REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

Université Mouloud Mammeri de Tizi-Ouzou

FACULTE GENIE ELECTRIQUE ET INFORMATIQUE

DEPARTEMENT INFORMATIQUE

Mémoire de fin d'études

En vue de l'obtention du Diplôme Master II en Informatique

Spécialité : Réseaux Mobilité et Systèmes Embarqués(RMSE)

Mécanisme léger de gestion de la confiance dans les RCSFs

Réalisé par :

M^{elle} CHERIF Amina

M^{elle} AIMEUR Chahrazed

Encadré par :

2012/2013

Résumé

Les réseaux de capteurs sans fil sont composés d'un grand nombre de nœuds capteurs déployés d'une manière dense et aléatoire dans un environnement pour collecter, traiter et transmettre des données vers la destination finale. La communication entre les nœuds est sans fil ce qui nécessite l'élaboration des protocoles de routage efficaces afin d'assurer le bon fonctionnement du réseau. Cela n'est pas suffisant car l'environnement de déploiement est souvent hostile ce qui rend le réseau vulnérable à plusieurs attaques des nœuds malicieux. Aussi, la consommation d'énergie et les capacités de calcul et stockage limitées favorisent l'apparition de mauvais comportements tels que l'égoïsme.

Ces mauvais comportements ne peuvent pas être détectés ou traités par les mécanismes de sécurité traditionnels d'où la nécessité d'élaborer d'autres solutions. La confiance est l'une de ces solutions, elle consiste à détecter les mauvais comportements en observant les interactions entre les nœuds.

Dans ce mémoire, nous nous sommes intéressés à l'un des protocoles de routage non sécurisé : EAR, nous avons introduit sur ce dernier un mécanisme léger de gestion de la confiance, cela nous a permis de mettre en place un nouveau protocole de routage sécurisé : TEAR.

Sommaire

Résumé ..... **VI**

Liste des figures ..... **X**

Liste des tableaux ..... **XI**

Introduction Générale **1**

Chapitre 1: Généralités sur les réseaux de capteurs **3**

1.1 Introduction 4

1.2 Capteur 4

1 .2.1 Définition d'un capteur 4

1.2.2 Architecture d'un nœud capteur 6

1.2.3 Système d'exploitation d'un capteur 7

1.3 Réseaux de capteur sans fil 7

1. 3.1 Caractéristiques des réseaux de capteurs sans fil 8

1.3.2 Communication dans les réseaux de capteurs sans fil 11

1.4 Domaines d'application des réseaux de capteurs sans fil 14

1.5 Axes de recherche pour les réseaux de capteurs sans fil 18

1.6 Conclusion 20

Chapitre2 : Routage dans les RCSFs **21**

2.1 Introduction 22

2.2 Facteurs de conception d'un protocole de routage 22

2.2.1 Déploiement des nœuds 22

2.2.2 Consommation énergétique 22

2.2.3 Modèle de livraison de données 23

2.2.4 Mobilité 23

2.2.5 Hétérogénéité des nœuds 23

2.2.6 Tolérance aux pannes 24

2.2.7 Scalabilité 24

2.2.8 Agrégation de données 24

2.2.9 Qualité de service 24

2.2.10 Connectivité 24

2.3 Métrique de routage 24

2.3.1 Consommation d'énergie 25

2.3.2 Nombre de sauts 25

2.3.3 Taux de perte de paquets de données 25
2.3.4 Délai de bout en bout 25
2.4 Classification des protocoles de routage 25
2.4.1 Classification selon la topologie du réseau 27
2.4.2 Classification selon le fonctionnement du protocole 28
2.4.3 Classification selon l'établissement des chemins 29
2.4.4 Classification selon l'initiateur de communication 29
2.5 Conclusion 32
Chapitre 3 : Confiance dans les RCSFs 33
3.1 Introduction 34
3.2 Définition de la confiance 34
3.2.1 Dans les réseaux sociaux et psychologie 34
3.2.2 Dans les réseaux informatiques 35
3.3 Caractéristiques de la confiance 35
3.3.1 La subjectivité 35
3.3.2 La confiance est liée à un risque 35
3.3.3 La non-transitivité 35
3.3.4 La dynamicité 35
3.3.5 L'asymétrie 35
3.3.6 Réflexivité (l'auto-confiance) 35
3.4 Confiance et sécurité dans les RCSFs 36
3.5 Gestion de la confiance dan les RCSFs 37
3.5.1 Etablissement de la confiance 38
3.5.2 Métriques d'évaluation de la confiance 38
3.5.3 Systèmes de gestion de la confiance 39
3.6 Quelques approches existantes sur la gestion de la confiance dans les RCSFs 41
3.6.1 Reputation based Framework for high integrity Sensor Networks (*RFSN*) 41
3.6.2 Group-Based Trust Management Scheme (*GTMS*) 43
3.6.3 Trust Based Routig (*TBR)* 46
3.6.4 Trusted Multi Wireless Agent Communication (*TMWC*) 48
3.6.5 A centralized Trust And Competence-based Energy-efficient routing scheme for wireless sensor networks (*TRACE*) 52
3.6.6 Trust-Aware Routing Framework (*TARF*) 54
3.6.7 Trust-aware Sensor Network Information Protocol for Efficient Routing (*T-SNIPER)* 56

3.6.8 Un mécanisme de routage sécurisé pour réseaux de capteurs sans fil statiques 57
3.6.9 Implémentation d'un protocole de routage basé confiance dans les nœuds capteurs sans fil 59
3.7 Conclusion 61
Chapitre 4 : Contribution 62
4.1 Introduction 63
4.2 Description de l'algorithme EAR 63
4.2.1Phase d'installation 63
4.2.1Phase communication de données 65
4.2.3 Phase de maintenance 66
4.3 Description de l'algorithme TEAR 66
4.3.1 Mécanisme de surveillance 66
4.3.2 Calcul de la confiance 67
4.3.3 Mis à jour de la confiance 67
4.3.4 Intégration de la confiance dans la phase de transmission 67
4.4 Conclusion 67
Chapitre5 : tests 68
5.1 Introduction 69
5.2 Quelques environnements de simulation 69
Nous citons dans ce qui suit quelques environnements de simulation : 69
5.2.1 Network simulator(NS2) 69
5.2.2 GLOSSIM 70
5.2.3 TOSSIM 71
5.2.4 OMNET++ 71
5.3 Simulateur OMNET++ 72
5.3.1 Fonctionnement 72
5.3.2 Plateforme 73
5.4 Tests et discussion des résultats 74
5.4.1 Critères de performance 75
5.4.2 Scenario de simulation 75
5.4.3 Discussion des résultats 75
5.5 Conclusion 76
Conclusion générale 77
Bibliographie 79

Liste des figures

Fig.1 : Exemples de modèles de capteurs sans fil…….. 5

Fig.2 : Architecture d'un nœud capteur……. 6

Fig.3 : Architecture d'un réseau de capteurs sans fil……. 8

Fig.4 : couverture d'un nœud capteur…….. 10

Fig.5 : pile protocolaire dans un RCSF…….14

Fig.6 : application dans le domaine médical.....…...16

Fig.7 : applications dans le domaine environnemental.....…...16

Fig.8: application dans le domaine militaire.....…...16

Fig. 9 : Classification des protocoles de routage pour les RCSFs ……...24

Fig. 10: Classes principales des protocoles de routage pour les RCSFs …..……..25

Fig. 11 : Sous classes des protocoles de routage pour les RCSFs ……..……25

Fig.12: classification des protocoles de routages dans les RCSFs……26

Fig.13 : Schéma des mauvais comportements dans un RCSF……..36

Fig.14 : Architectures des systèmes de gestion de confiance et de réputation…….39

Fig.15: Schéma du système de gestion de la confiance RFSN…… 40

Fig.16: Fenêtre de temps pour calculer l'intervalle de temps ……..42

Fig.17: Schéma de la plateforme TARF……...53

Fig.18 : modèle d'évaluation de confiance utilisé par TARF……...54

Fig.19: schéma de gestion de la confiance……58

Fig.20 : Organigramme de la phase installation dans EAR……... 64

Fig.21 : Organigramme de la phase communication de données dans EAR……...65

Fig.22 : plateforme de simulation……71

Fig.23 : graphes des paquets de données reçus avec succès……74

Liste des tableaux

Tab.1 : Caractéristiques de quelques modèles de capteurs sans fil…….....5

Tab.2 : Comparaison entre RCSFs et Ad-Hoc……..11

Tab.3**:** Tableau comparatif entre Bluetooth et ZigBee ……16

Tab.4 : Exemples de protocoles de routage dans les RCSFs et leurs classification.....29

Tab.5 : Métriques d'évaluation de la confiance, comportements et attaques …….....38

Tab.6 : Avantages et inconvénients des systèmes de gestion de la confiance dans les RCSFs……...39

Tab.7 : Estimation de la confiance dans TMWAC……...47

Tab.8 : Mis à jour de la confiance dans TMWAC……....48

Tab.9 : Métriques d'évaluation de la confiance……... 53

Tab.10: Liste des métriques de confiance……58

Tab.11 : Paramètres de simulation…….74

Introduction Générale

L'intérêt croissant des réseaux de capteurs sans fil(RCSFs) peut se justifier simplement par ce qu'ils sont : un grand nombre de nœuds capteurs de taille miniature, autonomes, à faible coût et multifonctionnels. Ces derniers sont déployés d'une manière aléatoire et dense dans des environnements parfois hostiles auxquels l'homme n'a pas accès. En raison de leurs caractéristiques intéressantes, les réseaux de capteurs peuvent être utilisés dans divers domaine tels que la gestion des catastrophes, la protection des frontières, la santé, le domaine militaire,…etc.

Dans un RCSFs, chaque nœud capteur a la possibilité d'accomplir trois taches : détecter les informations du phénomène observé, les traiter puis les communiquer a un autre nœud capteur à l'intérieur de sa zone de couverture via des ondes radio(communication sans fil) jusqu' a atteindre la destination finale qui est la station de base(*sink*). Par conséquent, la communication entre les nœuds d'un RCSF doit être régie par un ensemble de règles (protocoles) afin de leur permettre de fonctionner correctement, différents protocoles de routage ont été proposés. Les concepteurs lors de la conception d'un protocole de routage ; considèrent l'architecture et les exigences de l'application ainsi que les caractéristiques de nœuds capteurs.

Bien que les réseaux de capteurs sans fil continuent à évoluer et leur champ d'application à s'étendre, la liste des attaques internes et externes augmente. C'est la raison pour laquelle assurer la sécurité dans ce type de réseaux devient un enjeu très important. Toutefois, en raison des caractéristiques et contraintes des RCSFs, la sécurité pose des défis différents de ceux utilisés dans les réseaux traditionnels et ce notamment en ce qui concerne le bon acheminement des données vers la station de base, un nœud capteur peut présenter un comportement malicieux ou égoïste. Pour lutter contre ce genre de comportements, une solution a été proposée et qui repose sur l'utilisation des systèmes de gestion de confiance. Le mécanisme de gestion de la confiance peut être utile pour détecter les nœuds avec un mauvais comportent (égoïste ou malveillant) et pour faciliter le processus de prise de décision.

Notre travail se focalise sur l'étude de la confiance dans les RCSFs, puis introduire un mécanisme de gestion de la confiance dans un protocole de routage non sécurisé « EAR ».

Notre mémoire est organisé en cinq chapitres :

Le premier chapitre intitulé « Généralités sur les réseaux de capteurs sans fil » : est une introduction aux réseaux de capteurs sans fil. Nous y décrirons leurs caractéristiques, leurs architectures et leurs domaines d'applications.

Dans le deuxième chapitre intitulé « Routage dans les réseaux de capteurs sans fil » : nous nous intéresseront au routage dans les réseaux de capteurs sans fil. Nous allons détailler les

facteurs intervenant lors de la conception d'un protocole de routage, les métriques à prendre en considération, ainsi qu'une classification de ce type de protocoles.

Le troisième chapitre intitulé « La confiance dans les réseaux de capteurs sans fil » : est consacré à étudier le mécanisme de confiance. Nous définirons la confiance, ses caractéristiques et sa gestion dans les RCSFs.

Au quatrième chapitre intitulé « Contribution» : nous expliquerons le fonctionnement du protocole EAR, ensuite nous détaillerons le mécanisme de gestion de la confiance que nous proposons afin de l'améliorer.

Le cinquième et dernier chapitre intitulé « Tests », traite des simulations auxquelles nous avons procédés et des résultats que nous avons obtenus. Nous terminerons par une conclusion générale et quelques perspectives.

Chapitre 1

Généralités sur les réseaux de capteurs

1.1 Introduction

Les progrès dans les communications sans fil ont permis de développer des réseaux de capteurs sans fil (RCSFs) constitués de petits appareils, qui captent de l'information et collaborent les uns avec les autres pour la transmettre à la destination finale. Aujourd'hui, les réseaux de capteurs sans fil sont largement utilisés dans les zones commerciales et industrielles comme par exemple surveillance de l'environnement, la surveillance de l'habitat, la santé, la surveillance de processus, domaine militaire. L'utilisation des réseaux de capteurs sans fil augmente de jour en jour et en même temps elle est confrontée au problème de contraintes énergétiques en termes de durée de vie de la batterie limitée. Comme chaque nœud dépend de l'énergie pour ses activités, cela est devenu un enjeu majeur dans les réseaux de capteurs sans fil. Les RCSFs présentent de nombreux avantages notamment un coût réduit et une grande flexibilité.

1.2 Capteur

Avant la révolution des télécommunications et le développement des technologies sans fil, l'acheminement de l'information relevée par un capteur se faisait par un système de câblage coûteux, encombrant et nécessitant la mobilisation d'efforts humains relativement importants. Le spectre d'utilisation des capteurs restait très limité. Pour justifier le déploiement d'un réseau de capteurs, il fallait un très grand enjeu sécuritaire ou des perspectives de profits économiques importants.

À présent, l'intégration de capteurs et de communications sans fil a conduit à la naissance d'une nouvelle gamme de dispositifs électroniques ouvrant la voie à de nouvelles applications basées sur des capteurs sans fil, dotés de circuits « radio » leur permettant de transmettre et de recevoir de l'information sans avoir besoin de connexions filaires rigides.

1 .2.1 Définition d'un capteur

Un capteur (senseur) est un petit dispositif électronique autonome capable de transformer une grandeur physique observée (qui sera captée de l'environnement) en une grandeur utilisable qui sera à son tour traduite en une donnée binaire ; cette dernière pourra être mémorisée, traitée, transmise pour être exploitée avec d'autres informations. Parmi les différents types de mesures enregistrées par les capteurs, on peut citer entre autres : la température, l'humidité, la luminosité, l'accélération, la distance, les mouvements, la position, la pression, la présence d'un gaz, la vision (capture d'image) et le son... etc.

La plupart des capteurs dépendent de l'application pour lesquels ils ont été conçus (capteurs aquatiques, sous-terrain, etc ...) .Dans le monde, il existe plusieurs fabriquant de capteurs dont on peut citer :

- Crossbow (appelé aussi Xbow).
- Cisco.
- DASA.
- EuroTherm.
- Sens2B.

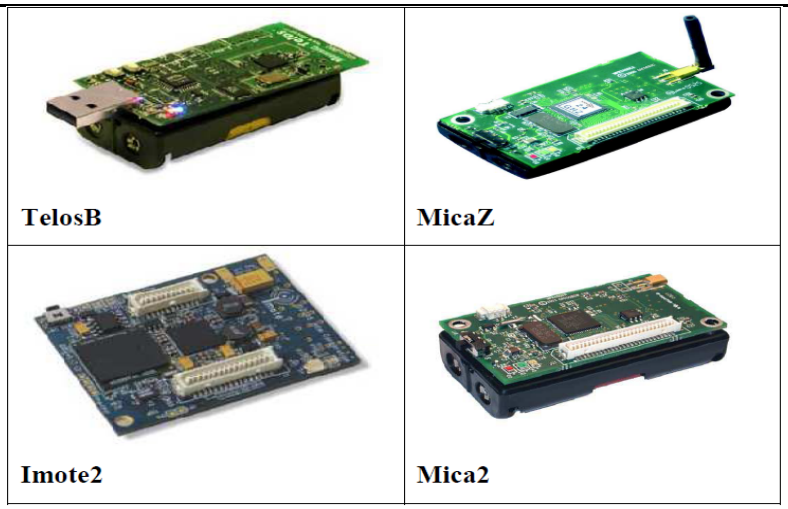

Fig.1 : Exemples de modèles de capteurs sans fil.

Le tableau suivant illustre différents capteurs et leurs caractéristiques :

			
Identification	**Mica2Dot (MPR500CA)**	**Mica2(MPR400CA)**	**Tmote Sky**
Microcontrôleur	ATmega128L	ATmega128L	MSP430F
Architecture	8-Bit	8-Bit	16-Bit
Fréquence	4MHz	7.3728MHz	8MHz
Mémoire de programmation	128Ko	128Ko	48Ko
Mémoire de données	4Ko	4Ko	10Ko
Mémoire de stockage	512Ko	512Ko	1024Ko
Module radio	CC1000	CC1000	CC2420
Bande de fréquence	315-916MHz	315-916MHz	2.4GHz
Débit maximal	38.4Kb /s	38.4Kb /s	250Kb /s

Tab 1. Caractéristiques de quelques modèles de capteurs sans fil [GIL 08]

1.2.2 Architecture d'un nœud capteur

Un nœud capteur est composé de quatre unités de base :

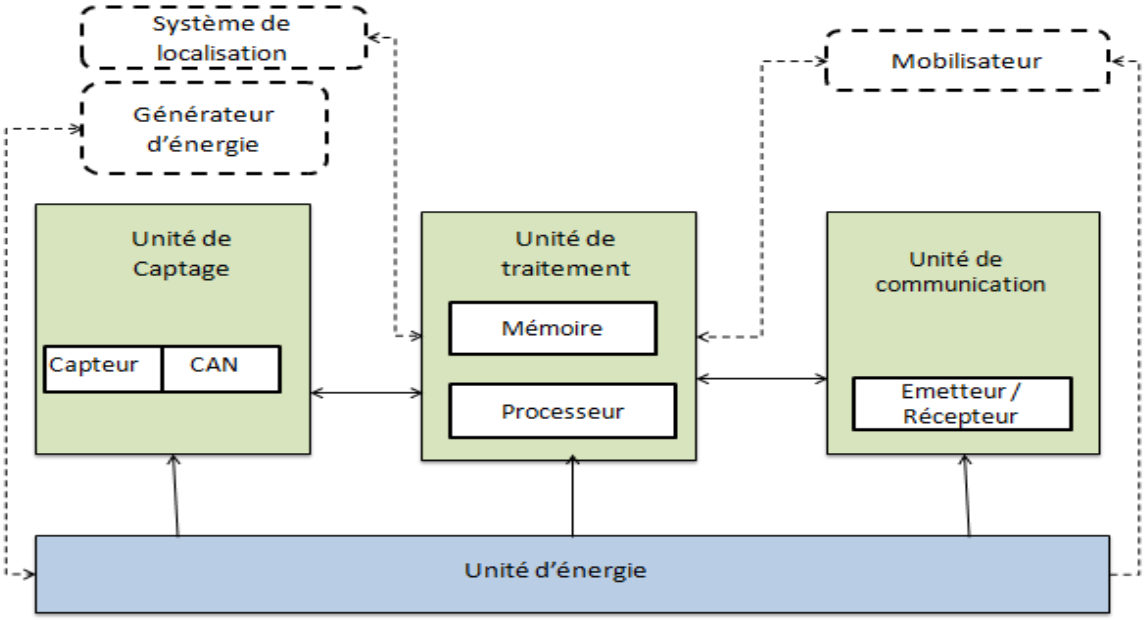

Fig.2 : Architecture d'un nœud capteur

Unité de captage (d'acquisition de donnée)

Elle est généralement composée de deux sous –unité : un capteur permettant de capter la donnée dans son environnement et un convertisseur analogique / numérique (CAN). Le capteur est responsable de fournir des signaux analogiques basés sur les phénomènes observés au convertisseur, ce dernier transforme ces signaux en un signal numérique compréhensible par l'unité de traitement pour pouvoir l'analyser.

Unité de traitement de donnée

Elle est constituée d'un processeur couplé à une mémoire de stockage intégrant un système d'exploitation spécifique. Elle possède deux interfaces une pour l'unité de captage et l'autre pour l'unité de communication. Elle contrôle les procédures permettant de collaborer les nœuds avec d'autres nœuds dans le but de réaliser les tâches d'acquisition ensuite les données collectées seront stockées dans l'unité de stockage.

Unité de transmission de donnée (communication)

Elle est équipée d'un couple émetteur/récepteur, aussi appelé *transceiver*. Cette unité est responsable de toutes les communications soit émission ou réception de donnée via un support de transmission radio.

Unité d'énergie

C'est l'élément primordial de l'architecture du capteur, elle est responsable de répartir l'énergie disponible aux autres unités mais à cause de sa taille réduite, l'énergie de la batterie ou bien la pile dont il dispose est limitée et généralement irremplaçable. Pour cela l'énergie est la ressource principale qui a une influence directement sur les durées de vie des capteurs.

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

1.2.3 Système d'exploitation d'un capteur

Un système d'exploitation OS (*Operating System*) est un ensemble de programmes ayant le rôle d'interface entre les ressources matérielles d'un dispositif et les applications utilisateurs. Les systèmes d'exploitation qui sont conçus pour les réseaux de capteurs sans fil sont très différents des systèmes d'exploitation traditionnels. En raison des limites (en termes d'énergie, capacités de calcul et stockage) imposées par les capteurs, ces OS sont réduits. Il existe plusieurs systèmes d'exploitation pour les RCSFs dont nous citons : MagnetOS, Contiki, AmbientRT, TinyOS, Contiki, le plus répandu est TinyOS. [ANT08]

TinyOs

TinyOS est un système d'exploitation open source pour les réseaux de capteurs sans fil. Sa conception a été entièrement réalisée en NesC, langage orienté composant syntaxiquement proche du C. La bibliothèque de composants de TinyOS est particulièrement complète puisqu'on y retrouve des protocoles réseaux, des pilotes de capteurs et des outils d'acquisition de données. Un programme s'exécutant sur TinyOS est constitué d'une sélection de composants systèmes et de composants développés spécifiquement pour l'application à laquelle il sera destiné (mesure de température, du taux d'humidité...).

