin fiable qui remplace le chemin défaillant. Par conséquent, tout nœud appartenant au chemin défaillant supprime le gradient correspondant pour éliminer la panne.

- **Recouvrement du chemin:**

Quand Tfd s'épuise, il déclare la défaillance d'un nœud. De ce fait, FaT2D lance un processus pour réparer le chemin défectueux en envoyant un message de demande d'exploration appelé « ExploreRequest ». Ce message contient les informations sur la route défectueuse et il est acheminé pour atteindre le nœud cible sans utiliser les transmissions bouclées ou rechercher les nœuds non adéquats.

Quand le nœud cible reçoit le message « ExploreRequest », il arrête de le transmettre, puis il lance une exploration par inondation comme dans « Direct Diffusion ». Cela génère une phase d'exploration afin de trouver un nouveau chemin fiable. L'élection de ce chemin se fait selon les règles utilisées dans «Direct Diffusion ».

- **Elimination des pannes:**

Pour chaque nœud intermédiaire recevant le message ExploreRequest, FaT2D vérifie si ce nœud appartient au chemin défectueux. Si c'est le cas, il aura un effet négatif pour renforcer son gradient. Ce dernier sera réélu par une 'exploration envoyé par le nœud

source du chemin correspondant. Ainsi, chaque nœud exécute un renfort local négatif à son voisin en amont, afin de supprimer le chemin brisé et arrêter l'envoi de données perdues.

Un des principaux défis dans la conception des protocoles de routage pour les réseaux de capteurs est l'efficacité énergétique en raison des ressources limitées que présentent les capteurs.

2.6 Conclusion

Dans les RCSF, l'objectif de la conception de protocole de routage est d'assurer la fiabilité de livraison de données à la station de base tout en prolongeant la durée de vie du réseau. Or, la consommation d'énergie dans les RCSF est dominée par la transmission de données et la réception. Par conséquent, les protocoles de routage dans RCSF doivent minimiser au moins les messages qui sont retransmis lors de l'occurrence d'une panne.

Dans ce chapitre, nous avons présenté d'une manière générale le principe de la tolérance aux pannes dans les réseaux de capteurs. Puis, nous avons fait le point sur le concept de la tolérance aux pannes dans les réseaux de capteurs pour assurer la fiabilité de délivrance de paquets à la station de base et pour garantir une couverture totale de la zone d'intérêt. Par la suite nous avons étudiée les protocoles de routage tolérants aux pannes. Notre constat nous a permis d'illustrer les limites de ces protocoles. D'où, nous avons pensé à améliorer TinyOS Beaconing qui est un protocole bien réputé mais qui n'est pas tolérant aux pannes. (Plus ancien crée en 2000 avec le système exploitation TinyOS), qui suit une architecture hiérarchie et qui est particulièrement intéressant pour les RCSF, Par ce que déjà adapté par défaut aux capteurs Mica2 .En effet, TinyOS beaconing constitue l'objet principal de notre étude. Ainsi, le chapitre suivant sera consacré pour son étude détaillée.

CHAPITRE 3

LE PROTOCOLE DE ROUTAGE

TINYOS BEACONING

3.1 Introduction

Suite aux différents défis des RCSF qu'on a vus dans le premier chapitre, l'université de Berkeley, en plus de nombreux contributeurs ont développé un système d'exploitation destiné au RCSF afin de faciliter l'implémentation et l'exécution de protocoles dédiés à ce type de réseaux. L'objectif consiste à minimiser la taille du code afin de respecter les contraintes de ressources énergétiques et physiques des nœuds capteurs. Ce système est intitulé TinyOS. Ce système exploitation est attaché avec un protocole de routage dite : TinyOS Beaconing « TOSB ».

Dans ce chapitre, Nous commençons tout d'abord par le système d'exploitation TinyOS, conçu pour les RCSF, et leurs caractéristiques principales, Puis nous parlons aussi du protocole de routage étudié dans ce mémoire avec une présentation générale, et le principe de fonctionnement puis on prend un exemple, puis leur fiabilité et quelques failles du protocole, et les travaux antérieurs penchant sur ce protocole, en fin étudiée la tolérance aux pannes dans TinyOS Beaconing (TOSB).

3.2 Le système d'exploitation TinyOS

Il a l'avantage de permettre une programmation simple et puissante tout en gardant la portabilité du code pour de nombreuses plateformes supportées. Il est utilisé par plus de 500 universités et centres de recherche dans le monde vu la caractéristique open source qu'il détient [43]. Il respecte une architecture basée sur une association de composants. Il utilise une programmation entièrement réalisée en langage NesC.

3.2.1 Présentation

TinyOS est un système d'exploitation open-source conçu pour des réseaux de capteurs sans-fil. Il respecte une architecture basée sur une association de composants, réduisant la taille du code nécessaire à sa mise en place. Cela s'inscrit dans le respect des contraintes de mémoires que disposent les réseaux de capteurs.

Figure 3.1 logo de TinyOS. [44]

Pour autant, la bibliothèque de composant de TinyOS est particulièrement complète puisqu'on y retrouve des protocoles réseaux, des pilotes de capteurs et des outils d'acquisition de données. L'ensemble de ces composants peut être utilisé tel quel, il peut aussi être adapté à une application précise. En s'appuyant sur un fonctionnement événementiel, TinyOS propose à l'utilisateur une gestion très précise de la consommation du capteur et permet de mieux s'adapter à la nature aléatoire de la communication sans fil entre interfaces physiques.

3.2.2 Propriétés

TinyOS est basé sur six grandes propriétés qui font que ce système d'exploitation, s'adapte particulièrement bien aux systèmes à faible ressources [45], comme illustre dans le tableau suivant (Table 2.1):

Propriété	**Valeur**
disponibilité	open-source
type	event-driven
langage	NesC
préemptif	non
temps réel	non
consommation	réduite

Table 3.1 Propriétés de TinyOS.[45]

- **Disponibilité et sources :** TinyOS est un système principalement développé et soutenu par l'université américaine de Berkeley, qui le propose en téléchargement sous la licence BSD et en assure le suivi. Ainsi, l'ensemble des sources sont disponibles pour de nombreuses cibles matérielles.
- **Event-driven :** Le fonctionnement d'un système basé sur TinyOS s'appuie sur la gestion des évènements se produisant. Ainsi, l'activation de tâches, leur

interruption ou encore la mise en veille du capteur s'effectue à l'apparition d'évènements, ceux-ci ayant la plus forte priorité. Ce fonctionnement évènementiel (event-driven) s'oppose au fonctionnement dit temporel (time-driven) où les actions du système sont gérées par une horloge donnée.

- **Langage :** TinyOS a été programmé en langage NesC, Le nesC est un prolongement du langage C. Il est conçu pour gérer les concepts et le modèle d'exécution de TinyOS.

  Le langage NesC est utilisé pour le Système d'Exploitation TinyOS approprié à ce genre de réseaux, c'est un langage intéressant mais trop complexe et assez long à comprendre.
- **Préemptif :** Le caractère préemptif d'un système d'exploitation précise si celui-ci permet l'interruption d'une tâche en cours. TinyOS ne gère pas ce mécanisme de préemption entre les tâches mais donne la priorité aux interruptions matérielles. Ainsi, les tâches entre-elles ne s'interrompent pas mais une interruption peut stopper l'exécution d'une tâche.
- **Pas de temps réel :** Lorsqu'un système est dit « temps réel » celui-ci gère des niveaux de priorité dans ses tâches permettant de respecter des échéances données par son environnement. Dans le cas d'un système strict, aucune échéance ne tolère de dépassement contrairement à un système temps réel. TinyOS se situe au-delà de ce second type car il n'est pas prévu pour avoir un fonctionnement temps réel.
- **Consommation :** TinyOS a été conçu pour réduire au maximum la consommation en énergie du capteur. Ainsi, lorsqu'aucune tâche n'est active, il se met automatiquement en veille.

3.2.3 Cibles possibles pour TinyOS

Il existe de nombreuses cibles possibles pour ce système d'exploitation embarqué. Malgré leurs différences, elles respectent toutes globalement la même architecture basée sur un noyau central autour duquel s'articule les différentes interfaces d'entrée-sortie, de communication et d'alimentation [45]. Voici un schéma représentant cette architecture :

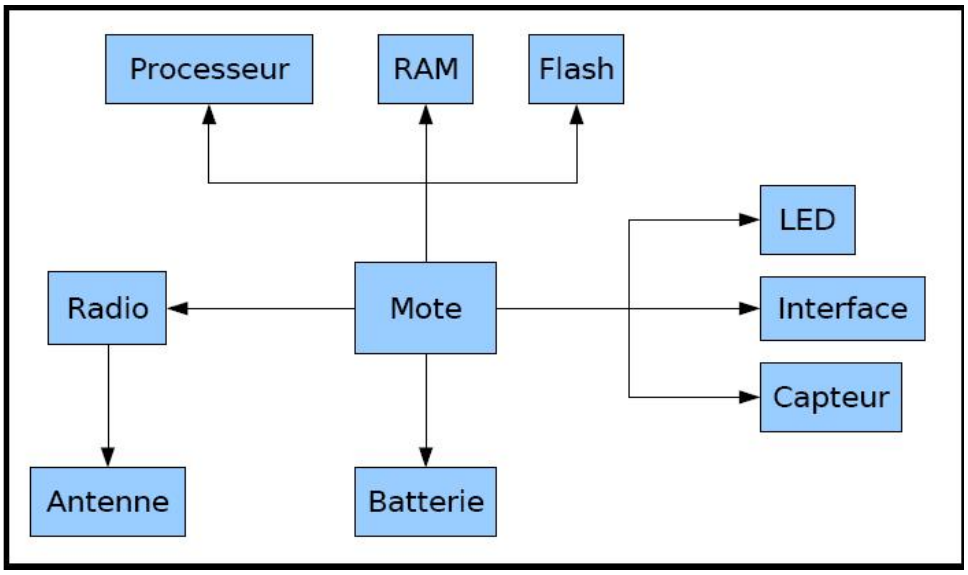


Figure 2.2 Architecture générale des cibles utilisant TinyOS [45].

- Mote, processeur, RAM et Flash : On appelle généralement Motes la carte physique utilisant TinyOS pour fonctionner. Celle-ci a pour cœur le bloc constitué du processeur et des mémoires RAM et Flash. Cet ensemble est à la base du calcul binaire et du stockage, à la fois temporaire pour les données et définitif pour le système TinyOS.
- Radio et antenne : TinyOS est prévu pour mettre en place des réseaux sans fils, les équipements étudiés sont donc généralement équipés d'une radio ainsi que d'une antenne afin de se connecter à la couche physique que constitue les émissions hertziennes.
- LED, interface, capteur : TinyOS est prévu pour mettre en place des réseaux de capteurs, on retrouve donc des équipement bardés de différents types de détecteurs et autres entrées.
- Batterie : Comme tous les dispositifs embarqués, ceux utilisant TinyOS sont pourvus d'une alimentation autonome telle qu'une batterie.

3.3 Le protocole TinyOS beaconing

Le protocole TinyOS Beaconing c'est un protocole utilisé en nœuds de mica à l'université de Berkeley, et fonctionne dans les réseaux de capteur avec le matériel restreint [46].

3.3.1. Principe de fonctionnement

Le protocole établit périodiquement un arbre minimale (Spanning tree), s'étendre à partir de la station de base. La station de base (dite la sink) propage le message qui est écarté par le réseau en vue de créer l'arbre de cheminement (Routage). Car c'est un protocole simple et général, son exécution est inférieure à celle de protocoles développés pour des applications spécifiques.

