RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITÉ MOULOUD MAMMERI DE TIZI-OUZOU
FACULTÉ DE GÉNIE ÉLECTRIQUE ET INFORMATIQUE
DEPARTEMENT INFORMATIQUE

MEMOIRE DE MASTER

Pour l'obtention du diplôme de Master en Informatique
Spécialité systèmes informatiques

TITRE

MODELE DE CONFIANCE POUR SECURISER LE ROUTAGE DANS LES RESEAUX DE CAPTEURS SANS-FIL

Réalisé par

Lynda TLILI

Directeur du mémoire

Mehammed DAOUI

Année universitaire 2010/2011

MEMOIRE DE MASTER

Pour l'obtention du diplôme de Master en Informatique
Spécialité systèmes informatiques

MODELE DE CONFIANCE POUR SECURISER LE ROUTAGE DANS LES RESEAUX DE CAPTEURS SANS-FIL

Réalisé par

Lynda TLILI

Directeur du mémoire

Mehammed DAOUI

Remerciements

Mes premiers remerciements et ma grande gratitude s'expriment envers le Dr Mehammed DAOUI, mon directeur de projet. Ses conseils et ses encouragements ont permis à ce travail d'aboutir. Ses capacités scientifiques et ses compétences étaient mon grand support. La liberté qu'il m'a accordée et les responsabilités qu'il m'a confiées ont beaucoup contribué à ma formation et à mon autonomie de travail. Ses lectures attentives, ses critiques et suggestions ont été d'une précieuse aide pour la réalisation de ce travail de recherche.

Je le remercie chaleureusement pour sa pédagogie, sa patience, sa disponibilité et son dévouement. Faire mon projet sous sa direction était pour moi un grand honneur et un immense bonheur.

Je remercie les membres du jury d'avoir accepté de juger ce modeste travail.

J'adresse également mes sincères remerciements à ma famille ; parents, grand parents, mon frère et ma sœur de m'avoir aidé à surmonter tous les obstacles et à me forger à travers les difficultés vécues durant toute cette période de travail.

Un remerciement particulier à une personne particulière qui a été continuellement présente, qui m'a beaucoup épaulée par son aide, soutien et encouragement.

Enfin, un grand merci à tous ceux qui m'ont aidé de prés ou de loin à la réalisation de ce travail.

Résumé

Les réseaux de capteurs sans-fils sont des systèmes distribués spécialement, composés de plusieurs dizaines de milliers de micro-capteurs. Ils mettent en jeu de nombreuses entités, souvent autonomes d'un point de vue énergétique. Ces entités remplissent essentiellement deux tâches : la collecte de mesures et la communication de mesures en direction d'une station de collecte. Ces entités sont généralement reliées par des réseaux de communication sans-fil. Dans de tels réseaux les liens sont asymétriques, la topologie est dynamique, la bande passante limitée et aucun organe dédié au routage n'est présent. L'ensemble des éléments du réseau participe activement au routage de l'information. Il est donc rendu plus difficile que dans les réseaux filaires traditionnels.

En effet, le processus de routage dans ce type de réseau est en saut par saut (multi-hop). La recherche de route repose nécessairement sur de l'inondation qui consiste à envoyer un message (par exemple la construction d'une route) à ses voisins pour qu'ils fassent de même etc. Le bon fonctionnement du routage dépend ainsi du comportement de l'ensemble des nœuds du réseau qui doivent respecter le protocole en usage. Il est très fréquemment supposé que ces nœuds sont de confiance.

Dans ce mémoire, on s'est intéressé au raisonnement de la confiance comme une solution de sécurité pour le routage dans les réseaux de capteurs, car cette approche s'adapte particulièrement à la nature de ce type de réseaux. Ainsi, on propose comme solution un modèle de confiance qui permet de sécuriser l'acheminement des données et qui veiller à ce que tous les nœuds aient un bon comportement et participe aux opérations de routage.

Mots-clés : réseaux de capteurs, routage, sécurité du routage, confiance, modèle de confiance.

Table des matières

Table des figures

INTRODUCTION GENERALE

Contexte, problématique, objectif et organisation du mémoire

Introduction générale

Contexte

Au cours de ces dernières années, la technologie des réseaux sans-fil n'a cessé de croître grâce aux développements technologiques dans divers domaines liés à la micro-électronique et aux communications sans-fil. Après les réseaux pour téléphones mobiles et les réseaux Ad-hoc, la recherche aujourd'hui s'oriente vers les réseaux de capteurs sans-fil.

Les réseaux de capteurs sont un nouveau paradigme des réseaux mobiles. Ils forment un type particulier des réseaux Ad-Hoc constitués de différentes entités mobiles inconnus et ne reposant sur aucune infrastructure fixe ou un contrôle centralisé, dans lesquels les nœuds sont des capteurs. Dans ce type de réseaux, les capteurs échangent l'information sur l'environnement afin d'établir une vue globale de la région surveillée. Cette information sera, ensuite, délivrée à l'utilisateur externe à travers le nœud passerelle « *Sink* ».

La propagation et l'acheminement de données dans un réseau de capteurs représentent une fonctionnalité très importante. En effet, la principale fonctionnalité de tels réseaux est l'opération de routage qui doit prendre en considération toutes les caractéristiques du réseau afin d'assurer les meilleures performances du système.

Le routage dans les réseaux de capteurs est très différent de celui des réseaux traditionnels. Dans les réseaux traditionnels, comme l'Internet ou les réseaux cellulaires, ce sont les routeurs dédiés qui prennent en charge de sauvegarder et de transférer les données pour les nœuds terminaux. Tandis que dans les réseaux de capteurs, puisqu'il n'existe pas de routeur dédié, le routage doit être effectué par chacun des nœuds du réseau pour assurer une disponibilité maximale de service de routage. Ainsi tout nœud est à la fois terminal et routeur, et il doit échanger avec d'autres nœuds non seulement du trafic d'applications, mais aussi des mésanges pour le contrôle du réseau et le routage des données.

Problématique

Le routage dans les réseaux de capteurs est différent de celui des réseaux classiques, il en est de même pour sa sécurité. Un défi important se présente alors au concepteur d'une application qui est la sécurité du routage. En effet, en l'absence d'une unité centrale et d'une infrastructure fixe, les solutions de sécurité classique ne sont pas adaptées aux réseaux de capteurs. De plus, pour sécuriser le routage dans un réseau classique, il est suffisant de protéger et d'authentifier les routeurs dédiées (sous l'hypothèse que les nœuds source et destination sont bienveillants), mais pour assurer la sécurité dans un réseau de capteurs, chacun des nœuds doit non seulement prendre la responsabilité de ses propres comportements mais aussi vérifier le comportement des autres nœuds, car chaque nœud représente un point de vulnérabilité dans le réseau. Ainsi, le bon fonctionnement du routage dépend essentiellement du comportement de l'ensemble des nœuds du réseau qui doivent se comporte tel que leur rôle le préconise, car il est très fréquemment supposé que ces nœuds sont de confiance.

Cependant, si aucun mécanisme n'est mis en place pour sécuriser les routes et inciter les nœuds du réseau a bien se comporter et à participer au routage, cela aura des conséquences indésirables sur les performances du routage surtout pour des applications qui ont besoin d'un court délai de routage. Car l'objectif principal du routage dans un réseau de capteurs est l'établissement correct et efficace de routes entre l'émetteur et le récepteur.

Objectif du mémoire

Étant donné les perspectives applicatives prometteuses des réseaux de capteurs ainsi que l'importance et la vulnérabilité de l'opération de routage, l'objectif du présent mémoire est de traiter le problème de sécurité du routage et de proposer un modèle permettant de protéger et de sécuriser le routage. Le choix des routes devra se faire sur la route la plus confiante de telle sorte que les messages puissent être acheminés en choisissant les routes de confiance avec une meilleure probabilité. La solution proposée doit prendre en compte les contraintes inhérentes à un réseau de

capteurs, notamment la nécessité de minimiser les coûts énergétiques, de mémoire de communication, …etc.

Organisation du mémoire

Le présent mémoire est organisé en trois chapitres répartis dans deux parties principales : une partie état de l'art et une partie solution. La partie état de l'art présente des généralités sur les réseaux de capteurs, le routage et la sécurité. La partie solution expose notre proposition pour sécuriser l'opération de routage dans les réseaux de capteurs.

Dans le chapitre I, on présente les réseaux de capteurs sans-fil, en passant par les caractéristiques, les domaines d'application, l'architecture, la communication ainsi que les différentes problématiques des réseaux de capteurs sans-fil.

Dans le chapitre II, on aborde le routage ainsi que la sécurité et le concept de la confiance dans les réseaux de capteurs sans-fil.

Dans le chapitre III, on propose notre le modèle de confiance pour sécuriser le routage dans un réseau de capteurs sans-fil.

Enfin, on termine par une conclusion générale et on présente quelques perspectives de travail pour le futur.

PREMIERE PARTIE

Etat de l’art : Réseaux de capteurs sans-fil et routage

CHAPITRE I

Introduction aux réseaux de capteurs sans-fil

I.1 Introduction

Les réseaux de capteurs sont le fruit des dernières avancées technologiques dans les domaines des réseaux sans-fil, des technologies "MEMS" (Micro-Electro-Mechanical Systems)[1] et des systèmes embarqués. Pour de faibles coûts, et avec des moyens abordables, il est dorénavant possible de concevoir des composants, à dimension réduite, intégrant un dispositif de captage et pouvant communiquer sur de faibles distances via des liaisons sans-fil. La mise en réseau de ces composants, appelés micro-capteurs, permet de réagir à des événements et d'analyser les données captées sur des zones étendues.

Dans ce qui suit, on étudiera ce type de réseaux sans-fil, ses principales caractéristiques, les différences qui les distinguent des réseaux ad hoc traditionnels ainsi que les éventuelles applications de ce type de réseaux très prometteur. En outre, l'architecture de communication dans les réseaux de capteurs sera détaillée ainsi que l'ensemble de facteurs influant sur sa conception. On présentera à la fin un ensemble de protocoles de routage qu'utilise ce type de réseau.

I.2 Réseaux Ad hoc

Un réseau Ad hoc, appelé généralement MANET (Mobile Ad hoc Network), est une collection d'unités mobiles munies d'interfaces de communication sans-fil, formant un réseau temporaire sans recourir à aucune infrastructure fixe ou administration centralisée. Dans de tels environnements, les unités se comportent comme des hôtes et/ou des routeurs [34].

Les nœuds des MANETs sont équipés d'émetteurs et de récepteurs sans-fil utilisant des antennes qui peuvent être omnidirectionnelles (broadcast), fortement directionnelles (point à point), ou une combinaison de ces deux types. Ils maintiennent d'une manière coopérative la connectivité du réseau, en fonction de leurs positions, la configuration de leurs émetteurs/récepteurs, la puissance de transmission et les interférences entre les canaux de communication. La modélisation

[1] Technologies qui font appel pour leur fabrication aux micro-technologies, qui permettent une production à grande échelle.

de cette connectivité est détaillée dans la section suivante. Un réseau ad hoc peut être isolé, mais il peut aussi avoir des passerelles ou des interfaces qui le relient à un réseau fixe.

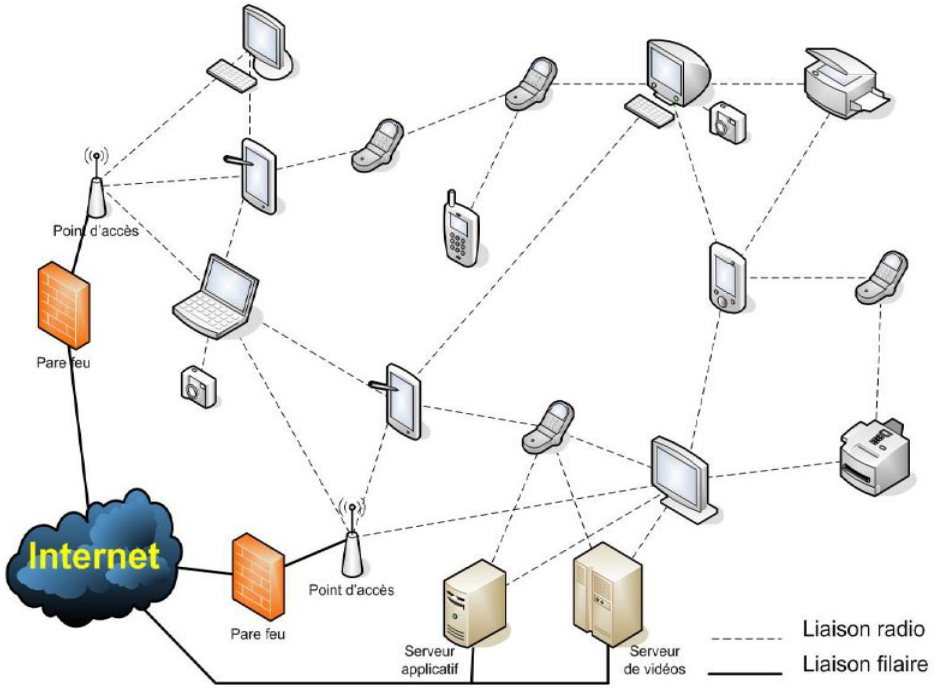


Figure I.1. Architecture d'un réseau sans-fil Ad hoc.

I.3 Capteurs sans-fil

Les capteurs sans-fil considérés ici sont conçus comme de véritables systèmes embarqués, dotés de moyens de traitement et de communication de l'information, en plus de leur fonction initiale de relever des mesures. Ils représentent une révolution technologique des instruments de mesure, issue de la convergence des systèmes électroniques miniaturisés et des systèmes de communication sans-fil.

L'architecture d'un nœud est complètement dépendante de l'objectif de son déploiement. Néanmoins, quatre unités de base sont présentes dans chaque capteur à savoir [16] :

- **L'unité de captage :** Transforme les signaux analogiques fournis par le capteur en un signal numérique compréhensible par l'unité de traitement ;

- **L'unité de traitement :** Gère les procédures permettant au nœud de collaborer avec le reste du réseau et peut aussi analyser les données captées pour alléger la tâche au collecteur ;

- **L'unité de transmission :** Effectue toutes les émissions et réceptions des données sur un medium sans-fil. Elle peut être de type radiofréquence (RF) ou de type optique ;

- **L'unité de contrôle d'énergie :** Est responsable de répartir l'énergie disponible aux autres modules et de réduire les dépenses en mettant en veille les composants inactifs par exemple.

En plus de ses quatre composants principaux, un capteur peut contenir, suivant son domaine d'application, des modules supplémentaires tels qu'un **générateur d'énergie** pour les cellules solaires, un **système de localisation** GPS (Global Positioning System)[2] ou un **système mobilisateur** chargé de déplacer les nœuds capteurs en cas de nécessité. La figure I.2 représente l'architecture générale d'un nœud capteur.

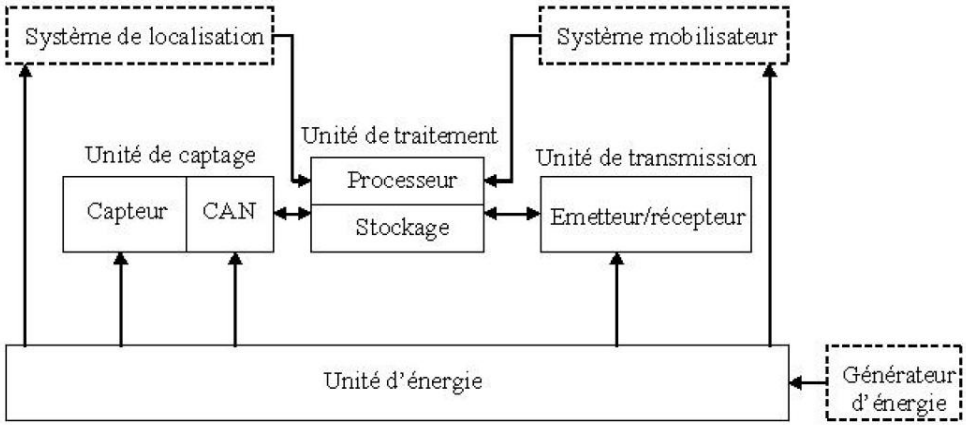


Figure I.2. Architecture d'un nœud capteur.

[2] Système de positionnement mondial et de géo-localisation fonctionnant au niveau mondial entièrement opérationnel et accessible au grand public.

I.4 Réseaux de capteurs sans-fil

Les réseaux de capteurs sans-fil sont considérés comme un type spécial des réseaux Ad hoc où l'infrastructure fixe de communication et l'administration centralisée sont absentes et les nœuds jouent, à la fois, le rôle des hôtes et des routeurs. Ce type de réseaux consiste en un ensemble de micro-capteurs éparpillés aléatoirement à travers une zone géographique qui définie le terrain d'intérêt pour le phénomène capté.

Les micro-capteurs déployés sont capables de surveiller, d'une manière continue, une grande variété de conditions ambiantes telles que la température, l'humidité, et de détecter également l'occurrence des évènements tel que les séismes,…etc. Malgré leur capacité limitées de captage et de traitement de donnée, qui n'est qu'une conséquence de leur taille miniaturisé (de l'ordre de 1 cm^3), les composants de communication sans-fil intégrés à ces capteurs leur permettent de collaborer et de coordonner entre eux afin d'accomplir des tâches de captage complexes.

I.5 Caractéristiques des RCSF

Les réseaux de capteurs sans-fil sont considérés comme un type spécial des réseaux Ad hoc et sont significativement différents des réseaux MANET traditionnels. En effet, Dans un réseau MANET, l'organisation des tâches, le routage ainsi que la gestion de mobilité sont principalement réalisés pour optimiser la qualité de service (QoS) et offrir une meilleure bande passante. Ces réseaux sont conçus pour fournir de bons débits de transfert sous les conditions de forte mobilité. Par ailleurs, comme leurs batteries peuvent être remplacées dés que nécessaire, la consommation d'énergie est donc d'une faible importance [14]. Les principaux caractéristiques des réseaux de capteurs se résument dans ce qui suit :

I.5.1 Densité importante des nœuds

Les réseaux de capteurs se composent généralement d'un nombre très important de nœuds pour garantir une couverture totale de la zone surveillée. Ceci

engendre un niveau de surveillance élevé et assure une transmission plus fiable des données sur l'état du champ de capteur.

I.5.2 Topologie dynamique

La topologie des réseaux de capteurs est instable ou dynamique est cela est due aux trois facteurs essentiels suivants :

- **La mobilité des nœuds :** Les nœuds capteurs peuvent être attachés à des objets mobiles qui se déplacent librement et arbitrairement, introduisant ainsi une topologie instable du réseau.

- **La défaillance des nœuds :** Du fait de l'autonomie énergétique limitée des nœuds, la topologie du réseau n'est pas fixée (les nœuds « morts » sont, d'un point de vue logique, simplement supprimés).

- **L'ajout de nouveaux nœuds :** De nouveaux nœuds peuvent facilement être rajoutés. Il suffit de placer un nouveau capteur qui soit dans la portée de communication d'au moins un autre nœud capteur du réseau déjà existant.

I.5.3 Auto organisation

L'auto organisation s'avère très nécessaire pour ce type de réseau afin de garantir sa maintenance. Pour remédier au problème de changement non prédictible de topologie, une auto-organisation du réseau s'avère nécessaire. C'est-à-dire que les nœuds doivent savoir localiser leurs voisins et établir des routes pour que l'information puisse circuler à travers le réseau.

I.5.4 Tolérance aux pannes

Le réseau doit être capable de maintenir ses fonctionnalités sans interruptions en cas de défaillance d'un ou plusieurs de ses capteurs. Cette défaillance peut être causée par une perte d'énergie, ou par dommage physique ou interférence de l'environnement. Le degré de tolérance dépend du degré de criticité de l'application et des données échangées.

I.5.5 Scalabilité

Les réseaux de capteurs peuvent contenir des centaines voire des milliers de nœuds capteurs. Un nombre aussi important engendre beaucoup de transmissions inter nodales et nécessite que le nœud *sink* (puits) soit équipé d'une mémoire importante pour stocker les formations reçues.