TinyOS s'appuie sur un fonctionnement évènementiel, c'est-à-dire qu'il ne devient actif qu'à l'apparition de certains évènements, par exemple l'arrivée d'un message radio. Le reste du temps, le capteur se trouve en état de veille, garantissant une durée de vie maximale connaissant les faibles ressources énergétiques des capteurs.

1.3 Réseaux de capteur sans fil

Un réseau de capteurs sans fil RCSF (*WSN* : *Wireless Sensor Network*) est un type particulier des réseaux Ad Hoc. Il est composé d'un ensemble de nœuds capteurs dont le nombre peut atteindre des centaines voire des milliers disséminés dans une zone géographique « champ de captage » afin de collecter des informations sur le phénomène observé, les traiter et les transmettre vers un nœud particulier appelé nœud puits ou station de base (*sink*) doté d'une grande capacité en terme d'énergie, mémoire et calcul, et à son tour les envoie vers l'utilisateur final via internet.

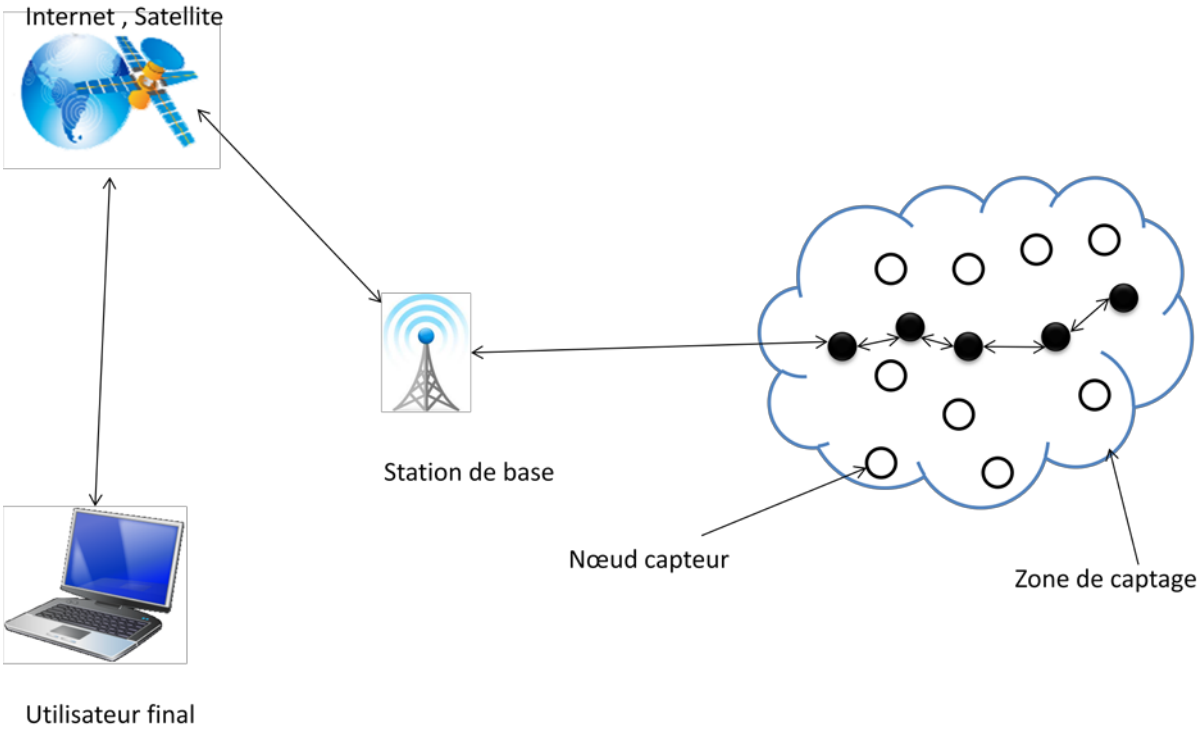

Fig.3 : Architecture d'un réseau de capteurs sans fil

1. 3.1 Caractéristiques des réseaux de capteurs sans fil

Les principales caractéristiques et contraintes [ZIA09] influençant la conception des RCSFs sont :

-Energie limitée

Dans un RCSF l'alimentation de chaque nœud est assurée par une source d'énergie limitée et généralement irremplaçable à cause de l'environnement de déploiement hostile. De ce fait, la durée de vie d'un RCSF dépend fortement de la conservation d'énergie au niveau de chaque nœud. Le mal fonctionnement d'un certain nombre de nœud entraîne un changement significatif sur la topologie globale du réseau et peut nécessiter une réorganisation totale de ce dernier.

-Auto-organisation

Les RCSFs sont des réseaux sans infrastructure fonctionnant sans intervention humaine. Cependant, les RCSFs doivent s'auto-organiser et de se modifier périodiquement de sorte qu'il puisse s'adapter aux changements de la topologie tout en assurant son fonctionnement.

-Ressources limités

Les nœuds qui composent le RCFS sont de très petite taille jusqu'à l'ordre d'une poussière (smart dust), suivant leur utilité. Par conséquent, leurs capacités de traitement, de stockage, de communication sont très limitées.

-Tolérance aux pannes

La tolérance aux pannes est définit par la capacité de maintenir les fonctionnalités du réseau même en cas de présence de pannes. Les défaillances rencontrées dans le réseau peuvent être causées par un manque d'énergie, dommage physique du capteur ou bien des interférences environnementales. Des techniques plus tolérantes doivent être appliquées afin d'assurer le bon fonctionnement du réseau.

-Scalabilité

Le nombre de nœuds capteurs peut atteindre des millions de nœuds pour permettre une meilleure granularité de surveillance. De plus, si plusieurs nœuds capteurs se retrouvent dans une région, un nœud défaillant pourra être remplacé par un autre. Le défi à relever par les RCSFs est d'être capables de maintenir leurs performances avec ce grand nombre de capteurs. Cependant, la densité de déploiement donne naissance à des challenges pour la communication entre les nœuds. En effet, elle provoque des collisions ou des endommagements des paquets transmis.

-Agrégation de donnée

La transmission des données sur les réseaux de capteurs est l'une des tâches gourmandes en consommation d'énergie. Cependant, une approche répandue consiste à agréger les données au niveau des nœuds intermédiaires.

-Médias de transmission

Les capteurs d'un RCSF sont reliés entre eux par un canal sans fil. La qualité du signal de transmission peut être dégradée à cause des collisions, des interférences, des diffractions, des réfractions, etc.

-Topologie dynamique

la topologie d'un RCSF peut être dynamique, ceci est dû à la mobilité des nœuds qui peuvent s'attacher à des objets mobiles, ou due à l'ajout ou à la suppression d'un nœud après le déploiement pour élargir le réseau ou pour remplacer les nœuds décédés ou défaillants.

-Coût de production

Les capteurs sont déployés par milliers. Cependant, leurs coûts de production doit rester aussi faible que possible. Ceci induit d'autres contraintes, principalement matérielles (faible

capacité de mémoire, faible puissance de calcul, etc.) puisque optimiser le coût de production revient à optimiser le coût des composants matériels.

-Sécurité limitée

Les RCSFs sont plus touchés par le paramètre de sécurité que les réseaux filaires classiques. Cela se justifie par les contraintes et limitations physiques qui font que le contrôle des données transférées doit être minimisé.

Le tableau suivant illustre une comparaison entre les réseaux Ad-Hoc et les RCSFs [VVS11] :

	Réseau de capteurs	**Réseau ad-hoc**
Composition	Petits micro-capteur	Portables, PDA
Flot de communication	Plusieurs à un (many to one)	Plusieurs à plusieurs (many to many)
Communication	Diffusion	Point à point
Mobilité	Mobilité faible	En constante évolution et mobilité forte
Relation entre les nœuds	Collaboration pour le même objectif	Chaque nœud à son propre objectif
Identification des nœuds	Très grand nombre de nœud n'ayant pas tous une ID	Présence de la notion d'ID
Objectif du réseau	Objectif ciblé	Générique /communication
Contrainte clé	Ressource énergétiques	Débit / QOS
Nombre de nœuds	Grand (de l'ordre de mille)	Moyen (de l'ordre de cent)
Les pannes	Plus susceptible aux pannes	Moins susceptible aux pannes
Capacité de traitement et de stockage	Moindre	Plus importante
Portée de communication	Courte	grande
Agrégation des données	Les nœuds agrègent les données	Pas d'agrégation
Standard communication	ZigBee IEEE 802.15.4 ISA100 IEEE 1451	IEEE 802.11

Tab.2: Comparaison entre RCSFs et Ad-Hoc

1.3.2 Communication dans les réseaux de capteurs sans fil

La communication dans les RCSFs est représentée par une pile protocolaire. Cette pile est utilisée par tous les nœuds capteur du réseau dans le but de standardiser la communication.

Elle comprend cinq couches et se caractérise par trois plans intégrant la prise en charge de la consommation d'énergie, la mobilité des nœuds et les traitements de données transmises dans les protocoles de routage.

1.3.2.1 Pile protocolaire

La pile protocolaire doit être conçue de sorte que le RCSF assure une bonne qualité de service et longue duré de vie. **[**ANU11]. Elle est utilisée par la station de base et tous les nœuds du réseau. La pile protocolaire combine entre la puissance et le routage et intègre des protocoles de routages. Elle est constituée des couches suivantes :

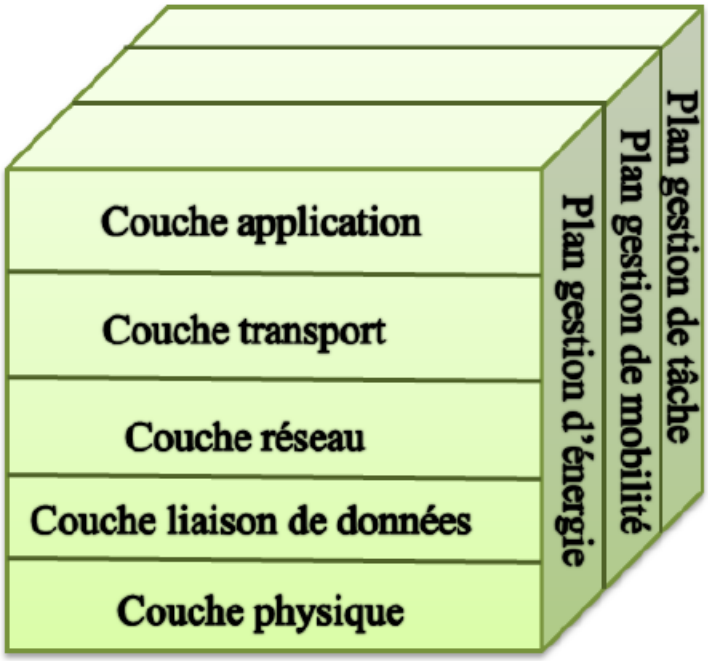

Fig.5 : pile protocolaire dans un RCSF [AKY 02]

-Couche application

Selon la tâche assignée aux capteurs, différentes applications peuvent être utilisées et bâties sur cette couche.

La couche application doit fournir des mécanismes qui permettent à l'utilisateur d'interagir avec le réseau à travers des interfaces, et éventuellement, par l'intermédiaire d'un réseau étendu (Internet à titre d'exemple), tout en restant transparente par rapport au matériel et aux

mécanismes de communication dans les couches inférieures. Parmi les protocoles d'application, nous citons : SMP (*Sensor Management Protocol*) et TADAP (*Task Assignement and Data Advertisement Protocol*) [AKY 02].

-Couche transport

Vérifie le bon acheminement des données et la qualité de la transmission, contrôle de flux, conservation de l'ordre des paquets et aussi la gestion des erreurs de transmissions.

-Couche réseau

Elle s'occupe du routage de données fournies par la couche transport. Elle établit les routes entre les nœuds capteurs et le nœud puits et sélectionne le meilleur chemin en termes d'énergie, délai de transmission, débit, etc. Les protocoles de routage conçus pour les RCSFs sont différents de ceux conçus pour les réseaux Ad Hoc puisque les RCSF sont différents selon plusieurs critères comme :

-L'absence d'adressage fixe des nœuds tout en utilisant un adressage basé-attribut.
-L'établissement des communications multi-sauts.
-L'établissement des routes liant plusieurs sources en une seule destination pour agréger des données similaires, etc.

Parmi ces protocoles, nous citons : LEACH *(Low-Energy Adaptive Clustering Hierarchy)* et SAR (*Sequential Assignement Routing*).

-Couche liaison de données

Est responsable de l'accès au media physique et la détection et la correction d'erreurs intervenues sur la couche physique. De plus, elle établit une communication saut-par-saut entre les nœuds. C'est-à-dire, elle détermine les liens de communication entre eux dans une distance d'un seul saut.

-Couche physique

Permet de moduler les données et les acheminer dans le media physique tout en choisissant les bonnes fréquences.

-Plan de gestion d'énergie

Ce plan contrôle l'utilisation de la batterie dans un nœud capteur. Par exemple, après la réception d'un message, le capteur éteint son récepteur afin d'éviter la duplication des messages déjà reçus. En outre, si le niveau d'énergie devient bas, le nœud diffuse à ses voisins une alerte pour les informer qu'il ne peut pas participer au routage et que l'énergie restante est réservée au captage.

-Plan de gestion de mobilité

Il détecte et enregistre le mouvement du nœud capteur. Ainsi, un retour arrière vers l'utilisateur est toujours maintenu et le nœud peut garder trace de ses nœuds voisins.

-Plan de gestion de tâche

Il balance et ordonnance les différentes tâches de captage de données dans une région spécifique. Il n'est pas nécessaire que tous les nœuds de cette région effectuent la tâche de captage au même temps, par contre certains nœuds exécutent cette tâche plus que d'autres selon leur niveau de batterie.

1.3.2.2. Standards de communication dans les réseaux de capteurs sans fil

Parmi les standards les plus adaptés aux RCSFs [MED10] nous citons :

La technologie Bluetooth (IEEE 802.15.1)

Ce standard de communication créé en 1994 par Ericsson, a été défini à la base pour remplacer les câbles. C'est une technologie radio courte distance, faible consommation, basée sur des puces électroniques peu coûteuses et destinées à simplifier les connexions entre appareils électroniques. Cependant, Bluetooth n'a pas seulement pour but de faire coopérer des périphériques de constructeurs différents en définissant un système de communication par ondes hertziennes sur la bande ISM7 de 2,4 GHz mais définit réellement une pile logicielle complète, contrairement à Wifi qui n'offre que le niveau 1 et le niveau 2 de la pile OSI. Elle permet aux périphériques de se découvrir et de communiquer entre eux sans savoir quels services ils offrent à la base. L'inconvénient de cette technologie est qu'elle est gourmande en énergie donc elle ne pourra pas être utilisée par des capteurs alimentés par des batteries.

La technologie ZigBee (IEEE 802.15.4)

Contrairement à la technologie Bluetooth où le débit est une priorité, l'émergence d'un nouveau type d'applications contraintes par la consommation énergétique pour une meilleure autonomie des dispositifs utilisés dans ce type de réseau a donné lieu à un nouveau standard à faible débit et à consommation réduite : IEEE 802.15.4. Ce nouveau standard, a été conçu par un groupe d'entreprises appelé la ZigBee Alliance pour connecter les dispositifs sans batterie ou contraint par leur batterie limitée en énergie.

Comme l'IEEE ne définit que la couche MAC et la couche physique, ZigBee spécifie les couches basses, MAC et physique et les couches hautes : la couche réseau et la couche allant du routage à l'application.

Ci-dessous un tableau comparatif entre les deux technologies de communications Bluetooth et ZigBee [MED10] :

Technologie	Zigbee	Bluetooth
IEEE	802.15.4	802.15.1
Besoins en mémoire	4-32 Kb	250 Kb+

Autonomie de la pile	Années	Jours
Vitesse de transfert	250 KB/s	1Mb/s
Portée	100 m	10-100 m

Tab.3: Tableau comparatif entre Bluetooth et ZigBee

1.4 Domaines d'application des réseaux de capteurs sans fil

Les nœuds capteurs peuvent être employés pour la capture continue, la détection d'événements, l'identification d'événements et la commande locale des déclencheurs. Le raccordement sans fils des nœuds de micro-capteur permet un large éventail d'applications, essentiellement dans le domaine militaire et environnemental [GIL 08] :

-**Application médicale**

Les applications liées à la santé représentent une part importante des travaux de recherche sur les réseaux de capteurs. Leur but est d'offrir un ensemble de services de surveillance à domicile.

Le projet STAR (Système Télé-Assistant Réparti), par exemple, consistait à concevoir une plateforme dédiée à la surveillance de personnes souffrant d'arythmies cardiaques. Ce système avait aussi un rôle préventif. En effet, les arythmies cardiaques sont des phénomènes difficiles à diagnostiquer de part leur nature intermittente et très aléatoire. Généralement, une personne qui souffre potentiellement de cette maladie se voit équiper d'un dispositif (Holter) effectuant un relevé de ses signaux électrocardiogrammes (ECG) pendant une durée variant de 24 à 48 heures. Si aucun trouble n'est observé mais que des symptômes persistent, elle est hospitalisée durant une courte période de manière à être soumise à un bilan complet. Même à la suite de tous ces examens, il est possible d'avoir des doutes sur le diagnostic.

Dans le cadre du projet STAR, la personne est équipée d'un capteur sans fil intelligent capable d'acquérir et d'analyser les signaux ECG en temps réel. Mais dans ce cas, contrairement aux Holters classiques, la durée d'observation est plus longue (une voire deux semaines) et surtout la personne peut être surveillée de chez elle. En effet, le capteur utilise un module de transmission sans fil Bluetooth qui lui permet de communiquer avec une passerelle présente au domicile du patient et connectée à Internet. Cette dernière relaie ensuite les données collectées par le capteur vers un centre de traitement et d'interventions situées au sein d'un hôpital. Le système peut ainsi être utilisé soit pour établir un diagnostic, soit pour prévenir les risques de mort subite liés aux arythmies cardiaques.

La prévention des risques de chute chez les personnes âgées est un autre exemple d'application. Ces chutes sont dans la plupart du temps causes de fractures (fémur, bassin,...) qui s'accompagnent de longues semaines d'inactivité ou dans le pire des cas d'invalidités partielles permanentes. Cette perte d'autonomie oblige la personne à faire appel à une aide soignante à domicile ou à intégrer un centre spécialisé. Dans une première étape, Les capteurs

sans fil déterminent le « degré d'équilibre » de référence de la personne. Il servira d'étalon pour les mesures effectuées durant les jours suivants afin d'évaluer les risques de chute et d'en avertir qui de droit.

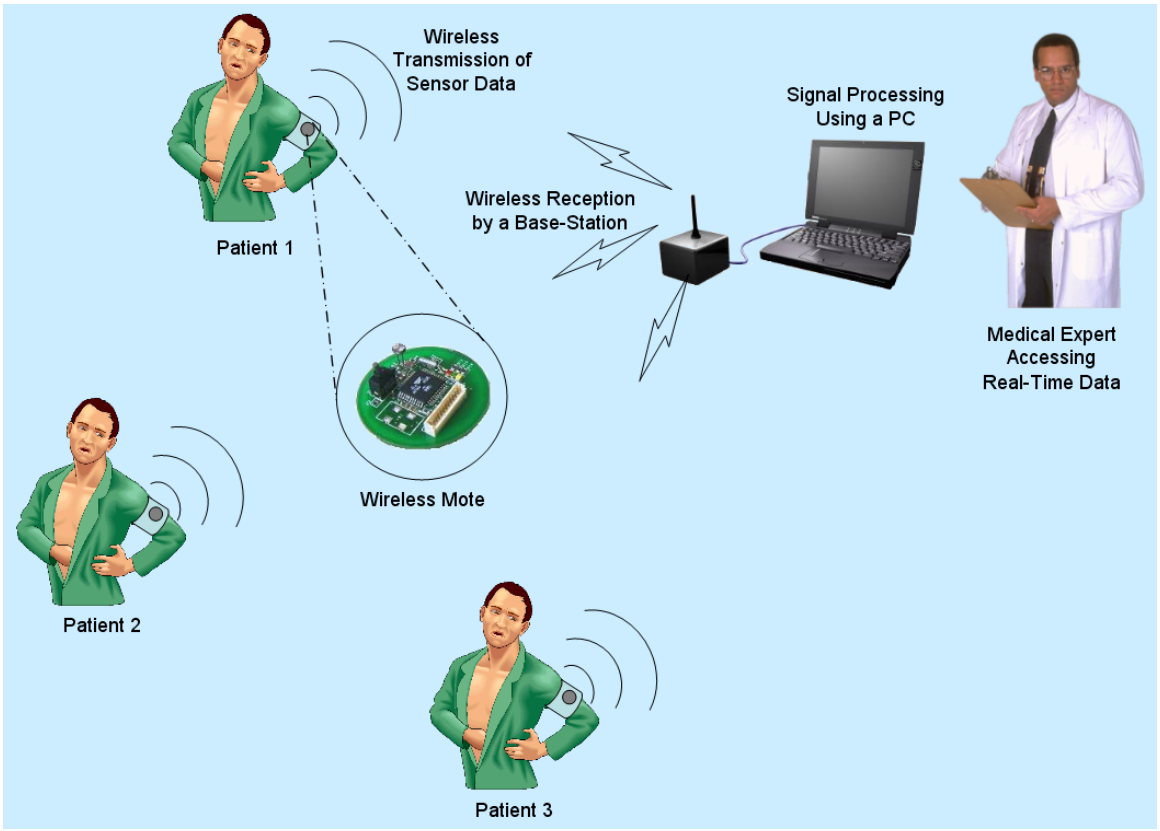

Fig.6 : application des RCSFs dans le domaine médical

- Application environnementale

Les RCSF donnent la possibilité d'étudier des phénomènes plus près que ne le permettent des dispositifs classiques. L'accessibilité à certains endroits est possible ou du moins simplifiée grâce aux RCSF. On peut prendre l'exemple d'une forêt tropicale comme la forêt amazonienne. Cette forêt est tellement dense et par certains points hostile à l'homme que l'utilisation d'un réseau de capteurs pour l'étudier pourrait être envisagée. Les capteurs pourraient être ainsi disséminés par voie aérienne sur un périmètre donné et renvoyer les données collectées par transmission sans fil. Le problème majeur dans ce mode de fonctionnement, en plus du développement de capteurs petits et robustes, est la récupération de ces mêmes capteurs après l'accomplissement de leur tâche.