Le protocole TinyOS Beaconing c'est un protocole à vecteur de distance sélectionne le prochain saut vers la station de base repose sur une certaine distance, comme métrique de routage, Dans TinyOS Beaconing, un message Beacon prévenant de la station de base est inondée dans le réseau, et chaque nœud choisit le nœud à partir duquel elle a reçu la première Beacon d'atteindre un nœud est utilisé comme indicateur (parent) [47].

Il fonctionne en deux phases :

1) Phase de distribution, où le réseau est structuré en arbre.

2) Phase de collection, où les données sont acheminées via l'arbre de routage. Durant la phase de collection, chaque parent doit attendre l'envoi de données par tous ses fils au nœud racine via l'arbre.

3.3.2 Description de protocole [57]

À l'origine, les auteurs de TinyOS proposent un protocole très simple de routage dans [47], appelé TinyOS Beaconing protocol , dans ce protocole, chaque nœud est adressé par un identifiant globalement unique, et la station de base initie périodiquement la découverte de route en inondant le réseau avec un message Beacon, Lors de la réception de la première Beacon à l'intérieur d'un intervalle de Beaconing unique, chaque noeud (chaque noeud représentant un capteur) stocker l'identifié immédiate de l'émetteur Beacon en tant que parent (vers le tronçon suivant de base station), et ce rediffuse le message Beacon après le remplacement de l'identifiant de l'expéditeur avec son propre identifiant. Comme pour chaque nœud un seul parent est stocké, le résultat d'un processus de transfert de données, chaque nœud recevant un paquet de données à transmet vers la station de base en envoyant le paquet à son parent, ce mécanisme dite **Beaconing** est une méthode simple pour construire un simple topologie de routage, où chaque nœud définit un voisin en tant que parent, si ce voisin se trouve sur le chemin le plus rapide vers la station de base, le protocole suppose des liens

symétriques dans le réseau et ne considère pas toute l'énergie pour optimiser la durée de vie du réseau[58].

Deux types de messages sont impliqués: messages Beacon hello et des messages des données.

La notation Ni → Nj .

M est utilisé pour indiquer que le nœud Ni transmet le message M au noeud Nj. A transmission de diffusion est indiquée par l'utilisation de la place de * ,Nj et indique que le message M est transmise à tous les nœuds à portée radio de Ni .ce qui suit est une brève description du protocole comme suit.

La station de base diffuse périodiquement une Beacon Hello qui est noyé dans le réseau.

B → *: (Beacon, IDB) (1)

Un nœud, lors de la première audition d'une Beacon Hello, rend le transmettions nœud de sa parent et ignore toutes les messages Beacon avenir. Le nœud retransmet alors le message Beacon avec son propre ID.

Nœud i → *: (Beacon, ID i) (2)

Ce processus est répété tout au long du réseau jusqu'à ce que l'arbre minimal soit établi. Un nœud source, lors de la détection d'un événement important dans son environnement, les données unicast à son nœud parent. Les messages de données sont unicast du nœud à nœud parent jusqu'à ce que la station de base est atteint.

Nœud i → Nœud parent : (Données, ID parent, CHARGE UTILE) (3)

3.3.3 Exemple

Tout d'abord, les inondations de station de base B du réseau avec un Beacon contenant son identifiant. Avant la rediffusion du message Beacon, Le nœud E, D et C remplace l'identifiant de l'expéditeur avec son propre identifiant pour indiquer à ses voisins qu'ils peuvent atteindre la station de base à travers E.

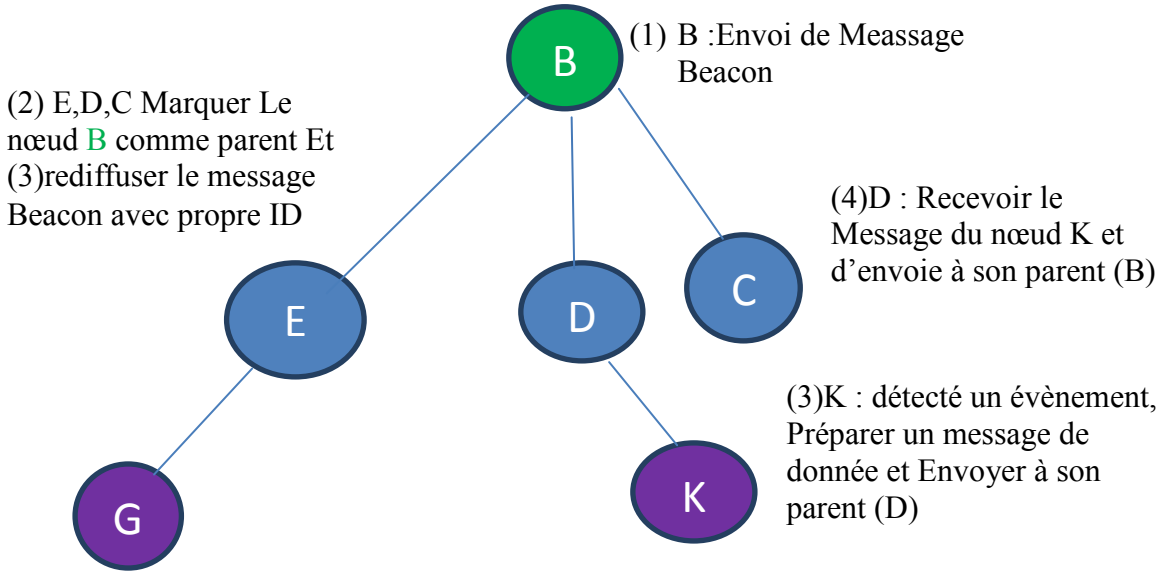


Figure 2.3 Exemple d'application le protocole TOSB .

3.3.4 Le format de paquet

Pour un capteur utilisant le système d'exploitation TinyOS, les messages transmis sur le réseau lors des envois et réceptions sont du type TOS_Msg. Les crickets émettent et reçoivent en broadcaste, c'est-à-dire qu'ils diffusent à tous les capteurs proches et non à un seul.

La transmission d'un message se fait octet par octet. Les messages sont envoyés et reçus grâce à des fonctions comme send(adr,size, TOS_Msg*) et TOS_Msg*receive(TOS_Msg) provenant des interfaces SendMsg et ReceiveMsg.

Voici ci-dessous, le format et la structure d'un message TOS_Msg dans TinyOs.

Dest	AM	Len	Grp	Data	CRC
2	1	1	1	0--29	2

Figure 3.2 : Format de paquet TinyOS.

- Dest: Adresse de destination (identifiant).
- AM : c'est un nombre pour spécifie le type de la fonction appropriée au capteur destinataire.
- Len: La longueur de paquet.
- Grp : Identificateur de Groupe.
- Data : Champ de Donnée.

- CRC :(Cyclic Redondancy Check) contrôle de la somme des données pour s'assurer qu'il ne se passe pas d'erreurs lors de leur duplication.

Le format de paquet de TinyOS sur la figure 2.3, il n'a pas le nœud de source l'information ; ceci laisse le réseau entier vulnérable à l'attaque d'étranger. N'importe quel nœud peut injecter un paquet avec peu d'effort. Pour détecter des erreurs de transmission, les expéditeurs de TinyOS calculent le contrôle par redondance de cycle d'un 16-bit (CRC) au-dessus du paquet. Le récepteur recalculé le centre de détection et de contrôle pendant la réception et le vérifie avec le champ reçu de centre la somme et de contrôle. S'ils sont égaux, le récepteur accepte le paquet et le rejette autrement [58].

3.4 Les faiblesses de protocole TinyOS Beaconing

On a cité quelques faiblesses concernant le protocole TinyOS Beaconing :

- Aucune considération de l'énergie n'implique une durée de vie de réseaux réduite.
- Il existe un chemin unique pour un nœud vers la station de base (arbre minimale).
- La récréation périodique de la topologie, si le seul mécanisme de tolérance aux pannes, s'occupe beaucoup d'énergie. Par ce que c'est un protocole proactif.
- Il y a aucun mécanisme de sécurité intégré.
- Ce protocole est très sensible à l'attaque, Les mises à jour de routage ne sont pas authentifiées.

3.5 Présentation des attaques dans le protocole Tinyos beaconing

Les différentes spécificités des réseaux de capteurs sans fil (énergie limité, faible puissance de calcul, utilisation des ondes radio, etc..) les exposent à de nombreuses menaces. Si certaines de ces menaces peuvent se retrouver dans les réseaux ad-hoc, d'autres sont spécifiques aux réseaux de capteurs sans fil et s'attaquent plus particulièrement à l'énergie limitée des capteurs.

On parlera d'attaque active si un attaquant modifie l'état du réseau, et d'attaque passive dans le cas où il ne cherchera qu'à l'écouter.

Ce protocole est très sensible à l'attaque, par rapport aux protocoles, tel que les mises à jour de routage ne sont pas authentifiées, comme vu dans la table suivant :

Protocole	Attaques appropriées
TinyOS beaconing	Bogus routing information, selective forwarding, sinkholes, Sybil, wormholes, HELLO floods
Directed diffusion	Bogus routing information, selective forwarding, sinkholes, Sybil, wormholes, HELLO floods
Protocol base-cluster (LEACH,TEEN,PEGASIS)	Selective forwarding, HELLO floods

Table 3.2 Les attaques contre les protocoles de routage proposés [55].

3.5.1 Attaque de Spoof information :

Ce protocole est très sensible à cette attaque. Les mises à jour de routage ne sont pas authentifiées, Il est possible pour n'importe quel nœud de prétendre être une station de base et de devenir la destination vers tous les nœuds dans le réseau,

Informations de routage fausses et rejoué (comme «**je suis la station de base**") envoyées par un adversaire peut facilement perturber l'ensemble du réseau.

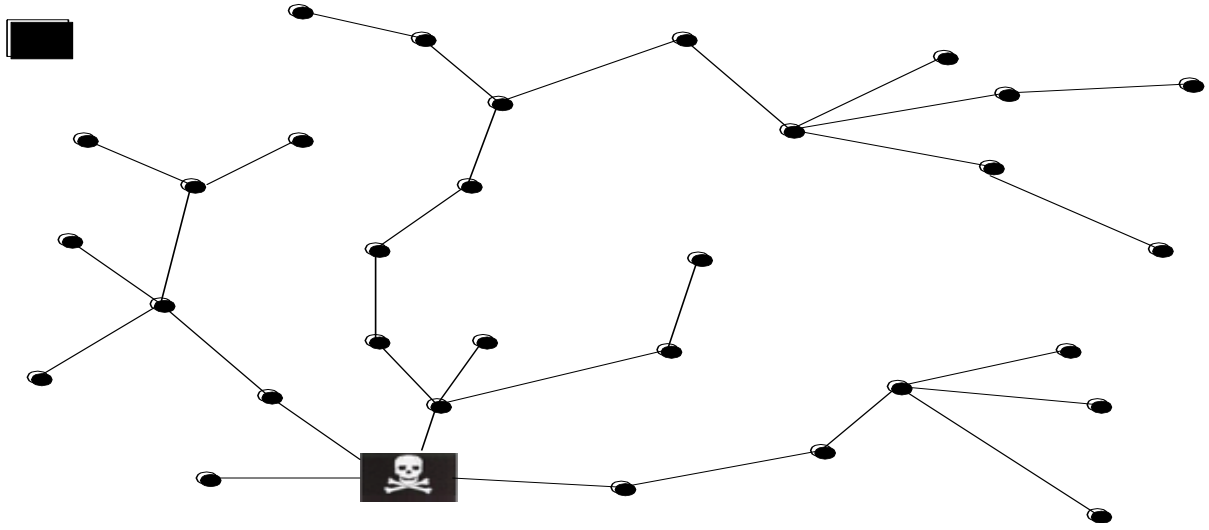


Figure 3.3 l'attaque de spoof information [55].