I.6 Domaines d'applications des RCSF

La miniaturisation, l'adaptabilité, le faible coût et la communication sans-fil permettent aux réseaux de capteurs d'envahir plusieurs domaines d'applications. Ils permettent aussi d'étendre le domaine des applications existantes.

Les réseaux de capteurs peuvent être composés, suivant leur utilisation, de différents types de nœuds capteurs, tels que les capteurs séismiques, thermiques, visuels, infrarouges, acoustiques et radar, ils sont capables de surveiller une grande variété de phénomènes ambiants. Parmi les domaines où ces réseaux se révèlent très utiles et peuvent offrir de meilleures contributions, on peut citer le militaire, la santé, l'environnemental, et les maisons intelligentes, …etc. [4].

I.6.1 Applications militaires

Le faible coût, le déploiement rapide, l'auto-organisation et la tolérance aux pannes sont des caractéristiques qui ont rendu les réseaux de capteurs efficaces pour les applications militaires.

En effet, comme beaucoup d'autres technologies de l'information, ces réseaux sans-fil proviennent principalement de la recherche militaire. Des réseaux de capteurs autonomes sont envisagés comme l'ingrédient essentiel dans cette lancée vers des systèmes de guerre centrés sur les réseaux. Ils peuvent être rapidement déployés et utilisés pour la surveillance des champs de bataille afin de fournir des renseignements concernant l'emplacement, le nombre, le mouvement, et l'identité des soldats et des véhicules, ou bien encore pour la détection des agents chimiques, biologiques et nucléaires.

I.6.2 Applications à la surveillance

L'application des réseaux de capteurs dans le domaine de la sécurité peut diminuer considérablement les dépenses financières consacrées à la sécurisation des lieux et des êtres humains. Ainsi, l'intégration des capteurs dans de grandes structures telles que les ponts ou les bâtiments aidera à détecter les fissures et les altérations dans la structure suite à un séisme ou au vieillissement de la structure. Le déploiement d'un réseau de capteurs de mouvement peut constituer un système d'alarme qui servira à détecter les intrusions dans une zone de surveillance.

I.6.3 Applications environnementales

Le contrôle des paramètres environnementaux par les réseaux de capteurs peut donner naissance à plusieurs applications. Par exemple, le déploiement des thermo-capteurs dans une forêt peut aider à détecter un éventuel début de feu et par suite faciliter la lutte contre les feux de forêt avant leur propagation. Le déploiement des capteurs chimiques dans les milieux urbains peut aider à détecter la pollution et analyser la qualité d'air. De même leur déploiement dans les sites industriels empêche les risques industriels tels que la fuite de produits toxiques (gaz, produits chimiques, éléments radioactifs, pétrole,…etc.). Dans le domaine de l'agriculture, les capteurs peuvent être utilisés pour réagir convenablement aux changements climatiques par exemple le processus d'irrigation lors de la détection de zones sèches dans un champ agricole.

I.6.4 Applications médicales

Dans le domaine de la médecine, les réseaux de capteurs peuvent être utilisés pour assurer une surveillance permanente des organes vitaux de l'être humain grâce à des micro capteurs qui pourront être avalés ou implantés sous la peau (surveillance de la glycémie, détection de cancers,…etc.).

Ils peuvent aussi faciliter le diagnostic de quelques maladies en effectuant des mesures physiologiques (la tension artérielle, battements du cœur,…etc.) à l'aide des capteurs ayant chacun une tâche bien particulière. Les données physiologiques

collectées par les capteurs peuvent être stockées pendant une longue durée pour le suivi d'un patient. D'autre part, ces réseaux peuvent détecter des comportements anormaux (chute d'un lit, choc, cri,…etc.) chez les personnes dépendantes (handicapées ou âgées).

I.6.5 Domotique

Avec le développement technologique, les capteurs peuvent être embarqués dans des appareils, tels que les aspirateurs, les fours à micro-ondes, les réfrigérateurs, les magnétoscopes, etc. Ces capteurs embarqués peuvent interagir entre eux et avec un réseau externe via Internet pour permettre à un utilisateur de contrôler les appareils domestiques localement ou à distance. Le déploiement des capteurs de mouvement et de température dans les futures maisons dites intelligentes permet d'automatiser plusieurs opérations domestiques telles que : la lumière s'éteint et la musique se met en état d'arrêt quand la chambre est vide, la climatisation et le chauffage s'ajustent selon les points multiples de mesure, le déclenchement d'une alarme par le capteur anti-intrusion quand un intrus veut accéder à la maison.

I.6.6 Applications commerciales

Les réseaux de capteurs possèdent également d'autres applications dans le domaine commercial, parmi les quelles on peut énumérer : la surveillance de l'état du matériel, la gestion des inventaires, le contrôle de qualité des produits, la construction des espace d'achat intelligents, le contrôle de l'environnement dans les bâtiments administratives, le contrôle des robots dans les environnements de fabrications automatiques, les jouets interactifs, les musées interactifs, le contrôle et l'automatisation des processus d'usinage, le diagnostique des machines, le transport, la détection et la surveillance des vols de voitures, le dépistage des véhicules, l'instrumentation des chambres blanches consacrées aux traitements des semi conducteurs,…etc.

I.7 Déploiement d'un RCSF

Les capteurs sont au préalable déployés sur une zone à surveiller. Pour satisfaire de nouvelles contraintes ou pour pallier des pannes, un déploiement de nœuds supplémentaires, dit *itératif*, peut être requis. Différents modes de déploiement sont envisageables et dépendent essentiellement de l'application de surveillance. Une fois déployés, on suppose que les capteurs sont statiques [14].

I.7.1 Phase de pré-déploiement et de déploiement

Les nœuds capteurs peuvent être éparpillés sur le champ de captage en masse ou placés d'une manière individuelle et ceci par le biais de plusieurs moyens tel que :

- Les jeter d'un avion,
- Utiliser une artillerie, roquette ou missile, ou
- Les placer nœud par nœud d'une façon manuelle ou en utilisant des robots.

Le nombre important de nœuds utilisés dans un réseau de capteurs empêche leur déploiement suivant un plan soigneusement établi, cependant un schéma général pour le déploiement initial doit être conçu pour permettre :

- De réduire les coûts d'installation,
- Augmenter la flexibilité d'arrangement des nœuds,
- Faciliter l'auto-organisation des nœuds et leur tolérance aux pannes.

I.7.2 Phase de post-déploiement

Après la phase de déploiement, la topologie du réseau peut subir des changements dus aux :

- Changement de position des nœuds,
- Accessibilité à cause du brouillage ou des obstacles en mouvements,
- Epuisement d'énergie,
- Mal fonctionnement des nœuds ou
- Des besoins pour leur application.

En effet, bien que les nœuds d'un réseau de capteurs puissent être déployés d'une manière statique, la panne matérielle constitue un évènement très commun à cause de l'épuisement d'énergie ou la destruction. Il est possible également d'avoir un réseau de capteur avec des nœuds mobiles qui ont une mobilité très élevée. Par conséquent, la topologie du réseau de capteur est exposée fréquemment aux changements après la phase de déploiement.

I.7.3 Phase de redéploiement des nouveaux nœuds

Des nœuds capteurs additionnels peuvent être installés pour remplacer ceux qui sont en panne ou bien pour répondre aux besoins des tâches assignées au réseau. Cette addition entraîne la réorganisation du réseau et le changement de sa topologie. Une bonne gestion du réseau, faisant face au facteur de changement fréquent de la topologie d'un réseau ad hoc caractérisé par une contrainte exigeante de consommation d'énergie doit passer obligatoirement par la conception des protocoles de routages spéciaux.

I.8 Architecture des RCSF

Un réseau de capteurs sans-fil est un ensemble de capteurs variant de quelques dizaines d'éléments à plusieurs centaines, parfois plus, utilisant des liens sans-fil pour la communication. Chaque réseau de capteurs a la capacité de collecter des données à partir d'un champ de captage, qui définit la zone d'intérêt pour le phénomène capté.

A l'aide d'une architecture multi sauts, un RCSF transmet les données collectées à un nœud puits (plusieurs à un), voir la Figure I.3. Ce dernier est considéré comme un point de collecte et peut transférer les données collectées via internet ou satellite à un ordinateur central "gestionnaire de tâche" pour leur traitement. De plus, des requêtes précisant le type de données requises et le début / arrêt de captage peuvent être envoyées par le biais du nœud puits aux nœuds capteurs (un à plusieurs).

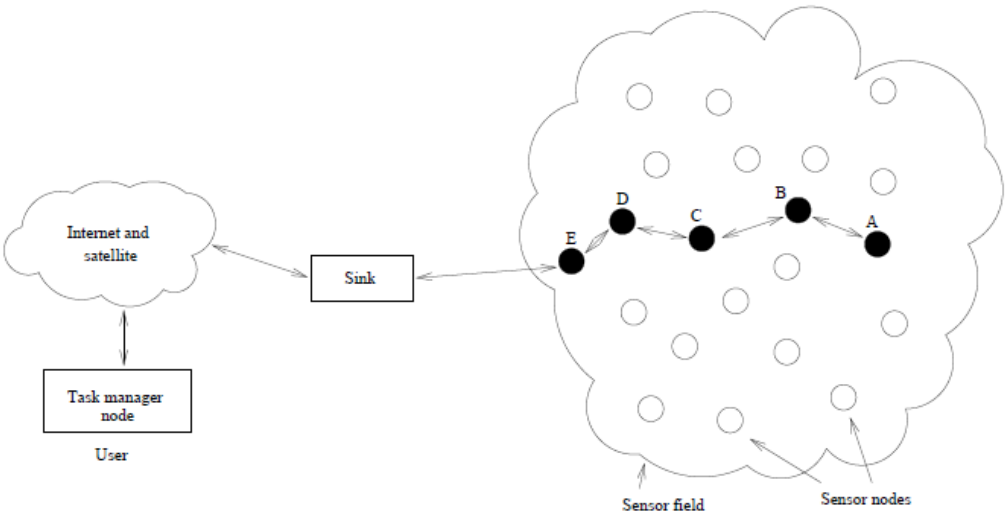


Figure I.3. Architecture d'un réseau de capteurs sans-fil.

Il existe deux types d'architectures pour les réseaux de capteurs sans-fil : l'architecture plate et l'architecture hiérarchique.

I.8.1 Architecture plate

Un réseau de capteurs sans-fil plat est un réseau homogène, où tous les nœuds sont identiques en termes de batterie et de complexité du matériel, excepté le nœud puits qui joue le rôle d'une passerelle et qui est responsable de la transmission de l'information collectée à l'utilisateur final. Selon le service et le type de capteurs, une densité de capteurs élevée (plusieurs nœuds capteurs/m^2) ainsi qu'une communication multi sauts peut être nécessaire pour l'architecture plate. En présence d'un très grand nombre de nœuds capteurs, le passage à l'échelle devient critique. Le routage et le contrôle d'accès au médium (MAC) doivent gérer et organiser les nœuds d'une manière très efficace en termes d'énergie.

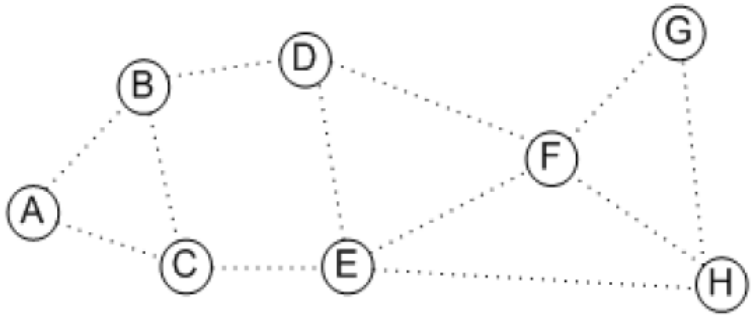


Figure I.4. Exemple de topologie plate.

I.8.2 Architecture hiérarchique

Une architecture hiérarchique a été proposée pour réduire la complexité de la plupart des nœuds capteurs et leur déploiement, en introduisant un ensemble de nœuds capteurs plus puissants. Ceci permet de décharger la majorité des nœuds simples à faible coût de plusieurs fonctions du réseau.

L'architecture hiérarchique est composée de plusieurs couches : une couche de capteurs, une couche de transmission et une couche de point d'accès. Cette architecture sans-fil est influencée par un certain nombre de facteurs et contraintes tels que la tolérance aux fautes, le redimensionnement, les coûts de production, l'environnement, la topologie du réseau, les contraintes matérielles, les médias de transmission et la consommation d'énergie.

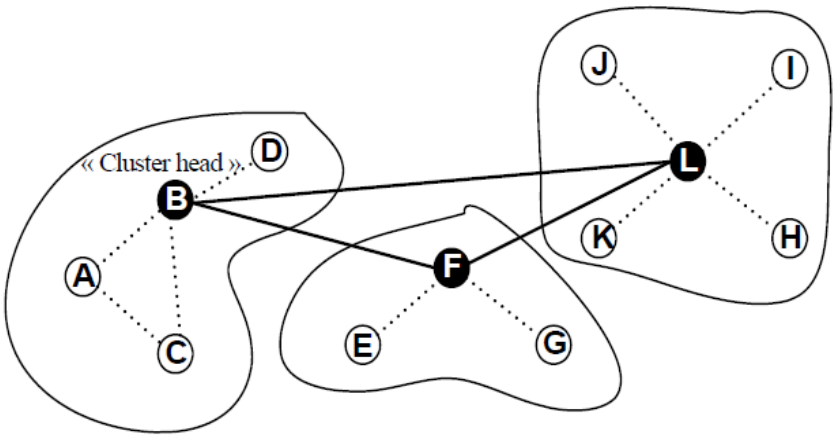


Figure I.5. Exemple de topologie hiérarchique.

I.9 Facteurs de conception des RCSF

La conception et la réalisation des réseaux de capteurs sans-fil est influencée par plusieurs paramètres, parmi lesquels on cite la tolérance aux pannes, la scalabilité, le coût de production, l'environnement d'exploitation, la topologie du réseau, les contraintes matérielles, le support de transmission et la consommation d'énergie. Ces facteurs importants servent comme directives pour le développent des algorithmes et protocoles utilisés dans les réseaux de capteurs. Ils sont également considérés comme des métriques de comparaison de performances entre les différentes applications des RCSF [16].

I.9.1 Tolérance aux pannes

La tolérance aux pannes dans un réseau de capteurs est la capacité de ce dernier à maintenir son bon fonctionnement malgré la présence de quelques défaillances. Ces défaillances peuvent survenir par manque d'énergie ou en raison de dommages physiques ou d'interférences environnementales. En effet, la panne de quelques nœuds entraine la perte des liens de communication et ainsi un changement significatif dans la topologie du réseau.

La tolérance aux pannes est donc la capacité de maintenir les fonctionnalités du réseau sans interruption due à une panne d'un nœud capteur.

I.9.2 Déploiement des nœuds

Le nombre de nœuds capteurs déployés dans un réseau peut être à l'ordre des centaines voire des milliers. Pour certaines applications, il peut atteindre quelques millions. Afin de garantir le bon fonctionnement du réseau, les nouveaux schémas de déploiement doivent être capables de travailler avec ce grand nombre de nœuds. Par ailleurs, ils doivent utiliser la propriété de haute densité dans les réseaux de capteurs ; et donc pouvoir déployer un grand nombre de nœuds dans une petite surface.

I.9.3 Contraintes matérielles

Un nœud doit être placé dans une petite surface n'excédant pas, généralement, un centimètre cube ($1cm^3$). En outre de cette contrainte de surface, un ensemble de conditions doit être satisfait. Un nœud capteur doit :

- Consommer le strict minimum d'énergie,
- Fonctionner dans de fortes densités,
- Avoir un faible coût de fabrication,
- Etre autonome,
- S'adapter à l'environnement.

I.9.4 Coût de production

Comme les RCSF consistent en un grand nombre de nœuds capteurs, le coût d'un seul capteur est très important pour définir le coût total de son réseau. Si ce dernier est plus cher que le déploiement d'un ensemble de capteurs ordinaires, alors le coût du RCSF n'est pas justifié. L'état de l'art définit le coût d'un réseau Bluetooth à 10$, et un nœud capteur à 1$.

I.9.5 Topologie du réseau

La disparition d'un nombre de capteurs dans le réseau, ainsi que le déploiement de nouveaux capteurs, rend la topologie du réseau fréquemment instable. La maintenance d'un réseau est d'autant importante que le changement de sa topologie.

I.9.6 Environnement

Les nœuds capteurs sont souvent déployés dans une région géographique distante et sans surveillance. Ils sont soumis à différentes conditions d'environnement ; ils peuvent fonctionner sous haute pression au fond de l'océan, dans un environnement dur tel que les champs de bataille ou même dans des milieux extrêmement froids.

I.9.7 Media de transport de données

Dans un réseau de capteurs, la communication à multi sauts entre les nœuds est réalisée avec des liens sans-fil à l'aide de media optique, infrarouge ou radio. La plus part des réseaux de capteurs utilisent des circuits de communication à radio fréquence grâce à leur faible coût ainsi que leur facilité d'installation. Le media optique est cependant utilisé dans les systèmes Smart Dust[3].

I.9.8 Consommation d'énergie

Les nœuds capteurs, étant des dispositifs micro-électroniques, peuvent être équipés seulement d'une source d'énergie limitée (<0.5 Ah, 1.2 V). Dans certains scénarios d'application, il est impossible de réapprovisionner de l'énergie. La durée de vie d'un capteur est donc dépendante de la durée de vie de sa batterie.

D'autre part, la retransmission des données, la réorganisation du réseau ainsi que le changement de sa topologie rendent la gestion et la conservation d'énergie d'une haute importance. Cette énergie est consommée par les différentes unités du capteur afin de réaliser les tâches de captage, traitement de données et communication. Cette dernière est l'opération qui consomme le plus d'énergie.

I.10 Communication dans les RCSF

I.10.1 Modèle en couches

Le rôle de ce modèle consiste à standardiser la communication entre les composants du réseau afin que différents constructeurs puissent mettre au point des produits (logiciels ou matériels) compatibles.

Contrairement aux réseaux traditionnels, les réseaux de capteurs utilisent une pile protocolaire de communication composée de cinq couches (une couche application, une couche transport, une couche réseau, une couche liaison de données

[3] Systèmes contenant des micro-nœuds qui peuvent être attachés à des objets ou même laissés flotter dans l'air. Ils utilisent des technologies MEMS pour implanter les fonctions de captage et de communication à travers un support optique.

et une couche physique) qui ont les mêmes fonctions que celles du modèle OSI ainsi que de trois niveaux ou plans intégrés dans la pile protocolaire pour la gestion de la puissance d'énergie, la gestion de la mobilité ainsi que la gestion des tâches (interrogation du réseau de capteurs) [14].

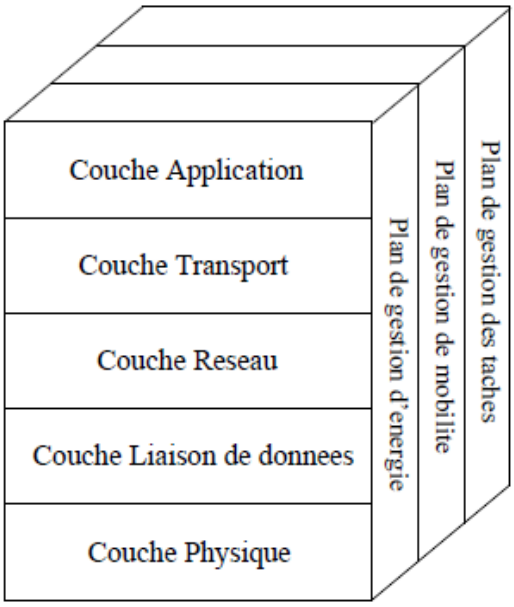


Figure I.6. Pile protocolaire dans les réseaux de capteurs.