Au-delà de l'exemple précédent, l'architecture d'un capteur sans fil avec un module de communication sans fil, une puissance de calcul raisonnable et un ensemble de capteurs dédiés à l'étude de grandeurs physiques rend possible son intégration dans un environnement physique donné. Les grandeurs physiques mesurées sont la température, l'humidité, la tension du sol, le degré de luminosité, le niveau sonore.

L'observation des animaux dans leur habitat prend une place importante dans les applications environnementales. Les capteurs sans fil déployés dans une réserve naturelle donnent des informations de localisation sur les animaux, leur état de santé, sur leur intégration dans un nouvel habitat. Les RCSF ont permis l'observation d'oiseaux sans troubler leur habitude en évitant une intervention humaine jugée inappropriée.

Le projet PODS, vise à comprendre le processus et les mécanismes de croissance de certaines plantes devenues rares et en danger d'extinction. L'objectif de cette étude est la réintroduction de celles-ci dans de nouveaux habitats propices à leur développement.

L'agriculture est un secteur où les RCSF sont de plus en plus utilisés. Les capteurs collectent des données sur les cultures et la qualité du sol et les transmettent à une station centrale présente dans la ferme. Si la station est connectée à Internet, il est possible, sous couvert d'une autorisation, d'accéder aux informations sur l'ensemble de l'exploitation.

La prévention des risques d'incendie ou d'inondation fait partie des domaines où les RCSF apportent les plus grandes perspectives. Dans ce type d'applications, les capteurs sans fil sont en charge de la détection de tous phénomènes anormaux observés dans leur périmètre d'action. Il peut s'agir d'une brusque augmentation de la température ou du taux d'humidité caractéristique d'un début d'incendie ou d'inondation. Chaque capteur est soit placé à un endroit connu, soit muni d'un système de localisation de type GPS. Ainsi, à l'autre bout du réseau, la station centrale peut fournir des renseignements précis permettant une intervention rapide et localisée.

Dans la surveillance des risques d'inondation, les capteurs sont obligatoirement étanches. Pour les incendies, ils doivent être assez robustes pour supporter pendant un temps suffisant de très fortes températures. Le capteur doit pouvoir détecter le départ du feu et transmettre le plus de données possibles avant sa détérioration.

Les RCSF aident également à l'étude de phénomènes complexes tels que les tremblements de terre, les éruptions volcaniques, les ouragans et les tsunamis. Ils fournissent des données permettant d'établir des modèles de prévision. Pour quelques applications présentées dans cette section, des systèmes filaires existaient déjà mais étaient plus difficiles à déployer et n'offraient parfois pas autant de fonctionnalités.

Fig.7 : applications des RCSFs dans le domaine environnemental

-Application militaire

Les applications militaires des RCSF sont multiples. Certaines ont pour but la protection des soldats engagés sur un champ de bataille. Une première application est de fournir au soldat des dispositifs destinés à surveiller ses signes vitaux. Equipé d'un module de repérage, il est possible de localiser la position de l'ensemble des membres d'une unité et d'établir ensuite une stratégie de défense ou d'attaque. La prévention liée aux attaques chimiques, biologiques voire nucléaires par une détection anticipée fait partie des applications envisagées pour les RCSF. Des capteurs mobiles sont envoyés en repérage sur un champ de bataille et donnent des indications sur les risques présents. Une zone délimitée autour d'un camp de base peut être surveillée à l'aide d'un RCSF. Une telle application repose sur des dispositifs spécifiques de détection présents sur les capteurs. Ces derniers sont positionnés dans des endroits précis et en charge de l'observation d'une zone donnée. En cas d'intrusion, un message est transmis à travers le réseau en direction des entités à alerter.

Ce type d'application est complexe à mettre en place. Une trop grande proximité des capteurs peut entraîner des erreurs d'appréciation. En effet, si deux capteurs sont trop proches l'un de l'autre, ils vont surveiller une même zone. Si les traitements effectués après un événement ne sont pas corrects, il se peut que l'on indique deux intrusions au lieu d'une ou l'inverse.

Le suivi à la trace (ou « mobile tracking » en anglais) accompagne parfois la détection d'une intrusion. Localiser avec précision les forces ennemies et suivre leurs déplacements est un avantage important durant une bataille. Cette opération est obtenue en plaçant à l'avance un réseau de capteurs tout au long d'un parcours qui pourrait être emprunté par l'ennemi. Les problèmes de cohérence entre le phénomène réel et l'observation qui en découle, soulevés pour l'application précédente restent valables. Les techniques de détection utilisent des capteurs vidéo, acoustiques et de chaleur.

Fig.8 : application des RCSFs dans le domaine militaire

1.5 Axes de recherche pour les réseaux de capteurs sans fil

Plusieurs travaux de recherche visent à proposer des solutions optimales et efficaces à un ou plusieurs problèmes des RCSFs. Parmi les principaux domaines de recherche pour les RCSFs [GIL 08] nous citons :

-Routage

Le domaine le plus étudié dans les RCSFs est le routage, plusieurs protocoles de routage ont été proposes pour minimiser les coûts de communication, afin de réduire la consommation énergétique. La majorité des recherches menées actuellement sur les protocoles de routage se focalisent sur le routage hiérarchique qui consiste à structurer le réseau en un ensemble de groupes nommés clusters selon un processus de clustering. Un cluster est constitué d'un chef "cluster head" et de ses membres.

-Localisation

Vu le très grand nombre des nœuds capteurs sur un RCSF et leur déploiement d'une manière ad hoc, de nombreux systèmes de coordonnées spatiales et virtuelles ont été proposes, auxquels les nœuds capteurs peuvent s'identifier pour se localiser dans le RCSFs.

-Sécurité

Les applications utilisant les RCSFs ont souvent besoin d'un niveau de sécurité élevé. Or, de part leurs caractéristiques, la sécurisation des RCSFs est a la source de beaucoup de travaux scientifiques et techniques proposant des solutions de sécurité efficaces.

Dans les premiers travaux sur les RCSF, les aspects liés à la sécurité avaient été peu ou pas abordés. Pour mettre en place une application de réseau de capteurs, il faut résoudre essentiellement les problématiques de routage, de gestion de données. La sécurité vient ensuite et s'appuie sur les ressources restantes.

Pourtant, les besoins en sécurité sont réels et indispensables. En effet, la confidentialité des données tout au long de la chaîne d'acquisition est une nécessité pour un bon nombre d'applications. Les données doivent donc être sécurisées durant la transmission par communication sans fil et, même parfois, durant le stockage. La sécurisation d'un réseau sans fil seul est déjà complexe car elle s'applique à un support de communication non guidé. L'ajout de mécanisme de cryptographie au niveau du stockage des données rend la tâche encore plus difficile au regard de l'énergie et de la puissance de calcul disponibles dans un capteur sans fil.

-La mise à l'échelle

Au niveau des réseaux sans fil Ad Hoc, le problème de mise à l'échelle ou d'extensibilité existe bien mais celui-ci est plus important dans les RCSF et le sera encore plus dans les années à venir. Les capteurs sans fil du futur sont destinés à avoir des dimensions microscopiques permettant, par exemple, de les disperser sur la zone à étudier à partir d'un hélicoptère. Des milliers voire des dizaines de milliers de capteurs pourront ainsi être disséminés dans un périmètre restreint.

La capacité de mise à l'échelle d'un réseau est son aptitude à être suffisamment flexible pour répondre aux variations du nombre de nœuds qui le composent. Logiquement, l'organisation structurelle et le protocole de routage d'un réseau sont évalués en augmentant progressivement le nombre de nœuds. A partir des résultats obtenus, on établit le profil du réseau dans lequel est présente sa capacité de mise à l'échelle. Toutefois, actuellement, que ce soit en simulation ou encore plus en réalité, les tests sur un grand nombre de nœuds sont difficiles voire impossibles à réaliser.

La dispersion à la volée d'un nombre important de capteurs sans fil dans un espace restreint crée des zones d'interférences ou de collisions de communication. Dans tout réseau sans fil, les problèmes de station cachée et exposée existent et sont amplifiés selon la quantité de nœuds au mètre carré ou densité du réseau.

1.6 Conclusion

Dans ce chapitre nous avons étudié les réseaux de capteurs sans fils. D'abord nous les avons défini comme des réseaux qui sont généralement composés d'un grand nombre de capteurs sans fil autonomes d'une taille miniature, à faible cout et multifonctionnels, peuvent être déployés d'une manière dense et aléatoire a proximité du phénomène surveillé ou a l'intérieur en vue de capter des informations, les traiter et enfin les communiquer vers la station de base. Les points suivants étaient de présenter leurs systèmes d'exploitation, caractéristiques puis exposer les différentes contraintes de conception des RCSFs puis citer quelques domaines d'application de ces derniers. Ensuite, nous avons terminé avec les axes de recherche.
Les RCSFs se caractérisent par leur limitation en énergie, en traitement et en stockage cela rend l'utilisation des protocoles et traitement des réseaux classiques sur ce type de réseau inefficace ce qui est le cas pour le routage qui sera étudié dans le prochain chapitre.

Chapitre2

Routage dans les RCSFs

2.1 Introduction

Dans un réseau de capteurs sans fil les nœuds collectent les données de l environnement (le phénomène observé), les traitent et les transmettent à la destination finale qui est la station de base (*sink*). À l'absence de l'infrastructure ou dans le cas où la transmission directe vers la station de base est impossible, les nœuds sources transmettent les données à travers des nœuds intermédiaires. Par conséquent [TEC10], chaque nœud doit choisir un voisin pour transmettre la donnée jusqu'à atteindre la station de base, cette méthode est : le routage.

Le problème du routage consiste à déterminer un acheminement optimal des paquets de données a travers le réseau. En prenant compte les caractéristiques des réseaux de capteurs sans fil, les protocoles de routage conçus aux réseaux Ad-HOC traditionnels ne s'adaptent pas avec ce genre de réseau, ce qui mène a soit les améliorer si c est possible, soit à concevoir de nouveaux protocoles de routage bien spécifiques aux réseaux de capteurs sans fil en respectant les caractéristiques de ce type de réseaux.

2.2 Facteurs de conception d'un protocole de routage

Concevoir un protocole de routage efficace pour un réseau de capteurs sans fil, qui assure la fiabilité de communication et prolonge la durée de vie du réseau ne se réalisera qu'en respectant certains facteurs entrainés par les caractéristiques des réseaux de capteurs sans fil (les caractéristiques vues en chapitre01 [SHI10]:

2.2.1 Déploiement des nœuds

Les nœuds capteurs dans un réseau de capteurs sans fil, sont déployés soit d'une manière déterministe ; soit d une façon aléatoire. Dans un déploiement déterministe, les nœuds capteurs sont placés manuellement et les données sont acheminées suivant des routes prédéterminées. Dans le cas d'un déploiement aléatoire, les nœuds capteurs sont dispersés aléatoirement en créant une infrastructure, si la distribution de ces derniers est uniforme, une organisation en clusters est nécessaire pour garantir une meilleure connectivité et consommation énergétique.

2.2.2 Consommation énergétique

La consommation énergétique est un facteur essentiel dans la conception d'un protocole de routage efficace. Un nœud capteur dépense plus d'énergie dans la phase de transmission de données par rapport à celle dépensée dans les phases de capture et traitement. L'épuisement de l'énergie est aussi relié a la puissance de transmission qui est proportionnelle à la distance au carrée ou plus ; ce qui explique le fait que le routage multi-sauts consomme moins d'énergie que dans une transmission directe dans le cas où les nœuds capteurs sont éloignés de la station de base. Si les nœuds capteurs sont très proches de la station de base alors dans ce cas la transmission directe sera la moins consommatrice d'énergie que le routage multi-sauts.

Actuellement, dans la majorité des applications, le déploiement des nœuds est aléatoire ce qui rend le routage multi-sauts inévitable.

2.2.3 Modèle de livraison de données

Selon l'application du réseau, la communication de données peut être classée en quatre catégories :

-Time driven

Recommandé pour les applications du monitoring où chaque nœud capteurs doit transmettre ses données périodiquement (dans un intervalle de temps prédéterminé).

-Event driven

Les données ne sont envoyées que lorsqu'un événement est détecté.

-Query driven

Chaque nœud transmet ses données à la réception d'une requête générée par la station de base ou un autre nœud capteur du réseau.

-Hybrid

La combinaison des trois modèles cités ci dessus.

2.2.4 Mobilité

Dans la plupart des travaux réalisés dans le domaine des réseaux de capteurs sans fil ; les nœuds capteurs sans supposés fixes. Mais, il existe des cas où la mobilité des stations de base et/ou les Clusters-Head est nécessaire. D'autre part, les événements observés peuvent être statiques ou dynamiques. Dans le cas des applications qui contrôlent des événements statiques, les données sont envoyées a la station de base une fois que l'événement se produit (le réseau adoptera un mode réactif). Par contre, la pluparts des applications qui contrôlent des événements dynamiques, nécessitent d'envoyer des rapports périodiques à la station de base ce qui conduit à générer un trafic très important.

Les protocoles de routage sont fortement influencés par le modèle de communication de données, en particulier, ce qui concerne la consommation d'énergie et la stabilité des routes.

2.2.5 Hétérogénéité des nœuds

Dans plusieurs études sur les réseaux de capteurs sans fil, touts les nœuds capteurs sont supposé homogènes (capacités en terme de calcul, mémoire et énergie). Cependant, selon l'application, un nœud capteur peut avoir un rôle particulier : capter la donnée, la relayer ou l'agrégation des données reçues. Si le nœud est chargé de réaliser les trois taches, son énergie va être rapidement épuisée. Comme solution, certaines applications proposent d'intégrer ou de designer des nœuds (cluster Head) qui seront plus puissants en énergie, bande passante et mémoire pour effectuer l'agrégation de données et envoyer le résultat à la station de base.

2.2.6 Tolérance aux pannes

Dans un réseau de capteurs sans fil, quelques nœuds peuvent être bloqués suite à un manque d'énergie, endommagés à cause d'un problème matériel ou des interférences environnementales. Cette défaillance ne doit pas affecter le fonctionnement global du réseau ; pour cela, un protocole de routage doit créer de nouvelles routes pour bien acheminer les données vers la station de base.

2.2.7 Scalabilité

Le déploiement des nœuds capteurs est souvent dense (le nombre peut être une centaine, milliers, ou encore plus). Une phase de redéploiement ou une extension peuvent être effectuées sur le réseau ; dans ce cas, le protocole de routage doit faire face à la dégradation des performances et maintenir le bon fonctionnement du réseau dense.

2.2.8 Agrégation de données

Les nœuds capteurs dans un réseau, peuvent générer des données redondantes (un capteur peut recevoir la même donnée depuis plusieurs autres capteurs du réseau). La transmission de la même donnée implique une perte d'énergie inutile, l'agrégation de données est le bon remède a ce problème, consiste soit à supprimer les données redondantes ; soit choisir le minimum, le maximum ou encore la moyenne des valeurs reçues.

Par conséquent, il est nécessaire lors de la conception d'un protocole de routage efficace de prendre en considération les techniques d'agrégation de données et de bien designer les nœuds capteurs qui s'en occuperont de ces opérations.

2.2.9 Qualité de service

Certaines applications exigent que les données doivent arrivées à la station de base en un intervalle de temps déterminé sinon elles seront jugées inutiles ce qui fait du temps de réponse un paramètre très important lors de la conception d'un protocole de routage. Mais, la conservation d'énergies dans la plupart des applications est plus prioritaire que la qualité de service vue qu'elle est fortement liée à la durée de vie du réseau ; suite à cela, le réseau est mené à réduire la qualité de service des données à fin d'augmenter sa durée de vie.

2.2.10 Connectivité

La forte densité dans un réseau de capteurs sans fil assure une connexion des nœuds capteurs. Par contre, les changements qui affectent la topologie peuvent éliminer des liens entre les nœuds (supprimer des routes) donc certains nœuds se retrouveront isolés. Un protocole de routage doit éviter l'isolement des nœuds capteurs et garantir une meilleure connectivité.

2.3 Métrique de routage

Une métrique de routage est une mesure utilisée pour sélectionner le meilleur chemin. Chaque protocole de routage est influencé par une ou plusieurs métriques et le choix d'une mauvaise métrique conduit à des boucles de routage (loops) et de création de chemins non optimaux. La conception des métriques de routage est reliée à la performance des protocoles de routage. Il existe plusieurs métriques qui ont été classées en cinq catégories [WAZ12] :

métriques générales, métriques de performance, métriques de sécurité, métriques de qualité de service, métriques de qualités des liaisons.

Nous citons dans ce qui suit quelques métriques :

2.3.1 Consommation d'énergie

Cette métrique est utilisée pour montrer combien un protocole de routage est efficace en énergie.

2.3.2 Nombre de sauts

Calculer le nombre de sauts du nœud source a la station de base en passant par les nœuds intermédiaires permettra de choisir le chemin ayant le minimum de sauts pour lui transmettre la donnée.

2.3.3 Taux de perte de paquets de données

Pour minimiser la perte des paquets de données dans le réseau, on calcule le ratio (taux) suivant : le nombre des paquets perdus sur le nombre total des paquets émis, si ce ratio est élevé il est nécessaire de penser à des solutions pour remédier à ce problème.

2.3.4 Délai de bout en bout

Un délai de bout-en-bout est le temps moyen nécessaire pour qu'un paquet envoyé de la source à la station de base. Pour des meilleures performances, le délai de bout-en-bout doit être le plus petit possible.

2.4 Classification des protocoles de routage

Le routage a été largement étudié et plusieurs approches ont été proposées. Ainsi, les protocoles de routage peuvent être classés selon différents critères, les auteurs de [ALK04] ont proposé une classification basée sur deux critères principaux : la topologie du réseau et le fonctionnement du protocole**.**

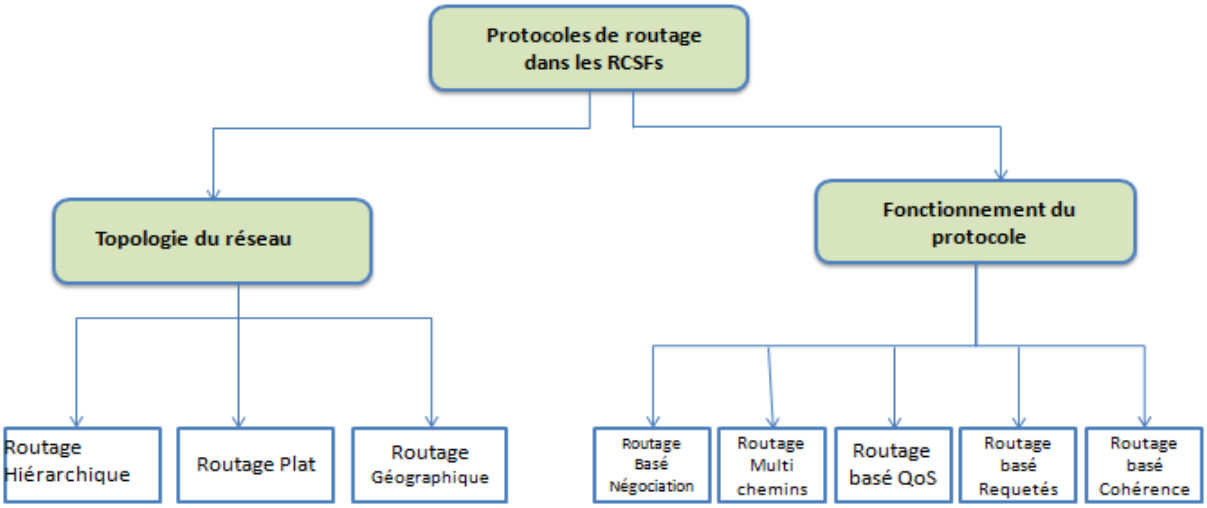

Fig.9 : Classification des protocoles de routage pour les RCSFs [ALK04]

Selon [MOH11], en se basant sur la classification précédente, un protocole de routage peut appartenir aux deux classes. Pour cela il a proposé une autre classification qui comporte trois classes principales (Classification selon la structure du réseau) et cinq sous classes (Classification selon la stratégie de routage du protocole).