3.5.2 Attaque du trou noir (black hole attack)

L'attaque du trou noir consiste tout d'abord à insérer un noeud malicieux dans le réseau [55].Ce nœud, par divers moyens, va modifier les tables de routage pour obliger le maximum de nœuds voisins à faire passer l'information par lui. Ensuite comme un trou noir dans l'espace, toutes les informations qui vont passer en son sein ne seront jamais retransmises [56].

La figure 3.4 représente un trou noir mis en place par un nœud malicieux X qui a modifié le routage pour que les nœuds fils (1, 3,9 … et 19) fassent passer l'information par lui pour communiquer entre nœud fils et la sink. Dans ce cas de figure, le trou noir X ne retransmettra aucune information, empêchant toute communication entre les différents nœuds fils et la sink..

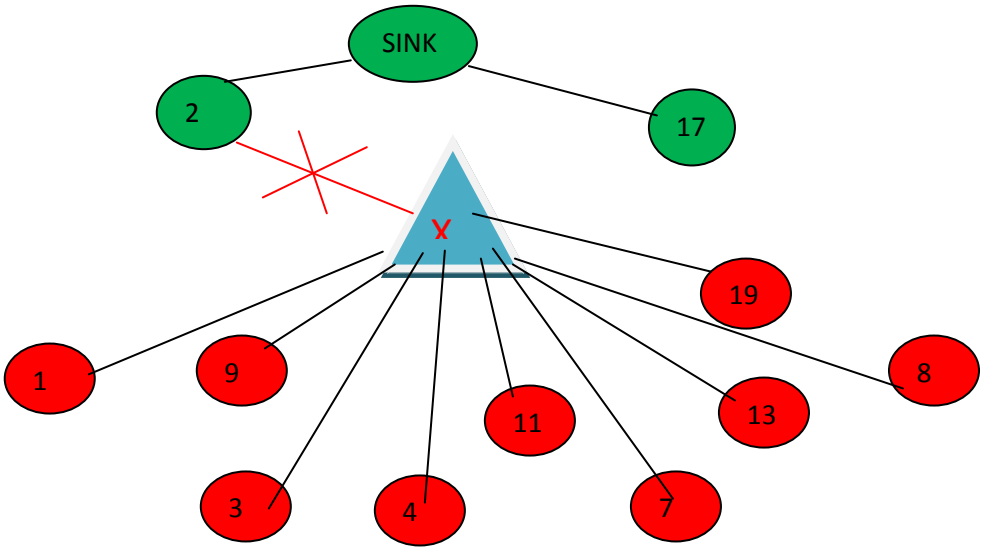


Figure 3.4 Exemple de trou noir dans TinyOS Beaconing

3.6 Synthèse des versions et propositions

Il existe plusieurs amélioration dans ce protocole, Mais la plupart du ces améliorations sont en terme de sécurité.

3.6.1 TinySec [49]

Ce protocole a la particularité d'être implémenté dans le noyau de TinyOS (couche radio), par chris Karlof et N. Sastry en 2003, et de rendre les opérations cryptographiques indépendantes des applications. TinySec suppose qu'initialement chaque nœud partage avec la station de base une clé secrète qui sert à dériver les clés de chiffrement et d'authentification pour des échanges protégés. TinySec prévoit aussi de définir une clé de groupe partagé par tous les nœuds ou un sous ensemble de nœuds, mais il ne précise pas les modalités de distribution de ces clés. C'est pourquoi beaucoup de chercheurs dans la gestion de clés dans les RCSFs ne le considèrent pas comme un protocole de gestion de clés.

TinySec propose deux services de sécurité :

1. Authentification seulement (TinySec-Auth)
2. Authentification avec confidentialité (TinySec-AE)

Avec la première, le paquet de données est envoyé sans qu'il soit encrypté, l'authentification est assurée par l'envoi de MAC du paquet. Le TinySec-AE encrypte le paquet et le MAC du paquet est calculé après l'opération de cryptage, le tout est envoyé vers le destinataire.le format de paquet de tinysec illustre dans la figure suivant .

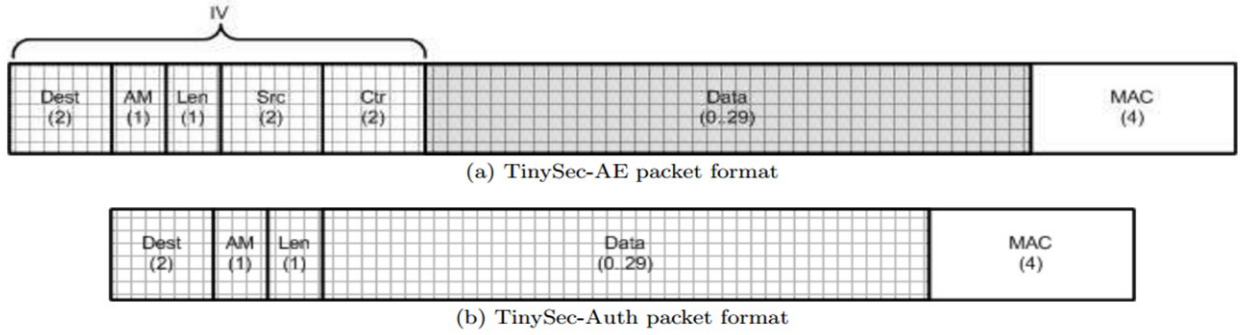


Figure 3.5 Le format de paquet de TinySec. [49]

3.6.2 Minisec [50]

MiniSec est une solution de sécurité pour TinyOS conçus par Mark Lui, Ghita Mezzour,. Il est le successeur de TinySec et ZigBee.MiniSec est basée sur le mode OCB de fonctionnement pour fournir le chiffrement et l'authentification en un seul passage. Le chiffrement utilisé est Skipjack par bloc[59].

MiniSec remplace la somme de détection et de contrôle de 2 octets par une étiquette de 4 octets, puisque l'étiquette protège déjà le paquet contre le tri fouillage. Dans le TinyOS original, la 1 identification du groupe de byte sert de forme brute de contrôle d'accès. Chaque ensemble de nœuds de communication partagent une identification du groupe différent, et des messages avec des identifications du groupe étrangères sont abandonnés. Cette ld de n'est plus nécessaire dans MiniSec parce que le contrôle d'accès est réalisé par l'utilisation de différentes clefs cryptographiques. En conclusion, semblable à TinySec, MiniSec exige une adresse de source de 2 bytes, qui est absente dans un paquet standard de TinyOS. Les frais généraux nets d'un paquet de MiniSec sont augmentation de 3 bytes au-dessus d'un paquet standard de TinyOS [32].

Les champs que la part de MiniSec avec TinyOS original sont :length, Frame Control Field, data sequence number, destination PAN address, destination address, et AM number.

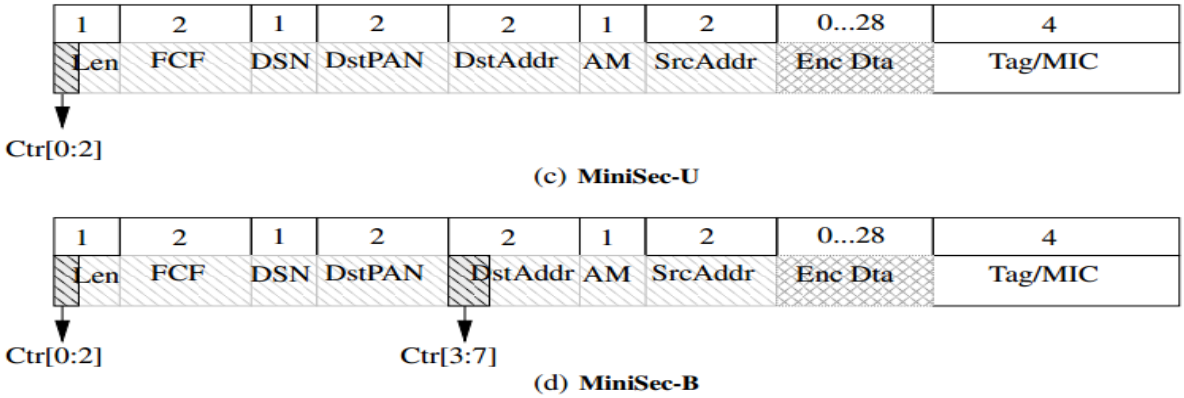


Figure 2.6 Le format de paquet de Minisec

3.6.3 TinyECC [51]

C'est la cryptographie sur les courbes elliptiques, ces dernières peuvent être utilisées pour des opérations asymétriques comme des échanges de clés sur un canal non sécurisé, on parle de ECC (Elliptic Curve Cryptosystem). L'usage des courbes elliptiques en cryptographie a été suggéré, par Neal Koblitz et Victor Miller .

L'avantage d'ECC est l'emploi de clés plus courtes que d'autres méthodes de cryptographique asymétrique telle que RSA, tout en fournissant un niveau équivalent ou plus élevé de sécurité. ECC emploie des points sur une courbe elliptique pour dériver une clé publique de 160 bits qui est équivalente, relativement au niveau de sécurité, à une clé de 1024 bits de l'algorithme RSA [52]. Par conséquent, une plus petite taille de clé permet d'exécuter plus rapidement l'opération de chiffrement (déchiffrement) et exige un besoin moindre en

mémoire. Un inconvénient, cependant, est que l'exécution des opérations de chiffrement (déchiffrement) par ECC prend plus de temps que dans la cryptographie symétrique.

Des résultats [53] prouvent que la cryptographie sur des courbes elliptiques est faisable sur des nœuds avec des ressources limités comparés à celui des crypto systèmes symétriques.

3.6.4 Le Protocole TinyOS BeaconingM [54]

Ce protocole de routage qui est appliqué dans les souterrains de la mine de charbon sur la base du protocole de routage TinyOS Beaconing et de la technologie de l'énergie-conscience. Le protocole amélioré peut répondre aux exigences de collecte de données dans une mine de charbon (TinyOS BeaconingMines).

Ce protocole apporte les modifications suivantes sur la base de TinyOS Beaconing.

1. Le nœud racine ne nécessite pas de diffusion périodique des mis à jour de routage car les nœuds dans le réseau sont statiques.
2. Ajouter le contrôle de couches et de nœuds fils pour éviter le déséquilibre provoqué par les nœuds de l'arbre avec beaucoup de nœuds fils et plusieurs couches.
3. Chaque nœud dans le réseau reçoit son accusé de réception depuis la station de base au lieu de son parent.