Le but d'un système en couches est de séparer le problème en différentes parties (les couches) selon leur niveau d'abstraction. Chaque couche du modèle communique avec une couche adjacente (celle du dessus ou celle du dessous). Chaque couche utilise ainsi les services des couches inférieures et en fournit à celle de niveau supérieur.

I.10.1.1 Rôles des couches

Dans ce qui suit on examinera les différentes couches qui constituent la pile protocolaire et on donnera le rôle et les fonctions de chacune d'entre elles.

a. Couche application

La couche application constitue l'ensemble des applications implémentées sur un réseau de capteurs. Ces applications devraient fournir des mécanismes permettant

à l'utilisateur d'interagir avec le réseau de capteurs à travers différentes interfaces, et éventuellement, par l'intermédiaire d'un réseau étendu (par exemple Internet). Elles permettent également de rendre transparents les mécanismes de communication dans les couches inférieures. Tout ceci, en offrant des interfaces pour la création et la diffusion de requêtes.

Bien que plusieurs domaines d'application ont été proposés et définis pour les réseaux de capteurs sans-fil, la conception des protocoles agissants dans la couche application reste largement inexploitée.

Parmi les protocoles d'application pour les réseaux de capteurs, on peut citer les trois protocoles suivants : protocole d'assignation des tâches *Sensor management protocol (SMP),* le protocole de publication de données et capteur de requêtes *Task assignement and data advertisement protocol (TADAP)* et le protocole de diffusion de données *Sensor query and data dessiminitation protocol (SQDDP),* ces protocoles sont nécessaires pour tous réseau de capteurs basé sur le schéma de couches protocolaires décrit précédemment.

b. Couche transport

La couche transport vérifie le bon acheminement des données et la qualité de transmission et sert également à maintenir le flux de données en cas de nécessité dans les applications utilisées. Les principaux objectifs de cette couche sont :

- Multiplexer et démultiplexeur les messages entre les applications et la couche réseau.
- Réaliser un contrôle de haut niveau sur les données.
- Réguler la quantité des données injectées dans le réseau.

Afin qu'un réseau de capteurs sans-fil puisse interagir avec un autre réseau tel qu'Internet, une connexion TCP ou UDP peut être nécessaire. Cependant toutes les communications entre la station de base et les nœuds capteurs doivent utiliser un protocole de type UDP en raison des limitations en ressources des nœuds capteurs.

c. Couche réseau

Dans un réseau de capteurs, les nœuds sont déployés d'une manière dense dans un champ de captage proche ou à l'intérieur du phénomène capté. Pour permettre la communication dans le réseau déployé, des protocoles de routage spéciaux basés sur la communication multi sauts sont nécessaires entre les nœuds capteurs et le nœud puits du réseau. Toutefois, et comme il a été mentionnée dans les sections précédentes, les techniques liées au routage dans les réseaux ad hoc, proposées dans la littérature ne peuvent pas répondre aux exigences uniques des réseaux de capteurs sans-fil, notamment dans l'absence d'un adressage global, et la priorité absolue donnée à la quantité d'énergie consommée par les nœuds.

En effet, la conception de la couche réseau dans un réseau de capteurs doit être guidée par les principes suivants :

- L'efficacité en consommation d'énergie est une considération prioritaire.
- Tous les protocoles dans les réseaux de capteurs prennent en charge les données d'application qui circulent dans le réseau (Data centric).
- L'agrégation des données est utile quand elle ne cache pas l'effort collaboratif des nœuds capteurs.
- Un réseau de capteur idéal garantit un adressage basé attributs et ses nœuds sont conscients de leur localisation.

d. Couche liaison de données

La couche liaison de données est principalement responsable de :

- Multiplexer le flux de données.
- Détecter et verrouiller les trames de données.
- Contrôler l'accès au support de transmission (Media Access Control).
- Assurer une connexion fiable (point à point ou point à multipoints) selon la topologie du réseau de capteurs.
- Contrôler les erreurs.

e. Couche physique

La couche physique est responsable du support acheminant les données communiquées entre les nœuds. Ainsi, il existe trois types de médias pouvant être utilisés pour les réseaux de capteurs : optique (Laser), les infrarouges et les radiofréquences.

Le mode de communication par radio fréquence est le plus facile à employer et il reste le mode préféré par la plupart des projets de recherche menés sur les réseaux de capteurs, car les paquets échangés dans ces réseaux sont de petite taille et ils sont transmis à un faible débit. La possibilité de réutilisation de fréquence est également considérable en raison de la petite distance entre les nœuds.

Ainsi, il est possible de résumer les tâches accomplies au niveau de la couche physique en quatre points :

- La sélection des fréquences.
- La génération des ondes porteuses.
- La détection du signal.
- La modulation.

I.10.1.2 Plans de gestion

a. Plan de gestion de l'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 captage.

b. Plan de gestion de la mobilité

Ce plan détecte et enregistre tout les mouvements des nœuds capteurs, d'une 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.

c. Plan de gestion des tâches

Lors d'une opération de captage 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 la quelle il a été déployé.

Pour cela, le plan 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.

I.10.2 Protocole de communication ZigBee

Les contraintes des réseaux de capteurs définies dans le paragraphe précédent, et en particulier celle portant sur la consommation, montrent clairement que les standards sans-fils classiques tels que Bluetooth ou WLAN (Wireless Local Area Network) ne sont pas adaptés pour être utilisés dans ce type de réseaux. Le premier standard à avoir été normalisé et prenant en compte ces nouvelles contraintes liées aux RCSF est le standard ZigBee.

ZigBee est un protocole de haut niveau permettant la communication de petites radios, à consommation réduite, basée sur le standard IEEE 802.15.4[4] pour les réseaux à dimension personnelle (Wireless Personal Area Networks : WPANs). Cette technologie a pour but la communication de courte distance telle que le propose déjà la technologie Bluetooth, tout en étant moins chère et plus simple [16].

[4] Protocole de communication défini par l'IEEE destiné aux réseaux sans-fil de la famille des LR WPAN (Low Rate Wireless Personal Area Network) du fait de leur faible consommation, de leur faible portée et du faible débit.

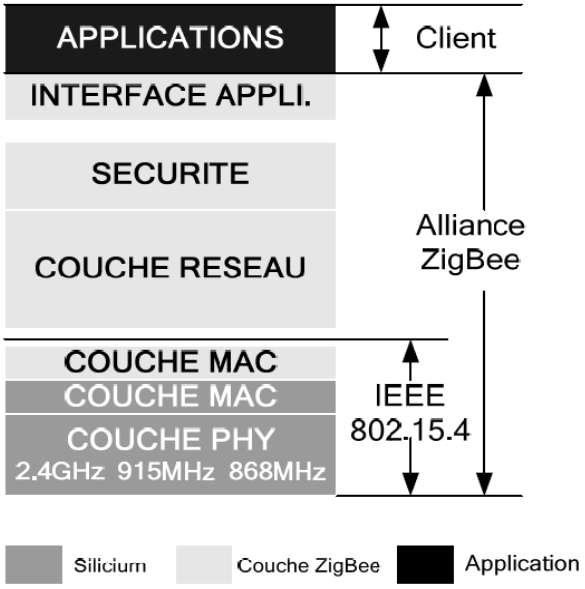


Figure I.7. Différence entre Zigbee et la norme IEEE 802.15.4.

I.11 Modèles de transmission de données dans les RCSF

La transmission de données dans les réseaux de capteurs peut se faire suivant plusieurs modèles dont on distingue trois essentielles [14] :

- Modèle Event Driven.
- Modèle Query Driven.
- Modèle Continuous.

I.11.1 Modèle Driven Event

La génération et la transmission des paquets de données sont commandées par la réalisation d'un événement. La plupart des applications *Driven Event* sont des applications intolérantes aux délais (temps réel), critiques, interactives et de non bout-en-bout. En fait, au lieu d'avoir un nœud émetteur et un autre récepteur de l'information, on trouve un nœud récepteur (le nœud de contrôle sink*)* et un groupe de nœuds capteurs, se trouvant proche de l'événement, qui sont tous des émetteur de la même information. La réussite de ces applications, pour ce modèle, repose essentiellement sur la détection de l'événement et la rapidité des prises des réactions nécessaires pour assurer l'aspect temps réel des applications. L'inconvénient majeur

de ce modèle est la redondance des données. En fait, les nœuds excités par le même événement envoient la même information au nœud de contrôle sink. Pour cela, un protocole de routage basé sur la négociation des données est recommandé.

I.11.2 Modèle Query Driven

Le modèle Query Driven est semblable au modèle Driven Event sauf que la collecte des informations sur l'état de l'environnement est initiée par des interrogations envoyées par le nœud de contrôle sink, alors que, pour le modèle précédant, elle est déclenchée suite à un événement détecté. La plupart des applications Query Driven sont des applications interactives, critiques, de non bout-en-bout et leur tolérance aux délais dépend de l'urgence de l'interrogation. Notons que le modèle Query Driven peut être utilisé pour contrôler et reconfigurer les nœuds. Par exemple, le sink peut envoyer des commandes au lieu des interrogations pour modifier le programme d'un nœud capteur, modifier son taux de trafic ou son rôle. Seul le nœud capteur jouant le rôle de sink est autorisé d'émettre des demandes d'interrogations ou des commandes et ce pour assurer l'ordre et l'hiérarchie de réseau de capteur.

I.11.3 Modèle Continuous

Dans le modèle continu, les nœuds capteurs envoient les informations d'une manière continue au nœud sink suivant un volume de trafic prédéterminé.

I.12 Différentes problématiques présentes dans les RCSF

Les axes de recherche dans les réseaux de capteurs sans-fil sont de caractère pluridisciplinaire, ils touchent les domaines de l'informatique, de l'automatique, du traitement du signal, de l'électronique, des nanotechnologies et des mathématiques. Les recherches dans le domaine des réseaux de capteurs ont révélé plusieurs problématiques, parmi ces problématiques on peut citer [32] :

- **Routage** : Le routage dans les réseaux de capteurs est une problématique importante. Les protocoles de routage des réseaux filaires ne sont pas adaptés

aux réseaux de capteurs. On peut facilement imaginer le nombre de mises à jour nécessaires lors du déploiement de 50 nouveaux capteurs dans une topologie de plusieurs milliers d'autres. L'un des principaux avantages du routage sur un ensemble dominant est qu'il est supporté par seulement une partie des nœuds du réseau. Seuls ces nœuds maintiennent des informations de routage et eux seuls auront à les mettre à jour en cas de modification de la topologie.

- **Consommation d'énergie** : L'énergie est considérée comme une ressource rare dans les applications de réseaux de capteurs sans-fil. En effet, les nœuds généralement utilisent des batteries, souvent non rechargeables, et généralement n'ont pas de mécanismes de production d'électricité. Il est communément dit que les applications pour lesquelles les réseaux de capteurs sont focalisés suggèrent que le changement des batteries est difficile ou impossible. Selon l'application, les nœuds pourraient être dans des endroits difficiles d'accès, sur un champ de bataille, et ainsi de suite. Il en résulte que l'efficacité de la gestion de l'emploi de l'´energie disponible est une question souvent vitale pour le réseau.

- **Ressources limitées** : La demande exige une tendance vers la miniaturisation des nœuds, ainsi que vers l'élargissement de la durée de vie et la baisse du prix des unités. Les nœuds ont donc des ressources extrêmement limitées, en comparaison avec l'équipement informatique que on a de nos jours (tels que les ordinateurs portatifs et les PDAs (*Personal Digital Assistant)*, etc.), en termes de mémoire disponible, de capacité et de vitesse de traitement, de débit, etc. En effet, des caractéristiques comme la haute vitesse de traitement et de transmission de données, ou une grande capacité de mémoire, sont des facultés qui amènent à une consommation énergétique très importante. Si on veut avoir de capteurs de taille microscopique, de faible consommation d'énergie et de faible coût de fabrication, on ne peut pas utiliser de microcontrôleurs ou transmetteurs radio de haute vitesse.

- **Dimension et densité du réseau** : Les réseaux de capteurs sont considérés comme des réseaux de très grande dimension, de l'ordre de plusieurs centaines à plusieurs milliers de nœuds, déployés de manière dense (chaque nœud peut avoir plusieurs dizaines de voisins). La forte densité du réseau peut entraîner des problèmes de congestion, si les nœuds essaient de communiquer au même moment, donc des retards dans la diffusion de messages et des pertes de paquets. La densité du réseau est généralement mise à profit pour partager le temps de travail entre les capteurs proches, et ainsi augmenter la durée de vie du réseau.

  Le facteur d'échelle est également important pour la conception des protocoles de communication et des traitements de données. Le routage de paquets doit être effectué d'une manière économique en énergie, sans pour autant que les nœuds soient obligés de minoriser toutes les routes possibles. Pour maîtriser la quantité d'information à faire remonter au puits, des algorithmes de fusion de données sont aussi à envisager.

- **Environnement de communication non contrôlable** : Il est habituel dans la littérature de prendre l'exemple d'un réseau de nœuds de capteurs déployé en larguant les capteurs depuis un avion. Pour ce type de déploiement, le positionnement des capteurs n'est pas contrôlé, de sorte que le réseau doit faire fac à des problèmes de connectivité d'un certain nombre de nœuds qui se retrouvent en dehors de la zone de couverture des autres nœuds, soit parce qu'ils sont trop éloignés, soit parce qu'ils sont tombés dans des lieux qui entravent la propagation des ondes radio ou tout simplement parce qu'ils ont été détruits. Les réseaux de capteurs héritent de tous les problèmes de l'usage d'une communication sans-fil, tels que des problèmes d'interférences et des problèmes de sécurité (attaques). Les signaux radio émis par les nœuds peuvent être sérieusement endommagés par les interférences présentes dans le milieu. Les basses fréquences peuvent être perturbées par le bruit des machines ou d'autres agents que ne sont pas nécessairement communicants, tandis que les hautes fréquences sont perturbées par d'autres équipements communicants que utilisent les mêmes bandes de fréquences.

- **Topologie dynamique** : Les réseaux de capteurs sont des réseaux dont la topologie peut changer très fréquemment. Ces changements topologiques peuvent être dus à la mobilité des nœuds. Mais même pour les applications où les nœuds sont fixes, des changements peuvent se produire lorsque des nœuds sont ajoutés ou enlevés, soit par action directe de l'utilisateur, soit par le basculement de l'état des nœuds (actif/endormi), soit par l'épuisement de l'énergie, ou la panne des nœuds. Ce changement aléatoire de la disposition des nœuds exige que les nœuds puissent s'auto-organiser et cela passe par des méthodes efficaces en énergie et robustes au facteur d'échelle.

- **Qualité de service** : Des protocoles au niveau de la couche MAC devraient être capables d'établir des priorités entre les flux, limiter les pertes de paquets vitaux pour la gestion du réseau, ou du moins en restreindre l'impact.

- **Diffusion de l'information** : Les protocoles de diffusion conçus pour les réseaux de capteurs doivent tenir compte de leurs spécificités ainsi que de leurs contraintes intrinsèques imposées. Ainsi, pour concevoir un protocole efficace, il faudrait assurer une couverture maximale des capteurs composant le réseau (taux d'accessibilité supérieur 90%), minimiser le nombre des réémetteurs et des réceptions redondantes ainsi que la consommation d'énergie.

- **Sécurité :** Pour les applications qui exigent un niveau de sécurité assez élevé telles que les applications militaires, des mécanismes d'authentification, de confidentialité, et d'intégrité doivent être mis en place au sein de leur communauté. Les algorithmes de cryptographie conçus pour les réseaux de capteurs doivent tenir compte des ressources limitées que présentent ces réseaux.

I.13 Conclusion

La flexibilité, la tolérance de fautes, le prix réduit et les caractéristiques rapides de déploiement des réseaux de capteurs offrent des possibilités infinies de développement dans tous les domaines d'application. Ceci nous permet de penser que les réseaux de capteurs feront bientôt partie intégrante de nos vies et satisferont sûrement les plus grands projets.

Cependant, bien qu'ils apportent de nombreux avantages, les réseaux de capteurs posent un certain nombre de défis scientifiques. En effet, la miniaturisation des batteries a entrainé un problème de limitation d'énergie. La consommation d'énergie représente ainsi un facteur majeur lors de la conception des réseaux de capteurs. De ce fait, les travaux doivent se porter sur l'élaboration de protocoles de communication minimisant la consommation énergétique. Les approches traditionnelles telles que les protocoles de routage développés pour les réseaux filaires ne sont pas adaptées aux réseaux de capteurs sans-fil. C'est pourquoi de nouvelles approches de routage doivent être mises en place afin de tenir compte des différentes contraintes imposées par les réseaux de capteurs sans-fil. Le chapitre suivant est consacré au routage dans les réseaux de capteurs sans-fil.

CHAPITRE II

Routage et confiance dans les réseaux de capteurs sans-fil

II.1 Introduction

L'opération de routage consiste à trouver un chemin optimal pour envoyer le message de la source à la destination. Dans le cadre des réseaux de capteurs, le routage doit être efficace en énergie. Pour cela, il faut bien sur être capable de trouver une route qui ne coute pas trop d'énergie, une route pas trop longue. Mais il faut aussi être capable de trouver ou de maintenir les routes sans dépenser trop d'énergie.

Dans le cadre des réseaux de capteurs sans-fil, les caractéristiques de ces derniers, font que le routage est une problématique importante. En effet, la densité importante des nœuds, leurs autonomies énergétiques limitées et la topologie qu'ils forment, exigent des protocoles de routage spécifiques, différents de ceux déployés dans les réseaux usuels afin d'assurer certains critères de performance.

Dans le présent chapitre, on étudie le routage dans les réseaux de capteur sans-fil. Notre objectif est de présenter la différente technique de routage, en passant initialement par les contraintes et les métriques de routage. Puis, par la suite, on présente les différentes familles de protocoles de routage déployés pour les réseaux de capteurs, ainsi que leurs caractéristiques. Et pour terminer, on donne un aperçu sur les vulnérabilités du routage et en conclue par les besoins de sécurité du routage des RCSF.

II.2 Contraintes de routage

Le routage dans les réseaux de capteurs diffère de celui des réseaux Ad Hoc dans les points suivants :

- Il est difficile d'établir un système d'adressage global pour le grand nombre de nœuds.
- Les applications des réseaux de capteurs exigent l'écoulement de données mesurées depuis des sources multiples vers la destination finale (nœud puits).
- Les différents capteurs peuvent générer les mêmes données à proximité d'un phénomène (problème de la redondance des données).

- Les nœuds capteurs exigent une gestion soigneuse des ressources.

En raison de ces différences, de nouveaux protocoles de routage ont été proposés dans les réseaux de capteurs.

II.3 Métriques 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 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).

II.3.1 Consommation énergétique

Les protocoles de routage utilisent cet ensemble de métriques pour minimiser la consommation d'énergie pendant le routage. 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 le 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 [1] :

a. Par considération de puissance

La route choisie est celle caractérisée par la somme des ED la plus élevée.

b. Par considération du coût

La route choisie est celle caractérisée par la plus petite somme des EN.

c. 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.

II.3.2 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 puits. La route choisie est celle qui contient un nombre minimum de nœuds (minimum de sauts) [1].

II.3.3 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. L'idée est de calculer le ratio 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].

II.3.4 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. 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].

II.4 Approches de routage dans les RCSF

Les réseaux étendus ont besoin d'algorithmes optimaux et adaptatifs pour faire parvenir les données d'un émetteur à un récepteur qui ne sont pas dans le même voisinage. Comme ces nœuds peuvent être très éloignés géographiquement et les technologies de communication sont souvent limitées en portée de transmission, l'utilisation d'algorithmes de routage, qui rendent possible cette communication d'un point à l'autre a travers plusieurs nœuds intermédiaires, devient impératif.