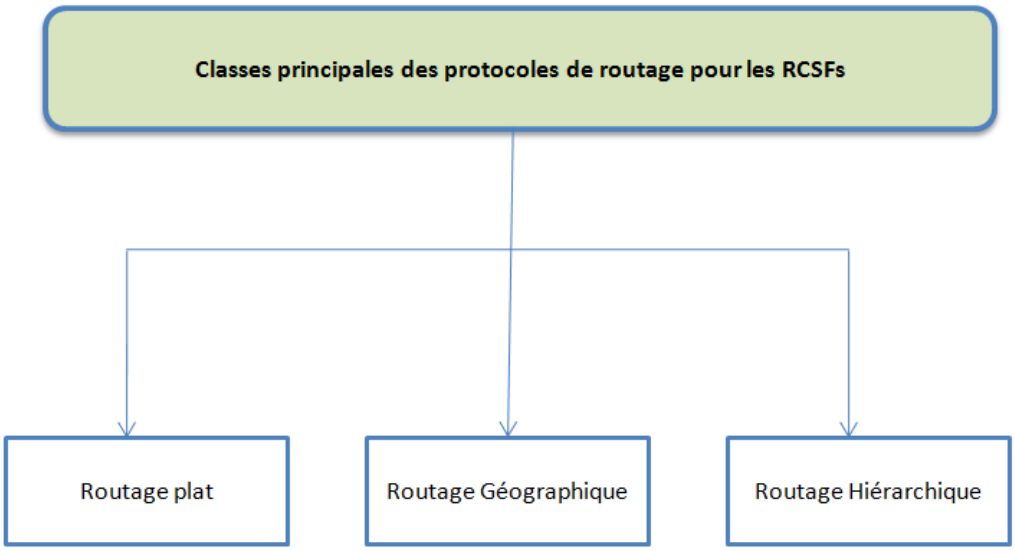

Fig. 10: Classes principales des protocoles de routage pour les RCSFs

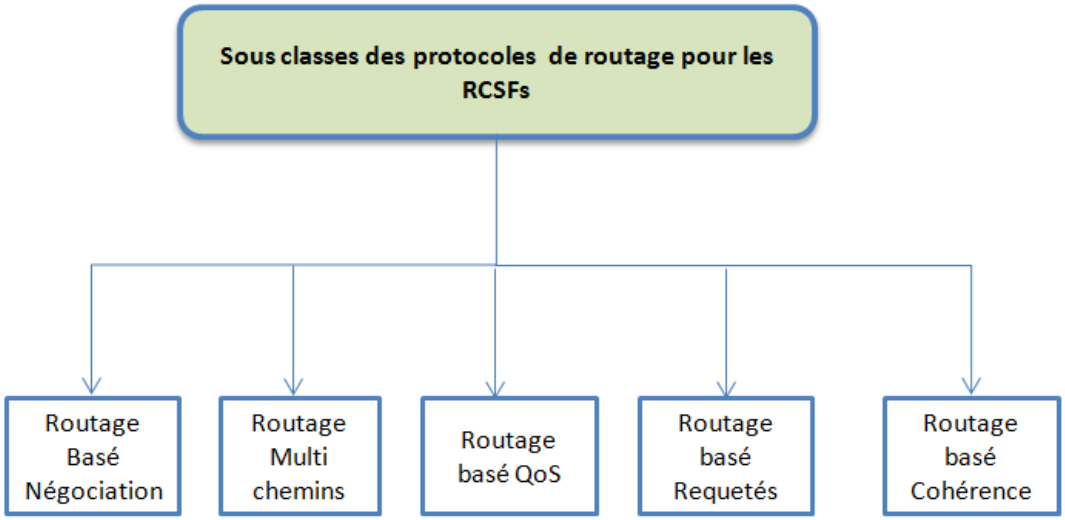

Fig. 11 : Sous classes des protocoles de routage pour les RCSFs [MOH11].

Les protocoles de routage peuvent aussi être classés selon l'établissement et la maintenance des routes, peuvent être séparés en trois catégories : les protocoles proactifs, les protocoles réactifs et les protocoles hybrides [PRE12].

Selon les auteurs de [RAJ09] les protocoles de routage peuvent aussi être classés selon l'initiateur de communication. L'initiateur peut être la destination (*destination initiator*) ou bien la source (*source initiator*).

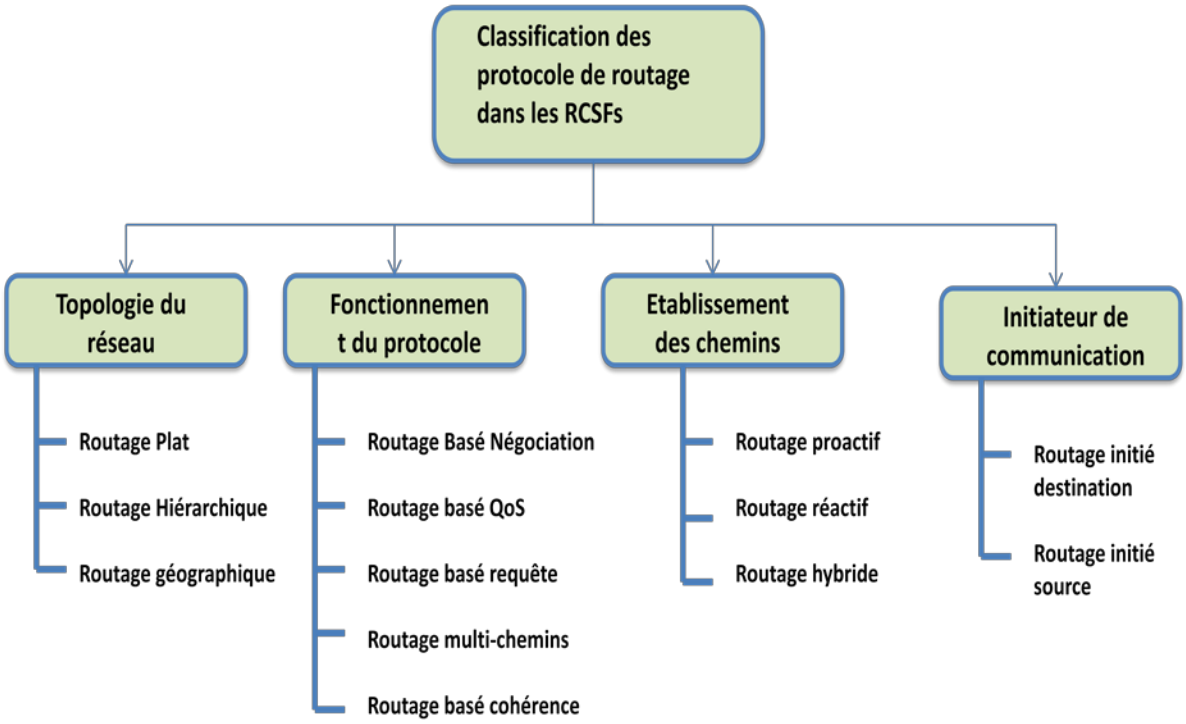

Fig.12: classification des protocoles de routages dans les RCSFs [RAJ09].

2.4.1 Classification selon la topologie du réseau

Selon les deux topologies des RCSFs on distingue trois types de protocoles [MAL12], [MAU07]:

-Protocoles de routage plats

Dans une topologie plate, les nœuds capteurs ont les mêmes rôles et collaborent ensemble pour router les données vers la station de base en adoptant un routage multi-sauts. En raison de la densité, le déploiement aléatoire et la faible capacité des nœuds capteurs; il est difficile voir impossible d'assigner un identifiant global est unique pour chaque nœuds capteurs ce qui a conduit au routage centré données (*data centric routing*) ; où le sink envoie des requêtes à certaines régions du réseau et attend les données qui lui seront envoyées par les nœuds capteurs de ces régions. L'utilisation des requêtes (pour demander les données) nécessite la désignation des attributs pour indiquer les propriétés des données**.**

-Protocoles de routages hiérarchiques

Dans une topologie plate, les nœuds capteurs ont les mêmes rôles et collaborent ensemble pour router les données vers la station de base en adoptant un routage multi-sauts. En raison de la densité, le déploiement aléatoire et la faible capacité des nœuds capteurs; il est difficile

voir impossible d'assigner un identifiant global est unique pour chaque nœuds capteurs ce qui a conduit au routage centré données (*data centric routing*) ; où le sink envoie des requêtes à certaines régions du réseau et attend les données qui lui seront envoyées par les nœuds capteurs de ces régions. L'utilisation des requêtes (pour demander les données) nécessite la désignation des attributs pour indiquer les propriétés des données**.**

-Protocoles de routages géographiques

Les protocoles de routage géographiques utilisent seulement les informations concernant les positions de leurs voisins directs (il n'exige pas des tables de routage de sorte qu'il n'y ait aucune surcharge de contrôle pour leur création et maintenance) Il ne nécessite pas d'inondation. Seuls les nœuds qui se trouvent dans la zone d'acheminement désigné sont autorisés à transmettre le paquet de données. La région de transmission peut être défini par le nœud source ou par des nœuds intermédiaires pour exclure les nœuds qui peuvent provoquer la déviation des paquets de données [RAM13]. Par contre, chaque nœud doit connaitre sa position et chaque nœud source doit connaitre la position de la destination. Ces positions peuvent être obtenues en utilisant un dispositif dédié (GPS par exemple) ou par l'application d'un mécanisme de localisation.

2.4.2 Classification selon le fonctionnement du protocole

La classification être le fonctionnement du protocole et on distingue [MOH12], [PRE12]:

-Protocoles de routage multi-chemin

Le principe de ces protocoles est d'utiliser plusieurs chemins entre la source et la destination, pour améliorer les performances du réseau. La tolérance aux pannes est mesurée par la possibilité q' un chemin alternatif existe entre une source et une destination lorsque le chemin principal échoue. Cette tolérance peut être renforcée en découvrant des chemins multiples entre la source et la destination. Ces chemins alternatifs sont maintenus en vie par l'envoi de messages périodiques. Par conséquent, la fiabilité du réseau peut être augmentée tout en accusant une surcharge de contrôle supplémentaire pour garantir la validité des chemins alternatifs.

-Protocoles de routage basés sur la négociation des données

L'idée principale du routage via négociation est d'utiliser des descripteurs de haut niveau pour décrire la donnée avant de l'émettre. Cela permettra aux nœuds de prendre des décisions afin d'éliminer les données redondantes. Cette prise de décision ce fait en échangeant une série de messages de négociation entre l'émetteur et le récepteur avant d'envoyer la donnée.

-Protocoles de routage basés sur les requêtes

Cette classe de protocoles se base sur l'envoi et la réception des requêtes sur les données. Le nœud puits propage une requête vers les nœuds du réseau, les nœuds ayant les données sollicitées par la requête répondent en émettant leurs données via le chemin inverse de la requête.

-Protocoles de routage basés sur la qualité de service

Le principe des protocoles de routage avec QoS se base sur le fait que le réseau doit être capable de satisfaire certaines métriques (latence, énergie des nœuds, bande passante, etc.) tout en acheminant le maximum de données vers la station de base.

-Protocoles de routage basés cohérence (ou non cohérence) des données

C est un routage basé sur le traitement des données. En routage basé non cohérence, les données sont localement traitées par les nouds avant de les transmettre. Par contre, dans un routage basé cohérence les données sont transmises a l'agregateur après un minimum de traitement comme par exemple la suppression de la redondance. [PAR12]

2.4.3 Classification selon l'établissement des chemins

Se devise en trois types :

-Protocoles de routage proactifs

Dans ce type de protocoles les meilleures routes vers toutes les destinations possibles sont établies au préalable. Ces routes sont sauvegardées dans les tables de routage même si elles ne sont pas utilisées. L'inconvénient majeur de ces protocoles est le besoin de conserver et contrôler la validité des tables de routage en permanence.

-Protocoles de routage réactifs

Le protocole de routage dans ce cas maintient des routes à la demande. Une procédure de découverte de route sera lancée lorsque le réseau a besoin d une route. L'inconvénient de ce type de routage qu'il est très couteux en transmission de paquets lors de la détermination des routes.

-Protocoles de routage hybrides

Combine les deux types de routage proactif et réactif.

2.4.4 Classification selon l'initiateur de communication

Dans un routage initié destination, la destination initié l'installation des routes vers la source tandis que dans un routage initié source, les routes sans mises en place sur la demande de la source et la source envoi les données une fois qu'elles soient disponibles.

Le tableau suivant illustre quelques exemples de protocoles de routage et leurs classifications : [RDE13].

Protocole de routage	**Classification**	**Auteurs et années**	**description**	**Consommation d'énergie**
SPIN (*Sensor Protocols for Information via Negotiation*)	-Protocole plat - réactif.	J. Kulik et al ,2002	-SPIN diffuse les informations d'une manière efficace dans le WSN. -Les données des nœuds utilisant SPIN sont appelé métadonnée.	Limitée
DD (*Directed Diffusion*)	-Protocole plat. - réactif.	Intanagonwiwat., C et al. 2000	-DD utilise une approche *data-centric.* -Il exige les interactions localisées entre les nœuds. -DD est caractérisé par : Gradient, Interests ,donnée et renforcement.	Limitée
TEEN(*Threshold sensitive Energy Efficient sensor Network*)	-Protocole hiérarchique	A.Manjeshwar and D.P Agrawal,2001	-Le seuil soft de TEEN peut varier et cela dépend de l'application cible et l'attribut détecté. -TEEN améliore l'efficacité des WSNs.	Élevé
LEACH (*Low Energy Adaptive Clustering Hierarchy*)	-Protocole hiérarchique.	Heinzelman, 2000	-Les clusters sont formés dynamiquement par les nœuds. -Dans le cluster les nœuds sélectionne le CH d'une manière aléatoire. -le CH transmit les informations collecté vers la station de base.	Élevé
APTEEN (*Adaptive Periodic Threshold-sensitive Energy Efficient sensor Network Protocol*)	-Protocole hiérarchique. -hybride.	A. Manjeshwar and D. P. Agrawal, 2009	-Après la formation de cluster, à chaque round le CH diffuse les attributs, seuil, plan de transmission (Schedule) et un compteur de temps. -APTEEN combine entre la politique proactif et réactif. -Il fournit la collection de donnée périodique ainsi que la détection d'événement.	Élevé

PEGASIS (*Power Efficient Gathering In Sensor Information System*)	-Protocole hiérarchique. -proactif.	Lindsey and Raghavendra 2002.	-Il est amélioré par rapport au protocole LEACH et il est proche de la chaîne optimale basé protocole. -Ce protocole permet de prolonger la duré de vie de WSN. -Il évite la formation des clusters et utilise un seul nœud pour communiquer avec la SB au lieu de plusieurs nœuds.	Maximum
HEED (*Hybrid Energy Efficient Distributed*)	-Protocole hiérarchique.	O. Younis, and S. Fahmy 2004.	-La formation de Cluster Head est basée sur la proximité du nœud à son voisin et son énergie résiduelle.	Faible
GEAR (*Geographic and Energy Aware Routing*)	-Protocole hiérarchique. -Basé localisation.	Yan Yu, Ramesh Govindan, Deborah Estrin , 2001	-GEAR découpe le réseau en region . -Il sélectionne le nœud voisin pour l'acheminement de donnée en tenant compte de son énergie résiduelle. - Il utilise algorithme récursive Geographic forwading ou restricted flooding pour la diffusion des paquets vers les régions destinataire.	Limité
GAF (*Geographic Adaptive Fidelity*)	-Protocole hiérarchique. -Basé localisation.	Takashi Osawa, Tokuya Inagaki,Susumu Ishihara,2008	-GAF est basé sur la localisation des nœuds. -Il utilise l'information de localisation des nœuds pour la formation des clusters.	Limité
SPEED	-Protocole hiérarchique. -Basé localisation.	Tian He , John A Stankovic, Chenyang Lu, Tarek Abdelzaher , 2003	-SPEED estime le délai de chaque saut . -Il assure une vitesse de livraison de paquet constante. -Le prochaine saut sera choisit parmi les voisins plus proche de la destination	Faible

Tab.4 : Exemples de protocoles de routage et leur classification

2.5 Conclusion

Le routage est une tache essentielle pour garantir un bon fonctionnement d'un réseau de capteurs sans fil. De multiples recherches ont été menées ce qui a permet de développer plusieurs protocoles de routage. Dans ce chapitre nous avons présenté les différents facteurs à prendre en considération afin de concevoir des protocoles de routages efficaces. Ces protocoles sont classés selon plusieurs critères (topologie du réseau, fonctionnement du protocole, …) et leurs performances sont évaluées par les métriques utilisées.

En raison de l'absence d'infrastructure, la nature des canaux de transmission sans fil (permet l'écoute facile de l'information) et le déploiement dans des environnements hostiles, les réseaux de capteurs sans fil sont vulnérables à plusieurs attaques internes et externes. En ce concentrant sur les attaques de routage, un nœud malicieux peut modifier, usurper, injecter des données et générer de faux messages. D'un autre coté, un nœud du réseau, afin de préserver son niveau d'énergie, peut ne pas transmettre une partie ou toute la donnée vers la destination présentant ainsi un comportement égoïste. L'impact de ces comportements malicieux (égoïsme, usurpation, modification, injection des données,…) peut être grave et peut conduire à l'effondrement du réseau ce qui rend inévitable la prise en considération de la sécurité lors de la conception des protocoles de routage. Plusieurs approches et techniques ont été proposées afin de sécuriser les réseaux de capteurs sans fil telles que le cryptage, l'authentification et la confiance, la dernière approche sera l'objectif du prochain chapitre.

Chapitre 3

Confiance dans les RCSFs

3.1 Introduction

Les réseaux de capteurs sans fil (RCSFs) sont composés d'un grand nombre de nœuds capteurs autonomes qui surveillent et réagissent aux conditions environnementales et transmettre les données recueillies en coopération à la station de base en utilisant des canaux sans fil. En raison des ressources limitées de ces derniers, il est difficile d'intégrer des mécanismes de sécurité traditionnels telle que l'authentification, et la cryptographie. En conséquence, les réseaux de capteurs sans fil sont sujettes à différents types d'attaques malveillantes, comme déni de service, attaques sur les protocoles de routage ainsi que les attaques par rejeu. Les systèmes cryptographiques classiques sont incapables de prévenir ces types d'attaques. Nous devons améliorer les protocoles de sécurité avec des techniques de gestion de la sécurité et de confiance. Cependant les systèmes traditionnels de gestion de la confiance développées pour les réseaux câblés et sans fil peuvent ne pas convenir pour les réseaux avec des petits nœuds de capteurs en raison d'une bande passante limitée et les contraintes de nœud strictes en termes de puissance et de mémoire.

3.2 Définition de la confiance

La confiance est un facteur essentiel dans tout type de réseaux, sociaux ou informatiques. Elle devient un facteur important pour les membres du réseau pour faire face à l'incertitude sur les futures actions des autres participants. Ainsi, la confiance devient particulièrement importante dans les systèmes distribués ou transactions sur Internet.

Dans la littérature, la notion de confiance a été largement étudiée selon différentes approches dans divers domaines tel que la psychologie, la sociologie, l'économie, politique….etc. Cependant, il n existe pas une seule définition de la confiance, elle dépend du domaine et des auteurs :

3.2.1 Dans les réseaux sociaux et psychologie

Définition.1 **:** Selon [DUE62], la confiance peut être définit comme une décision par rapport à une perception individuelle des coûts et bénéfices dont dépend cette décision. Lors d'une décision de confiance, l'individu est confronté à un chemin ambigu dont les issues dépendantes d'une tierce personne peuvent être perçues positives ou négatives. L'individu perçoit les issues négatives plus importantes que les issues positives. En choisissant de faire confiance l'individu suppose que l'issue positive se produira plutôt que l'issue négative. L'individu est donc confiant aux capacités et intentions de la tierce personne dont dépend l'occurrence de l'issue positive.

Définition.2 **:** [LUH79] inscrit la confiance dans une réalité sociale multidimensionnelle. Il la voit donc comme un fait basique, car un individu effectue les choix de faire confiance quotidiennement afin de s'adapter dans son environnement et affirme que la confiance se base sur une notion de risque.

Définition.3 **:** La confiance (ou symétriquement la défiance) est un niveau particulier de la probabilité subjective avec laquelle un agent accomplira une action spécifique, à la fois avant que nous ne puissions suivre chaque action (ou indépendamment de sa capacité de même pouvoir la tracer) et aussi dans un contexte dans lequel cela affecte notre propre action. [GAM00]

***Définition.4* :** Selon [GRA03], l'acte de faire confiance se réalise dans un contexte spécifique et se définit par une croyance quantifiée quant aux habilités de l'entité qui est crue. Cette quantification peut être une échelle de valeurs ou une simple classification.
***Définition.5*:** La confiance est la dépendance qu'une entité est prête à accepter vis-à-vis d'une chose ou d'une personne dans une situation donnée avec un sentiment de sécurité relative, même si des conséquences négatives sont possibles. [AUD07]
Définition.6 : La réputation est ce que l'on dit ou croit sur le caractère permanent ou d'une chose. [SAK13]

3.2.2 Dans les réseaux informatiques

Définition.1 : La confiance est la probabilité subjective pour laquelle le nœud A dépend de la fiabilité du nœud B dans l'exécution d'une action. [MOM 07]
Définition.2 : La réputation d'un nœud est l'observation globale de sa fiabilité dans le réseau sans fil. En outre, la fiabilité peut être évaluée à partir de ses comportements passés et actuels. [SAK13]

Dans ce qui suit, on s'intéressera à la confiance dans les réseaux de capteurs sans fil.

3.3 Caractéristiques de la confiance

On présentera dans ce qui suit quelques caractéristiques de la confiance: [MOM 07]

3.3.1 La subjectivité

La confiance est basée sur les observations des comportements des nœuds faites par d'autres nœuds du réseau.

3.3.2 La confiance est liée à un risque

Un réseau de capteurs sans fil qui ne court aucun risque n a pas besoin d'établir des relations de confiance entres ses nœuds**.**

3.3.3 La non-transitivité

Si un nœud A fait confiance au nœud B, le nœud B fait confiance au nœud C, cela n'implique pas que le nœud A fait confiance au nœud C.

3.3.4 La dynamicité

Les valeurs de la confiance qu'un nœud calcule pour ces voisins peuvent augmenter ou diminuer à travers le temps selon les comportements que présentent ces derniers (ces voisins).

3.3.5 L'asymétrie

Si un nœud A fait confiance a un nœud B cela ne signifie forcement que le nœud B fait confiance au nœud A.

3.3.6 Réflexivité (l'auto-confiance)

Un nœud a toujours confiance en lui-même.

3.4 Confiance et sécurité dans les RCSFs

Les réseaux de capteurs sans fil sont utilisés dans différents domaines : militaire, santé, contrôle de l'industrie, contrôle de véhicules, contrôle d'avions, … etc. ce qui fait de la sécurité un élément essentiel dans chacun d'eux et surtout dans le cas militaire et de surveillance, et cela afin d'assurer l'intégrité et la confidentialité des informations sensibles.

Les nœuds capteurs sans fil sont caractérisés par leurs faibles capacités de calcul, de stockage, par une énergie limité et la communication entre ces derniers ce fait a travers des canaux de transmission sans fil qui sont accessible par n'importe quel nœud (y compris les nœuds malicieux) présent dans l'environnement observé même s'il ne fait pas partie du réseau, cela augmentera le risque que certains nœuds approuvent de mauvais comportements qui mèneront au disfonctionnement du réseau.