3.7 Etude de la tolérance aux pannes dans Tinyos Beaconing (TOSB)

Suite à notre analyse du protocole TOSB de point de vue tolérance aux pannes, nous avons noté un seul mécanisme. En effet, Tinyos Beaconing traite les pannes grâce aux avantages qu'offre cette particularité l'utilisation de la recréation périodique de l'arbre acheminement, c-à-dire d'élimination des capteurs qui tombe en panne

Néanmoins, TOSB souffre de certaines limitations lui empêchant d'avoir une meilleure gestion de pannes. Ces limitations sont les suivantes :

- Détection et recouvrement retardés des pannes.
- Grande perte de données ; due à la détection retardée de la panne et à son recouvrement inefficace.
- Mauvaise gestion de l'énergie ; due au choix empirique des routes et au gaspillage de l'énergie durant l'envoi des données perdues via le chemin défaillant

- Mécanisme d'élimination de panne inefficace ; puisque le chemin défaillant continue à envoyer (et donc perdre) les données malgré le traitement effectué après la détection de la panne.
- Arbre d'cheminement : il existe un chemin unique vers la station de base .c'est à dire si un nœud dans le chemin tombe en panne (épuisement d'énergie par exemple) le message est perdu. implique une grande perte de donnée (Taux de perte augmenter).

3.8 Conclusion

Dans ce chapitre, nous avons présenté le protocole de routage TOSB et nous avons fait une étude sur la tolérance aux pannes dans notre protocole. Notre constat nous a permis d'illustrer les limites de ce protocole. D'où, nous avons pensé à améliorer TOSB qui est un protocole bien réputé mais qui n'est pas tolérant aux pannes. Dans le prochain chapitre nous présentons la solution proposée et son évaluation.

CHAPITRE 4

SOLUTION PROPOSEE : TOLERENT-TOSB

4.1. Introduction

L'objectif principal de ce chapitre est de proposer une solution qui se charge d'améliorer le protocole de routage TOSB de telle sorte qu'il soit tolérant aux pannes. Notre premier but est d'atteindre un niveau de tolérance aux pannes acceptable sans dégrader les performances du réseau. De ce fait, nous avons établi un nouveau protocole appelé T-TOSB (Tolérant-TOSB) qui est en mesure de pallier les limites de TinyOS Beaconing dans un environnement non idéal.

Dans ce chapitre, nous montrons l'apport du protocole T-TOSB par rapport au protocole TOSB en termes de tolérance aux pannes en comparant des métriques de performances via l'implémentation et l'évaluation des deux protocoles. Pour cela, nous commencerons par une étude détaillé de la solution propose, puis nous décrirons la mise en œuvre de l'implémentation de toutes les modèle et les structures de données utilisées. Nous terminerons ce chapitre par une présentation et analyse des résultats de simulations.

4.2. Etude de la solution proposée

L'évaluation du protocole TOSB, nous a permis de déduire que ce protocole n'est pas tolérant aux pannes. Dans cette optique et pour pallier cette limite, nous avons proposé une version améliorée de ce protocole appelée T-TOSB afin de le rendre plus tolérant aux pannes. Notre proposition se base sur les trois règles suivantes :

- Détection instantanée de panne.
- Recouvrement rapide de panne.
- Détention et diminution de l'effet de panne.

Pour se faire, nous définissons de nouveaux paramètres qui associent à chaque nœud.

Nous respectons le fonctionnement de protocole de base « TOSB », en gardant les mêmes étapes avec l'ajout des techniques d'amélioration suivant :

4.2.1 Contrôle de niveau d'énergie :

Un certain niveau d'énergie au niveau de nœud parent p : L'énergie est une ressource critique dans un réseau de capteurs, Pour équilibrer l'usage d'énergie dans un réseau nous divisons l'énergie d'un nœud en trois niveau [07], avec un niveau d'énergie bien déterminé :

1. **Niveau normal :** lorsqu'un nœud capteur possède un niveau d'énergie supérieur au niveau normal, il peut effectuer toutes les opérations de réception et transmission sans se soucier de son niveau d'énergie. Tel que l'énergie de nœuds > Niv_En1, et Niv_En1=10% de l'énergie initial, dans la section 4.5.3 montrer pourquoi utiliser cette valeur.
2. **Niveau moyen :** C'est le deuxième niveau d'énergie. Un nœud qui atteint ce niveau d'énergie, Tel que l'énergie de nœuds <= Niv_En1,ce déclare a ces nœuds fils en leur transmettant un paquet d'alerte du niveau d'énergie (paquet EE_Parent : Epuisement Energie Parent), pour informer les nœuds fils à changer leurs parent comme illustre dans la figure 4.1.Ces derniers (les nœuds fils) peuvent changer leurs parent après la réception de ce paquet, utiliser le deuxième parent s'il existe .sinon lancer un découverte de nouveau parent avec la diffusion de paquet DP (Découverte d'un nouveau parent), comme illustre dans la figure 4.2.

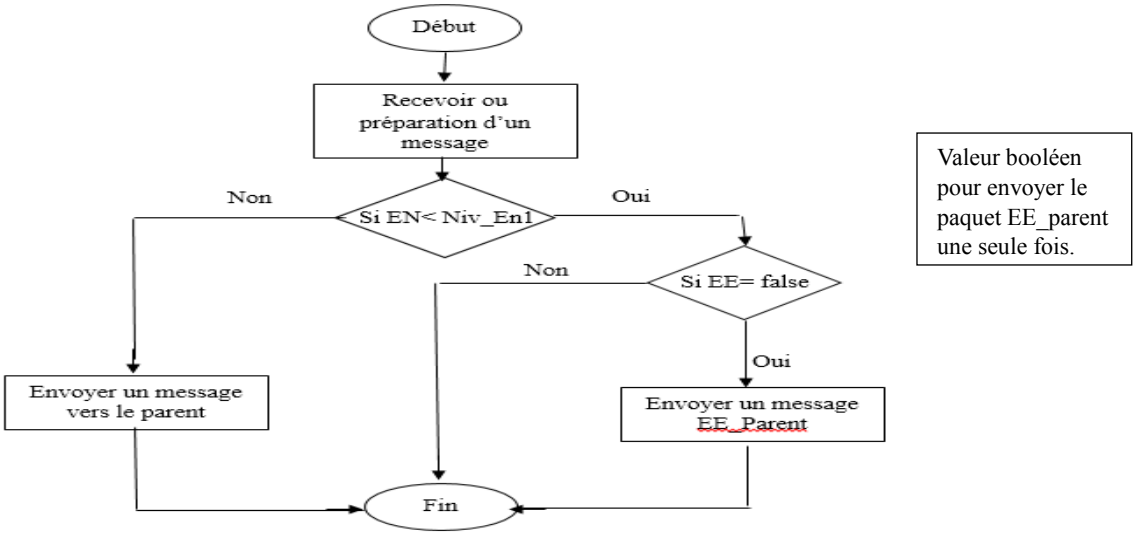


Figure 4.1 Déroulement de message Mesage EE_Parent

3. **Niveau bas :** quand un nœud atteint ce niveau d'énergie il ne peut plus recevoir les paquets, Tel que l'énergie de nœud <= Niv_En2 (Niv_En2=5% de l'énergie initial, aussi dans la section 4.5.3 montrer pourquoi utiliser cette valeur). l'énergie restante lui permettra de transmettre les paquets déjà reçus et les données qu'il va capter jusqu'à l'épuisement de son énergie.

4.2.2 Le routage multi-chemin

Utilise un algorithme préventif pour déterminer plusieurs chemins depuis chaque nœud vers la station de base, Ceci garantit la présence de plus d'un chemin fiable pour la transmission et offre une reprise rapide du transfert en cas de panne sur le chemin principal et choisissant un des chemins qui restent. Pour chaque nœud dans le réseau il y a deux parents. Sauf les nœuds de premier niveau (voisin de la SB, prof =1), possède une seul parent.

1- **Un parent primaire :** définit comme le meilleur chemin vers la station de base (SB) en termes de consommation d'énergie. Utilisé pour transmettre les données vers la station de base.
2- **Un parent secondaire :** définit comme une route réservé, si le premier parent tombe en panne à cause d'épuisement d'énergie, utiliser le parent secondaire (après la réception de paquet EE_Parent) pour transmettre les données vers la station de base, sans envoyer le message DP (Minimiser le trafic et l'énergie).c-à-dire aucun émission ou réception dans l'opération de découverte nouveau parent juste un traitement .

Ce chemin alternatif augmente la fiabilité de transmission de données entre les nœuds source et leurs voisins dans la direction de la station de base qui relaient les paquets envoyés par ces derniers. En outre, les applications de type Event-Driven exigent que les informations recueillies par les capteurs doivent être transmises immédiatement à la station de base

Le niveau de parent secondaire inférieur ou égale à le niveau de parent primaire pour l'évitement de boucle (prof_parent2 <= prof_parent1 et parent (parent1) différent de parent (parent2)).par ce que la communication dans RCSF de type tous vers un (voire la section 1.4.2).

4.2.3 Recouvrement de route

Suite à la réception d'un message EE_Parent, marquer ce parent comme en panne, Si le deuxième parent est vide, lancer la découverte de nouveau parent avec la diffusion de message DP (Decoverte_parent). À la suite après la répondre de nœud voisin choisi le

meilleur route.si ne recevoir aucun nouveau parent il reste router sur l'ancien parent, c'est un technique curative permet de créer un nouveau chemin qui soit le plus fiable pour retransmettre les données, comme illustré dans la figure 4.2

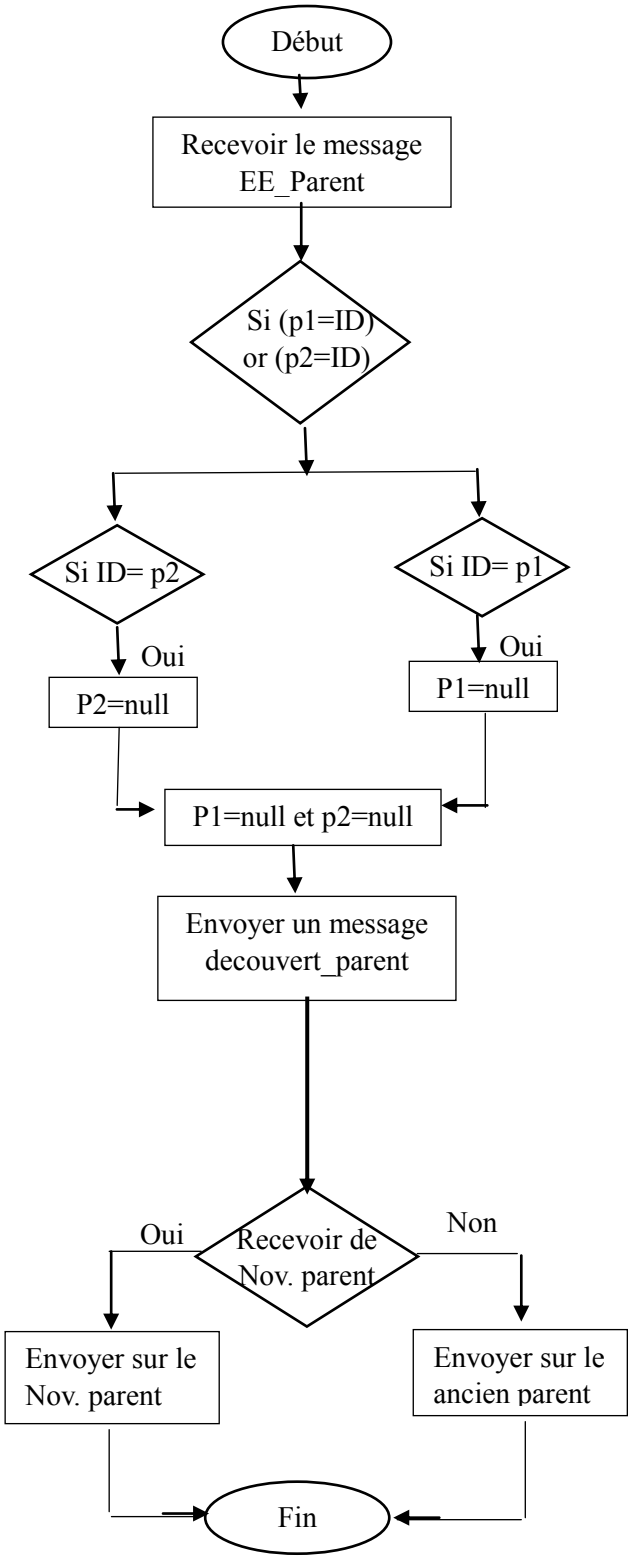


Figure 4.2 Déroulement de la phase de découverte du nouveau parent.