Le routage ad-hoc pour les réseaux sans-fil a été développé pour les réseaux d'ordinateurs ou de véhicules. Les réseaux de capteurs sans-fil sont un cas très particulier des réseaux ad-hoc, différents en termes d'échelle et en termes de limitations de ressources. De nombreuses approches ont été proposées afin d'assurer une transmission efficace et de prolonger la durée de vie des réseaux.

On peut classer les approches de routage pour les réseaux de capteurs sans-fil en quatre grandes classes, comme le montre la figure II.1.

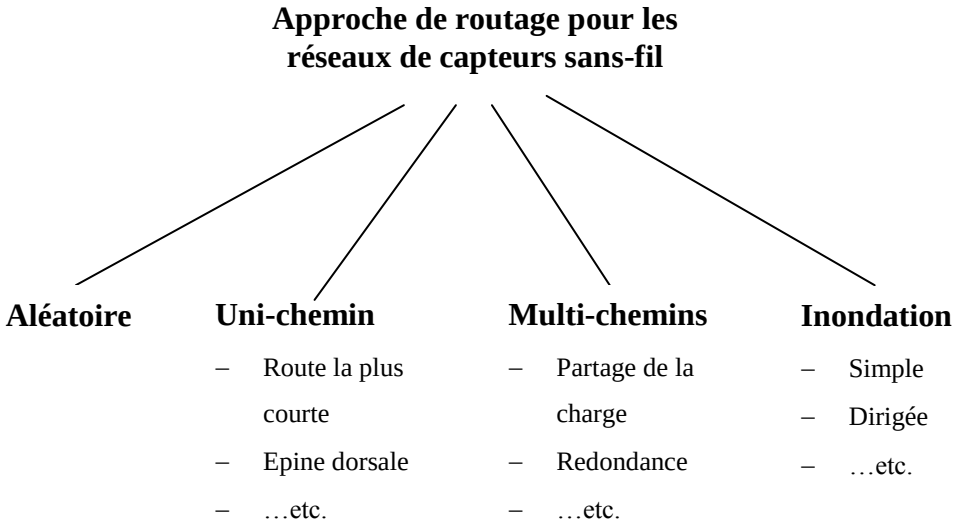


Figure II.1. Approches de routage pour les réseaux de capteurs sans-fil.

II.4.1 Routage aléatoire

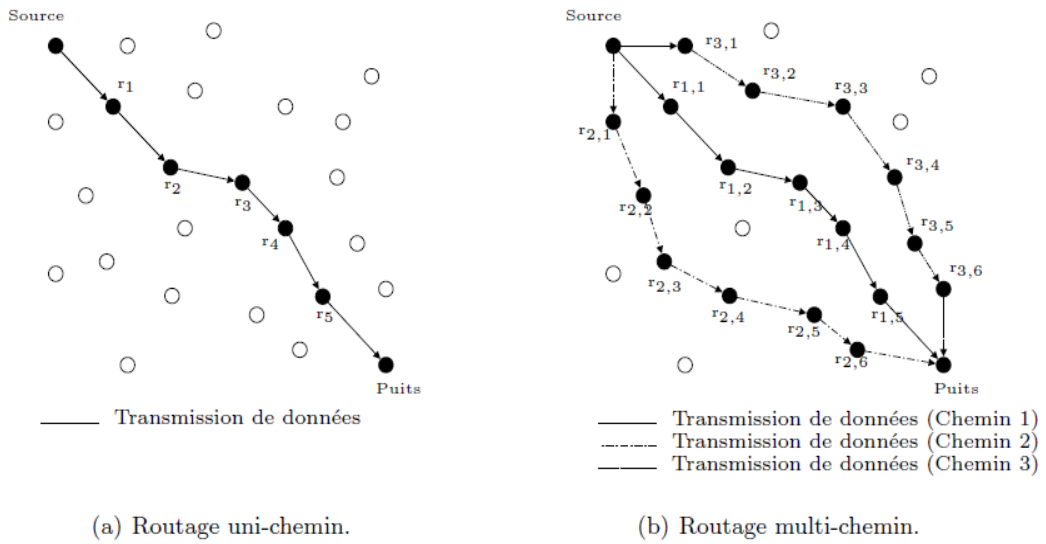
Dans le cas d'une stratégie de routage aléatoire, le paquet de données est envoyé à un nœud du voisinage au hasard (c'est une marche aléatoire). On peut aussi se limiter aux nœuds qui remplissent certaines conditions, par exemple, ceux qui sont plus proche du puits que le nœud source [15].

II.4.2 Routage uni-chemin

Dans le routage uni-chemin (uni-path) une et une seule route (peut être « optimale ») est sélectionnée avant la transmission, de manière a assurer l'arrivée des paquets par le « meilleur » chemin (voir figure II.1 (a)) [15].

II.4.3 Routage multi-chemins

Dans une approche multi-chemins (multi-path), plusieurs chemins sont sélectionnés. A partir de la, soit les paquets sont envoyés de manière répétée par les différents chemins pour augmenter la probabilité d'arrivée au puits, soit les paquets sont envoyés alternativement sur un chemin parmi toutes les routes sélectionnées pour mieux repartir le trafic sur les nœuds du réseau (voir figure II.2 (b)) [15].



(a) Routage uni-chemin. (b) Routage multi-chemin.

Figure II.2. Routage uni-chemin et multi-chemins.

II.4.4 Routage par inondation

La technique d'inondation (*flooding*) est une technique classique qui peut être utilisée pour le routage dans les réseaux de capteurs. Dans cette approche, chaque nœud recevant une donnée ou un paquet de contrôle le diffuse à tous les nœuds voisins jusqu'à ce que le nombre maximum de sauts pour ce paquet soit atteint ou le paquet arrive à sa destination [15].

L'inondation est une technique réactive qui ne nécessite pas une maintenance coûteuse de la topologie du réseau, ni des algorithmes complexes pour la découverte des routes. Elle augmente la probabilité d'arrivée des paquets, au prix d'une augmentation de la charge du réseau, mais elle présente plusieurs inconvénients (l'implosion, le chevauchement, ignorance de ressources,...etc.).

II.5 Routage des paquets

Afin de comprendre les attaques sur les protocoles de routage, il est nécessaire de comprendre leur fonctionnement global.

II.5.1 Détection de voisinage

Les réseaux de capteurs sont caractérisés par une topologie dynamique et changeante. Afin de détecter tout changement dans le réseau et générer les informations sur la topologie, les protocoles de routage se basent essentiellement sur la détection et la mise à jour de la liste des voisins de chaque nœud [1].

Dans le but de découvrir les nœuds voisins, chaque nœud envoie périodiquement à tous des messages HELLO. Ces messages contiennent les informations concernant les nœuds voisins, les nœuds qui sont choisis comme MPR (Multi-Point Relais)[5] et la liste des nœuds qui sont déclarés par ce nœud comme asymétriques.

[5] Un sous-ensemble de nœuds arbitraires voisins à 1 saut symétriques qui sont sélectionnés pour transférer le trafic de données.

La Figure II.3 décrit le processus de découverte des voisins entre deux nœuds A et B. En premier, le nœud A envoie à B un message HELLO qui ne contient aucune information. Une fois B reçoit ce message, il enregistre A comme voisin asymétrique car B ne trouve pas son adresse dans le message. Le nœud B envoie par la suite un message HELLO déclarant qu'il entend A. Ce dernier trouve son adresse dans le message et enregistre B comme voisin symétrique. À son tour, B trouve son adresse dans le message HELLO de A et déclare ce dernier comme voisin symétrique.

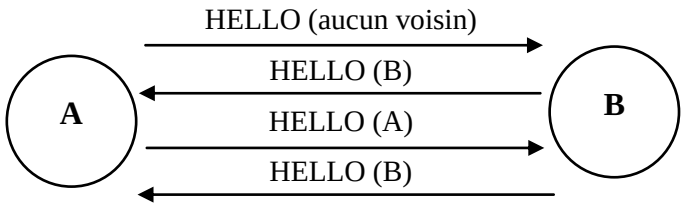


Figure II.3. Découverte de voisinage.

C'est ainsi que chaque nœud du réseau génère périodiquement des messages HELLO avec une duré de vie égale à 1 (TTL=1)[6]. Ces messages sont reçus par les voisins à 1 saut et ne sont pas relayés par ceux-ci.

II.5.2 Construction des routes

La communication dans les RCSF est basée sur différents paradigmes de communication; un à un, plusieurs à un et un à plusieurs. La communication un à un est utilisée dans des réseaux de type événement, un nœud capteur détecte une activité qui doit être signalée a une entité lointaine. Dans le paradigme plusieurs à un, les nœuds capteurs collectent des données a partir de leur environnement et les transmettent vers un centre de traitement appelé *puits*.

L'acheminement de ces données utilise des routes construites à l'aide de protocoles de routage qui se basent généralement sur un paradigme de communication un à plusieurs. Dans les différents types de communications, les paquets traversent le réseau saut par saut jusqu'à ce qu'ils atteignent leurs

[6] Temps de vie (TTL) est un mécanisme qui limite la durée de vie des données dans un ordinateur ou un réseau.

destinations, et chaque nœud intermédiaire relais ces paquets. Le rôle du nœud relais est de transmettre le paquet reçu au prochain saut, après l'avoir traite. Parmi les relais dans les RCSF, nous citons le relais des messages de demande de route RREQ (Route REQuest) pour la construction des routes.

II.5.2.1 Message Route Request (RREQ)

Le relais de message RREQ est indispensable pour la construction des routes dans les RCSF. En effet, les RCSF utilisent des protocoles de routage, centralisés ou distribués, pour la recherche et la construction de ces routes. La recherche se fait par la diffusion du message RREQ. Chaque nœud qui reçoit cette requête devient un nœud relais, et traite le message avant de le rediffuser. Le traitement de ce message consiste à modifier et à mettre à jour certains champs du paquet tels que la source du paquet et la distance en nombre de sauts par rapport au nœud émetteur. Les champs du paquet peuvent varier selon le protocole de routage sélectionne. L'information portée sur ces champs sera utilisée pour la décision de routage, y compris la sélection de(s) parent(s) (dans des protocoles de routage multi-chemins) et la construction des tables de routage [5].

II.5.2.2 Message Route Replay (RREP)

Après l'envoi d'un message RREQ par le nœud puits, le nœud intermédiaire qui reçoit ce paquet, diffuse à son tour le paquet RREQ en rajoutant son adresse à la liste de nœuds intermédiaires à condition qu'il n'en soit pas le destinataire et que sa table de routage n'indique pas de chemin pour le nœud recherché. Cela dit, dans le cas où le nœud intermédiaire possède dans sa table de routage un chemin pour le nœud destinataire, il renvoie directement un message de type **Route Reply (*Route REPply*)** au nœud puits en indiquant ce chemin [5].

Si un nœud reçoit un paquet de données pour une destination vers laquelle il ne peut plus émettre, il renvoie un message d'erreur de type **Route Error (*Route ERRor*)** vers la source du paquet de données. La route doit alors être supprimée de la table de routage.

La figure II.4 schématise l'évolution des messages lors de la découverte de route.

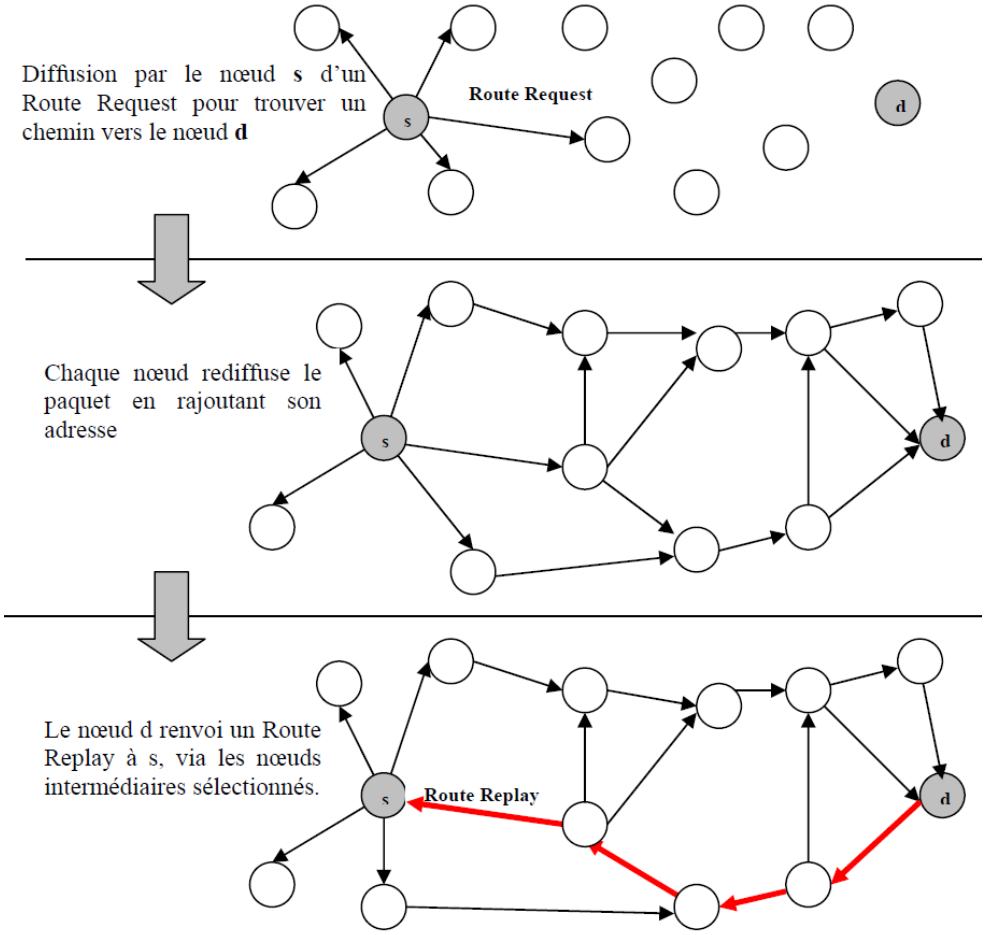


Figure II.4. Procédure de découvertes de route.

II.5.3 Choix de la route

Lorsque la réponse atteint l'initiateur de la découverte de route, ce dernier met à jour sa table de routage avec cette nouvelle route, qui consiste en la liste des nœuds intermédiaires avec un cout associé.

Le cout sert aux nœuds à effectuer un choix entre deux routes menant à la même destination. Dans les réseaux de capteurs, ce cout peut être basé en plus du nombre de nœuds intermédiaires traversés, sur des critères plus complexes qui caractérisent ce type de réseaux comme la consommation de l'énergie, la mémoire, la perte de paquets…etc. Si l'initiateur reçoit ultérieurement une indication comme quoi

cette destination peut être jointe avec un cout plus faible d'énergie par un autre chemin, la table de routage sera mise à jour avec la route ayant le cout le plus faible.

II.6 Protocoles de routage

II.6.1 Caractéristiques

Dans un réseau de capteurs, les nœuds capteurs sont dispersés à forte densité pour observer un phénomène dans une région. Par conséquence, ils sont très proches les uns des autres. Dans un tel scénario, les réseaux de capteurs utilisent une communication multi-sauts. Comparée à une communication sans-fil à longue distance, la communication multi-sauts présente une bonne solution pour le problème de propagation et de dégradation de signal. De plus, les nœuds consomment moins d'énergie ; ce qui caractérise les protocoles de routage par les principes suivants :

- **Consommation efficace de l'énergie :** Comme vu précédemment, l'énergie est une ressource critique d'une considération importante et dont les protocoles de routage doivent en tenir compte.

- **Adressage basé-attribut :** Dans un réseau de capteurs l'information est décrite en utilisant des attributs. En effet, l'utilisateur est plus intéressé de l'information fournie par le réseau que du nœud donnant cette information. Ainsi, il interroge le réseau en utilisant les attributs du phénomène observé.

- **Techniques Data-Centric :** Les réseaux de capteur emploient principalement des techniques centrées données à l'aide de requêtes sur les attributs du phénomène ; L'agrégation de données : l'agrégation de données est une technique qui résout le problème d'implosion dans le routage centré-données ; elle combine les données provenant de plusieurs nœuds en une information significative. Comme le montre la Figure1.4, une fusion de données est effectuée lorsque l'information est acheminée depuis les nœuds sources vers le collecteur, par exemple, le nœud E agrège les données provenant des nœuds A et B.

– **Intégration facile :** Le protocole de routage doit être facilement intégré dans d'autres réseaux, ex : Internet, dans le but d'acheminer les données vers l'utilisateur final.

II.6.2 Taxinomie

Les protocoles de routage proposés pour les réseaux de capteurs sans-fil peuvent être vus de plusieurs angles différents. De ce fait, un ensemble de critères sont défini pour les classifier. On distingue particulièrement, deux principaux critères pour classifier les protocoles de routage dans les réseaux de capteurs sans-fil à savoir : la structure du réseau et le type de protocole [15].

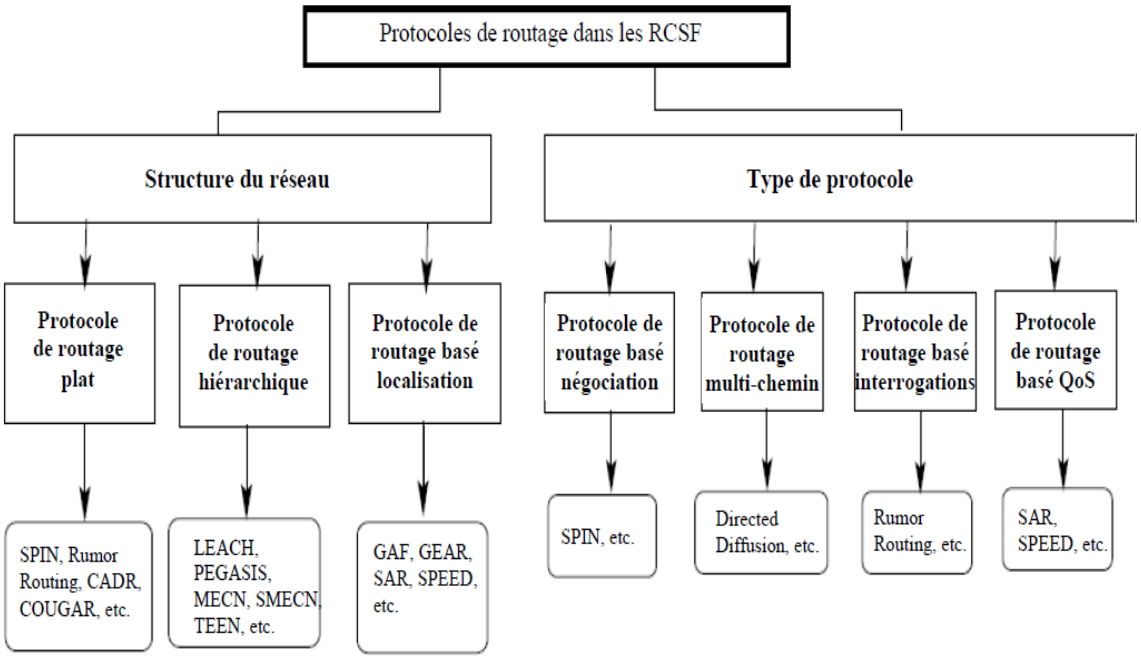


Figure II.5. Classification des protocoles de routage dans les RCSF.

II.6.2.1 Classification selon la structure 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.

a) Protocoles de routage plat (flat based-routing)

Ces protocoles considèrent que tous les nœuds sont identiques, c'est à dire ont les mêmes fonctions à exécuter sauf le nœud de contrôle sink qui est chargé de collecter toutes les informations issues des différents nœuds capteurs pour les transmettre vers l'utilisateur final. La décision d'un nœud de router des paquets vers un autre dépendra de sa position et pourra être remise en cause au cours du temps [19].