Il existe deux types de mauvais comportements dans les RCSFs :

-Comportement malicieux

Lorsqu'un nœud malicieux s'introduit dans un réseau, il sera capable de communiquer avec les nœuds de ce dernier donc il aura la possibilité d'intervenir dans la transmission de données en modifiant ou supprimant des paquets de données, perturber le bon fonctionnement du protocole du routage en modifiant les informations sur le routage ou en fabriquant de fausses informations et en usurpant l'identité d'autres nœuds.

-Comportement égoïste

On distingue deux types de comportement égoïstes :

L'auto-exclusion (self-exclusion)

C'est le cas ou le nœud ne participe pas dans la phase d'établissement des routes ce qui lui permettra de réserver son énergie car il ne participera pas a la transmission de données.

La non –transmission (non-forwarding)

Dans ce cas le nœud égoïste participe dans lors de l'établissement des routes mais il refusera de transmettre les données qu'il reçoit afin de préserver son énergie

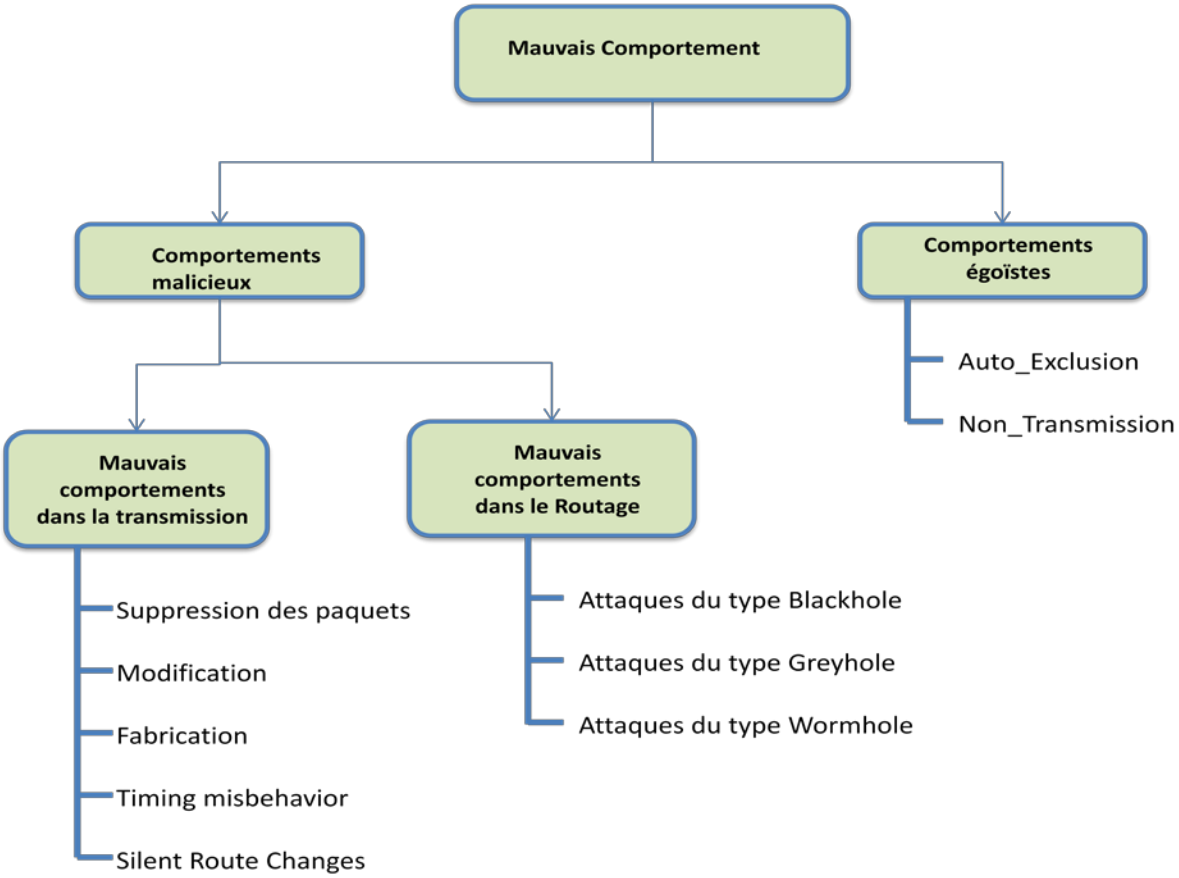

Fig.13 : Schéma des mauvais comportements dans un RCSF.

L'utilisation des mécanismes de sécurité traditionnels comme la cryptographie et l'authentification ne sont pas tout le temps une solution efficace, cela est dû à deux raisons principales. Tout d'abord, la limitation en termes d'énergie, de capacité de calcul et de stockage des nœuds capteurs rend la mise en œuvre de ces mécanismes couteuse. Puis, les nœuds capteurs peuvent prouver des comportements inattendus comme le cas de l égoïsme ce qui perturbera le bon fonctionnement du réseau [THE10]. Pour lutter contre ce genre de comportements, une approche empruntée de la société humaine a été proposée et qui repose sur l'établissement de la confiance entre les nœuds capteurs.

3.5 Gestion de la confiance dans les RCSFs

La gestion de la confiance est l'activité de création de Systèmes et méthodes qui permettent de faire des évaluations et des décisions relatives à la fiabilité des transactions avec un potentiel de risque élevé. [JOS07]

La gestion de la confiance dans les RCSFs devrait être aussi simple que possible, et devrait détecter les différentes attaques facilement, et de gérer et mettre à jour des relations de confiance entres les nœuds.

3.5.1 Etablissement de la confiance

En général, l'établissement de la confiance se fait en trois étapes **:**

3.5.1.1 Surveillance des interactions entre nœuds

Chaque nœud surveille et enregistre ses interactions avec ses voisins. Ces interactions seront utilisées par la suite dans le calcul de la valeur de la confiance.

La confiance basée sur les interactions directes entre deux nœuds voisins (voisins immédiats) est appelée **confiance directe** (Direct trust). D' autre part, Un nœud peut recevoir des recommandations faites par les autres nœuds jugé digne de confiance dans leur voisinage dans ce cas la confiance est appelée **confiance indirecte** (Indirect trust).

3.5.1.2 Modélisation de la valeur de la confiance

La modélisation de la confiance est la représentation mathématique de l'opinion que peut avoir un nœud sur un autre nœud du réseau. [MOM10]

La valeur de la confiance dépend du modèle utilisé. Yu et al [YAN11] ont introduit plusieurs approches représentatives pour construire le modèle de confiance, dont nous citons :

-Bayesian trust model *:* basé sur l'approche bayésienne.

-Entropy trust model : basé sur l'approche entropique.

-Game theory trust model : basé sur l'approche théorie des jeux.

-Fuzzy trust model : basé sur l'approche floue.

3.5.1.3 Evaluation de la confiance des nœuds

Pour chaque comportement surveillé , une valeur de confiance peut être calculée en se basant sur l'observation des interactions entre nœuds où chaque interaction est marquée soit comme un succès ou un échec.ces valeurs de confiance sont ensuite utilisées pour évaluer la fiabilité d'un nœud qui peut être exprimée soit :

-Comme un niveau de confiance parmi un ensemble de niveaux défini (par exemple : moyenne, haute, basse).

-Comme un taux de réussite (interactions réussies divisé par le nombre total d'interactions), la valeur de ce taux appartiendra à l'intervalle [0,1]

-Comme une valeur de confiance qui représente la différence entre les interactions réussies ou non réussies, cette valeur appartiendra à l intervalle [-1, 1].

3.5.2 Métriques d'évaluation de la confiance

Interpréter la confiance comme une mesure d'évaluation de la fiabilité d'un nœud a permis l'émergence de nombreuses métriques, et cela dépend des multiples aspects de son comportement qui peuvent être surveillés.

Le tableau suivant représente une liste de métrique d'évaluation de la confiance, des comportements qui peuvent être surveillé ainsi que les différentes attaques qui compromirent ce genre de comportements :

métrique de confiance	comportement surveillé	attaque adressée
1. paquet de données transmis.	Message de données / transmission de paquets de données.	Trou noir. Nœud puis .sélective noir, déni de service, comportement égoïste.
2. paquets de contrôle envoyés.	transmission de messages de contrôle.	contrôle / routage des messages abandonnes
3. la précision de paquets de données.	l'intégrité des données.	la modification des données de message.
4. la précision de paquets de contrôle.	contrôle de l'intégrité des paquets.	Sybil et d'autres atack est base sur le routage de message modofies.
5. disponibilité Bases sur balise / message hello.	transmission en temps opportun de routage périodique d'informations de	passive eavedropping. confiance de nœud.
6. Adressage de paquets modifiés.	lien/disponibilité de nœud. l'adresse du paquet de	Sybil , wormehole
7. Cryptographie.	transmission. possibilité de réaliser le cryptage.	authentification des attaques. inconduite liée au routage spécifique.
8. protocole d'exécution du routage.	protocole de routage action spécifique (réaction pour specifier le routage des	l'action protocole.
9. batterie/durée de vie.	messages) ressources énergétiques	disponibilité de nœuds.
10. la cohérence de la valeur / des données déclarées.	restantes. consistance des resultats de capteurs. (par exemple, l'humidité de l'énergie).	nœuds compromis.
11. Communication de capteurs.	rapports d'événements (demande specefique).	comportement de noeud égoïste au niveau de l'application.
12. Réputation.	valeur de confiance observé par des tiers.	mauvaise attaque en bouche.

Tab.5 : Métrique d'évaluation de la confiance, comportements et attaques [THE10].

3.5.3 Systèmes de gestion de la confiance

On distingue trois types de systèmes de gestion de la confiance **:**

3.5.3.1 Systèmes de gestion centralisés

Dans les systèmes de gestion centralisés, les informations sur un nœud du réseau sont collectées et enregistrées par un serveur central. Ces informations correspondent aux différentes expériences (interactions) que les autres membres du réseau ont pu avoir avec ce nœud. A partir de ces expériences le serveur central attribut pour chaque nœud du réseau une valeur de confiance qui sera par la suite partagée avec l'ensemble du réseau. L'inconvénient de ces systèmes est qu'un nœud aura une seule valeur de confiance sur ses voisins et la défaillance du serveur central mènera à la destruction du système.

3.5.3.2 Systèmes de gestion distribués

Pour remédier au problème du serveur central, les systèmes de gestion distribués ont été proposés. Dans ces derniers, chaque nœud calcule la valeur de confiance de ses voisins et les enregistre dans une table.

3.5.3.3 Systèmes de gestion hybrides

Combinent les propriétés des deux systèmes ; centralisés et distribués. Ils sont utilisés avec les méthodes de clusterisation, où le cluster-Head agit comme un serveur qui calcule les valeurs de confiance pour l'ensemble des membres de son groupe et chaque nœud calcule les valeurs de confiance des ses propres voisins.

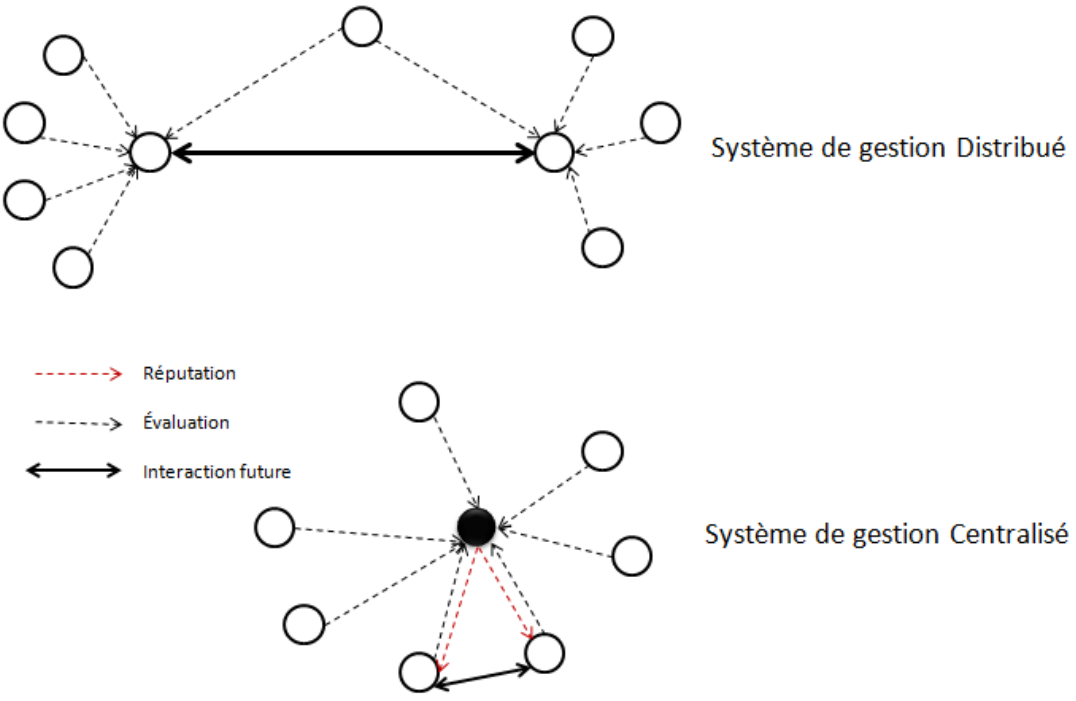

Fig.14 : Architectures des systèmes de gestion de confiance et de réputation.

Le tableau suivant illustre les avantages et les inconvénients de chaque type de systèmes de gestion de confiance : [KHT12].

	Avantages	**Inconvénients**
Centralisé	-Génère moins de calcules -Consomme moins d'espace mémoire	-Moins faible -Augmente le cout de communication
Distribuer	-Plus faible -Extensible	-Génère plus de calcules -Consomme plus d'espace mémoire
Hybride	-Un cout de communication réduit par rapport au système Centralisé -Consomme moins d'espace mémoire et génère moins de calcules que le système distribuer -Plus faible et plus flexible que le système centralisé	-Génère plus de calcules et exige plus d'espace mémoire que le système centralisé. -Moins fiable et moins extensible que le système distribué.

Tab.6: Avantages et inconvénients des systèmes de gestion de la confiance

3.6 Quelques approches existantes sur la gestion de la confiance dans les RCSFs

Dans cette section nous citons quelques systèmes de gestion de la confiance dans les RCSFs :

3.6.1 Reputation based Framework for high integrity Sensor Networks (*RFSN*)

Ganeriwal et Srivastava ont proposé [GAN04] un système basé réputation où les nœuds maintiennent une valeur de réputation pour les autres nœuds et l'utilisent pour évoluer leur fiabilité .l'architecteur du système est représentée dans le schéma suivant :

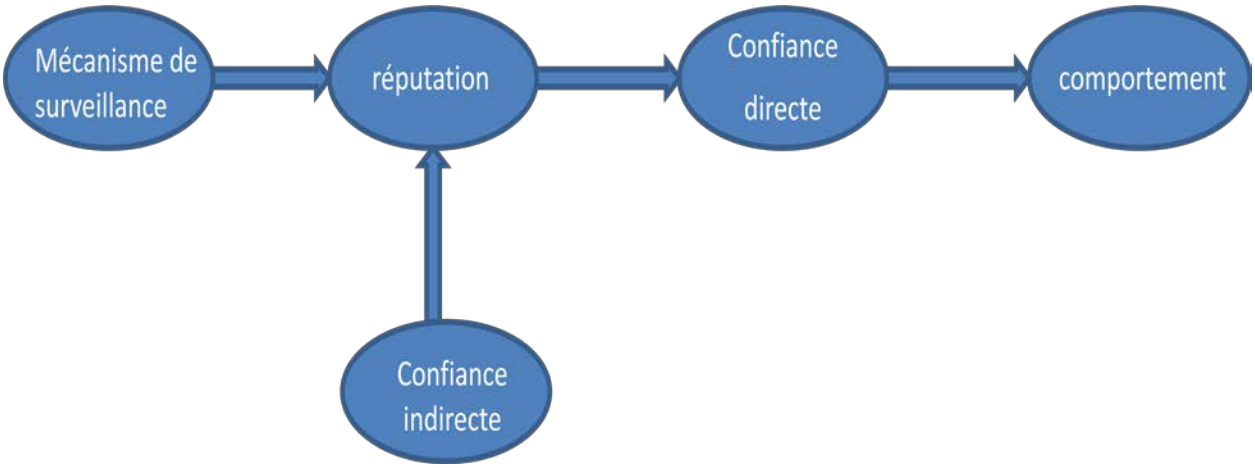

Fig.15: Schéma du système de gestion de la confiance RFSN.

-Mécanisme de surveillance (watchdog mechanism)

Le nœud observe ses interactions directes avec les autres nœuds et les classes en réussies et échouées.

Ce mécanisme est responsable de la collecte des observations et pour la prise de décision.

-Réputation

La réputation est considérée comme une probabilité, elle est représentée par une formule bayesienne plus précisément un système de réputation Beta.

$$\text{Rij} = \frac{p(\text{Dij}\ /\text{Rij})*\text{Rij}}{\sum P\ (\text{Dij}/\text{Rij})*\text{Rij}}$$

Rij : réputation du nœud j maintenance par le nœud i

Dij : observation directes du nœud J faites par le nœud i

$$\text{Rij} = \text{beta}\ (\alpha j + 1,\ \text{Bi}+1)$$

Tel que :

α j =interactions réussies entre Ni et Nj

Bj= interactions échouées entre Ni et Nj

-Confiance (trust)

La confiance est une prévision subjective d'un nœud Ni sur le comportement futur d'un nœud Nj.

Dans RFSN, la confiance est obtenue en calculant l'espérance statique de la probabilité représentant la réputation entre les deux nœuds.

$$\text{Tij} = \text{E(Rij)} = \text{E}\ (\text{beta}\ (\alpha\ \text{j}+1.\text{BJ}+1) = \frac{\alpha \text{j}+1}{\alpha \text{J}+\text{Bj}+2}$$

-Comportement

Pour qu'un nœud Ni décide si un nœud Nj est coopérant ou non, leur valeur de confiance Tij est comparée à un seuil (TH).

$$B_{ij} = \begin{Bmatrix} cooperant \forall T_{ij} \geq TH \\ non\_cooperant \forall T_{ij} < TH \end{Bmatrix}$$

-Confiance indirecte (seconde hand information)

Basé sur les interactions indirectes, un nœud Ni demande les valeurs de réputations à propos d'un nœud Nj par recommandations.

3.6.2 Group-Based Trust Management Scheme (*GTMS*)

Les auteurs de [RIA09] ont proposé un système léger de gestion de la confiance pour les RCSFs distribués. Ce système fonctionne en trois phases :

-Calcule de la confiance au niveau d'un nœud

Le calcul de la confiance se fait en utilisant soit :

-Time-Based Past Interaction Evaluation

Une évaluation basée sur les interactions effectuées dans la passé avec son voisin direct sera effectué où Chaque nœud considère une fenêtre de temps Δt qui est composée d'un certain nombre d'unités de temps, à chaque fois Δt glisse d'une unité de temps puis calcule le nombre d'interactions réussies ainsi que celles qui ont échouées durant cette fenêtre.

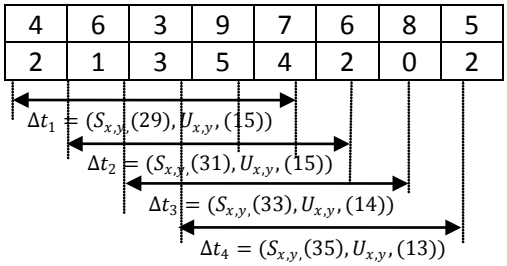

Fig.16: Fenêtre de temps pour calculer l'intervalle de temps

Tel que :

$S_{x,y}$: nombre d'interactions réussies entre les noeuds x et y
$U_{x,y}$: nombre d'interaction échouées entre les noeuds x et y

La valeur de la confiance $T_{x,y}$ (c'est une valeur entières comprise entre 0 et 100) attribuée par le nœud x à son voisin y est donnée par la formule suivante :

$$T_{x,y} = \left[100\left(\frac{S_{x,y}}{S_{x,y}+U_{x,y}}\right)\left(1-\frac{S_{x,y}}{1+S_{x,y}}\right)\right]$$

Après avoir calculé la valeur de confiance, un état est attribué au voisin concerné comme suit :

$$Mp(T_{x,y}) = \begin{cases} digne\ de\ confiance & 100-f \le T_{x,y} \le 100 \\ Incertain & 50-g \le T_{x,y} < 100-f \\ Indigne\ de\ confiance & 0 \le T_{x,y} < 50-g \end{cases}$$

Tel que :

f : représente la moitié de la moyenne des valeurs de confiance calculées par le nœud x

g : représente le tiers de la moyenne des valeurs de confiance calculées par le nœud x

f et g sont calculées comme suit :

$$f_{j+1} = \begin{cases} 1/2\left[\left(\frac{\sum_{i\in R_x} T_{x,i}}{|R_x|}\right)\right] & 0 < |R_x| \leq 1-n \\ f_j & |R_x| = 0 \end{cases}$$

$$g_{j+1} = \begin{cases} 1/3\left[\left(\frac{\sum_{i\in M_x} T_{x,i}}{|M_x|}\right)\right] & 0 < |M_x| \leq 1-n \\ g_j & |M_x| = 0 \end{cases}$$

Tel que :

R_x représente l'ensemble des nœuds digne de confiance pour le nœud x

M_x représente l'ensemble des nœuds indigne de confiance pour le nœud x

n est le nombre total de nœuds.

-Peer Recommandation Evaluation

Quand un nœud x à besoin d'une recommandation au sujet d'un noeud y, il sollicite tous ses membres excepté ceux qui ne sont pas dignes de confiance puis effectue le calcul suivant :

$$T_{x,y} = \left[\frac{\sum_{i\in R_x \cup C_x} T_{x,i} \times T_{i,y}}{100 * j}\right]; \quad j = |\, R_x \cup C_x| \leq n-2$$

Tel que :

j est le nombre de membres dignes de confiance ou incertains.

-Calcule de la confiance au niveau de CH

GTSM considère qu'un CH est un nœud dont les capacités de calcul et de stockage sont plus grandes que celles des autres nœuds.