4.3 Choix de l'outil de simulation

Avant sa mise en place, le déploiement d'un RCSF nécessite une phase de simulation afin de s'assurer du bon fonctionnement de tous les protocoles de communication qu'il utilise.

En effet, pour de grands réseaux, le nombre de capteurs peut atteindre plusieurs milliers et entraine donc un coût financier relativement important. Ainsi, il faut réduire au maximum les erreurs de la conception. Malgré cela, il reste des facteurs réels qui ne peuvent être pris en compte par la simulation, tels que les contraintes physiques (perturbations électromagnétiques, inondations, etc.) ou les aléas (détériorations dues à un animal, etc.). Pour arriver à simuler le comportement des capteurs au sein d'un RCSF.

Un bibliothèque puissant a été développée et proposé pour la modélisation des graphes sous le nom de Networkx [67] sous l'interpréteur Python [68]. Le principal but d'utilisation de ce Networkx est de créer une modélisation très proche de ce qui se passe dans les RCSF dans le monde réel. Une économie d'effort et une préservation du matériel sont possibles grâce à cet outil. Cette bibliothèque utiliser dans des nombreux des travaux des recherche comme SEIF [59], HDMRP [60], et [61].

4.4 Paramètre de Simulations

Nous avons simulé le protocole T-TOSB et T-TOSB on utilisant networkx [67], une bibliothèque graphique pour python. dans notre simulation, nous avons simuler les modèles permettant des échanges de paquets et pour la découverte des nœuds voisins et de contrôle (Beacon,…), et des échanges de paquets de données pour la détection des évènements, et la consommation d'énergie, Dans ce qui suit, nous présentons les modèle utiliser pour la simulation .

4.4.1 Modèle d'énergie

Nous avons utilisé le modèle de consommation d'énergie de W. Heinzelman [12] proposent un modèle radio de consommation d'énergie (voir figure 3). Ainsi, Les paramètres d'énergies sont représentés dans le tableau 3. :

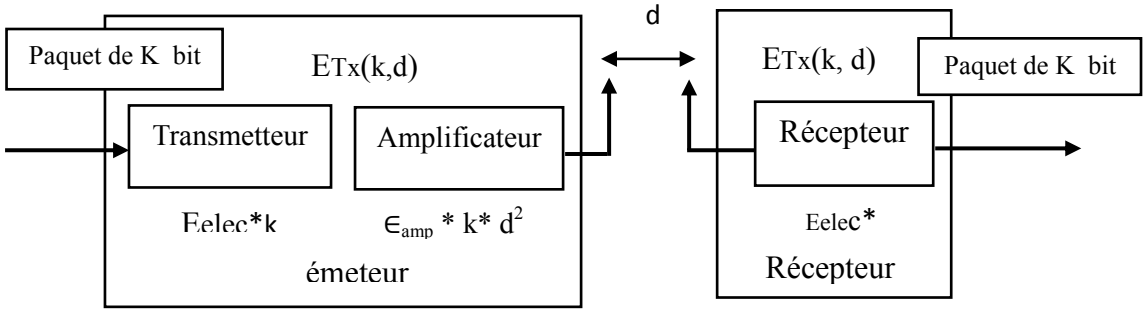


Figure 4.3 Modèle de consommation d'énergie pour la communication

La figure 4.3 Schématise le modèle radio, Pour une transmission d'un message de k-bits sur une distance d, le nœud capteur consomme E_{Tx} (k, d) donné par les formules 1 et 2. Et pour Réception d'un message de k-bits, le nœud capteur consomme $E_{Rx}(k)$ donné par la formule 3.

$$E_{Tx}(k, d) = k * E_{elec} + k \times \varepsilon_{fs} * d^2 \quad d < d_0 \quad (1)$$

$$E_{Tx}(k, d) = k * E_{elec} + k \times \varepsilon_{amp} * d^4 \quad d_0 < d < D_{max} \quad (2)$$

$$E_{Rx}(k) = k * E_{elec} \quad (3)$$

Paramètre	Valeur
E0 : énergie initiale de la batterie	2 joule [39]
Eamp : facteur d'amplification	0.0013e-12 joules/bit/m^4
Eelec : énergie électronique	50e-9 joules/bit
ε_{fs}	10 e-12 joules /bit/m^2

Table 4.1 Paramètres de modèle d'énergie.

L'énergie restante Er des nœuds capteurs est exprimée par la différence entre l'énergie initiale et l'énergie consommée par le capteur. Initialement, elle contient E0, et au cours de la simulation elle est mise à jour par l'affectation suivante :

Er= Er - Ex tel que : { Si émission alors Ex = l'énergie consommée lors de l'émission.
Sinon si réception alors Ex = l'énergie consommée lors de la réception.

4.4.2 Modèle taille des paquets

La taille des paquets que nous avons utilisés est représentée dans le tableau 3.4.

Paramètre	Valeur
Donnée	40-240 bit
Beacon de TOSB	40 bit
Beacon de T-TOSB (+prof, Niveau Energie)	56 bit
EE_Parent (ID de parent)	40 bit
DP (Découverte_parent, ID de parent)	40 bit
Rep_DP réponse DP(ID_Decoverte, ID_SRC ,Prof, Energie)	64 bit

Table 4.2 Taille des paquets.

4.4.3 Déploiement de capteur

Néanmoins, un déploiement aléatoire peut être obtenu à partir d'une distribution de capteurs à des individus. Dans ce travail, nous supposerons des réseaux déployés aléatoirement uniforme. Sur une surface rectangulaire de dimensions (700x500) M^2, et la station de base se trouve à au milieu (350,250). La portée de communication est fixée à 90 m. Nous avons réalisé les simulations avec un nombre de 80 nœuds ou avec une liste de taille de nœuds différent 60, 80, 100 120,140, à 160.

Un lien existe entre deux nœuds si leur distance est inférieure ou égale à la zone de couverture radio qui est un paramètre de l'algorithme de génération de topologie. Ce type de topologie est communément utilisé pour simuler Les RCSF .Une fois disséminés, il est couramment admis que les capteurs sont statiques.

Modèle	**Paramètre**	**Valeur**
Consommation d'énergie	E0 : énergie initiale de la batterie	2 joules [39]
	Eelec : énergie électronique	50e-9 joules/bit [12]
	ε_{fs}	10 e-12 joules /bit/m^2 [12]
Taille de paquet	Donnée	62-240 bit
	Beacon de TOSB, EE_Parent , DP	40 bit
	Beacon de T-TOSB	56 bit
	Rep_DP (réponse DP)	64 bit
Déploiement	Surface	700 m x 500 m [39]
	La portée Maximale	90 m
	Nombre des nœuds	80 ou (60, 80,100, 120,140 et 160)

Table 4.3 Paramètres du contexte de la simulation.

4.5 Evaluation de performances

Pour évaluer les performances T-TOSB, nous avons procédé à le comparer au protocole de routage TOSB. Pour cela, nous avons effectué des simulations avec les mêmes paramètres et métriques pour les deux protocoles, Par la suite, nous simulons la panne des nœuds avec cause d'épuisement d'énergie, dans le but de vérifier son effet pour les deux protocoles. Dans cette partie, nous évaluons d'abord des métriques différents et nous les comparons pour les deux protocoles TOSB et T- TOSB.

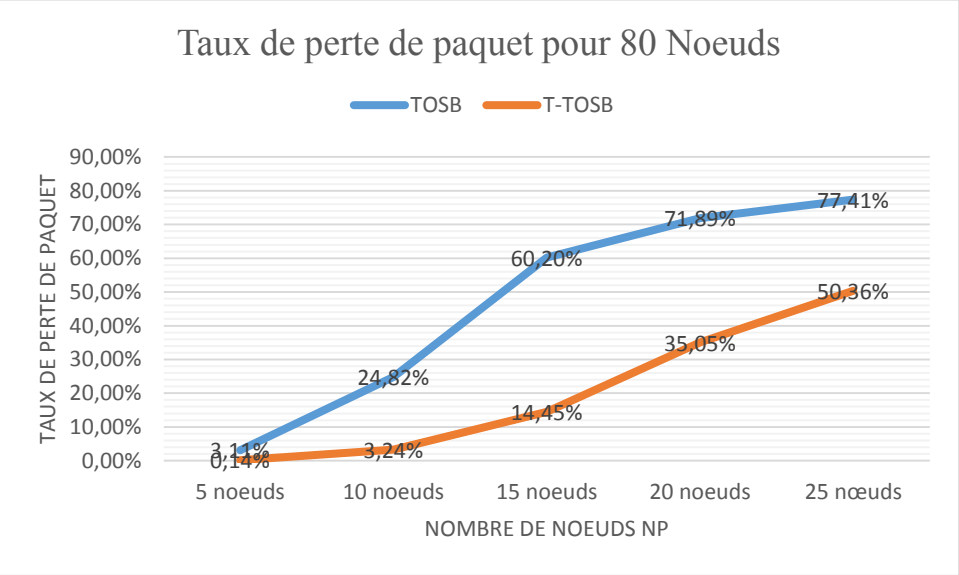
4.5.1 Taux de perte de paquets

Le choix de cette métrique, comme étant un critère de performance, revient à sa nécessité dans certaines applications où les données échangées sont très critiques. Pour la mesurer, nous calculons la moyenne des taux de perte de paquets entre le nœud de détection et la station de base. Ainsi, le protocole T- TOSB ne doit pas mener à une forte perte de paquets de données par rapport à TOSB. De plus, nous vérifions, pour les deux protocoles, l'effet de la panne des nœuds sur l'augmentation de nombre de paquets de données perdus.

Pour tester le taux de pertes de paquets, il est nécessaire de calculer le ratio des paquets perdus et des paquets envoyés.

Dans le premier cas on a fixé le nombre des nœuds mais on a varié le nombre de nœud tombe en panne NP (NP : Nœud en Panne) ,5 jusqu'à 25 nœuds choisir aléatoirement.

- Pour 80 nœuds avec les nœuds NP, Le taux de perte est présenté dans la figure suivante. On a fait le test avec plusieurs façons (1000 fois) pour bien présenter le taux.



de perte des paquets.

Figure 4.4 Taux de pertes de paquets pour 80 nœuds

Comme illustre la figure 4.4, nous remarquons que le taux de perte des paquets dans TOSB augmente plus que dans T-TOSB à chaque fois qu'on augmente le nombre des nœuds NP.

Dans le deuxième cas on utilise une liste de nœuds de taille variable avec 20% comme nœuds NP (NP : Nœud en Panne), la figure 4.5 montre le résultat relevé après plusieurs simulations (100 fois) dans le but de bien présenter le taux de perte des paquets.