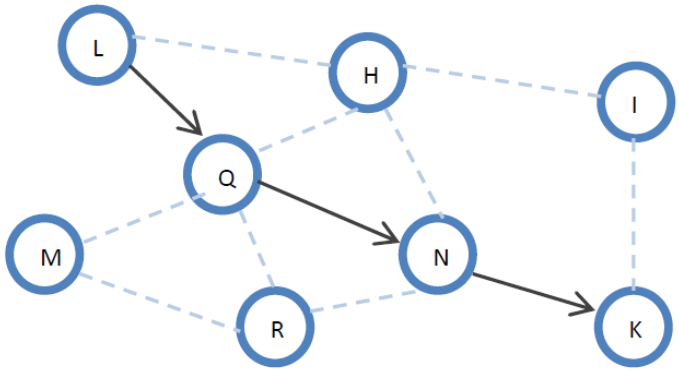


Figure II.6. Routage plat (flat based-routing).

b) Protocoles de routage hiérarchique

Ces protocoles fonctionnent en confiant des rôles différents aux nœuds du réseau. Le principe des protocoles de routage hiérarchique est basé essentiellement sur les clusters Head.

En effet, il s'agit de construire des clusters (groupe de nœuds) avec un chef par cluster qui se chargera de transmettre les messages générés par son cluster aux autres chefs de clusters pour atteindre la destination finale. Le choix du chef de cluster (cluster Head) est fait soit à tour de rôle, soit selon le nombre de voisins en considérant comme cluster Head le nœud avec le plus de voisins, soit selon le niveau de l'énergie résiduelle, …etc.

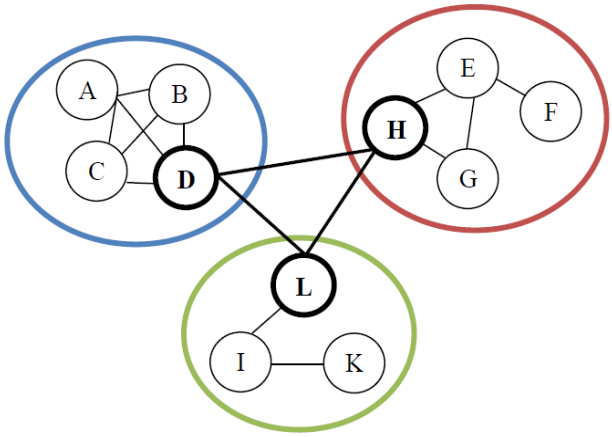


Figure II.7. Routage hiérarchique.

Ce type de routage offre de nombreux avantages pour les réseaux dont leurs nœuds sont sédentaires et disposent de suffisamment d'énergie.

c) Protocoles basés sur la 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 [7].

Dans les réseaux de capteurs, on considère que la position du nœud est plus importante que son identité (adresse). Ce type de protocoles considère que les nœuds connaissent leur position respective et sont capables de connaître la position des autres nœuds. Ainsi, cette information est utilisée pour diriger les messages vers la région dans laquelle se trouve la destination.

Un routage est dit basé-localisation lorsque les décisions de routage sont basées sur la position des nœuds. On distingue trois principales décisions de routage géographique, qui dépendent, soit de :

- *La progression* (le nœud dont la projection est la plus proche de la destination est choisi comme prochain nœud),

- *La distance* (le nœud le plus proche de la destination en termes de distance est choisi comme prochain nœud,

- *La direction* (le nœud voisin le plus proche de la droite (Source, Destination) en direction de la destination est choisi).

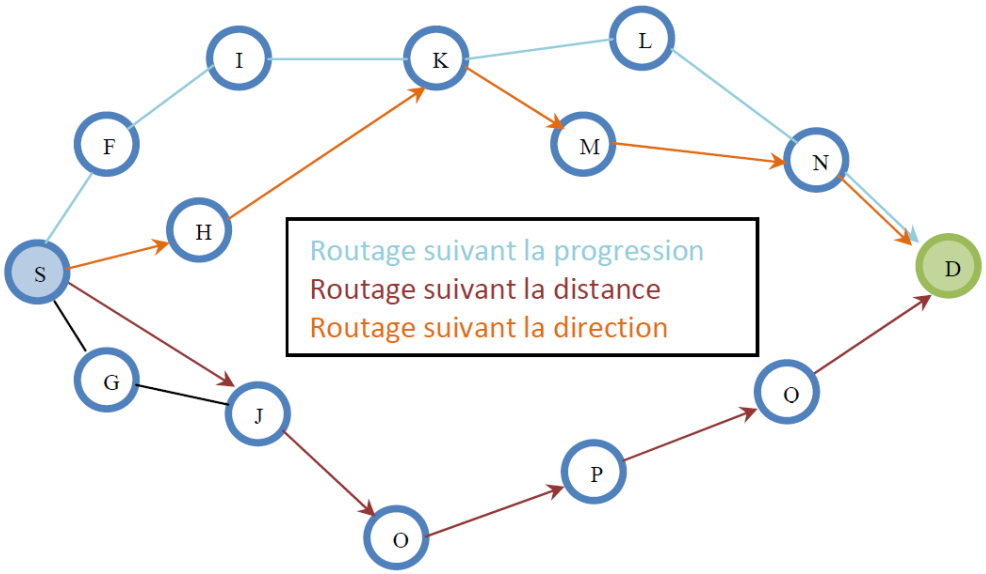


Figure II.8. Routage basé sur la localisation.

II.6.2.2 Classification selon le type de protocole

a) Protocoles basés sur la négociation

En détectant le même phénomène, les nœuds capteurs inondent le réseau par les mêmes paquets de données. Ce problème de redondance peut être résolu en employant des protocoles de routage basés sur la négociation. En effet, avant de transmettre, les nœuds capteurs négocient entre eux leurs données en échangeant des paquets de signalisation spéciales, appelés *métadonnées.* Ces paquets permettent de vérifier si les nœuds voisins disposent des mêmes données à transmettre. Cette

procédure garantit que seules les informations utiles seront transmises et élimine la redondance des données [7].

b) Protocoles multi-chemins

Les protocoles de routage multi-chemins se basent sur l'adoption de plus qu'un chemin menant vers la destination, et ce, pour avoir des chemins de secours si jamais le chemin principal serait rompu [7].

c) Protocoles basés sur les interrogations

Ces protocoles sont basés sur le *modèle Query Driven*. La collecte des informations sur l'état de l'environnement est initiée par des interrogations envoyées par le nœud puits. La plupart des applications *Query Driven* sont des applications interactives, critiques, de non bout-en-bout et leur tolérance aux délais dépend de l'urgence de l'interrogation [5].

Le modèle *Query Driven* peut être utilisé pour contrôler et reconfigurer les nœuds. Par exemple, le nœud puits peut envoyer des commandes au lieu des interrogations pour modifier le programme d'un nœud capteur, modifier son taux de trafic ou son rôle. Seul le nœud capteur jouant le rôle de nœud puits est autorisé d'émettre des demandes d'interrogations ou des commandes et ce pour assurer l'ordre et l'hiérarchie de réseau de capteur [24].

d) Protocoles basés sur la qualité de service (QoS)

Ce type de protocoles tend à satisfaire certaines métriques, pendant la transmission des données vers la destination finale. Parmi ces métriques, on cite : le délai de bout-en-bout, la gigue, l'énergie consommée, …etc. [21].

Dans ce type de protocoles, les performances du réseau sont prises en compte pour garantir un délai de bout-en-bout raisonnable qui répond aux besoins de l'application. C'est surtout le cas des applications industrielles et militaires.

II.7 Sécurité et confiance dans le routage

La sécurité est un sujet important à traiter, surtout pour les applications dans le domaine des réseaux de capteurs dites sensibles à la sécurité (par exemple une application du type champ de bataille). Effectivement, les réseaux de capteurs sont connus pour leur mobilité, leur topologie dynamique, donc ils sont généralement considérés difficiles à sécuriser [22].

II.7.1 Objectifs de la sécurité

Les objectifs de la sécurité dans les RCSF ne sont pas différents de ceux dans les autres réseaux classiques. En effet, elle vise à assurer que l'information soit correcte, qu'elle n'ait pas été altérée et émane effectivement de la source légitime.

Un service de sécurité est un service qui améliore la sécurité du traitement et du transfert des données. La sécurité dans les RCSF vise donc à assurer les services de base suivants :

a. Authentification

Elle permet de coopérer au sein des RCSF sans risque, en contrôlant et en identifiant les participants. En effet, la communication entre deux nœuds dans un environnement ouvert est confrontée aux risques qu'il y ait d'autres nœuds qui cherchent à emprunter une identité des nœuds légitimes pour s'approprier leurs données. Dans ce cas, si l'authentification est mal gérée, un attaquant pourra facilement se joindre au réseau et injecter des messages erronés s'il réussit à s'emparer de cette identité.

L'utilisation d'un code d'authentification MAC (Message Authentification Code), permet d'assuré à la fois l'authentification de l'origine et l'intégrité du message.

b. Intégrité de données

Ce service permet de vérifier que les données ne subissent aucune altération ou destruction volontaire ou accidentelle, et conservent un format permettant leur utilisation lors de leurs traitements, de leurs conservations ou de leurs transmissions. Elle peut être assurée par l'utilisation des fonctions de hachage cryptographiques qui permettent d'obtenir pour chaque message une empreinte numérique.

c. Confidentialité

Une fois les parties authentifiées, la confidentialité reste un point important, étant donnée la communication sans-fil des RCSF. Elle permet de garantir que l'information n'a pas été divulguée et que les données ne sont compréhensibles que par les entités qui partagent un même secret. La confidentialité peut être assurée par l'usage de la cryptographie à clé symétrique ou asymétrique.

d. Fraîcheur

Même si la confidentialité et l'intégrité des données sont assurées, on doit également assurer la fraîcheur de chaque message. Officieusement, la fraîcheur de données suggère que les données soient récentes, et elles s'assurent qu'aucun vieux message n'a été rejoué.

Elle concerne la fraicheur de données et la fraicheur des clés. Puisque tous les réseaux de capteurs fournissent quelques formes de mesures variables dans le temps, on doit assurer que chaque message est frais. La fraicheur de données implique que les données soient récentes, et elle assure qu'aucun adversaire n'a rejoue les vieux messages.

e. Non-répudiation

Elle consiste à maintenir, rendre disponible et valide un élément de preuve concernant un événement ou une action revendiquée de façon à résoudre des litiges sur la réalisation ou non de l'événement ou de l'action. C'est donc un mécanisme

prévu pour assurer l'impossibilité que la source ou la destination puisse nier avoir reçu ou émis un message.

f. Contrôle d'accès

Le contrôle d'accès est un service très important qui consiste à empêcher des éléments externes d'accéder au réseau, et cela en attribuant aux participants légitimes des droits d'accès afin de discerner les messages provenant des sources internes du réseau de ceux externes.

g. Disponibilité

Ce service désigne la capacité du réseau à assurer ses services pour maintenir son bon fonctionnement en garantissant aux parties communicantes la présence et l'utilisation de l'information au moment souhaité. Comme les nœuds capteurs peuvent jouer le rôle de serveurs, la disponibilité reste difficile à assurer. En effet, un nœud peut ne pas servir à des informations pour ne pas épuiser ses ressources d'énergie, de mémoire et de calcul en provoquant ainsi un mauvais comportement. Cette propriété reste difficile à assurer dans les RCSF étant donnée les contraintes que présentent ces réseaux.

II.7.2 Vulnérabilités du routage

Les réseaux de capteurs sont exposés à un grand nombre de vulnérabilités, surtout au niveau routage. Etudier les vulnérabilités dans la couche réseau des RCSF peut nous permettre de reconnaitre toutes les attaques à éviter, afin d'établir un environnement sécurisé qui satisfait les besoins de sécurité de chacune des applications des RCSF.

Comme, on a déjà signalé, le routage dans les réseaux de capteurs est très différent de celui des réseaux traditionnel. Il en est de même pour sa sécurité. Ainsi, les mécanismes de sécurité conçus pour les réseaux filaires et cellulaires ne sont pas adaptés à ces réseaux pour les raisons suivantes :

- **Nœuds compromis :** Les nœuds capteurs sont plus faciles à compromettre que ceux dans un réseau traditionnel, parce qu'ils sont de nature mobile et sans-fil donc physiquement plus petits et plus faciles à déplacer et à attaquer. De plus, parce qu'ils peuvent éventuellement entrer et/ou sortir du réseau de temps à autre, et que les réseaux de capteurs peuvent être divisés et/ou fusionnés, donnant aux attaquants plus de chances de compromettre des nœuds sans être aperçus.

- **Faible capacité, ou nœuds hétérogènes :** La capacité souvent limitée des nœuds et l'utilisation de batteries pour l'alimentation des équipements sont aussi des faiblesses des réseaux de capteurs. Ainsi, les nœuds capteurs ont une durée de vie limitée. De plus, pour gagner plus de ressources, des nœuds peuvent aussi être "gourmands", par exemple vouloir gagner plus de bands passante.

- **Manque de coopération :** Parce que les nœuds dans un réseau de capteurs ont tendance à être égoïstes à cause du manque de ressource, nous devons assurer la coopération entre eux. Malheureusement, il est difficile de détecter des nœuds égoïstes : les nœuds peuvent tout simplement être silencieux et/ou refuser de transférer les données. Quand de tels nœuds sont nombreux dans le réseau, la disponibilité du service de routage est atteinte.

- **Manque d'organisation :** Le manque d'organisation influence elle aussi la sécurité des réseaux de capteurs. Parce qu'un nœud n'a pas forcément de connaissance sur les autres lors de la montée du réseau, la confiance apriori peut ne pas exister. De plus, parce qu'il n'y a pas forcément de serveur central, la distribution et la gestion (surtout la révocation) de clés peuvent être difficiles à réaliser. D'autre part, comme le réseau est dynamique, il n'est pas facile de gérer l'adhésion des membres du réseau. Tous ces problèmes génèrent de sérieuses difficultés pour la sécurité du routage.

- **Mobilité** : La mobilité des nœuds rend la topologie des réseaux de capteurs instable. Il n'est donc pas facile pour un nœud de connaître correctement son

voisinage et la topologie du réseau. Les attaquants peuvent ainsi forger et diffuser de fausses informations de topologie pour réaliser leurs attaques. Par ce moyen, un protocole de routage non-sécurisé peut facilement être attaqué. De plus, la mobilité des attaquants peut aussi les rendre plus difficiles à détecter ou localiser.

- **Interface sans-fil (radio) :** L'interface sans-fil (dans la plupart des cas l'interface radio) des nœuds pose aussi des problèmes dans le routage. A cause de la nature de radio en transmission qui est la diffusion, chaque paquet émit dans le réseau, que ce soit en unicast ou en diffusion, pourrait être reçu par tout voisin de son émetteur. De plus, le problème des nœuds cachés, où deux émetteurs qui ne peuvent pas entendre l'un à l'autre envoient à un même récepteur en même temps, peut causer collisions. En outre, le problème de nœud exposé, où les nœuds dans la portée d'un émetteur d'une session en cours sont interdits d'émettre, peut gaspiller la bande passante du réseau. D'autres problèmes tels que les pertes de paquets, l'atténuation de signal,… etc., existent aussi dans les réseaux de capteurs à cause de l'interface sans-fil.

II.7.3 Besoins de sécurité du routage

Après avoir discuté les problèmes du routage dans les réseaux de capteurs et les raisons pour lesquelles les solutions de sécurité classiques ne sont pas adaptées, on peut identifier les nouveaux besoins de la sécurité du routage dans les réseaux de capteurs qui sont :

- **Nœuds compromis :** Parce que les nœuds compromis ne peuvent pas être détectés par simple authentification, ce problème ne peut pas être résolu par l'utilisation de cryptographie. Donc, nous devons considérer spécialement d'autres solutions pour ce problème.

- **Ressources limitées :** Puisqu'ils ont été plutôt désignés pour les nœuds physiquement plus forts, les mécanismes de sécurité des réseaux traditionnels sont inadaptés à l'environnement des réseaux de capteurs. Ils ont donc besoin de nouvelles solutions de sécurité qui doivent être économes en termes de

puissance de calcul, de consommation d'énergie et de la charge du trafic. En outre, ces nouveaux mécanismes doivent aussi être équitables au niveau de l'utilisation de ressources du réseau.

- **Egoïsme des nœuds** : Normalement, le problème d'égoïsme n'existe pas dans les réseaux traditionnels où les nœuds ne dépendent pas des autres mais se reposent sur les routeurs dédiés pour assurer la fonctionnalité du routage. Donc, de nouveaux mécanismes doivent être désignés pour garantir la coopération des nœuds dans des réseaux de capteurs.

- **Confiance entre les nœuds :** Les solutions de sécurité pour les réseaux traditionnels s'appuient souvent sur des relations de confiance préalablement établies ou des autorités de confiance à tierces. Elles utilisent les primitives cryptographiques symétriques et/ou asymétriques pour authentifier les nœuds et sécuriser les échanges de données. Afin d'utiliser ces moyens cryptographiques dans les réseaux de capteurs, on doit étudier comment établir des autorités de confiance et/ou des relations de confiance entre les nœuds sans l'aide d'aucune infrastructure.

- **Mobilité :** Il n'y a pas autant de mobilité dans les réseaux filaires. De plus, dans les réseaux cellulaires ce sont des infrastructures qui gèrent la mobilité. Donc, des protocoles de routage capables de découvrir correctement la topologie du réseau même sous attaques doivent être conçus spécialement pour les réseaux de capteurs.

- **Communication sans-fil:** Parce que les solutions traditionnelles exigent souvent un échange fiable de messages, elles sont souvent non adaptées aux réseaux de capteurs, car ils ont besoin de mécanismes tolérant aux fautes et ayant un faible surcoût.

II.7.4 Concept de la confiance

Tous les types d'interactions, de transactions et de communications dans la vie humaine sont basés sur un aspect fondamental qui est la confiance, dit en anglais

« Trust » [44]. Comme les réseaux de capteurs peuvent consister en plusieurs nœuds dont chacun est étranger par rapport aux autres, ils ont besoin donc de ce concept avant de procéder à tout genre d'échanges de données et d'informations.

II.7.4.1 Définition de la confiance

La confiance est la ferme conviction en la compétence d'une entité à agir comme il lui est prévu. Cependant, cette valeur n'est pas fixe mais plutôt dépend du comportement de l'entité dans un contexte spécifique et à un moment donné. C'est un concept qui concerne les éléments du réseau et qui se base sur des observations et sert à caractériser les interactions entre ces différents éléments [46].

La confiance et la sécurité sont deux notions étroitement interdépendantes. En effet, la cryptographie est un moyen pour garantir la sécurité mais qui exige l'existence de la confiance dans le processus d'échange des clés. De façon similaire, un échange fiable de clés ne peut avoir lieu sans la mise en place des services de sécurité requis [38].

D'un point de vue mathématique, la confiance est définie comme étant une probabilité. Dire qu'on a confiance en quelqu'un veut dire que la probabilité qu'il va exécuter une action bien spécifique est assez élevée pour l'engager et coopérer avec lui. Une telle définition, implique la possibilité d'avoir un modèle mathématique pour mesurer ou évaluer la confiance [41].

II.7.4.2 Types de confiance

On distingue en général deux types de confiance à savoir :

- La confiance assurée.
- La confiance décidée.

a. Confiance assurée (confiance aveugle)

Elle est acquise a priori, sans réelle évaluation du risque, ceci peut être le cas parce que l'on estime que la réalisation du risque est très improbable, que les

inconvénients possibles sont minimes par rapport aux avantages attendus, ou encore que l'on n'ait pas vraiment d'alternative [34].

b. Confiance décidée

Elle est le résultat d'un réel processus d'appréciation du risque (évaluation des avantages attendus de la décision et des inconvénients qui peuvent en découler) et décision parfaitement consciente. Celle-ci sous-entend que la décision prise peut conduire à une déception, et un regret de l'avoir prise. Elle ne peut donc être requise que dans le cas où les dommages possibles sont supérieurs aux avantages reçus [34].

II.7.4.3 Propriétés de la confiance

Les principales propriétés de la confiance peuvent se résumer comme suit :

– **La relativité :** Puisque ce n'est pas une notion ou valeur absolue. En effet, quelqu'un à confiance en un autre ce n'est que compte tenu de sa capacité à exécuter une action ou à fournir un service dans un contexte spécifique et un instant donné.