A ce niveau chaque CH réalise deux calculs de confiance, le premier est pour situer l'état de son propre groupe, et le second pour les autres groupes

-Calcul de l'état de son propre groupe

Chaque CH diffuse périodiquement une requête vers ses membres leur demandant de lui envoyer pour chacun ses états de confiance$s$. Supposons que dans un groupe il y a $n+1$ nœuds y compris le CH, alors le CH maintiendra la matrice des états de confiance suivante :

$$TM_{ch} = \begin{bmatrix} s_{ch,1} & s_{1,ch} & \cdots & s_{n,1} \\ s_{ch,2} & s_{1,2} & & s_{n,2} \\ \vdots & & \vdots & \vdots \\ s_{ch,n} & s_{1,n} & \cdots & s_{n,n-1} \end{bmatrix}$$

$s_{ch,1}$ Représente l'état de confiance du attribué par le CH au nœud 1.

Le CH assigne un état de confiance global à un nœud donné en se basant sur la différence relative aux états de confiance considérés par ce nœud vis à vis des autres membres. Ceci peut être représenté par une distribution qui suit une loi normale standardisée.

Le CH défini une variable aléatoire X tel que :

$$X(s_{i,j}) = \begin{cases} 2 & si \quad s_{i,j} = digne\ de\ confiance \\ 1 & si \quad s_{i,j} = incertain \\ 0 & si \quad s_{i,j} = indigne\ de\ confiance \end{cases}$$

Assumant que cette variable aléatoire est uniforme, et considérant que S_m est la somme de m telle variable, alors S_m suit une loi normale d'après le Théorème de central limite (toute somme de variables aléatoires indépendantes et identiquement distribuées tend vers une variable aléatoire normale) dont l'écart type est de $\sqrt{\frac{m}{3}}$. Le CH définie une valeur de confiance pour chacun de ses membre suivant la variable aléatoire Z_j :

$$Z_j = \frac{\sqrt{3}\left(X(s_{ch,j}) + \sum_{i=1,i\neq j}^{m} X(s_{i,j}) - m\right)}{\sqrt{m}}$$

Si $Z_j \in [-1;1\ ]$ alors le nœud *j* est considéré incertain

Si $Z_j > 1$ alors le nœud *j* est considéré digne de confiance

Si $Z_j < -1$ alors le nœud *j* est considéré indigne

-Calcul des états des autres groupes

Durant les communications inter-clusters, chaque CH maintient une table où il sauvegarde les anciennes interactions avec les autres CHs. De la même manière qu'au niveau d'un simple

nœud au sein d'un groupe, un CH *i* calcule la valeur de confiance $T_{i,j}$ d'un autre CH *j* en se basant soit sur les interactions effectuées dans le passé ou soit par recommandation de la station de base.

$$T_{i,j} = \begin{cases} \left[100\left(\frac{S_{i,j}}{S_{i,j}+U_{i,j}}\right)\left(1-\frac{S_{i,j}}{1+S_{i,j}}\right)\right] & PI_{i,j} \neq \varphi \\ BR_{i,j} & PI_{i,j} = \varphi \end{cases}$$

Si le CH *i* n'a pas encore effectué d'interactions avec le CH *j* c.-à-d.$PI_{i,j} = \varphi$, alors il sollicite la station de base pour une recommandation.

-Calcule de la confiance au niveau de SB

De la même manière aussi la station de base maintient un registre des interactions avec les CHs :

$$T_{BS,j} = \left[100\left(\frac{S_{BS,j}}{S_{BS,j}+U_{i,j}}\right)\left(1-\frac{S_{BS,j}}{1+S_{BS,j}}\right)\right]$$

Périodiquement, la station de base sollicite les CHs pour qu'ils envoient chacun leur vecteur de confiance :

$$\overrightarrow{T_{ch}} = (T_{ch,1}, T_{ch,2}, \dots, T_{ch,|G|-1})$$

A la réception de tous les vecteurs, la confiance d'un groupe est calculée comme suit :

$$T_{BS,G_1} = \left[\frac{\sum_{1=1}^{|G_i|-1}(T_{BS,ch_i})(T_{G_i,G_1})}{|G|-1}\right], \dots, T_{BS,G_m} = \left[\frac{\sum_{1=1}^{|G_i|-1}(T_{BS,ch_i})(T_{G_i,G_{|G|}})}{|G|-1}\right]$$

T_{BS,G_1} : est la valeur de confiance du CH *i* à la station de base, T_{G_i,G_1} est la valeur de la confiance du groupe G_1 au groupe G_i et G est le nombre de clusters dans le réseau.

3.6.3 Trust Based Routig (*TBR)*

TBR [FEN11] considère deux niveaux de confiance, le premier concerne la confiance entre un nœud simple et ses voisins du groupe et le second porte sur les confiances intergroupes. Les critères de confiance pris en compte dans ce protocole sont : l'intimité, l'honnêteté, l'énergie, et l'anti égoïsme. La valeur de la confiance est un nombre réel compris entre 0 et 1, la valeur 1 indique une totale confiance, la valeur 0,5 indique l'incertitude et la valeur 0 est synonyme d'absence totale de la confiance. $T_{i,j}(t)$: exprime la confiance du nœud *j* vu par le nœud *i* à l'instant *t*, elle est calculée comme suit :

$$T_{i,j} = w_1 T_{i,j}^{intimacy}(t) + w_1 T_{i,j}^{honesty}(t) + w_1 T_{i,j}^{energy}(t) + w_1 T_{i,j}^{unselfis\ hness}(t)$$

$w_1, w_2, w_3\ et\ w_1$: sont des poids associés aux quatre critères de confiance considérés avec $w_1 + w_2 + w_3 + w_1 = 1$

-Calcul de la confiance au niveau d'un nœud

La confiance attribuée au voisin *j* par le nœud *i* dans un groupe donné est calculée comme suit :

$$T_{i,j}^{X}(t) = \begin{cases} (1-\alpha) T_{i,j}^{X}(t-\Delta t) + \alpha T_{i,j}^{X,direct}(t) & si\ i\ et\ j\ sont\ des\ voisins \\ avg_{k \in N_i}\{\gamma T_{i,j}^{X}(t-\Delta t) + (1-\gamma) T_{k,j}^{X,recom}(t)\} & sinon \end{cases}$$

$T_{i,j}^{intimacy\ ,direct}(t)$: exprime le nombre d'interactions entre les nœuds *i* et *j* par rapport au nombre maximum d'interactions effectuées par le nœud *i* avec un autre voisin dans le groupe durant l'intervalle de temps [0, t]

$T_{i,j}^{honesty\ ,direct}(t)$: exprime la croyance du nœud *i* sur la non compromission de son voisin *j* à l'instant *t*

$T_{i,j}^{energy\ ,direct}(t)$: exprime le pourcentage d'énergie restante au voisin *j* observé par le nœud *i*

$T_{i,j}^{unselfis\ hness\ ,direct}(t)$: donne une idée sur le degré d'égoïsme du voisin j vu par le nœud i sur l'intervalle [0,t]

Dans le cas où le nœud *j* ne se trouve pas dans le voisinage direct du nœud *i*, alors ce dernier utilisera les expériences passées ainsi que les recommandations des voisins *k* en communs pour mettre à jour $T_{i,j}^{X}(t)$, γ est utilisé pour pondérer entre les deux contributions et exprime aussi la diminution de la confiance dans le temps :

$$\gamma = \frac{1}{1 + \beta T_{i,k}^{honesty}(t)}$$

Le facteur $\beta \geq 0$ spécifie l'impact des recommandations indirectes dans $T_{i,j}^{X}(t)$ de telle sorte que le poids assigné à celles-ci soit normalisé par rapport à 1. Essentiellement, la contribution des recommandations indirectes augmente proportionnellement avec l'augmentation de β ou$T_{i,k}(t)$.

-Evaluation de la confiance CH – nœud

Chaque nœud transmet ses états de confiance relatives à ses voisins du même groupe à son CH, celui-ci appliques une analyse statistique sur les valeurs $T_{i,j}$ afin d'évaluer la confiance du CH envers ses membres *j*

Modèle de performance

Un modèle de probabilité est développé pour étudier le comportement des nœuds. Ce modèle considère les deux aspects suivant :

Egoïsme

La probabilité pour qu'un nœud devienne égoïste augmente avec l'énergie consommée (un nœud ayant moins d'énergie cesse de coopérer pour l'acheminement de données) et le nombre de voisins égoïstes. Elle calculée comme suit :

$$P_{selfish} = \frac{1}{2}\left(\frac{E_{cons}}{E_{init}} + \frac{N_{neighbor}^{unselfish}}{N_{neighbor}}\right)$$

Honnêteté

Un nœud a plus de risque d'être compromis si son énergie restante est basse (pas assez d'énergie pour exécuter les mécanismes de défense) et son voisinage est compromis, la compromission est donnée par :

$$\lambda_c = \lambda_{c-1}\left(\frac{E_{init}}{E_{remain}} + \frac{N_{neighbor}^{compromised}}{N_{neighbor}^{healthy}}\right)$$

3.6.4 Trusted Multi Wireless Agent Communication (*TMWC*)

L'idée principale du protocole TMWAC [VER11] consiste calculer et d'estimer des valeurs de confiances des noeuds dans le réseau en tenant compte de leur comportements et cela à fin d'éviter toute interaction avec des nœuds jugés indigne de confiance.

-Gestion de la confiance

Chaque agent affecte des valeurs de confiances Trust[i] à ces voisins. Si Trust[i] > seuil prédéfinit donc l'agent i est digne de confiance si non il est jugé indigne de confiance et considéré comme étant un agent malveillant (défaillant).

Le fonctionnement d'un agent malveillant est dégradé c à d il effectue que les taches minimale et évite toute tache coopérative en lui affectant le nouveau rôle BACKUP qui est le rôle d'un simple membre qui ne peut pas être ni représentant ni un nœud de liaison .Tous les voisins d'un agent malveillant passent au mode dégradé ensuite ils seront mis en quarantaine pour ne pas influencer sur le comportement global du système.

-Estimation de la confiance

Chaque agent réalise localement des estimations de confiance en observant les messages émis dans son voisinage. Même si l'authentification est impossible, les agents doivent utiliser un identifiant (véritable ou usurpé) lors de l'envoi d'un message. Nous proposons ici d'estimer la confiance qu'à un agent dans l'usage d'un identifiant (plutôt que dans un agent authentifié par une identité).
Une nouvelle valeur de confiance est créée à chaque fois qu'un nouvel identifiant *id* est utilisé dans le voisinage d'un agent. Cette valeur est comprise dans l'intervalle [0; 1] avec pour valeur initiale une confiance maximale (Trust(id) = 1).

Mensonge sur	No	Detection par le neoud n	Baisse de la confiance
id	1	Si id utilisé=id de n	Trust(id)=0
	2	Si id utilisé=id de la station de collecte	Voir plus bas le processus *new group checking*
group	3	Si n est le représentant d'un groupe et que son groupe n'est pas inclus dans l'ensemble des groupes du message	Trust(id)=0
	4	Si un nouveau groupe G est présenté et que l'agent qui l'introduit est le seul agent à faire une liaison avec ce groupe	Voir plus bas le processus *new group checking*
Rôle	5	Si le nœud revendique un rôle de liaison vers un groupe G	voir plus bas le processus *new group checking*

Tab.7 : Estimation de la confiance

- Les situations 1 et 3 font respectivement référence au cas où un nœud perçoit un message utilisant son propre identifiant et au cas où un représentant perçoit un message venant d'un de ses voisins n'indiquant pas qu'il appartient au groupe du représentant. Dans ces cas, le message est indéniablement un mensonge visant soit à usurper l'identité d'un nœud, soit à cacher l'existence d'un groupe. La confiance est alors abaissée au plus bas niveau.

-La situation 2 correspond au cas où la station de collecte, supposée fixe apparaît à côté d'un nœud pendant son exécution. Cela reste possible car le capteur peut être mobile mais il se peut aussi qu'un agent tente d'usurper l'identité de la station de collecte. Les quatrième et cinquième situations où un voisin déclare appartenir à un nouveau groupe et éventuellement devenir nœud de liaison peuvent aussi arriver du fait d'une mobilité. Cela peut aussi être une tentative d'altérer le routage. Dans ces trois cas, le mensonge est ici suspecté mais sans certitude. La réaction à cette suspicion consiste alors à démarrer un processus (*new group checking*) visant à envoyer une requête à la station de collecte (cas 2) ou au représentant du groupe G (cas 4 et 5) lui demandant si le nœud v est bien dans son voisinage. Cette requête est envoyée par inondation à tous les voisins du nœud suspectant le mensonge et précise que la route de ce message doit éviter le nœud v. À chaque fois que le destinataire final reçoit cette requête, il y répond en indiquant si le nœud suspect v est dans son voisinage ou non. Il est bien entendu possible que v puisse percevoir ce message, car il est dans le voisinage du nœud

l'ayant initialement émis et renvoie une fausse réponse usurpant encore l'identifiant concerné. Suivant les réponses reçues à cette requête, la confiance est mise à jour comme indiqué dans le tableau suivant:

Réponses reçues	Baisse de la confiance
Aucune réponse	Pas de baisse
Toutes les réponses indiquent que v est dans le groupe G	Pas de baisse
Toutes les réponses indiquent que v n'est pas dans le groupe G	Trust(id)=Trust(id)-α
Des réponses différentes sont reçues	Trust(id)=Trust(id)-β

Tab.8 : Mis à jour de la confiance.

Si aucune réponse n'est reçue ou si toutes indiquent que v est dans le groupe G, il n'y a probablement pas de mensonge. Si toutes les réponses indiquent que v n'est pas dans le groupe G, il peut soit y avoir un mensonge soit une croyance de v temporairement fausse. La confiance est alors réduite d'une valeur α mais pas à la valeur minimale.
Le dernier cas consiste en une situation où des réponses différentes arrivent. Il se peut que cela soit dû à de fausses réponses renvoyées et que v soit un usurpateur. Il reste néanmoins une possibilité plus rare dans laquelle v est dans le groupe G quand son représentant reçoit et répond à une partie des requêtes et l'ait quitté quand il répond aux requêtes restantes. La sanction β sur la confiance doit ici être plus importante mais pas encore maximale. Nous proposons de fixer ces sanctions dans l'intervalle $0 < \alpha < \beta < 1$. La valeur minimale de la confiance est fixée à 0 et ramenée à cette valeur si une décroissance amène une confiance négative.

-**Recouvrement de la confiance**

Il est nécessaire que la confiance dans un voisinage puisse être rétablie. La mobilité, même faible, du réseau fait qu'un nœud malveillant peut être amenée à quitter un voisinage. Il peut aussi être tout simplement retiré du réseau ou ne plus fonctionner faute d'énergie. Il se peut également qu'une défiance vis-à-vis d'un voisinage ne soit pas la cause d'une malveillance mais d'une cooccurrence d'événements exceptionnels ayant entrainés plusieurs suspicions. Le rétablissement de la confiance s'opère ici par un phénomène d'oubli avec une lente augmentation de la confiance avec le temps. L'algorithme 1 implémente ce phénomène.

Algorithm 1 Algorithme de recouvrement de la confiance

```
For all id in neighborhood.getUsedIds() do
    Trust(id)=(1-λ)*Trust(id)+ λ
End for
```

Deux facteurs paramètrent la vitesse du rétablissement de la confiance : (i) la fréquence μ à laquelle l'algorithme de rétablissement est invoqué; (ii) le taux d'évaporation de la sanctionλ, avec $0 < \lambda < 1$ indiquant la quantité de confiance regagnée à chaque cycle. La valeur de ces paramètres dépend principalement de la mobilité supposée des nœuds. En présence d'une

mobilité forte, nous recommandons une fréquence et un taux d'évaporation importants car les voisinages devraient souvent varier. Si la mobilité est faible, le réseau sera plutôt statique et il est préférable de ralentir le rétablissement avec des valeurs plus faibles pour ces paramètres.

-Prise de décision de confiance

La confiance dans les identifiants est utilisée pour estimer la confiance du voisinage dans son ensemble. Le voisinage d'un nœud est jugé indigne de confiance s'il existe au moins un identifiant dans lequel le nœud n'a pas confiance. Le seuil θ représente la valeur de confiance minimale en dessous de laquelle un nœud est jugé indigne de confiance. Ce seuil prend une valeur dans $0 < \theta < 1$.

Algorithm 2 Algorithm de décision de confiance dans le voisinage

```
For all id in neighborhood.getU sedIds() do
  If Trust(id)<0 then
     Returm distrusted
  End if
End for
    Return trusted
```

-Adaptation du modèle MWAC

Lorsqu'un nœud n'a pas confiance dans son voisinage, il adopte un fonctionnement dégradé et participe au minimum au routage. Le mode dégradé correspond dans MWAC à un nouveau rôle BACKUP. L'algorithme 3 est une adaptation du processus d'affectation des rôles.

Algorithm 3 Adaptation de l'affectation des rôles

```
 If  neighborhood.isEmpty() then
    // No possible organizational structure
 Else if neighborhood.trust()=distrusted then
      MyRole←BACKUP
Else if myRole=REPRESENTATIVE and neighborhood.nbO f Representative()>0 then
     conflictResolutionProcedure()
else if  neighborhood.nbO f Representative()=0
then
     myRole←REPRESENTATIVE
else if neighborhood.nbO f Representative()=1
then
     myRole←SIMPLEMEMBER
else {neighborhood.nbO f Representative()>1}
    myRole←CONNECTION
end if
```

Le nouveau rôle BACKUP correspond au même fonctionnement que le rôle de simple membre, excepté qu'il est impossible d'évoluer vers un rôle de représentant ou de liaison.

-Mise en quarantaine

L'échange de recommandations ou/et la construction collective de réputations est une pratique classique en gestion de la confiance pour augmenter le nombre d'informations prises en entrée et accélérer l'apprentissage de valeurs de confiance précises. Cependant, l'absence d'authentification nous empêche l'usage de ces techniques car elles nécessitent aussi d'associer une valeur de confiance ou de réputation à une identité indéniable

L'échange de valeur de confiance ne présente dans notre cas que peu d'intérêt. Par contre, le fait de savoir que certains voisins d'un nœud ont adopté un rôle BACKUP est utile. Cela signifie qu'il y a probablement un agent malveillant à proximité et peut-être dans le voisinage direct du nœud qui reçoit cette information.

A fin de partager cette information, nous proposons ici une seconde variante de MWAC où les agents prennent en compte l'éventuel rôle BACKUP de leurs voisins. Un nœud informe ses voisins de son rôle dans le message classique d'introduction envoyé périodiquement, et dans le cas du rôle BACKUP [id*], il y ajoute les identifiants ([id*]) en lesquels il n'a pas confiance. L'objectif est de propager ce message à tous les voisins présumés du nœud ayant cet identifiant afin que ceux-ci passent également en mode dégradé. Si tout le voisinage du nœud déviant est en mode dégradé, son entourage dans le réseau sera mis en quarantaine et il ne pourra plus nuire au bon fonctionnement du système.

La prise en compte du rôle des voisins afin de partager les informations de confiance nécessite une adaptation de l'algorithme 2 de décision de confiance telle que présentée par l'algorithme4.

Algorithm 4 Décision de confiance intégrant le rôle des voisins

```
For all id in neighborhood.getUsedIds() do
    If Trust(id)<0 then
        Return distrusted
    End if
    If (role(id)=BACKUP(IDS)) and (IDS∩neighborhood.getUsedIds()≠0) then
    return distrusted
    End if
End for
    return trusted
```

3.6.5 A centralized Trust and Competence-based Energy-efficient routing scheme for wireless sensor networks (*TRACE*)

TRACE [AYM11] consiste à interdire tous type de communication avec des nœuds ayant un mauvais comportement. A fin d'évaluer le comportement de chaque nœud capteur la SB calcule différentes métriques de qualité comme : malveillance, coopération, compatibilité, duré de vie de la batterie, confiance de transmission et de la donnée

-Calcule de la valeur de malveillance d'un nœud (Maliciousness)

La station de base calcule pour chaque nœud i la valeur de malveillance qui est une valeur comprise entre 0 et 1comme un, selon la formule suivante :

$$Maliciousness = \frac{\text{Count of bad packets received from node}}{\text{Total count of packets received from node}}$$

-Calcul de coopération d'un nœud

La coopération d'un nœud N est définit comme étant la volonté que ce nœud coopère avec d'autres nœuds à fin de transmettre un paquet de données ou bien un message vers la SB. Elle est calculée par la formule suivante:

$$cooperation(N) = \frac{\sum \mathrm{a_i}\ x\ f\_conter_{in}}{\sum \mathrm{a_i}\ x\ s\_conter_{in}}$$

Tel que : a représente le poids de chaque liaison montante d'un nœud qui est lié à son niveau de malveillance. a est calculé comme suit :

$$\mathrm{a_i} = 1 - maliciousness(i)$$

-Calcule de compétence d'un nœud

C'est la capacité qu'un nœud envoie correctement un paquet vers la SB.la compétence est une valeur calculé par la SB pour chaque nœud capteur i ayant envoyé un paquet cette dernière. La compétence est comprise entre 0 et 1 qui est un rapport entre le nombre de paquet reçu par la SB et le nombre de paquet envoyé par ce nœud i comme suit :

$$competence = \frac{\text{Count of packets received by sink}}{\text{Count of packets sent by node}}$$

Ensuite la SB calcule deux valeurs de confiance pour chaque nœud dans le réseau : valeur de confiance de donnée et une autre valeur pour la confiance de transmission.

-Calcule de Confiance de donnée

La valeur de la confiance d'une donnée d'un nœud N est utilisée par les autres nœuds afin de transmettre la donnée ou l'écarter. Elle est calculée en fonction de niveau de malveillance et la coopération d'un nœud (pour forcer les nœuds à coopérer à fin d'augmenter leur valeur de confiance).Les valeurs de confiances de données sont comprises entre 0 et 1 .Elle est calculée comme suit :

$$\text{Data Trust} = (1 - maliciousness)x(cooperation)$$

-Calcule de confiance de transmission

Indique la confiance dans la capacité qu'un nœud i transmet avec succès un paquet vers la station de base. Elle est calculée en fonction de valeur de compétence et celle de duré de vie de la batterie qui est comprise entre 0 et 1.

$$\text{Forwarding Trust} = (Estimated\ Battery\ Life)x(Competence)$$

-Différents mauvais comportements des nœuds

-Nœud malveillant : est un nœud qui envoie des mauvais paquets (erronés ou malveillants) à la station de base.