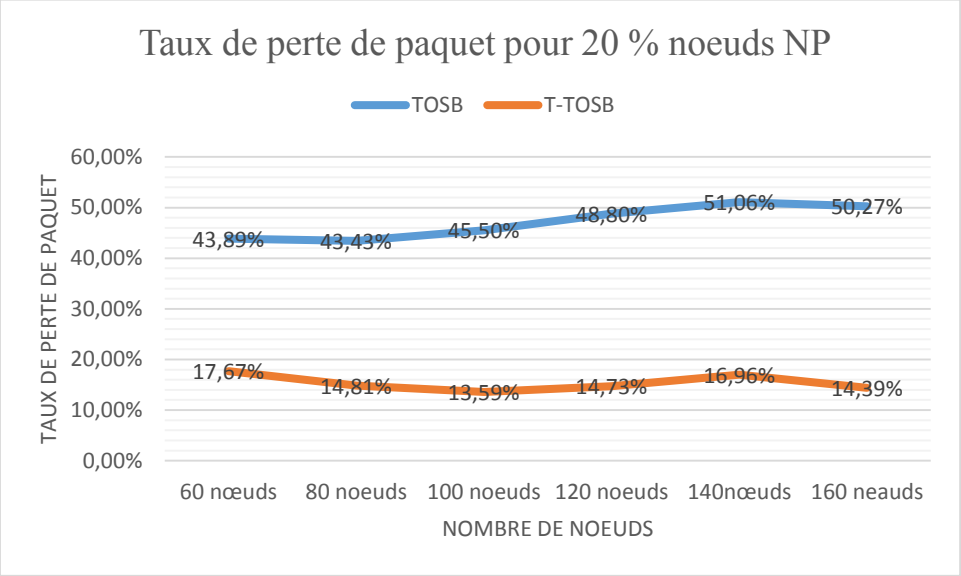


Figure 4.5 Taux de pertes de paquets (20% nœuds NP).

Comme le montre la figure 4.5, Le taux de perte dans la version améliorée T-TOSB est bien plus inferieur que celui-ci du protocole de base avec une amélioration d'environ 30%.car les deuxième parent ou les nouvelle parents (après l'opération de découverte :DP) prennent la responsabilité de faire passer les données à la station de base. C-à-dire réduire le taux de perte. Ainsi le mécanisme de gestion d'énergie pour équilibrer la charge entre les nœuds.

4.5.2 Consommation énergétique

Nous nous sommes intéressés essentiellement à la consommation d'énergie des nœuds puisqu'elle constitue un paramètre primordial pour la détermination de la durée de vie d'un RCSF. Nous analysons donc l'impact de mécanismes de tolérance aux pannes intégrés dans le protocole T-TOSB sur l'énergie consommée par rapport au protocole TOSB.

Pour ce faire, nous prenons comme critère, l'énergie moyenne consommée par nombre de nœuds du réseau, après N*100 détection, tel que N est le nombre de nœuds (utiliser pour équilibrer entre le nombre de nœuds et le nombre de détection).

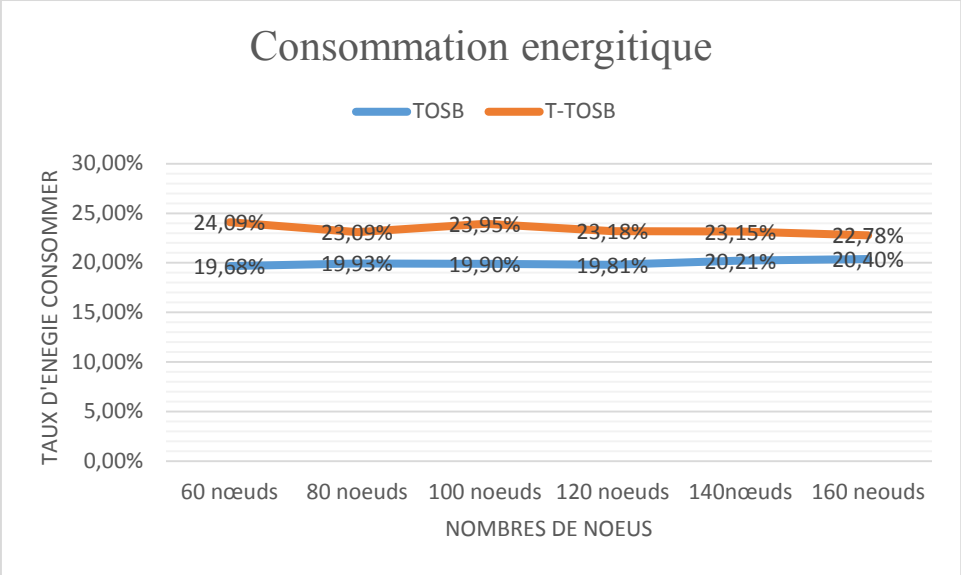


Figure 4.6 Variation de consommation d'énergie au nombre de nœuds.

Comme l'illustre la figure 4.6, nous remarquons que la moyenne d'énergie consommée dans le réseau est indépendante du nombre de nœuds déployés à cause de la topologie hiérarchique du protocole TOSB qui le rend très scalable. En effet, quand la taille du réseau augmente, le nombre de nœud parent augmente. Ainsi, TOSB maintient la consommation d'énergie des nœuds quel que soit la taille du réseau.

Par ailleurs, nous constatons un taux de 4% (au pire de cas ,120 nœuds) d'énergie supplémentaire dissipée pour notre protocole T-TOSB par rapport au protocole T-TOSB. Cela revient à l'augmentation du nombre de messages de contrôle par les mécanismes de tolérance aux pannes. (EE_Parent, DP,…), Ainsi, Les message de donnée transmis vers la station de base par ce que T-TOSB réduire le taux de perte implique l'augmentation d'énergie consommer.

4.5.3 Le temps moyen avant la défaillance (MTTF) :

Il représente une mesure importante pour évaluer la contribution d'une solution pour améliorer la durée de vie du réseau. Elle est définie comme la durée moyenne de temps pendant lequel un système est considérée comme fonctionnel et peut fournir des données détectées à la station de base [59].

L'application de cette définition, nous avons considéré qu'une topologie de routage n'est pas fonctionnelle lorsque certains capteurs deviennent incapables d'atteindre à la station de base.

Pour tester le MTTF, il est nécessaire de calculer le ratio des paquets envoyés avant que le premier nœud devient incapable d'atteindre la station de base. La figure 4.7 représente les résultats de comparaison de MTTF dans le protocole TOSB et T-TOSB. Pour test on a fait plusieurs simulations (100 fois) afin de bien présenter le MTTF.

Dans le premier cas on a fixé le niveau d'énergie 1(Niv_En1) à 10% de l'énergie initial, et le niveau d'énergie 2(Niv_En2) à 5% de l'énergie initial, pour le protocole améliorée T-TOSB.

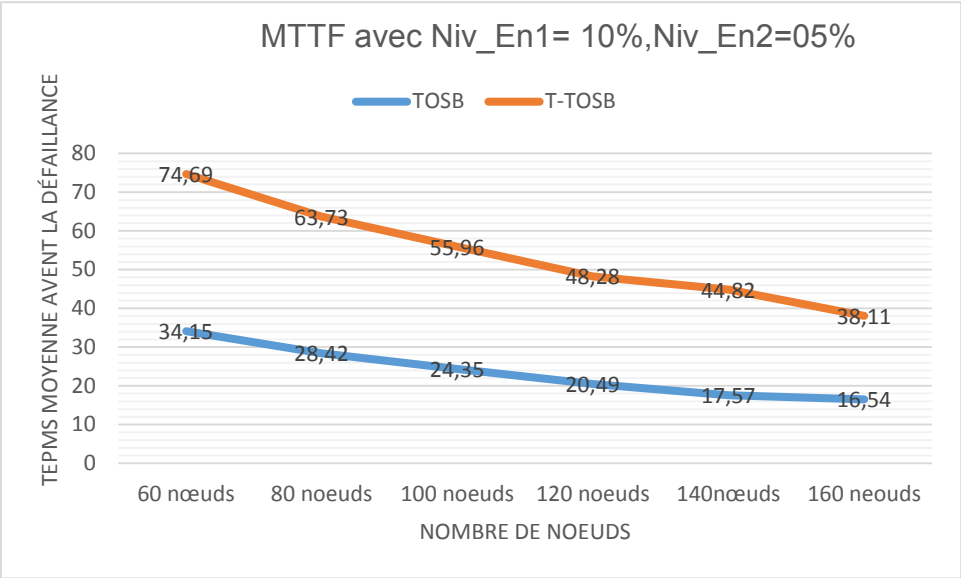


Figure 4.7 Variation de l'MTTF au nombre de nœuds.

Comme l'illustre le résultat de la figure 4.7 Nous remarquons que le temps moyen avant la première défaillance dans le protocole T-OSB est bien plus supérieur que le temps moyen pour le protocole TOSB. Il varie entre 16,68% jusqu'à 61.5% selon le nombre de nœuds déployés ; à chaque fois que le nombre de ces derniers augmente, Le MTTF décroissant. De plus, nous pouvons bien distinguer que le MTTF est plus élevé, approximativement de 30%, dans T-TOSB que dans TOSB. Cette différence revient aux mécanismes adoptés de tolérance aux pannes.

Pour assurer un meilleur choix de niveau d'énergie pour le protocole amélioré T-TOSB tel que utiliser les même niveau d'énergie de premier cas (le niveau d'énergie 1(Niv_En1) à 10% de l'énergie initial, mais le niveau d'énergie 2(Niv_En2) à 5% de l'énergie initial), il faut étudier le protocole en variant les niveaux d'énergies selon le tableau 4.4 suivant :

Niveau d'énergie 1 (Niv_En1)	2%	5%	10%	15%	20%	25%
Niveau d'énergie 2 (Niv_En2)	1%	2%	5%	8%	10%	12%

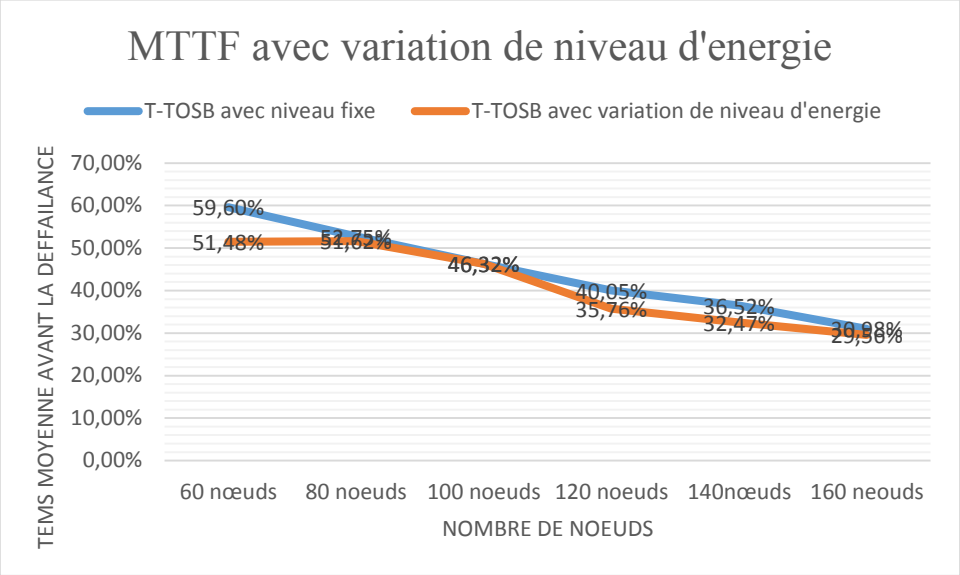


Table 4.4 Variation de niveau d'énergie

Figure 4.8 MTTF avec variation de niveau d'énergie.