– **L'arité :** Une relation de confiance peut être seulement entre deux entités « one to one », « one to many », « many to one » comme dans le cas d'un employeur et ses employés ou encore « many to many » qui veut dire une confiance mutuelle entre par exemple les membres d'un groupe ou d'un comité.

– **L'asymétrie :** Une personne peut avoir confiance en une autre mais pas vice vers ça.

– **La transitivité :** Bien que dans la littérature il est mentionné que la confiance ne doit pas être transitive, quelques scénarios font preuve de transitivité. Le concept de délégation de la confiance (autoriser quelqu'un à prendre une décision à sa place) est l'exemple d'application de la transitivité de la confiance. Cependant, cette propriété est à éviter ou à utiliser avec précaution pour ne pas tomber dans des erreurs d'estimation du niveau de confiance.

II.7.4.4 Intérêt de la confiance dans le routage

L'utilisation de la confiance pour atténuer les menaces de sécurité a été un domaine important pour la recherche. L'établissement et la gestion de la confiance entre les entités peuvent être effectués de façon centralisée à travers une autorité fiable, de façon distribuée ou encore la combinaison des deux.

La gestion de la confiance est éployée pour garantir la tolérance aux fautes et aux intrusions et sert à délivrer un service correct en dépit de la présence des attaques surtout avec la naissance de ce nouveau paradigme de la confiance distribuée (Distributed Trust).

Le recours à un modèle de confiance dans les solutions de sécurité pour le routage dans les réseaux de capteurs est une direction prometteuse, surtout que ces réseaux ne possèdent pas une infrastructure préexistante ce qui fait que les solutions de sécurité doivent être décentralisées et se faire de manière autonome.

La notion de confiance est intéressante dans les réseaux de capteurs surtout pour prendre par exemple la décision à propos de :

- La validité d'une information de routage.
- La loyauté d'un nœud qui sert de relais dans la route qui mène vers la destination.
- L'allocation optimale des ressources compte tenu des exigences en termes de sécurité des applications qui les demandent.

II.8 Conclusion

La propagation et l'acheminement de données dans un RCSF représentent une fonctionnalité très importante. Ils doivent prendre en considération toutes les caractéristiques du réseau afin d'assurer les meilleures performances du système.

Le routage dans les RCSF est un processus de coopération entre les nœuds pour découvrir les nœuds voisins, sélectionner les routes et acheminer les données.

Ce processus repose essentiellement sur la confiance de chaque nœuds a concernant les informations reçus des autres nœuds.

Comme les réseaux de capteurs, peuvent consister en plusieurs nœuds dont chacun est étranger par rapport aux autres, ils ont donc besoin d'instaurer un certain niveau de sécurité avant de procéder à tout genre d'échanges de données et d'informations. Ainsi, comme tous les types d'interactions, de transactions et de communications dans la vie humaine sont basés sur un aspect fondamental qui est la confiance.

Dans le chapitre suivant, on propose une solution qui intègre le raisonnement de la confiance dans le processus de routage afin de sécuriser l'acheminement des données dans un réseau de capteurs et rendre la prise de décision concernant le choix des routes plus robuste.

DEUXIEME PARTIE

Solution proposée : Modèle de confiance pour le routage

CHAPITRE III

Modèle de confiance pour le routage

III.1 Introduction

Le routage multi-sauts dans les réseaux de capteurs repose essentiellement sur la participation active de chaque nœud. Il est alors essentiel de s'assurer que les nœuds jouent correctement leurs rôles surtout que ces réseaux soulèvent de nombreux problèmes de sécurité. Par ailleurs, l'absence d'infrastructure se traduit par la nécessité d'intégrer, au sein de chaque nœud, les mécanismes lui permettant d'assurer sa propre sécurité et celle de tout le réseau.

Dans ce chapitre, on propose une solution permettant d'intégrer la notion de la confiance dans le routage des réseaux de capteurs. Car on a jugé intéressant d'introduire ce concept afin d'en tirer profit pour des besoins de sécurité.
Le modèle qu'on propose permet aux nœuds d'acheminer les données via des routes fiables et sûres afin d'assurer la sécurité et le bon fonctionnement du routage.

III.2 Définition du problème

Les réseaux de capteurs sans-fil mettent en jeu de nombreuses entités, souvent autonomes d'un point de vue énergétique. Ces entités remplissent essentiellement deux tâches : la collecte de mesures et la communication de mesures en direction d'une station de collecte. Ces entités sont généralement reliées par des réseaux de communication sans-fil. Dans de tels réseaux aucun organe dédié au routage n'est présent et l'ensemble des éléments du réseau participe activement au routage de l'information.

En effet, les communications dans ce type de systèmes sont en saut par saut (multi-hop). La recherche de route repose nécessairement sur de l'inondation qui consiste à envoyer un message à ses voisins pour qu'ils fassent de même. Ainsi, la sécurité du processus de routage dépend essentiellement de la coopérativité et de la fiabilité de l'ensemble des nœuds du réseau qui sont fréquemment supposés être de confiance.

Cependant, dans un réseau de capteurs, les nœuds peuvent facilement devenir malveillants ou non fiables à cause de l'instabilité des liens radio ou après avoir été corrompus. Par conséquent, la sécurité du routage des informations, devient compromise si un nœud ne se comporte pas tel que son rôle le préconise.

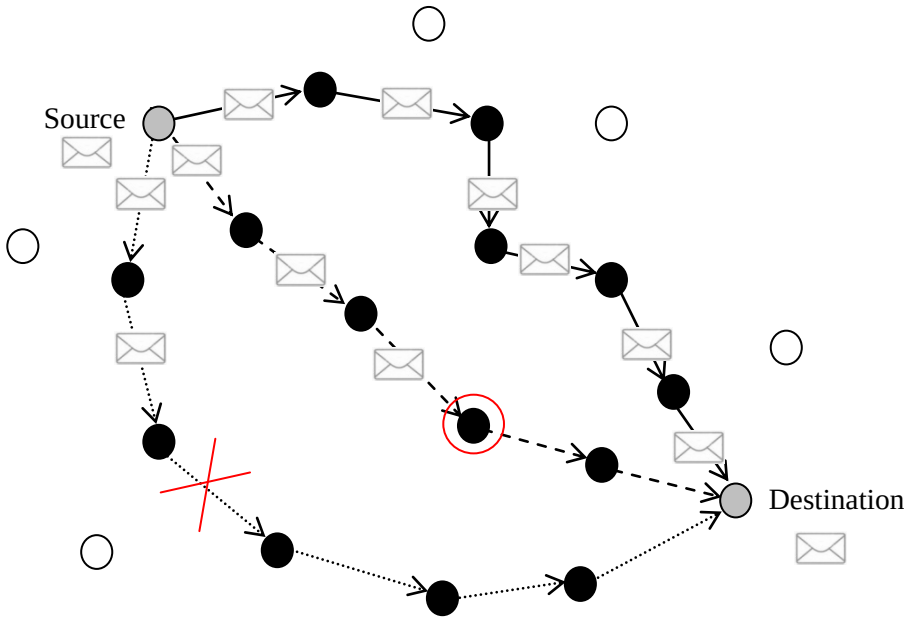


Figure III.8. Routage avec des nœuds malveillants.

Ainsi, comme le comportement et la coopération des nœuds dans le réseau, jouent un rôle très important dans l'acheminement des données dans un réseau de capteurs. La notion de confiance, quoiqu'implicite, constitue alors le levier incontournable à l'émergence d'une solution globale au problème de sécurité entre les entités qui participent aux opérations de routage. Ceci fait appel à un modèle théorique pour mesurer le niveau de confiance des routes à emprunter et obliger tous les nœuds du réseau à bien se comporter afin de d'assure la sécuriser et le bon fonctionnement du routage.

III.3 Description du modèle de confiance

Dans ce qui suit, on propose un modèle de confiance capable de proposer un niveau de sécurité adapté au routage dans les réseaux de capteurs et dont le niveau pourra évoluer dans le temps en fonction des comportements des nœuds capteurs.

Un tel modèle sera employé essentiellement pour assurer le bon fonctionnement du routage en veillant à la coopérativité et au bon comportement des capteurs dans le réseau. Le modèle de la gestion de la confiance explicité ci-dessus sera intégré dans le processus de routage en vue de mesurer le niveau de confiance de chaque route afin de garantir l'acheminent des données jusqu'au nœud de destination par le chemin le plus confiant. De plus, la gestion de la confiance permet aux entités de raisonner avec la confiance, rendant ainsi les capteurs plus robustes pour la prise de décision concernant le choix des routes.

III.3.1 Hypothèses

Pour assurer le bon déroulement de notre modèle de confiance, on définit les hypothèses suivantes :

- Le réseau de capteur est dynamique (les nœuds sont mobiles).
- Les nœuds capteurs sont homogènes : Ils sont similaires dans leurs capacités de traitement, de communication, d'énergie et de stockage.
- Le déploiement des nœuds est aléatoire : Les voisins de n'importe quel nœud ne sont pas connus avant le déploiement.
- Le réseau à une tautologie plate.
- Les communications entre les nœuds sont bidirectionnels, si un nœud x peut recevoir un message du nœud y alors x peut envoyer un message à y.

III.3.2 Notation

Les notations utilisées dans notre modèle de confiance :

Notation	Description
N_i	Le nœud numéro i dans le réseau
V_{Ci}	– Valeur de confiance du nœud i – Valeur continue dans l'intervalle] 0, 1]
V_{Ri}	– Valeur de réputation du nœud i – Valeur continue dans l'intervalle [0, 1] – Utilisée pour estimer la V_{Ci}
C_{Ri}	– Valeur continue dans l'intervalle] 0, 1] – La confiance de route d'une source à une destination – Donne la valeur de confiance de la route choisie – Basée sur la moyenne des V_{Ci} des nœuds
K_i	Clé privé du nœud i
MAC_{Ki}	Code d'authentification de message utilisé pour authentifier un message entre la source et la destination

Figure III.2. Tableau de notation utilisée.

III.3.3 Idée de base

Le modèle de confiance proposé à pour objectif de protéger et de sécuriser le routage dans un réseau de capteurs et plus particulièrement la phase d'acheminement des données d'un nœud source à un nœud de destination. L'idée de base est d'aider les nœuds sources dans leurs choix de routes en trouvant la route ayant un taux élevé d'acheminement de paquets.

Après un déploiement aléatoire des capteurs, le modèle de confiance affecte à chaque nœud du réseau une valeur de confiance et une valeur de réputation, qui seront mises à jour dynamiquement. Par la suite, si un nœud S veut envoyer des données à un nœud D, notre modèle de confiance mesure la confiance de toutes les routes établies entre le nœud S et le nœud D. Ainsi, avant d'acheminer ses données, le nœud émetteur compare les valeurs de confiance des routes trouvées et achemine ses paquets via la route dont le degré de confiance est le plus élevée.

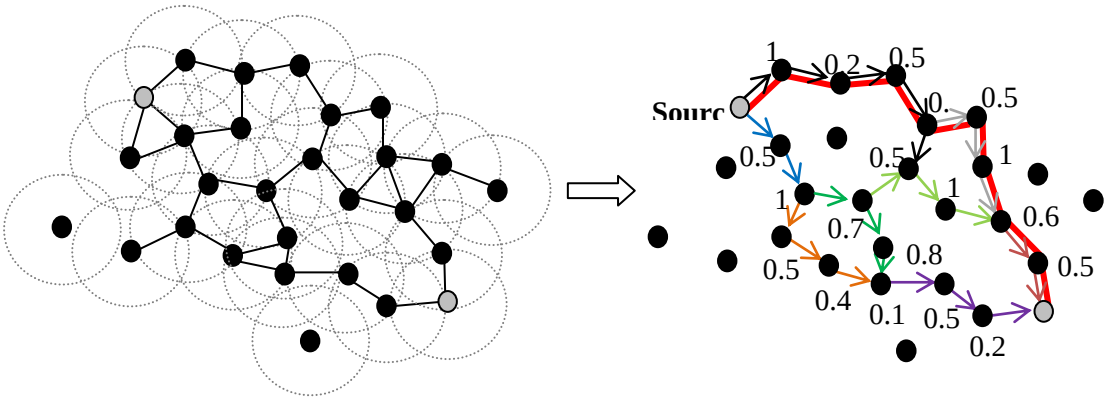


Figure III.3. Idée de base du modèle de confiance proposé.

De cette manière, le processus de routage dans un réseau de capteurs devient plus sûr et plus sécurisé en dépit des mauvais comportements des nœuds dans le réseau.

III.3.4 Fonctionnement

Le changement fréquent de la topologie dans les réseaux de capteurs fait que le routage des données devient de plus en plus vulnérable si un nœud ne se comporte pas tel que son rôle le préconise. Ainsi le modèle proposé se base essentiellement sur la confiance et la réputation des nœuds pour évaluer la confiance d'une route afin d'assurer la sécurité du routage et éviter autant que possible d'acheminer les données par une route non confiante.

La figure suivante présente les différentes phases de fonctionnement de notre modèle de confiance.

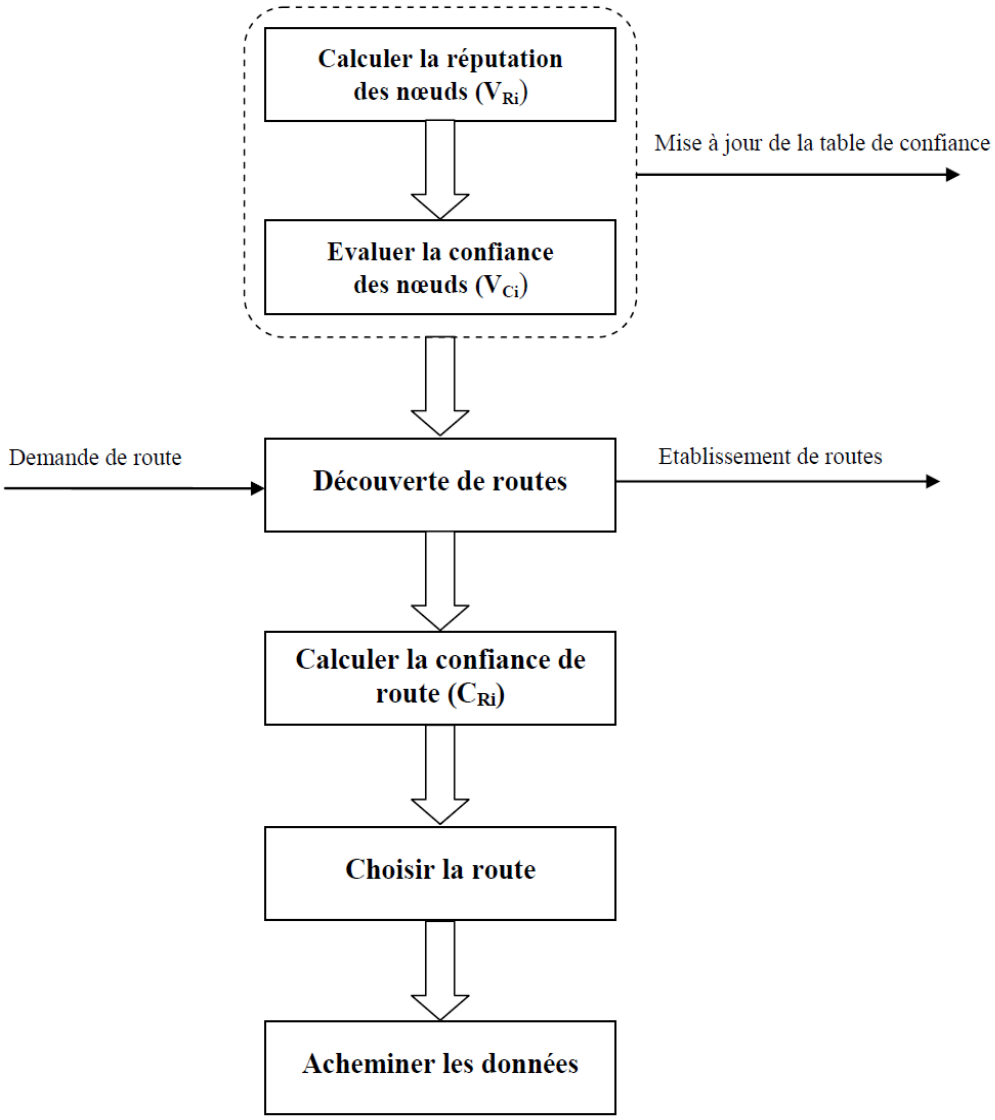


Figure III.4. Fonctionnement du modèle de confiance.

III.3.4.1 Calculer la réputation

Le calcul de la réputation est basé sur le paramètre de coopération des nœuds dans le réseau. La définition de ce paramètre consiste à calculer pour chaque nœud la proportion de paquets bien retransmis par rapport au nombre total de paquets devant être transmis sur une période durant laquelle on collecte les informations captées par les nœuds capteurs.

Supposons qu'on a deux nœuds voisins Ni et Nj. Si le noeud Ni envoie un certain nombre de paquets de données au nœud Nj avec un autre nœud comme destination, alors après une période de temps, on calcule la valeur de réputation (V_{Ri}) du nœud Nj avec la formule suivante :

$$V_{Ri} = \text{Nombre des paquets acheminés / Nombre total des paquets} \quad ...(1)$$

Ainsi, cette valeur de réputation augmente au fur et à mesure que le nœud prouve sa coopération et son bon comportement dans le réseau et diminue sinon. Dans le cas où le nœud Nj réussit à acheminer la totalité des paquets reçus par le nœud Ni, le taux de transmission atteindra un seuil de 100% et sa valeur de réputation V_{Ri} sera égale à 1. Dans le cas contraire, si le nœud Nj n'achemine aucun des paquets reçus par Ni alors son taux de transmission sera nul et sa réputation V_{Ri} sera donc égale à 0. Donc, la réputation V_{Ri} sera toujours comprise entre les deux valeurs 0 et 1.

III.3.4.2 Evaluer la confiance

L'évaluation de la confiance d'un nœud est indispensable au fonctionnement de notre modèle de confiance pour sécuriser le routage. Elle est l'élément fondateur de notre modèle de confiance. Le calcul de la confiance a essentiellement pour rôle d'estimer le niveau de confiance de chaque nœud du réseau pour aider l'émetteur dans son choix de route.

Algorithme de calcul de la confiance (V_{Ci})

On propose dans ce qui suit, un algorithme de calcul de confiance qui est exécuté par chaque nœud du réseau. Au début, notre algorithme initialise les deux valeurs V_{Ci} et V_{Ri} à 0.5, puis, après une période de temps, il calcule la nouvelle valeur de réputation avec la formule (1). Ensuite, il évalue la confiance du nœud en testant la valeur de réputation calculée.

L'idée consiste à découper l'intervalle [0,1] de la réputation en trois intervalles de même longueur (0.33) chacun ($[0, \frac{1}{3}[$, $[\frac{1}{3}, \frac{2}{3}[$ et $[\frac{2}{3}, 1]$), afin d'évaluer

la coopération et le comportement d'un nœud dans le réseau. Puis, on estime la confiance du capteur comme suit :

- Si $\mathbf{V_{Ri} \in [0, \frac{1}{3}[}$ alors la confiance V_{Ci} diminue d'un pas de 0.1.
- Sinon, si $\mathbf{V_{Ri} \in [\frac{1}{3}, \frac{2}{3}[}$ alors la confiance V_{Ci} ne change pas.
- Enfin, si $\mathbf{V_{Ri} \in [\frac{2}{3}, 1]}$ alors la valeur V_{Ci} augmente d'un pas de 0.1.