-Nœud non-coopératif : est un nœud qui ne coopère pas avec d'autre nœud c'est à dire ne transmit pas les paquets pour ces voisins .La station de base peut détecter ce type des nœuds en comparant la valeur de sa compétence et celle de sa coopération .Si sa coopération est moins que sa compétence donc un tel nœud peut dégrader le fonctionnement du RCSF.

-Nœud diffusant des paquets inconnus ce qui permet de diminuer la performance du réseau. Cependant ils ne peuvent pas affectés le système car ces paquets sont abandonnés donc CENTER fournit une forte défense aux ce genre attaques.

-Isolation des nœuds malveillants

Les nœuds malveillant et non-coopérant sont isolés après un nombre de périodes, calculées tenant compte leurs confiances de données et l'historique de leurs comportements. L'historique de comportement d'un nœud est mémorisé par la SB en gardant une trace du nombre de fois que le nœud a été précédemment trouvé mauvais. Chaque fois qu'un nœud est banni du système, le nombre de périodes est incrémenté.

3.6.6 Trust-Aware Routing Framework (*TARF*)

TARF [GUO12] est une plateforme de routage dynamique, elle fournit une solution de routage fiable dans l'environnement des RCSFs. Cette plateforme est constituée de quatre composants : métrique d'évaluation de la confiance, détection du comportement qui est fondé sur la surveillance d'autre nœuds, évaluation de la confiance qui s'effectue suivant plusieurs facteurs qui sont : auto-observation, recommandation, réputation et modèle de routage basé sur la confiance.

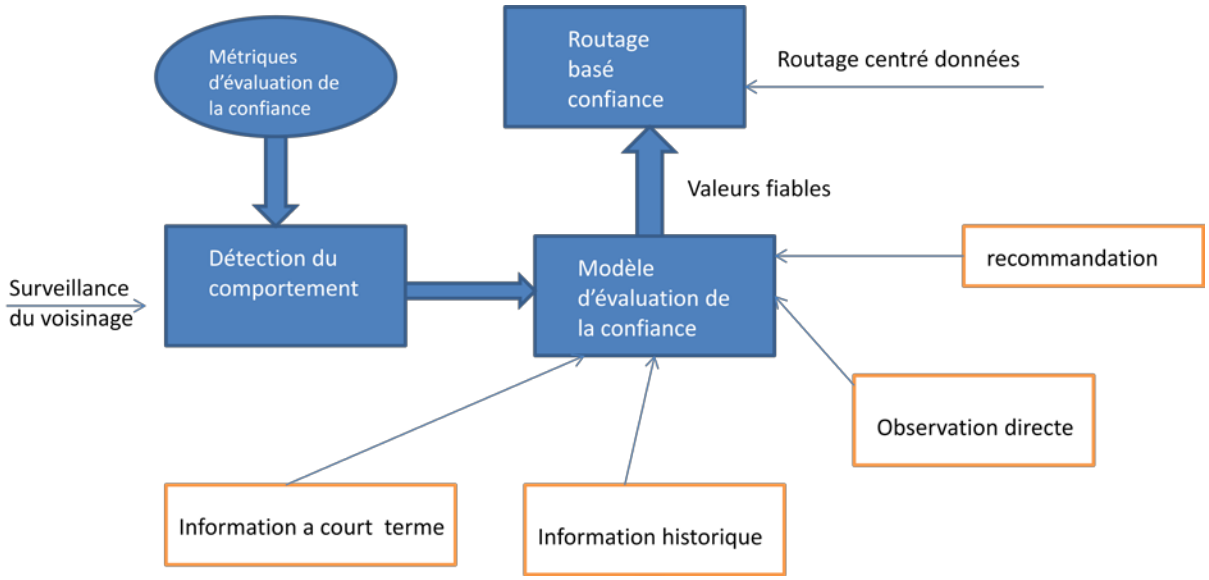

Fig.17: Schéma de la plateforme TARF.

-Métriques d'évaluation de la confiance

Les métriques d'évaluation utilisées dans ce système sont représentées dans le tableau suivant :

Métriques d'évaluation de la confiance
Vérification de la cryptographie (TE_V)
Observation de la transmission des paquets (TE_p)
Observation de la modification des paquets (TE_m)
Vérification des messages de routage (TE_R)

Tab.9 : Métriques d'évaluation de la confiance

-Modèle d'évaluation de la confiance

Le schéma suivant représente le modèle d'évaluation de la confiance :

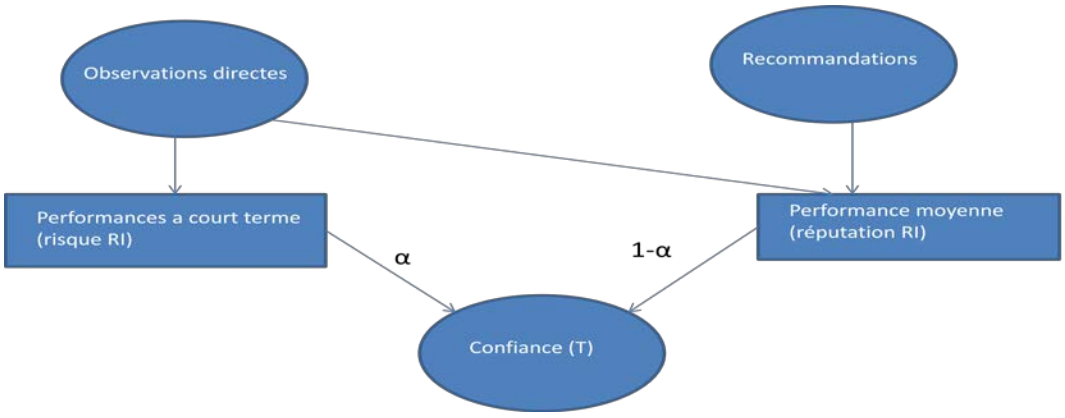

Fig.18 : modèle d'évaluation de confiance utilisé par TARF

Dans ce modèle la confiance (T) est déduite à partir de la réputation (RE) et le risque (RI), ces derniers sont ajustés par un facteur α :

$$T = \begin{cases} (1-\alpha, \alpha) x (R_E, R_i)^T , & 0 \leq \alpha \leq 1 \\ R_i , & if\ \alpha = 1 \\ R_E, & if\ \alpha = 0 \end{cases}$$

-Détection du comportement

Surveille les interactions des nœuds voisins afin de détecter les nœuds malveillants.

-Routage basé confiance

Les valeurs de confiances affectées aux nœuds dans le RCSF sont utilisées pour guider le processus de routage à fin de choisir la meilleure route.

3.6.7 Trust-aware Sensor Network Information Protocol for Efficient Routing (*T-SNIPER)*

T-SNIPER [SOU10] est une plateforme basée confiance .Elle permet de déterminer les meilleurs chemins pour chaque nœud vers la SB. Cette plateforme évalue la confiance entre deux nœuds en tenant compte des valeurs de réputations perçues et suggérées.

La réputation perçue est la valeur de la confiance accordée à un nœud i, par le nœud j, sur la base du montant de l'interaction entre i et j (facteur de proximité rij). La valeur du facteur d'proximité d'un nœud est initialement à zéro. Avec le temps, les données sont collectées par le nœud et les lectures respectives commencent à affecter le résultat d'ensemble, le facteur de proximité affecté au nœud commence à augmenter, cela dépend du seuil de réponse d'un une tâche particulière, Tθ, et l'écart absolu moyen du seuil de popularité nœud, il peut être déterminé comme suit ce dernier sera calculé comme suit:

$$MAD = \frac{1}{n-1} \sum_{i=1}^{n} (y_i - \bar{y})^2$$

Avec :

n : représente le nombre de taches Tθ.

Le facteur de proximité est calculé par la formule suivante :

$$r = \frac{1}{n-2k} \sum_{i-k+1}^{n-k} r(i)$$

Avec : n (≥ 5) est l' nombre de lectures nécessaires à l'acquisition d'un niveau acceptable la valeur de r ; k est la dimension de coupe pour éliminer les k plus grand et k plus petit parmi n valeurs.

La réputation d'un nœud est une valeur dynamique qui dépend de plusieurs facteurs tel que : l'énergie d'un nœud, nombre de paquets de données reçus ou transmit par un nœud. Elle est calculée comme suit :

$$T_{ij} = \sum_{i=1}^{n} [w_{ij} \times T_{ij}]$$

W_{ij} : poids entre les nœuds i et j qui est compris entre 0 et 1 ; n est le nombre totale de nœuds ; et $T_{i,j}$ est la confiance de j attribué par i.

Si le facteur de proximité est négligeable, W_{ij} est égale à la valeur de confiance suggéré par le nœud j. Pour chaque interaction entre i et j, W_{ij} s'incrémente. Comme les nœuds i et j commence à interagir, à chaque interaction avec succès le poids attribué est incrémenté entre -1 et 1. Par conséquent, si le nœud i, arrive toujours à rencontrer le délai d'attente tout en communiquant avec nœud j, le poids serait diminué à -1, à un point qu'il sera déclaré non digne de confiance

Avec n : le nombre totale de nœuds ; W_{ij} : le poids entre le nœud i et le nœud j et T_{ij} est la confiance de j attribué par i.

3.6.8 Un mécanisme de routage sécurisé pour réseaux de capteurs sans fil statiques

Les auteurs de [XUA08] ont proposé un modèle de confiance qui repose sur trois métriques :

-La première métrique utilisée dans cet algorithmes est le taux de transmission des paquets, défini comme le rapport de $replay_{i,j}$ (nombre de paquets réponses reçus depuis Nj) sur $n_{i,j}$ (le nombre de paquets émis de Ni vers Nj)durant une fenêtre de temps fixe :

$$TF_{i,j} = \begin{cases} \frac{reply_{i,j}}{n_{i,j}}, n_{i,j} > 0 \\ T_{i,j} . \frac{Treply_{i,j}}{Tn_{i,j}}, n_{i,j} = 0 \end{cases}$$

Tel que :

$treplay_{i,j}$:est le nombre total des paquets réponses envoyés de Nj vers Ni.

$Tn_{i,j}$: est le nombre total de paquets envoyés de Ni vers Nj.

-La deuxième métrique d'évaluation de la confiance est l'énergie résiduelle où chaque nœud peut évaluer l'énergie résiduelle de ses voisins :

$$TE_{i,j} = \begin{cases} 0, EE_{i,j} \geq ER_j \\ -0.5, EE_{i,j} < ER_j \end{cases}$$

Tel que :

$EE_{i,j}$: l'énergie résiduelle de j évoluée par Ni.

ER_j : l'énergie résiduelle de Nj.

-La dernière métrique est le nombre de sauts :

Soient :

$D_{i,x}$: les sauts de Ni vers la station de base.

($D_{i,x}$ - 1) : le minimum de sauts effectué de Ni vers la station de base.

($D_{i,x}$ + 1) : le maximum de sauts effectué de Ni vers la station de base.

La confiance pour cette métrique est alors calculée comme suit :

$$TD_{i,j} = \begin{cases} 0, (D_{i,x} + 1) \geq D_{j,x} \geq (D_{i,x} - 1) \\ -0.5, D_{j,x} < (D_{i,x} - 1) \end{cases}$$

-Apres avoir toutes les valeurs de confiance pour les différentes métriques ; la confiance totale sera obtenue comme suit :

$$T_{i,j} = TF_{i,j} . (1 + TE_{i,j} + TD_{i,j})$$

Pour évaluer la confiance d'un nœud, sa valeur sera comparé à un seuil □, si la confiance d'un nœud est inferieur à □/2, le nœud sera jugé indigne de confiance et sera mis dans la liste noire.

3.6.9 Implémentation d'un protocole de routage basé confiance dans les nœuds capteurs sans fil

Les auteurs de [THE10**]** ont proposé un protocole de routage distribué basé confiance qui intègre à la fois la confiance directe et la confiance indirecte (réputation).

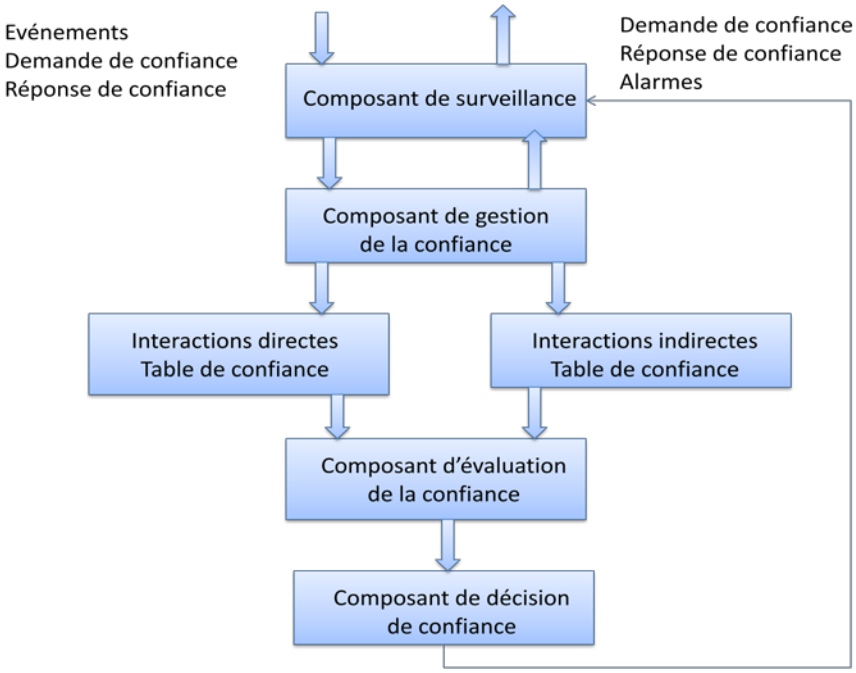

Fig.19: schéma de gestion de la confiance

L'une des innovations de ce protocole est d'offrir une protection contre plusieurs types d'attaques en se basant sur un ensemble de métriques représentées dans le tableau ci dessous :

Métriques de confiance
Transmission
ACK-réseau
Intégrité de données
Authentification des nœuds
Confidentialité des données

Réponses de réputation
Validation de la confiance
Energie résiduelle

Tab.10: Liste des métriques de confiance

-Confiance directe

Pour chaque comportement observé, un nœud Ni calcule une valeur de confiance pour son voisin Nj selon la métrique (m) citée dans le tableau précédent en calculant le nombre d'interactions réussies sur le nombre total d'interactions suivant la formule suivante :

$$\mathrm{T}_{\mathrm{m}}^{\mathrm{i,j}} = \frac{S_m^{i,j}}{S_m^{i,j} + U_m^{i,j}}$$

Tel que : $S_m^{i,j}$: le nombre d'interactions réussies entre Ni et Nj pour le comportement observé m.

$U_m^{i,j}$: Le nombre d'interactions échouées entre Ni et Nj pour le comportement observé m.

Apres avoir calculé toutes les valeurs de confiance directe pour chaque comportement observé, la valeur totale de la confiance directe est obtenue par l'addition de ces dernières :

$$\mathrm{T}^{\mathrm{i,j}} = \sum_{i=1}^{7} \left[w_m \times \mathrm{T}_{\mathrm{m}}^{\mathrm{i,j}} \right]$$

-Confiance indirecte (réputation)

Chaque nœud Ni envoi une demande de réputation à propos de l'un de ses voisins Nj choisi aléatoirement.

Selon les réponses reçues la confiance indirecte est calculée :

$$IT^{i,j} = \frac{\sum_p^k (DT^{i,Np} * DT^{Np,j})}{\sum_p^k DT^{Np,J}}$$

-Confiance totale

Une fois que la confiance directe et la confiance indirecte sont obtenues, la confiance totale sera calculée par la combinaison de ces deux dernières valeurs :

$$TT^{i,j} = C^{i,j} * DT^{i,j} + \left(1 - C^{i,j}\right) * TT^{i,j}$$

Ce mécanisme de gestion de la confiance est intégré par la suite dans un protocole de routage basé localisation.

$$\check{R}F^{i,j} = W_d * T_d^{i,j} + W_t * TT^{i,j}$$

3.7 Conclusion

La confiance est un facteur important dans tout type de réseau que se soit social ou informatique. Dans ce chapitre, pour bien comprendre la notion de confiance dans les RCSFs, nous avons tout d'abord donné un aperçu sur ses différentes définitions dans divers domaines, ses caractéristiques. Ensuite, nous avons expliqué la relation entre la sécurité et la confiance dans les RCSFs. La mise en place de la confiance dans les RCSFs nécessite l'implémentation de tout un système de gestion de la confiance qui peut être classé en trois catégories : les systèmes de gestion centralisés, distribués ou hybrides.

Dans le chapitre suivant nous allons présenter le fonctionnement du nouveau protocole de routage que nous proposons, qui représente une amélioration du protocole EAR en introduisant un mécanisme léger de gestion de confiance.

Chapitre 4

Contribution

4.1 Introduction

La propagation et l'acheminement de données dans un RCSF représentent une fonctionnalité très importante. Plusieurs protocoles de routage ont été proposés pour les RCSF grâce aux avantages qu'ils présentent. Bien que les techniques de routage semblent prometteuses, elles restent un sujet à plusieurs défis à surmonter, à savoir celui de la sécurité de communication. Parmi ces protocoles, on distingue EAR [RAH02] qui suit une architecture plate et qui a était proposé pour remédier a la contrainte d'énergie afin d augmenter la durée de vie du réseau.son principe est en quelque sorte similaire a celui de la diffusion ; plusieurs routes sont maintenues entre la station de base et la source. Cependant la différence est que dans la diffusion la donnée est envoyée à travers toutes les routes à un intervalle régulier, tandis qu'EAR utilise une seule route qui sera choisi selon sa probabilité.

4.2 Description de l'algorithme EAR

EAR se déroule en trois phases pour chaque round :

4.2.1Phase d'installation

-La station de base diffuse un message d installation SetUpMsg en initialisant son cout a zéro :

$$Cost\ (N_D) = 0$$

-Chaque nœud intermédiaire qui reçoit un SetUpMsg il le rediffuse à ses voisins qui sont loin de la station de base et proche du nœud source. c.à.d. un nœud Ni rediffuse le message a un voisin Nj seulement si Nj satisfait :

$$d(N_i, N_s) \geq d\left(N_s, N_j\right)$$

$$d(N_i, N_D) \leq d\left(N_j, N_D\right)$$

Tel que : d (Ni, Nj) est la distance entre Ni et Nj.

Un nœud Nj qui reçoit un message d installations d un nœud voisin Ni :

-Calcule le coût pour atteindre la destination à travers ce voisin selon la formule suivante :

$$C_{N_j, N_i} = Co\hat{u}t(N_i) + M\acute{e}trique(N_j, N_i)$$

Seuls les voisins avec des chemins de faible coût sont ajoutés à la table de routage (FTj).

$$FT_J = \left\{i \middle| C_{Nj,Ni} \leq \propto (min_k C_{Nj,Nk})\right\}$$

-La métrique d'énergie est calculée selon la formule suivante :

$$\text{Cij}=e_{ij}^{\propto} = e_{ij}^{\propto}\ R_i^{\beta}$$

Tel que :

Cij : la métrique entre Ni et Nj.

e_{ij} : l'énergie utilisée pour transmettre et recevoir sur le lien.

Ri : l'énergie résiduelle au nœud Ni normalisée à l'énergie initiale du nœud.

α et β : des poids utilisés pour choisir la meilleur métrique

-Calcule une probabilité pour chacun de ses voisins et l'insert dans sa table de routage :

$$P_{N_j,\ N_i} = \frac{1/C_{N_j,N_i}}{\sum_{k\in FT_j} 1/C_{N_j,N_k}}$$

-Une fois que toutes les probabilités des nœuds voisins sont calculées, le nœud calcule son cout moyen pour atteindre la destination selon la formule suivante :

$$Coût\ (N_j) = \sum_{i\in FT_j} P_{N_j,N_i} \times C_{N_j,N_i}$$

-Vérifie le TTL :

Si TTL = 0 alors il écarte le message d installation.

Sinon il insert son cout moyen et le rediffuse a ses voisins.