Comme l'illustre le résultat de la figure 4.8, nous remarquons que temps moyen avant la première défaillance pour les deux protocoles décroisse avec l'augmentation des nœuds dans le réseau commençant par 60% en décroissant jusqu'à environ 30%. A partir du résultat la valeur de niveau d'énergie optimal est (Niv_En1=20%, Niv_En2=10%). De plus, nous pouvons bien distinguer que le MTTF est plus élevé, approximativement de 7%, dans T-TOSB avec niveau d'énergie variant que dans T-TOSB avec niveau d'énergie fixé dans (Niv_En1=20%, Niv_En2=10%). Cette différence se situe qu'au les niveaux d'énergie suivant (Niv_En1=5%, Niv_En2=2%) ne sont pas tolérables aux pannes par ce que l'énergie restant ne pas satisfaire pour assurer vivre longtemps.

4.5.4 Temps de convergence

Temps nécessaire pour la création de la topologie.

La figure 4.9 représente les résultats de comparaison de temps de convergence dans le protocole TOSB et T-TOSB.

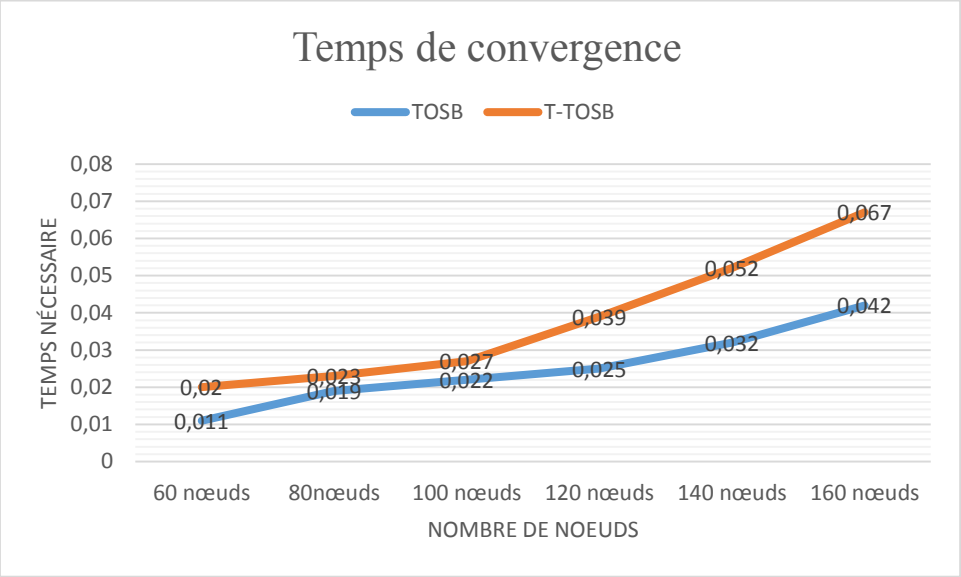


Figure 4.9 Temps de convergence

Comme l'illustre le résultat de la figure 4.9, nous remarquons que le temps de convergence varie entre 0.01 ns et 0.07 ns selon le nombre de nœuds déployés ; à chaque fois que le nombre de ces derniers augmente, le temps de convergence augmente. De plus, nous pouvons bien comprendre que le temps de convergence nécessaire est plus élevé approximativement de 0.02 ns, dans T-TOSB que dans TOSB. Cette différence revient à l'augmentation du nombre des massages reçus presque jusqu'à 2 fois pour affecter le deuxième parent dans T-TOSB ainsi qu'à la classification des parents (parent1 s'il dispose du meilleur chemin en terme d'énergie nécessaire pour atteindre la station de base que le parent2).

4.6 Conclusion

Dans ce chapitre, pour pallier les limite de TOSB, nous avons proposé une version améliorée de ce protocole appelée T-TOSB de telle sorte qu'il soit tolérant aux pannes d'épuisement d'énergie. Nous avons présenté une étude de la solution proposée, et l'environnement pour simuler et évaluer le protocole TOSB. Dans cet environnement, nous avons utilisé Networkx qui est une bibliothèque légère dédiée pour la manipulation des graphes.

Les résultats de simulation ont montré de meilleurs résultats concernant le taux de perte de paquets pour T-TOSB avec une amélioration évidente jusqu'à 40% par rapport au protocole TOSB et sans dégrader les performances du réseau (consommation d'énergie, durée de vie…).

CONCLUSION GENERALE

Les réseaux de capteurs sont composés d'un très grand nombre de dispositifs de communication ultra petits, autonomes avec des ressources de calcul et d'énergie limitées. Ils sont actuellement considérés comme l'une des technologies qui bouleverse notre façon de vivre, grâce à leur utilisation dans différents domaines d'application.

Cependant, les réseaux de capteurs sans fil rencontrent plusieurs problèmes qui affectent leur bon fonctionnement dû à leurs caractéristiques ; tels que la limitation de batterie, le type de communication, les environnements hostiles où sont déployés les capteurs. Par ailleurs, ces réseaux sont caractérisés par les pannes des nœuds qui peuvent causer un dysfonctionnement du réseau. Dans cette optique, il est commode de proposer des protocoles de routage tolérants aux pannes.

Une panne au niveau d'un capteur peut se produire à cause d'une perte de connexions sans fil due à l'extinction du capteur suite à l'épuisement de sa batterie, par conséquence, il faut faire face à cette panne en proposant un protocole tolérant aux pannes.

Dans ce mémoire, nous avons réalisé une étude pour atteindre un routage efficace avec tolérance aux pannes dans les réseaux de capteurs sans fil. Cet aspect est fondamental pour ce genre de réseau où le routage se réalise en collaboration avec les différents nœuds du réseau. De ce fait, un protocole de routage doit prendre en compte les contraintes matérielles d'un capteur : une batterie faible, une capacité de stockage modeste, une bande passante faible, etc.

En effet, nous avons implémenté le protocole T-TOSB et nous l'avons comparé avec le protocole TOSB. Les résultats de simulation ont été concluants : les performances du réseau avec une réduction de la perte de paquets transitant dans le réseau, et n'ont pas été dégradées après l'amélioration concernant la consommation d'énergie. De plus, le protocole T-TOSB est en mesure de pallier à la panne d'épuisement d'énergie visant le protocole TOSB.

Enfin, comme perspectives nous envisageons d'étudier les points suivants :

- Développer des mécanismes de tolérance aux pannes plus élaborés pour prendre en charge les autres types de pannes comme destruction physique d'un nœud, panne de module radio.
- La sécurité et l'agrégation de données pour T-TOSB
- Implémenter notre protocole T-TOSB sur des capteurs réels.

REFERENCES BIBLIOGRAPHIQUE

[01] Y. Yasser, « Routage pour la Gestion de l'Energie dans les Réseaux de Capteurs Sans Fil », Thèse de Doctorat, Université de Haute Alsace, juillet 2010.

[02]I. Akyildiz, W. Su, E. Cayirci, Y. Sankarasubramaniam. « A survey on sensor networks » , IEEE Communications Magazine, vol. 40, no. 8, pp. 102-114, Georgia Institute of Technology, Atlanta, USA. Août 2002.

[03] A. Delye, V. Gauthier, M. Marot, and M. Becker. «Etat de l'art sur les réseaux de capteurs ». Rapport de Recherche INT N-05001RST GET-INT, UMR5157 SAMOVAR.

[04] B. Khalifa. "La sécurité dans les réseaux de capteurs sans fil", conférence à l'université de Bechar. Printemps 2006.

[05] TinyOS small :http://www.tinyosmall.com/product_p, consulté le : 21-04-2013

[06] B. Kechar, « Problématique de la consommation de l'énergie dans les réseaux de capteurs sans fil », Séminaire LIUPPA, Université de Pau et des Pays de l'Adour, 14 Octobre 2007.

[07]Y. Younes «Minimisation d'énergie dans les réseaux de capteur » Mémoire de magistère, Université de UMTOO, tiziouzou, Algérie, 26 Décembre 2012.

[08]K. Holger and Andreas Willig. "Protocols and Architectures for Wireless Sensor Networks".Wiley, 2005.

[09] R. KACIMI. « Techniques de conservation d'énergie pour les réseaux de capteurs sans fil », Thèse de Doctorat, université de Toulouse décembre 2009.

[10] Kamal BEYDOUN, «Conception d'un protocole de routage hiérarchique pour les réseaux de capteurs». Thèse de Doctorat, décembre 2009.

[11] M .Messai, « Sécurité dans les Réseaux de Capteurs Sans-Fil», Mémoire de magistère, Universitéde Béjaia,2008.

[12]W. Heinzelman, A. Chandrakasan, H. Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Micro sensor Networks", In proc of the Hawaii International Conférence on Systems Science, vol. 8, pp. 8020, January 2000.

[13]D.Boubiche, «Protocole de routage pour les réseaux de capteurs sans fil», Mémoire de magistère, Université de l'Hadj Lakhdar, Batna, Algérie, 2008

[15]CrossBow. Sensor Boards, https://www.xbow.com/Products/productdetails.aspx?sid=158. Consulté le : 10/04/2013

[16]T. Lemlouma, « Le routage dans les réseaux mobiles Ad Hoc », Mini projet, Institut National de Recherche en Informatique et Automatique INRIA, 2000.

[17]D. Culler, D. Estrin, et M. Srivastava. Guest editors "introduction :Overview of sensor networks. Computer", 37(8) :41-49, August 2004. 5, 6, Institut National des Télécommunications, Evry, France, 2005.

[18] L .ZIANE KHODJA, « La structuration et la sécurisation des réseaux de capteurs » , Master 2 Recherche Informatique, IFSIC ,2009.

[19]A. PERRIG, J. STANKOVIC, D. WAGNER: «Security in Wireless Sensor Networks», In Communications of the ACM, 2004, Vol. 47, No. 6.

[20]M. SAXENA: «Security in Wireless Sensor Networks: A Layer based Classification», Purdue University, 2007.

[21]Andreas A. Strikos. "A full approach for Intrusion Detection in Wireless SensorNetworks". School of Information and Communication Technology KTH Stockholm, Sweden 16453 March 1, 2007.

[22] W. Znaidi,M. Menier, J.Babau. "An Ontology for Attacks in Wireless Sensor Networks". INSTITU NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE N° 6704 Octobre 2008.

[23] B.Kaci. « Détection d'intrusion dans les réseaux de capteurs sans fils », Master Recherche 2, IFSIC-Rennes 1 ,2009/2010.

[24] Y.Khalfaoui ,«Routage dans les réseaux de capteur sans fils», Projet de fin d'étude, Centre universitaire Mustapha Stambouli, Mascara, 2006.

[25] G.L. Aceves, S.Roy, « Node-Centric Hybrid Routing for Ad Hoc Networks», mobiwac, International Mobility and Wireless Access Workshop (MobiWac'02), Page(s): 63-63, University of California at Santa Cruz, 2002.

[26] L. Khelladi, N.Badache, « Improving Directed Diffusion With Power-Aware Topology Control For Adaptation to High Density », LOCALGOS'08 workshop, in conjunction with The 4th IEEE/ACM International Conference on Distributed Computing In Sensor SystemS (DCOSS 2008), Algeria, 2008.

[27] A. Bouabdallah, H. Betthahar, Y.Challal, «Les Réseaux de capteurs (WSN: Wireless Sensor Networks)», Cours, Université de Technologie de Compiègne, France, 2008.