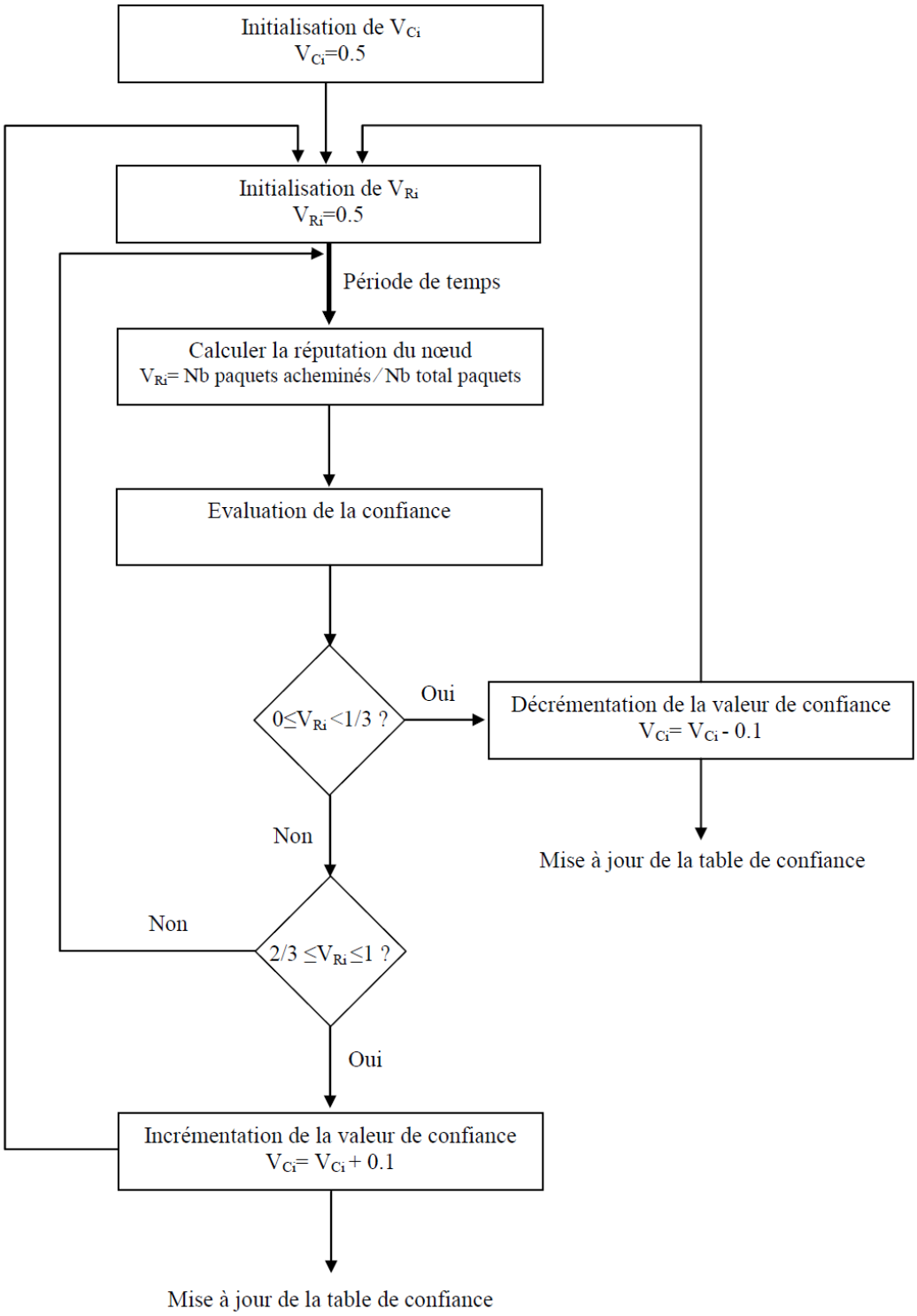


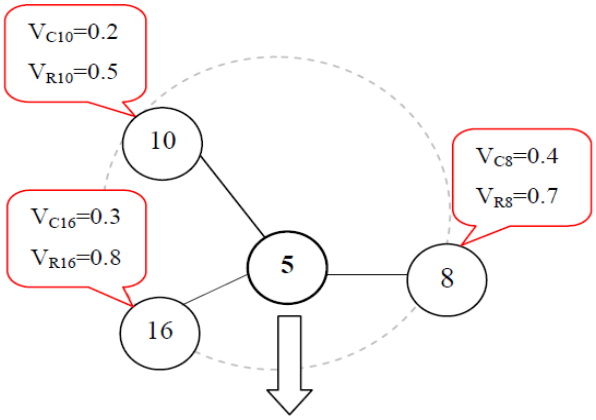
Figure III.5. Algorithme d'évaluation de la confiance d'un nœud.

La valeur de confiance V_{Ci} générée par cet algorithme est directement liée à la réputation (V_{Ri}). Cette valeur augmentera pour un nœud faisant preuve d'un bon comportement et d'une certaine coopérativité et démunira dans un cas contraire.

III.3.4.3 Modification de la table de voisins

Pour trouver la route de confiance qui mène vers la destination, le nœud source doit connaitre au préalable les valeurs de confiance de chaque nœud de cette route. Pour ce faire, on propose d'augmenter la table de voisins de chaque nœud de deux champs qui sont respectivement, la valeur de confiance (V_{Ci}) et la valeur de réputation (V_{Ri}).

Ainsi, chaque nœud capteur du réseau contiendra une table qui sauvegarde à la fois, la liste de ses voisins ainsi que les valeurs de confiance et de réputation associées à chacun d'eux. Et cette table sera mise à jour dynamiquement à chaque nouvelle période pour réévaluer les valeurs de réputation et de confiance de N_i, et à chaque fois qu'un nouveau nœud est ajouté au voisinage.



Nœuds voisins	V_{Ci}	V_{Ri}
10	0.2	0.5
16	0.3	0.8
8	0.4	0.7

Figure III.6. Table de voisins avec les valeurs de confiance et de réputation.

III.3.4.4 Calculer la confiance de route

Initialement, avant de calculer la confiance de route, notre modèle de confiance suppose qu'il existe entre chaque couple de nœud émetteur et récepteur au moins deux routes afin de différencier les routes en termes de valeur de confiance.

Ainsi, pour calculer la confiance de route (C_{Ri}), on intègre dans les paquets RREP un compteur « n » de nombre de sauts avec une valeur initiale zéro et la valeur de confiance de route (C_{Ri}) qu'on calcule avec la formule ci-dessous, en récupérant au préalable, au niveau de chaque nœud traversé sa valeur de confiance (V_{Ci}).

$$C_{Ri} = {}^{1}/_{n} \sum_{i=1}^{n} Vci \quad \ldots(2)$$

De même, chaque message RREP va subir le même traitement au niveau de chaque nœud et la valeur C_{Ri} qui se cumule au fur et à mesure, durant la propagation des RREP, elle sera sauvegardée dans la table de routage du nœud courant.

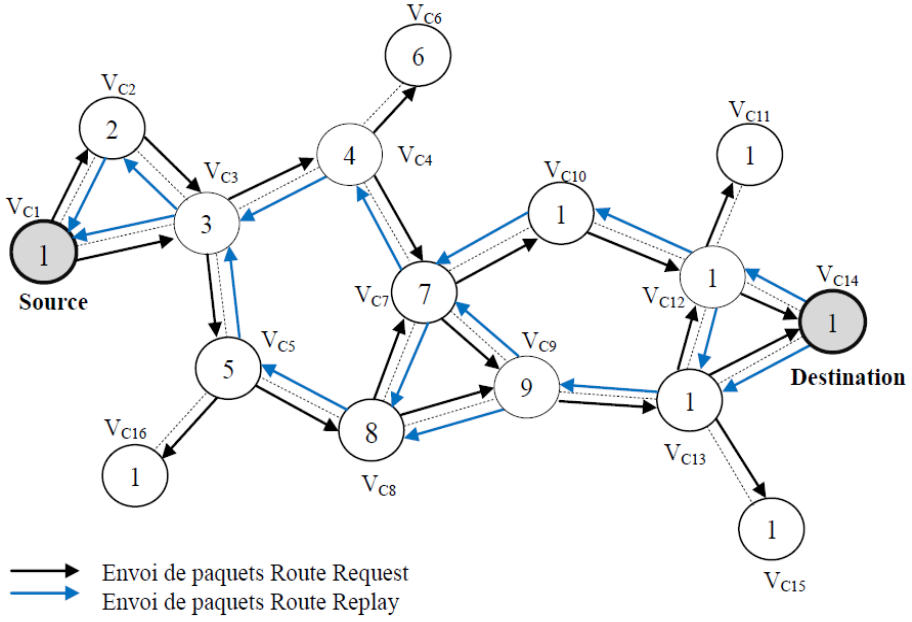


Figure III.7. Découverte de routes.

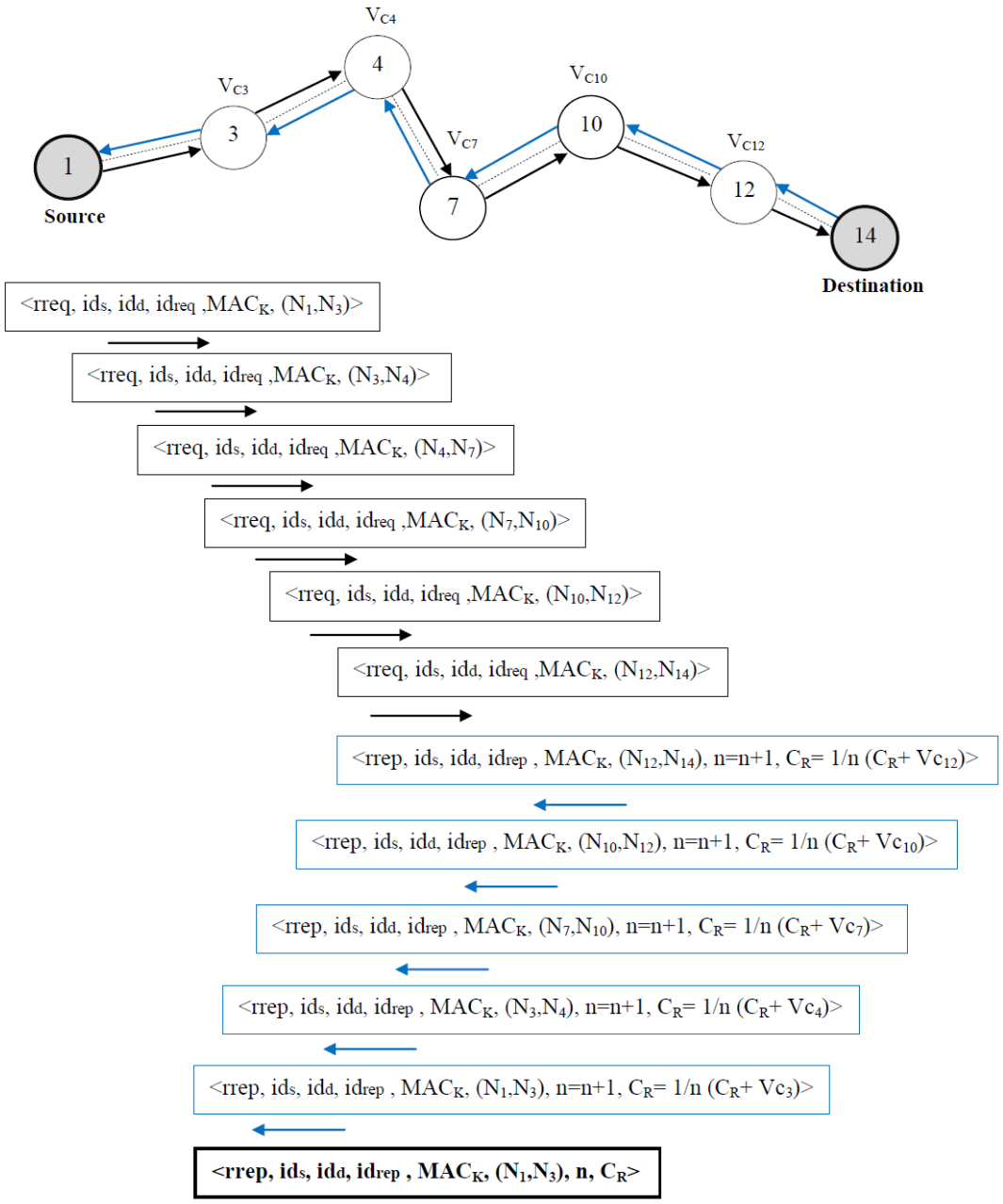


Figure III.8. Calcule de la confiance d'une route.

id_s : Adresse du nœud source.

id_d : Adresse du nœud de destination.

id_{rep} : Identifiant de la requête.

MAC_{ki} : Code d'authentification de nœud.

C_{Ri} : Confiance de route.

Le fait d'intégrer le calcul de la confiance de route dans les messages RREP, permet d'une part d'envoyer les données à travers la route ne comportant que des nœuds ayant un bon comportement, et d'autre part, de réduire sensiblement la charge du réseau et la consommation inutilement de l'énergie par les nœuds capteurs.

III.3.4.5 Choix de la route

Pour découvrir la route la plus sécurisée (valeur de confiance élevée) qui mène vers une destination D, le nœud source, attend l'arrivée des messages RREP avec les valeurs de la confiance des routes, puis il met à jour sa table de routage. Ainsi, pour effectuer son choix, il compare ces différentes valeurs de confiance de routes, puis dirige le paquet à transmettre que vers le nœud voisin dont le degré de confiance est supérieur aux autres. De même, le nœud source fera le même traitement à chaque saut en acheminant au fur et à mesure ces paquets à travers la route jugée fiable avec un grand niveau de confiance et une grande certitude.

Dans la figure précédente, en comparant, au fur et à mesure la valeur C_{Ri} à chaque saut, le nœud N_1 choisit la route <1; 2 ; 3 ; 4 ; 7 ; 10 ; 12 ; 14> pour envoyer ses données au nœud N_{14}, car c'est la route la plus confiante et la plus fiable.

III.4 Gestion des comportements des nœuds

Comme on l'a dit précédemment, dans un réseau de capteurs, les nœuds peuvent facilement devenir non fiables et avoir un mauvais comportement influençant négativement l'opération de routage dans le réseau. Pour gérer cela, on propose d'observer et d'analyser les comportement des nœud dans le réseau en se basant sur la confiance et la réputation, puis on calcule la moyenne de la confiance et de la réputation de telle façon qu'elle puisse fournir une estimation la plus juste possible du comportement du nœud. Pour détermine son statut dans le réseau et décider par la suite de sa punition ou de sa récompense.

Ainsi, si un nœud veut transmettre ses propres paquets à travers le réseau, il a tout intérêt à afficher ses bonnes intentions en coopérant au processus de routage dans le réseau. Cependant, il est clair qu'un nœud malveillant n'ayant pas spécialement besoin ou envie de transmettre son propre trafic peut très bien avoir un comportement malveillant tout à fait gratuit.

Pour ce faire, on calcule pour chaque nœud le rapport entre la confiance et la réputation comme suit :

$$R\ (V_{Ci}, V_{Ri}) = \frac{V_{Ci} + V_{Ri}}{2} \quad \ldots(3)$$

A partir de la valeur trouvée dans (3), on décide du nombre de paquet à transmettre pour ce nœud en considérant ce nombre en pourcentage comme suit :

- Si $\mathbf{R\ (V_{Ci}, V_{Ri}) = 0.5}$ alors **Nbp= 50%** (on achemine la moitié des paquets du nœud).
- Si $\mathbf{R\ (V_{Ci}, V_{Ri}) > 0.5}$ alors **Nbp=100%** (on achemine la totalité des paquets du nœud).
- Si $\mathbf{R\ (V_{Ci}, V_{Ri}) < 0.5}$ alors $\mathbf{Nbp = V_{Ci} * 100}$ (on achemine les paquets du nœud en fonction de sa valeur de confiance).

Une telle idée permet d'obliger l'ensemble des nœuds à coopérer et avoir un bon comportement du point de vue de la retransmission des paquets. Il s'agit donc bien dans ce cas là de rendre le routage performant et résistant à l'action des nœuds malveillants.

III.5 Exemple applicatif

Soit l'exemple suivant (figure) illustrant le déroulement de notre modèle de confiance pour sécuriser le routage des données dans un réseau de capteurs.

Etape 1

- On déploie aléatoirement un RCSF avec 14 nœuds.
- Chaque nœud du réseau commence avec une confiance moyenne et une réputation moyenne (V_{Ci}=0.5 et V_{Ri}=0.5).
- Après chaque période de temps, les valeurs V_{Ci} et V_{Ri} seront recalculées.

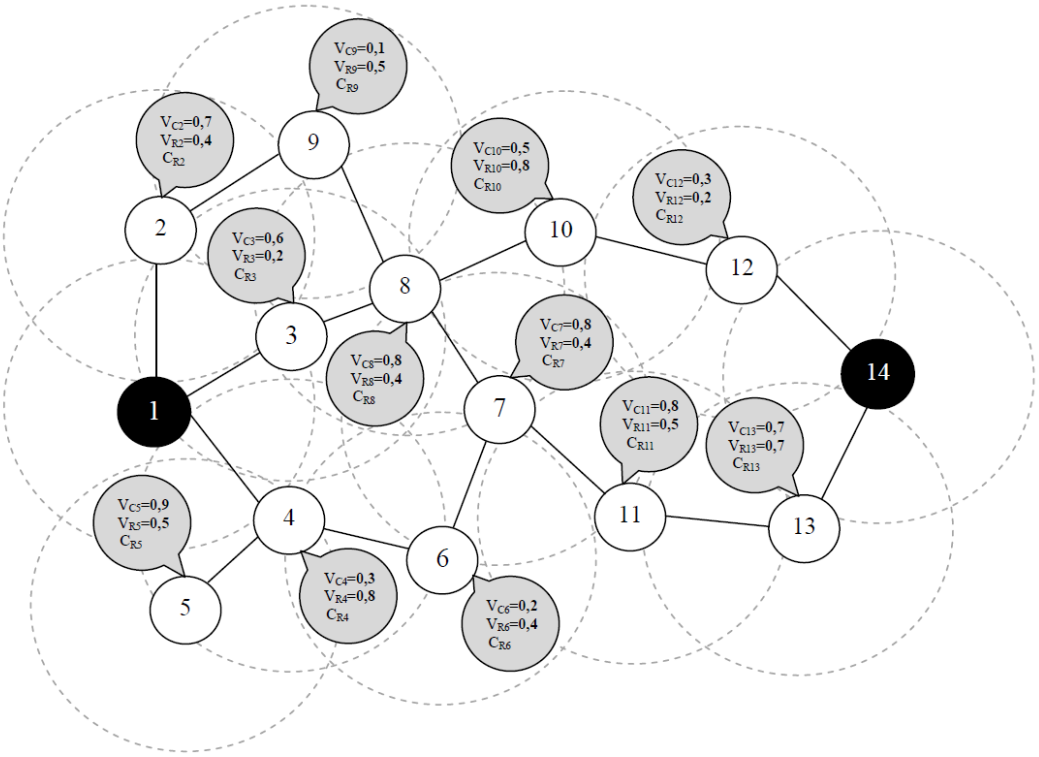


Figure III.9. Déploiement de quelques capteurs.

Etape 2

- On suppose, que le nœud 1 veut envoyer des données au nœud 14.
- Le nœud 1 initie une découverte de routes en envoyant des paquets RREQ.
- Chaque nœud qui reçois le paquet RREQ le retransmet à son voisin s'il n'est pas le destinataire, jusqu'à arrivé au nœud de destination.

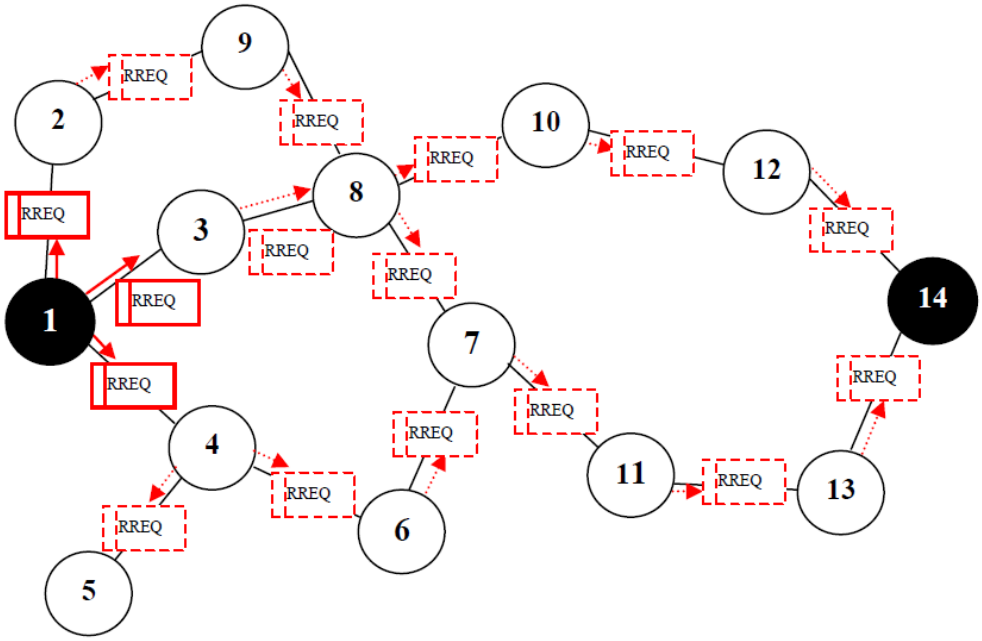


Figure III.10. Envoi de paquets RREQ.

Etape 3

- Une fois que le nœud 14 reçoit les paquets RREQ, il répond au nœud 1 par des paquets RREP.
- Les paquets RREP jusqu'à ce qu'ils arrivent au nœud 1 (la source).
- Chaque paquet RREP récupère à son passage par chaque nœud la V_{Ci}, la V_{Ri} et effectue le calcule de la C_{Ri}.

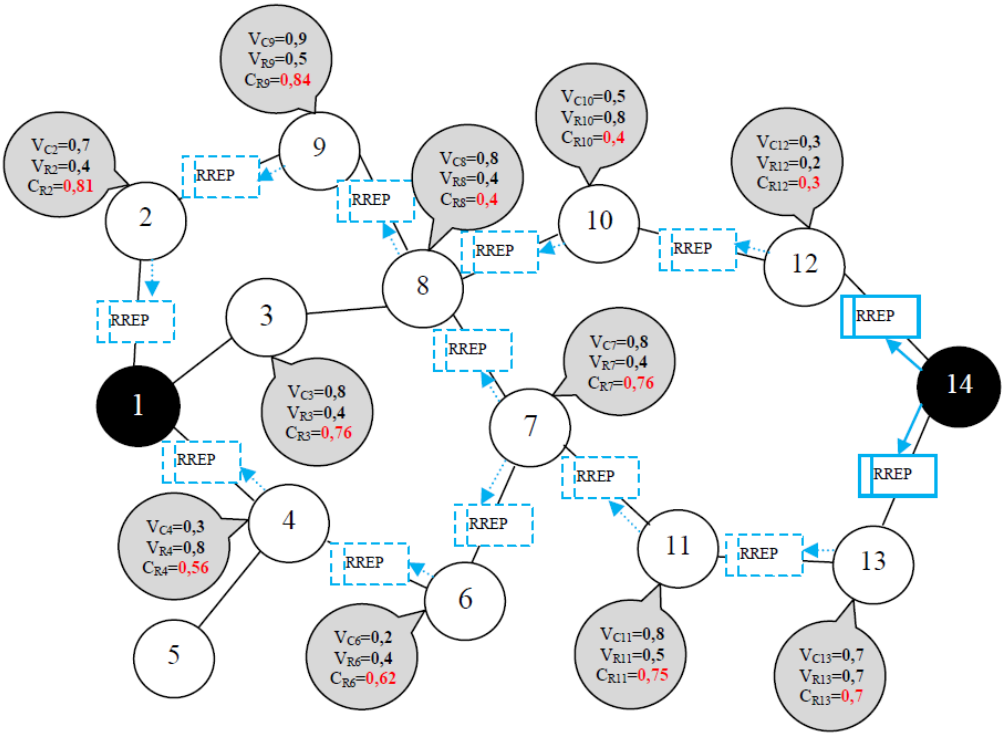


Figure III.11. Envoi de paquets RREP.

Etape 4

- Pour estimer le chemin de confiance, chaque nœud regarde dans sa table de routage puis dirige ses paquets vers le nœud dont la C_{Ri} est la plus élevée.
- Le nœud 1, regarde dans sa table de routage et compare les valeurs C_{R2} , C_{R3} et C_{R4}.
- Le nœud 1 trouve que le max (C_{R2}, C_{R3}, C_{R4})= C_{R2}
- il dirige alors ses paquets vers le nœud 2 qui jugé de confiance.
- Arrivés au nœud 2, celui-ci fait le même traitement que le nœud 1 pour réacheminer ses paquets.
- L'opération se répète jusqu'à ce que les paquets arrivent au nœud 14.

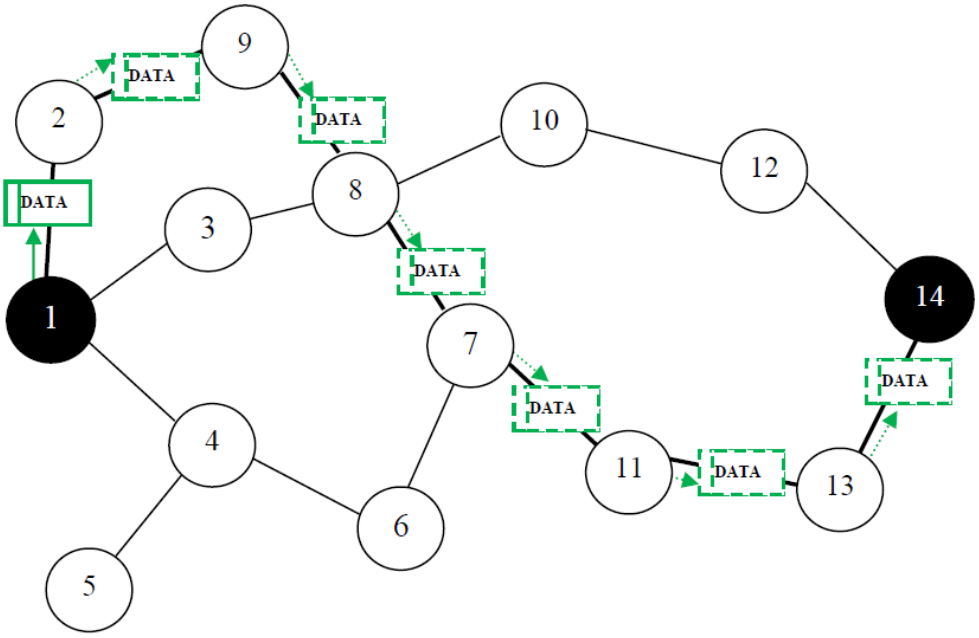


Figure III.12. Envoi des données à travers la route de confiance.

Ainsi, pour acheminer ses paquets jusqu'au nœud 14, le nœud 1 à choisit la route <1, 2, 9, 8, 7, 11, 13, 14> qui est jugée de confiance et plus sécurisée.

III.6 Routage basé sur le modèle de confiance

Comme les performances du routage dans un réseau de capteurs dépendent essentiellement de la coopérativité et la fiabilité des capteurs, il est important de garantir un certain niveau de sécurité. Notre modèle de confiance sera employé pour augmenter le niveau de sécurité du processus de routage dans un réseau de capteurs.

L'intégration de ce modèle de confiance à une application dans le domaine des réseaux de capteurs, apporte de nombreux avantages à savoir :

- Optimisation de la consommation d'énergie.
- Optimisation du délai de routage.

III.7 Conclusion

Le modèle de confiance qu'on a proposé, est une solution simple basée sur la gestion de la confiance de façon dynamique afin d'assurer la sécurité et le bon fonctionnement du routage des données envoyées par la source dans un réseau de capteurs en garantissant l'évolution des activités du réseau en dépit de la présence de nœuds qui ont un mauvais comportement. De plus, il offre un niveau de sécurité acceptable et adapté aux contraintes des réseaux de capteurs notamment la minimisation des coûts énergétiques dans le processus de choix de routes.

CONCLUSION GENERALE

Conclusion et perspectives

Conclusion et perspectives

Conclusion

Dans ce mémoire, on a présenté notre travail de recherche portant sur les réseaux de capteurs sans-fil. En particulier, on a choisi d'étudier la sécurité du routage, et on s'est intéressé au concept de la confiance comme une solution de sécurité. Ce concept s'adapte particulièrement à la nature mobile, dynamique, distribuée et auto-organisée des réseaux de capteurs.

La première objectif à été l'étude du routage dans les réseaux de capteurs, afin de faire ressortir ses vulnérabilités et ses besoins de sécurité dans le but de proposer par la suite une solution de sécurité pour rendre le processus de routage plus fiable et cela en exploitant des informations et des opérations déjà existantes dans le routage des réseaux de capteurs.

Notre contribution est la proposition d'un modèle basé sur le raisonnement de la confiance permettant de sécuriser l'opération de routage. Ainsi, en agissant directement sur l'étape de choix de route, notre solution permet à un nœud source de toujours diriger les données à acheminées uniquement à travers les routes dont le niveau de confiance est plus élevé que les autres. L'intégration du concept de la confiance nous permet de juger le comportement de chaque nœud et d'estimer son taux de coopération dans le processus de routage afin de valider le choix de la route pour relayer les données.

De plus, pour augmenter la portée de notre modèle de confiance et garantir autant que possible la fiabilité des nœuds, on a envisagé des contremesures permettant de sanctionner les nœuds se comportant mal au sein du réseau ou les récompenser dans le cas contraire.

En résumé, l'intégration du raisonnement de la confiance dans le routage permet d'assurer la sécurité et le bon fonctionnement des opérations de routage et de

garantir autant que possible la fiabilité des routes, en obligeant les nœuds du réseau à se comporter tel que leur rôle le préconise.

Perspectives

En perspectives, on envisage de recourir à une simulation et d'établir des exemples afin de vérifier le degré de performance de notre modèle de cofinance et mesurer l'impact de telles solutions sur les opérations de routage, tout en prenant en compte les contraintes inhérentes à un réseau de capteurs, notamment la nécessité de minimiser les coûts énergétiques, de mémoire et de communication.

Il faut aussi réfléchir en termes de nouvelles extensions du travail, de greffer notre modèle de confiance à un protocole de routage existant pour mieux analyser le modèle dans des conditions réelles.

Au final, il existe plusieurs aspects de la confiance qui n'ont pas été exploité dans ce travail. Par exemple, le concept de la confiance sociale. Cette idée pourrait être intéressante dans le contexte de certaines applications de réseaux de capteurs. Au lieu de vérifier le comportement individuel de chaque nœud, on désigne un nœud spécial qui évalue la confiance de ses voisins et génère un rapport qui permettra de décider si se nœud va participer au routage.

Enfin, pour clore ce mémoire, on espère que notre étude trouvera un bon écho et formeront un petit noyau de recherche pour tout intéressé par la sécurité du routage dans les réseaux de capteurs.

Bibliographie

[1]. E. DHIB, *Routage avec QoS temps réel dans les réseaux de capteurs*, mémoire, Ecole supérieur des communications de Tunisie, 2006/2007.

[2]. F.Z. BENHAMIDA, *Tolérance aux pannes dans les réseaux de capteurs sans-fil*, mémoire, Ecole Nationale Supérieure en Informatique Alger, 2008/2009.

[3]. S. MOAD, *La consommation d'énergie dans les réseaux de capteurs sans-fil*, Etude bibliographique, IFSIC-Rennes 1, 2007/2008.

[4]. M.M. DIOURI, *Réseaux de capteurs sans-fil: routage et sécurité*, mémoire, INSA de Lyon, 2009/2010.

[5]. G. SHARMA, *Routing in wireless sensor networks*, Master of Engineering, university Patiala, 2009.

[6]. K. BADER, *Détection d'intrusions dans les réseaux de capteurs sans-fil*, Rapport de stage, IFSIC-Rennes 1, 2009/2010.

[7]. M. OULARBI et S. KASSAB, *Elaboration d'un protocole de routage efficace en énergie pour réseaux de capteurs sans-fil*, mémoire, ESI, 2009/2010.

[8]. N. LASLA, *La gestion de clés dans les réseaux de capteurs sans-fil*, mémoire, I.N.I, 2006/2007.

[9]. M.L. MESSAI, *Sécurité dans les Réseaux de Capteurs Sans-fil*, Mémoire, Université de Bejaia, 2007/2008.

[10]. L. ZIANE KHODJA, *La structuration et la sécurisation des réseaux de capteurs*, IFSIC de Lyon ,2010.

[11]. S. ATHMANI, *Protocole de sécurité pour les réseaux de capteurs sans-fil*, mémoire, Université Batna, 2010.

[12]. A. BADAOUI et Y. KHENFOUCI, *Approche d'authentification dans les réseaux de capteurs pour la pédagogie*, mémoire, E.S.I, 2008/2009

[13]. A. BERRACHEDI et A. DIARBAKIRLI, *Sécurisation du protocole de routage hiérarchique LEACH dans les réseaux de capteurs sans-fil*, mémoire, E.S.I, 2008/2009.

[14]. L. KHELLADI & N. BADACHE, *Les réseaux de capteurs : état de l'art, rapport de recherche*, Université de Bab Ezzouar, 2004.

[15]. L. DAUMAS & O.UBERTI, *Implémentation d'un protocole de routage dans un réseau de capteurs sans-fils*, mémoire, Université d'Avignon, 2008.

[16]. H. JMEL - M. CAUDRON - A. BRISSET - P. M. GUITARD, *Réseaux de capteurs sans-fils*, projet avancé, Université de Lyon, 2008.

[17]. J. VAUDOUR, *Élaboration de couches MAC et réseau pour un réseau de capteurs*, mémoire, Université de Toulouse, 2006.

[18]. M. Yasser ROMDHANE, *Evaluation des performances des protocoles S-MAC et Directed Diffusion dans les réseaux de capteurs*, mémoire, Ecole supérieur des communications de Tunisie, 2006/2007.

[19]. G. CHALHOUB, *Routage et MAC dans les réseaux de capteurs sans-fil*, article, 2010.

[20]. F. ABDELFATAH, *Développement d'une bibliothèque de capteurs*, rapport, Université de Montpellier, 2008.

[21]. A. LUKOSIUS, *Context Routing in Wireless Sensor Networks*, projet de master, Université of Bremen, 2006.

[22]. A. BEGHRICHE, De *la Sécurité à la E-Confiance basée sur la Cryptographie à Seuil dans les Réseaux sans-fil Ad hoc*, mémoire, Université de Batna, 2008/2009.

[23]. H. ABROUG, *Architecture pour la localisation et l'isolement des nœuds corrompus dans un réseau Ad Hoc*, mémoire, ESCT, 2004/2005.

[24]. P. SONDI OBWANG, *Le routage à qualité de service dans les réseaux de capteurs*, thèse, Université de Valenciennes, 2010.

[25]. M. BADRA, *Le transport et la sécurisation des échanges sur les réseaux de capteurs*, thèse, Telecom Paris, 2009.

[26]. X. XUE, *Mécanismes de sécurité pour des protocoles de routage des réseaux de capteur sans-fil*, thèse, Telecom Paris, 2006.

[27]. C. BURGOD, *Contribution à la sécurisation du routage dans les réseaux de capteurs sans-fil*, thèse, Université de Limoges, 2009.

[28]. A. MAKHOUL, *Réseaux de capteurs : localisation, couverture et fusion de données*, thèse, Université de Franche-Comté, 2008.

[29]. M. LEHSAINI, Diffusion *et couverture basées sur le clustering dans les réseaux de capteurs : application à la domotique*, thèse, Université de Franche-Comté, 2009.

[30]. K. HEURTEFEUX, *Protocoles localisés pour réseaux de capteurs*, thèse, Université de Lyon, 2009.

[31]. A. BUHRIG, Optimisation *de la consommation des nœuds de réseaux de capteurs sans-fil*, thèse, Institut National Polytechnique de Grenoble, 2008.

[32]. L. SAMPER, *Modélisations et analyses de réseaux de capteurs*, thèse, Institut National Polytechnique de Grenoble, 2008.

[33]. Hung-Cuong LE, *Optimisation d'accès au médium et stockage de données distribuées dans les réseaux de capteurs*, thèse, Université de Franche-Comté, 2009.

[34]. A. BEGHRICHE et A. BILAMI, *Un modèle de confiance pour l'authentification dans un réseau sans-fil Ad hoc*, Journées Ecole Doctorale & Réseaux de Recherche en Sciences et Technologies de l'Information JED'08, Université Annaba, Juin 2008.

[35]. J-B. HUBAUX, L. BUTTYAN, V. CAPKUN, *The quest for securing in mobile Ad hoc networks, in 2nd ACM Symposium on mobile Ad hoc Networking and Computing*, Octobre 2001.

[36]. Y. CHUN HU, A. PERRIG and D.B. JOHNSON, ARIADNE, *A secure on-demand routing protocol for Ad hoc networks*, Proceedings of the 8th ACM International Conference on Mobile Computing and Networking, 2002.

[37]. B. DAHILL, B. LEVINE, E. ROYER, C. SHIELDS, *A Secure Routing Protocol for Ad hoc Networks*, Proceedings of the 10th Conference on Network Protocols (ICNP), November 2002.

[38]. M. BEGHRICHE et A. BILAMI, *De la sécurité à la e-confiance dans les réseaux sans-fil Ad hoc*, 1st Workshop on Next Generation Networks: Mobility (IEEE WNGN 2008), Fès Maroc, 2008.

[39]. P. MICHIARDI, R. MOLVA, *Core: A Collaborative Reputation Mechanism to Enforce node Cooperation in Mobile Ad hoc networks*, in Communication and Multimedia Security 2002 Conference, 2002.

[40]. V. LEGRAND et S. UBEDA, *Vers un modèle de confiance pour les objets communicants : une approche sociale*, Centre d'Innovations en Télécommunications & Intégration de services CITI INRIA ARES, INSA de Lyon, mars 2004.

[41]. V. LEGRAND, F. NAIT-ABDESSELEM, et S. UBEDA, *Etablissement de la confiance et réseaux Ad hoc : un état de l'art*, dans 2ème rencontre francophone sur Sécurité et Architecture Réseaux, Nancy France, 2003.

[42]. V. LEGRAND, D. HOOSHMAND, and S. UBÉDA, *Trusted ambient community for self-securing hybrid networks*, INRIA, Research Report 5027, 2003.

[43]. Lin CHEN, *Les comportements égoïstes et malveillants dans les réseaux sans-fil*, thèse, Télecom Paris, 2008.

[44]. H. ASMAA ADNANE, *La confiance dans le routage Ad-hoc*, thèse, Université Rennes, 2008.

[45]. V. LEGRAND, S. GALICE, S. UBEDA, *Identification pour les réseaux spontanés*, article, Laboratoire CITI - INRIA ARES, Université de Lyon, 2008.

[46]. S. GALICE, M. MINIER et S. UBEDA, *Gestion de la confiance dans les communautés Ouvertes*, article, Centre d'Innovations en Télécommunications et Intégration de services CITI/INSA-Lyon - INRIA/ARES, 2009.

[47]. C.T. PHAN LE, *Utilisation de la notion de confiance dans les organisations*, Rapport de stage, Université de Rennes, 2008.

[48]. J. ROUCHIER, *La confiance à travers l'échange*, PhD thesis, Université de Montpellier, 2000.

[49]. J. SABATER and C. SIERRA, Reputation *and social network analysis in multi-agent systems*, In Proceedings of the first international joint conference on Autonomous agents and multiagent systems, ACM Press, 2002.