[28] A.Makhoul, A.Mostefaoui, J.Bahi, « A Mobile Beacon Based Approach for Sensor Network Localization », Third IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, Page(s): 44 – 44, Washington DC, USA, 2007.

[29] C.Richard, H. Snoussi, M.Essoloh, « Localisation distribuée dans les réseaux de capteurs sans fil par résolution d'un problème quadratique », Revue, éditée par : GRETSI, Groupe d'Etudes du Traitement du Signal et des Images, Université de Technologie de Troyes, Septembre 2007.

[30] I.Mahgoub, M.Ilyas, « Sensor Network Protocol», Hardcover Book, ISBN: 0849370361, Number of pages: 248, USA, 27 Janvier 2006.

[31] Eya Dhib, « Routage avec QoS temps réel dans les réseaux de capteurs », Projet fin d'étude ingénierie de réseaux, Ecole Supérieure des Communications de Tunis, 2007.

[32] A.Kamal, J.Al-Karaki, « Routing Techniques in Wireless Sensor Networks: A Survey», IEEE Wireless communications, Page (s): 6-28, Iowa State University, USA, 2004.

[33] Y.Romdhane, « Evaluation des performances des protocoles S-MAC et Directed Diffusion dans les réseaux de capteurs», Projet de fin d'études, Ecole Supérieure des Communications de Tunis (Sup'Com), 2006 / 2007.

[34] V.Felea, « Routage dans les réseaux de capteurs sans fil »,Journées ResCom Strasbourg, Université de franche comté, 9-10 Octobre 2008.

[35]Y.Challal,« Réseaux de Capteurs Sans Fils »,Cours, Systèmes Intelligents pour le Transport, Université de Technologie de Compiègne, France, 17 Novembre 2008.

[36] S.Fdida, Y.Barouni, « Modèle générique pour le routage orienté contenu », Document scientifique, hal-00260342, Laboratoire d'informatique de Paris 6, Université Pierre et Marie Curie, Mars 2008.

[37] L.Khelladi, N.Badache « Les réseaux de capteurs: état de l'art », Rapport de recherche, Algérie, Février 2004.

[38]H.Hadjammar, N.Doufene,« Routage dans les réseaux de capteurs : optimisation du protocole Directed Diffusion», Projet de fin d'étude, Institut National de formation en Informatique INI, Algérie, 2006.

[39] M.L.MESSAI, « Gestion d'un Parking par un Réseau de Capteurs Sans Fils», UAMB, Ecole Doctorale en informatique ReSyD Bejaia 2010.

[40]F.Z.Benhamida, « La tolérance aux pannes dans les réseaux de capteurs sans fil », Rapport du mini projet, Institut National de Formation en Informatique INI, Algérie, 2006/2007.

[41] G.CHALHOUB, « Les réseaux de capteurs sans fil », Complexe scientifique des Cézeaux, France,2010.

[42]M.Badnet, N.Belloir «Réseaux de capteurs : Mise en place d'une plateforme de test et d'expérimentation », Master Technologie de l'Internet 1ère année, France, 2005/2006

[43] S.Tixier, « TinyOS », Mini rapport, LIF12, Université Lyon 1, 6 Décembre 2007.

[44]Le site officielle de Tinyos : www.tinyos.net, consulté le : 16-05-2013.

[45] R. Kacimi , « Premiers pas avec TinyOS », Cours Télécommunications et Réseaux ,ENSEEIHT , 3ème année 2010-2011.

[46]P. Levis, S. Madden, J. Polastre, R. Szewczyk, K. White-house, A. Woo, D. Gay, J. Hill, M. Welsh, E. Brewer, andD. Culler." TinyOS: An operating system for wireless sensor networks. In W. Weber, J. Rabaey, and E. Aarts, editors,Ambient Intelligence. Springer-Verlag, New York, NY, 2004.

[47] J.Hill, R.Szewczyk, A.Woo, S.Hollar, D.Culler, K.Pister "System Architecture Directions for Networked Sensors" Department of Electrical Engineering and Computer Sciences University of California, Berkeley Berkeley, CA 2000

[48] F. Hu and N. K. Sharma. "Security considerations in ad hoc sensor networks". Ad Hoc Networks 3, Elsevier Science, pp. 69–89, 2005.

[49]C. Karlof, N. Sastry, and D. Wanger. "TinySec: A Link Layer Security Architecture for Wireless Sensor Networks". Proceeding 2nd ACM Conference on Embdded Networked

Sensor Systems (SenSys 2004), Baltimore, Maryland, Etats-Unis, pp. 162-175, november 2004.

[50]M.Luk, G.Mezzour, A.Perrig, V.Gligor « MiniSec: A Secure Sensor Network Communication Architecture »,IPSN'07, April 25-27, 2007, Cambridge, Massachusetts, USA

[51] P. Ning and A. Liu. "TinyECC: Elliptic Curve Cryptography for Sensor Networks". 2007, available on: http://discovery.csc.ncsu.edu/software/TinyECC/

[52]A. S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz. "Energy analysis of public-key cryptography for wireless sensor networks". Pervasive Computing and Communications, IEEE International Conference, pp. 324-328, on 8-12 March 2005.

[53]J. Grobschadl. "TinySec: A Security Architecture for Wireless Sensor Networks (Extended Abstract)". CoNEXT'06, Lisbon ACM, December 2006.

[54] Z.Sun, X.Zhang, Hui Li., and Anqi Li, «The Application of TinyOS Beaconing WSN Routing Protocol in Mine Safety Monitoring », IEEE ,2008, China.

[55] C. Karlof and D. Wagner. "Secure routing in wireless sensor networks: Attacks and countermeasures". In IEEE International Workshop on Sensor Network Protocols and Applications, pages 113–127, February 2003.

[56] D.MARTINS, H.GUYENNET ," Etat de l'art Sécurité dans les réseaux de capteurs sans fil" .SAR-SSI 2008 : 3rd conférence on Security of Network Architectures and Information Systems, France (2008).

[57] K.Saghar, W.Henderson and D.Kendall , "Formal modelling and analysis of routing protocol security in wireless sensor networks". PGNet, 2009 .

[58]J.Lopez ,J. Zhou "Wireless Sensor Networks Security Javier Lopez" ,Cryptology and information security series, CISS , page1702008.

[59] A Ouadjaout, Y.Challal, N.Lasla, M. Bagaa, "SEIF: Secure and Efficient Intrusion-Fault tolerant routing protocol for wireless sensor networks ", IEEE International Conference on Availability, Reliability and Security, Spain (2008)

[60] A. HADJIDJ , A. Bouabdallah , Y. Challal " HDMRP: An Efficient Fault-Tolerant Multipath Routing Protocol for Heterogeneous Wireless Sensor Networks",Spring 74, 2012, pp 469-482

[61] Y. Challal, A. Ouadjaout, N. Lasla, M. Bagaa, A. Hadjidj “Secure and efficient disjoint multipath construction for fault tolerant routing in wireless sensor networks” Journal of Network and Computer Applications 34 (2011) 1380–1397.

[62] B. Selic. "Fault tolerance techniques for distributed systems". www.ibm.com/developerworks/rational/library/114.html, 2013.

[63] Ajay, N.Tarasia, S. Dash, S.Ray, ARSwain "Une erreur dynamique tolérant protocole de routage pour prolonger la durée de vie des réseaux de capteurs sans fil» (IJCSIT),International Journal of Computer Science et Technologies de l'Information, Vol. 2 (2),2011, 727-734.

[64] Guowei Wu, ChiLin, Feng Xia, Lin Yao, il Zhanget Liu Bing «Saut dynamique en temps réel Fault-Tolerant protocole de routage pour les réseaux de capteurs sans fil» de la Fondation nationale des sciences naturelles de Chine par la concession numéro 60703101 et n ° 60903153 (2010).

[65] Z Che-Aron, W.Al-Khateeb, et F.Anwar «Le Renforcement de tolérance de panne Mécanisme de protocole de routage AODV pour le réseau de capteurs sans fil» ,IJCSNS International Journal of Computer Science et de sécurité réseau, Vol.10 No.6, Juin 2010.

[66] F. Z Benhamida, Y. Challal «FaT2D: Fault Tolerant Diffusion Réalisé pour les réseaux de capteurs sans fil »,2010 de la Conférence internationale sur la disponibilité, la fiabilité et la Security 2010 IEEE DOI 10.1109/ARES.2010.35 112.

[67] Le site officielle de la biblithéque Networkx : https://networkx.lanl.gov/hg/networkx consulte le :04-04-2013

[68] Le site officielle de python : www.python.org , consulte le : 24-03-2013.

ملخص : ان شبكة الاستشعار اللاسلكية (WSN) هي عبارة عن مجموعة من العقد التي تتواصل عن طريق وصلات لاسلكية لمراقبة ظاهرة معينة. نظرا للقيود الخاصة بـ (WSN) .فإنها تتطلب تنفيذ بروتوكولات توجيه جديدة، كما أن هذه البروتوكولات تتطلب على وجه الخصوص دمج تقنيات التعايش مع الأخطاء.

في عملنا هذا نقترح حلا يخص التعايش مع الأخطاء على مستوى بروتوكول TinyOS Beaconing ، لهذا اقترحنا تقنية جديدة تمسى بـ T-TOSB، الحل المقترح يتمثل في الكشف عن خطأ نضوب الطاقة ومعالجته لضمان أحسن معدلات ضياع حزم المعلومات. كما أظهرت نتائج المحاكاة نجا عة التحسينات في T-TOSB من حيث معدلات الحزم الضائعة حيث يقدر الفارق بحوالي 40 % .وهذا من دون التأثير على أداء الشبكة (استهلاك الطاقة ، مدة حياة...).

الكلمات المفتاحية : WSN، TOSB T-TOSB، التعايش مع الخطأ ، نضوب الطاقة.

Abstract: A wireless sensor network (WSN), is a set of nodes communicating by wireless links to observe a given phenomenon. Given their specific constraints, WSN require the implementation of new routing protocols. In particular, these protocols must be fault-tolerant.

In this paper, we propose a fault-tolerant solution for TinyOS beaconing protocol (TOSB). Our solution called Tolerant-TOSB, offers a curative solution fault detection and recovery of energy depletion. Concerning the packet loss rates, the simulation results show a real improvement of about 40% compared to the basic TOSB protocol, and without degradation of performance (energy consumption, lifetime …).

Keywords: WSN, TOSB T-TOSB, fault tolerance, energy depletion.

Résumé : Un réseau de capteurs sans fil (RCSF) est un ensemble de nœuds communicants par des liaisons sans fil pour observer un phénomène donné. Vu leurs contraintes particulières, les RCSF demandent la mise en œuvre de nouveaux protocoles de routage. Plus particulièrement, ces protocoles nécessitent l'intégration de techniques tolérantes aux pannes.

Dans ce mémoire, nous proposons une solution tolérante aux pannes pour le protocole TinyOS Beaconing (TOSB). Notre nouvelle technique appelée : Tolérant–TOSB, offre une solution curative de détection et recouvrement de pannes d'épuisement d'énergie. Concernant le taux de perte de paquets, les résultats de simulation ont montré que le protocole amélioré apporte une amélioration évidente d'environ 40% par rapport au protocole TOSB et sans dégrader les performances du réseau (consommation d'énergie, durée de vie…).

Mots clés : RCSF, TOSB, T-TOSB, tolérance aux pannes, épuisement d'énergie.