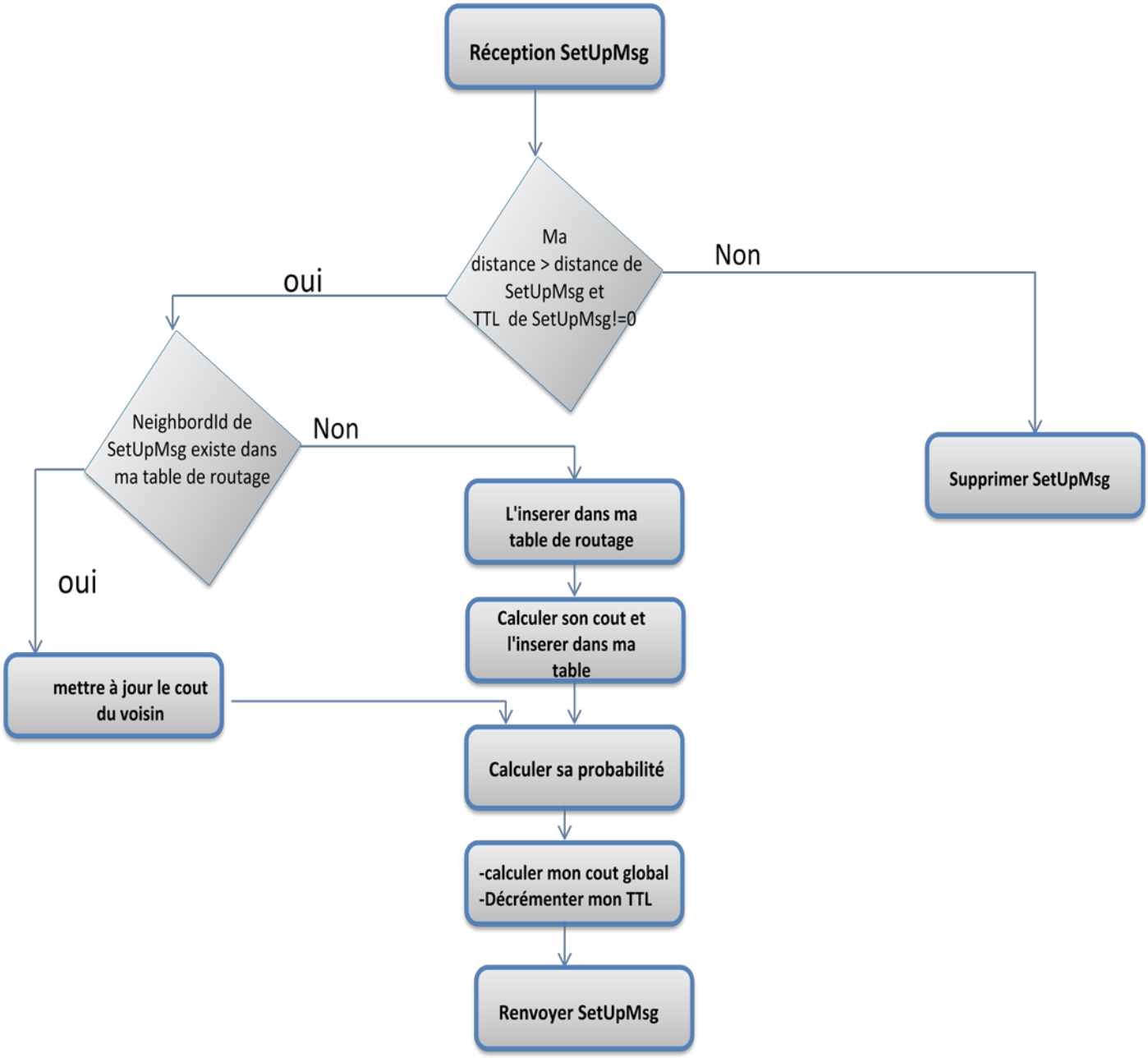

Fig.20 : Organigramme de la phase installation dans EAR.

4.2.1Phase communication de données

-Un nœud source pour transmettre son paquet de données il choisit dans sa table de routage le voisin ayant une plus grand probabilité.

-Un nœud intermédiaire quand il reçoit un paquet de données il l'envoie a son tour a son voisin ayant une plus grande probabilité dans sa propre table de routage, jusqu' a y arriver a la destination (station de base).

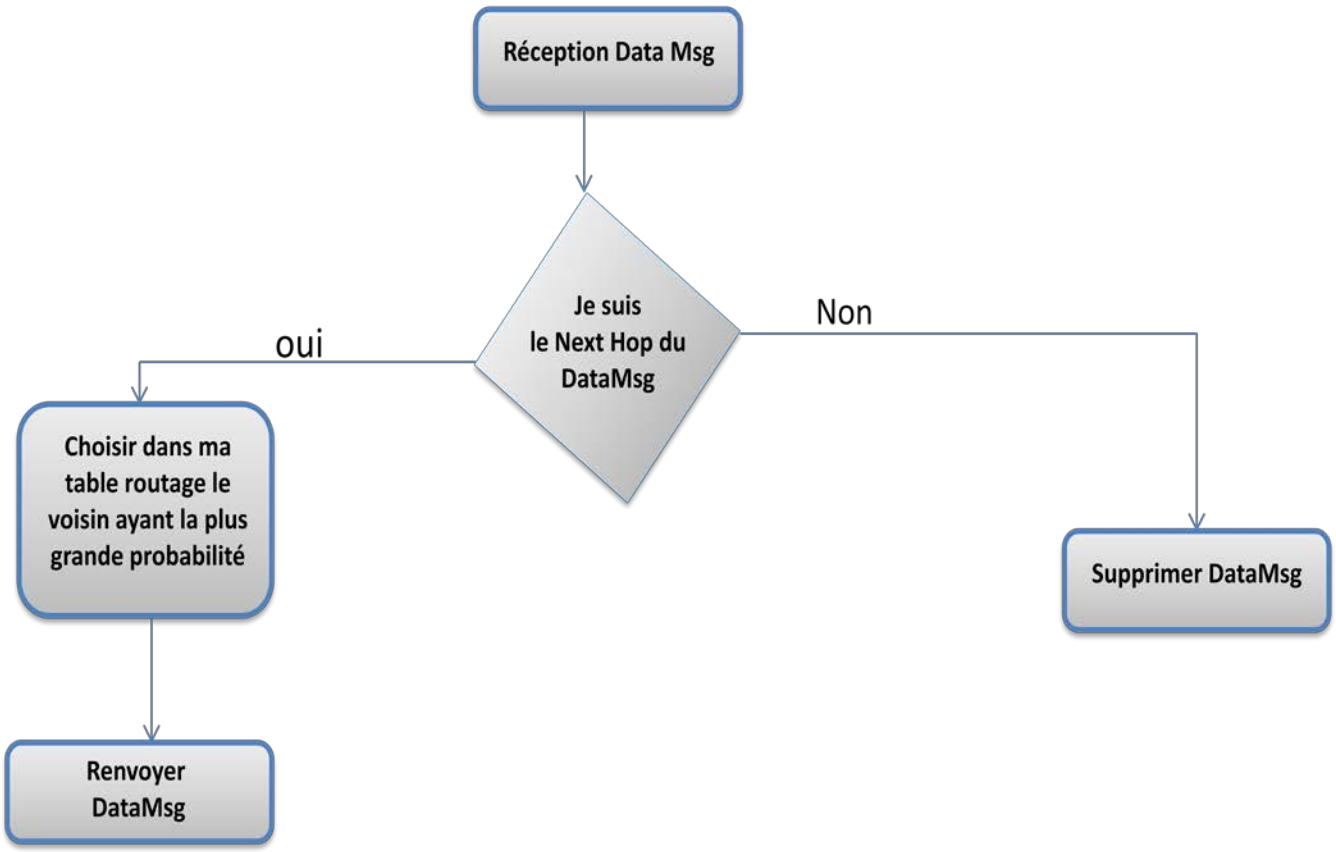

Fig.21 : Organigramme de la phase communication de données dans EAR.

4.2.3 Phase de maintenance

A chaque round la station de base diffuse un SetUpMsg pour la maintenance des routes.

Notre amélioration repose sur l'intégration d'un mécanisme de gestion de la confiance au protocole EAR afin de faire face à l'égoïsme qui peut apparaitre sur certains nœuds du réseau.

4.3 Description de l'algorithme TEAR

Initialement la valeur de confiance que chaque nœud affecte à ses voisins est à 1. Ces valeurs varient dans l'intervalle [0,1] :

4.3.1 Mécanisme de surveillance

Quand un nœud Ni transmet un paquet de données a son voisin Nj, il verifie si ce dernier a bien retransmet le paquet (vue que le Nj est dans le rayon de transmission de Ni ; Ni pourra facilement écouter son voisin Nj). Ensuite Ni stocke le nombre d'interactions réussies et celui des interactions échoués.

4.3.2 Calcul de la confiance

-La confiance sera calculée selon la formule suivante :

$$\mathrm{T}_{\mathrm{Ni,Nj}} = \frac{S_{Ni,Nj}}{S_{Ni,Nj} + U_{Ni,Nj}}$$

Tel que :

$S_{Ni,Nj}$: Le nombre d'interactions réussies entre Ni et Nj.

$U_{NiN,j}$: Le nombre d'interactions échouées entre Ni et Nj.

4.3.3 Mis à jour de la confiance

A chaque réception d'un paquet de données suite à une écoute, le nombre d'interactions réussies augmente et la valeur de confiance sera recalculée.

4.3.4 Intégration de la confiance dans la phase de transmission

La valeur de la confiance de chaque voisin sera combinée avec sa valeur de probabilité pour obtenir le score du chemin :

$$\mathrm{score}_{\mathrm{Ni,Nj}} = (1-\alpha)\ \mathrm{P}_{\mathrm{Ni,Nj}} + \alpha\ \mathrm{T}_{\mathrm{Ni,Nj}}$$

Tel que : α est le facteur d'équilibrage.

Lorsqu'un nœud doit transmettre un paquet de données, il cherche son voisin ayant un plus grand score.

4.4 Conclusion

Dans ce chapitre nous avons présenté un mécanisme léger de gestion de confiance afin d'améliorer le protocole de routage EAR. Nous avons donc détaillé le fonctionnement du protocole EAR. Ensuite, nous avons détaillé notre mécanisme de gestion confiance, nous avons commencé par la métrique d'évaluation de la confiance, comment calculer la valeur de confiance et enfin l'intégrer dans le protocole EAR.

Dans le chapitre suivant, nous allons implémenter sous OMNET++ le protocole EAR et TEAR à la présence des nœuds égoïstes et comparer les résultats obtenus.

Chapitre5

Tests

5.1 Introduction

Afin d'évaluer les performances des protocoles EAR et TEAR, nous avons eu recours à la simulation qui consiste à reproduire le comportement des entités du monde réel dans le monde virtuel. Pour cela, nous avons choisi le simulateur OMNET++ qui simule les réseaux de capteurs sans fil et qui nous a permis d'implémenter et de tester les deux protocoles.

5.2 Quelques environnements de simulation

Nous citons dans ce qui suit quelques environnements de simulation [ABD12] :

5.2.1 Network simulator(*NS2*)

« NS2 » désigne la deuxième version du NS (*Network Simulator*), C'est un simulateur à événements discrets dans le temps. Il a été conçu pour être un simulateur générique. Par conséquent, il constitue un support important pour la simulation des protocoles standards tels que TCP, IP, et ce, aussi bien à travers les réseaux filaires qu'à travers les réseaux sans fils. Il supporte également les réseaux ad hoc et les réseaux de capteurs et comprend quelques protocoles implémentés tel que *Directed Diffusion*. NS est un simulateur multicouches et son développement suit une approche orienté-objet en utilisant deux langages de programmation : C++ et OTCL (Object Tools Command Langage dérivé de TCL). Effectivement, le noyau, les modèles, les protocoles et les composants de base sont écrits en C++, tandis que les interfaces sont implémentées en OTCL. Des scénarios de simulation, écrits en OTCL, peuvent être introduits afin de décrire les conditions de la simulation, essentiellement, la topologie du réseau, les caractéristiques des liens physiques, les protocoles utilisés et les communications qui ont eu lieu. L'utilisation de l'OTCL permet aussi à l'utilisateur de créer ses propres procédures. Une fois le scénario défini, NS entame la simulation et génère un fichier de trace « .log ». Ce fichier est interprété par l'outil NAM (*Network Animator*), associé au simulateur NS, afin de visualiser des animations de la simulation (transfert des paquets, taille des paquets, remplissage des files d'attentes, etc.).

Avantages

- NS2 est un logiciel de simulation multicouches ;

-Il est complètement libre et existe pour plusieurs plateformes ;

- Son développement orienté-objet permet l'ajout de composant à la demande ;

-Sa popularité a permis l'enrichissement de sa bibliothèque de protocoles.

Inconvénients

- Il n'est pas destiné aux RCSFs, ce qui limite beaucoup son utilisation dans ce domaine ;

- Ses modèles standards contiennent peu de paramètres de configuration ;

- La dépendance entre les modèles rend difficile l'ajout de nouveaux modèles ;

-Inadapté aux réseaux de grande taille ;

-Difficile à utiliser et à intégrer dans des applications.

5.2.2 GLOSSIM

GloMoSim (*Global Mobil Simulator*) est un environnement de simulation pour les réseaux sans fils de grande taille. Il a été développé par PCL (*Parallel Computing Labaratory*) de l'UCLA (*University of California, Los Angeles*) dans le cadre du projet DARPA GOLOMO (*GLObalMobil information system*). Ce simulateur s'appuie sur la capacité de simulation parallèle des événements décrits de PARSE (*Parallel Simulation Environnement for Complex systems*). Ce dernier est développé par PCL de l'UCLA à base de C-AINSI avec quelques possibilités héritées du C++. Il introduit les notions des entités, pouvant s'exécuter en parallèle, et de messages, échangés entre ces entités. GloMoSim est construit suivant une approche basée sur les couches, qui est similaire au modèle à sept couches de l'OSI. Les couches constituant l'architecture de ce simulateur sont les suivantes : mobility, radio propagation, radio model, packet reception models, data link (MAC), network *(routing*), transport et application. Des fonctions standards (API) sont utilisées pour assurer la communication et l'échange de services entre ces couches. Avant de démarrer une simulation, l'utilisateur doit saisir les paramètres de configuration dans deux fichiers : app.conf et config.in. Le premier contient les paramètres relatifs à la couche applicative tandis que le second contient la description :

• Des couches PHY, MAC, réseau et transport

• Du canal radio

• Des scénarios de mobilité

• De l'environnement (terrain, nombre de noeuds, etc.)

• De la durée de la simulation

• Du type de statistiques à prendre en considération qui seront enregistrées dans un fichier: glomo.stat.

On dispose également d'une interface graphique java rudimentaire pour l'affichage des dimensions du terrain, des communications radios et de la mobilité des nœuds.

Avantages

-L'exécution parallèle augmente considérablement la sociabilité de la simulation : des réseaux de cent miles noeuds peuvent être simulés ;

-GloMoSim est disponible gratuitement et en open source pour Windows et Linux.

Inconvénients

-L'utilisation du GloMoSim nécessite une maîtrise du langage PARSEC ;

-Les versions disponibles de GloMoSim n'exploitent pas totalement la puissance du parallélisme et ce, afin de favoriser QualNet (version commerciale de GlomoSim) ;

-La documentation est peu disponible.

5.2.3 TOSSIM

TOSSIM est un simulateur à événements discrets basé sur la programmation par événements en utilisant un langage spécifique appelé NesC Il a été conçu pour simuler les réseaux de capteurs en utilisant la plateforme TinyOS. Son principal but est de créer une simulation très proche de ce qui se passe dans ces réseaux dans le monde réel. Il simule le réseau au niveau des bits et chaque interruption dans le système est capturée. Pour une compréhension moins complexe de l'activité d'un réseau, Tossim est équipé d'une interface graphique, TinyViz, qui donne un aperçu de notre réseau de capteurs à tout moment.

Avantages

-Tossim simule fidèlement le comportement d'un réseau en s'appuyant sur la plateforme TinyOs. En effet le code de simulation peut être exécuté directement dans un capteur utilisant le système TinyOS ;

- Il simule un réseau d'une manière simple et efficace ;

- Il supporte un grands nombre de noeuds qui peut aller jusqu'à un millier ;

- Grace à L'interface graphique TinyViz, on peut visualiser les échanges radios pour avoir une vue globale du réseau.

Inconvénients

-Tossim oblige les utilisateurs à exécuter le même code sur tous les capteurs. Pour corriger ce problème, les capteurs doivent être identifiés par des numéros et des conditions doivent être utilisées dans le code pour différencier le rôle de chaque capteur ;

-TOSSIM fournit seulement une abstraction de certains phénomènes du monde réel ;

-Manque de souplesse et d'extensibilité puisqu'il est lié à une interface de visualisation conçue séparément.

5.2.4 OMNET++

OMNeT++ est un simulateur développée par Andras Varga, chercheur à l'université de Budapest .Il peut être utilisé pour la modélisation des réseaux câblés, les communications sans fil, des protocoles, des multiprocesseurs de systèmes distribués ,

l'évaluation des aspects de performance des systèmes logiciels complexes ainsi la validation d'architectures matérielles, etc.…

Actuellement, Ce simulateur est utilisé par des dizaines d'université pour la validation de nouveaux matériels et logiciels, ainsi que pour l'analyse des performances et l'évaluation des protocoles de communications. OMNET++ est devenu rapidement une plateforme de simulation populaire que ce soit pour la communauté des scientifiques ou des industriels.

Un modèle de simulation OMNET++ consiste en un ensemble d'entités appelées « Modules » qui communiquent entre elles en échangeant des « Messages » qui seront émis à travers des « Connections » et des « gates ».

Avantages

-Son approche modulaire permet la combinaison et la réutilisation des modèles de simulation ;

- Le développement avec OMNeT++ se fait en C++, ce qui facilite son intégration dans d'autres environnements de développement ;

-Il offre des bibliothèques très riches qui comprennent des supports d'entrées/sorties, manipulation de données et représentations graphiques ;

-La description des modules se fait avec le langage NED qui est simple à utiliser :

- L'interface graphique GNED d'OMNeT++ permet de construire des modules avec une génération automatique de la description NED.

Inconvénients

-OMNet++ n'est pas prévu pour la simulation de RCSFs ;

- Plusieurs concepteurs travaillent sur OMNeT++ pour l'enrichir de modèles destinés aux réseaux sans fil. Toute fois ces travaux étant indépendants, il n'existe aucune plateforme pour les regrouper.

5.3 Simulateur OMNET++

5.3.1 Fonctionnement

OMNET++ (*Objective Modular Network Test-bed in C++*) est un simulateur Open Source basé composant. Il est utilisé généralement dans la modélisation et la simulation des systèmes utilisant des approches à événement discret parmi eux on peut citer :

- La modélisation des réseaux de communications.
- La modélisation de différents protocoles.
- La modélisation de réseau de fils d'attente.
- Validation des architectures hardwares.
- Évaluation de performance d'aspects des systèmes complexes.

OMNET++ est composé d'un ensemble de modules hiérarchiques simples et composés reliés entre eux par des connexions et communiquent via l'envoie de messages [MAL05].

Les modules simples sont programmés en C++, tandis que les modules composés constitués de plusieurs modules simples, sont programmés dans le langage de haut niveau NED. Un module peut envoyer ces messages via ces ports (interfaces d'entrés et sorties des modules) mais il peut aussi envoyer le message directement vers le module destinataire. [AND]

5.3.2 Plateforme

La plateforme de simulation est illustrée dans la figure suivante :

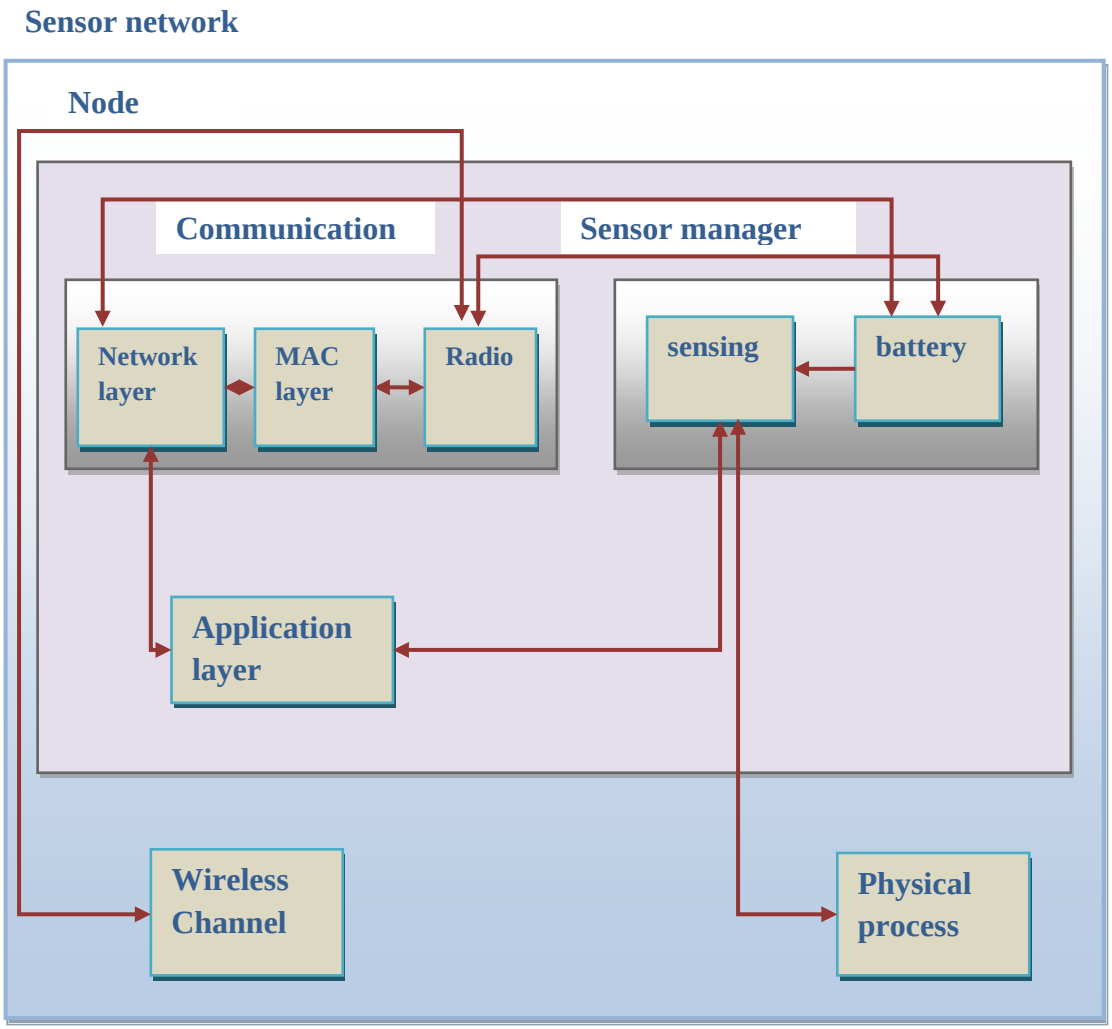

Fig.22: plateforme de simulation

La plateforme de simulation est modélisée par le module composé SensorNetwork qui est constitué de trois modules reliés entre eux par des connexions bidirectionnels : le module composé Node représente les nœuds capteurs et le nœud Sink et les deux modules simples :

WirelessChannel modélise le canal de transmission sans fils dans le réseau et PhysicalProcess représente le processus physique.

Le module composé Node est constitué de trois modules qui sont connectés entre eux par des liens bidirectionnels .Ces modules sont : les deux modules composés Communication et SensorManager et le module simple Application.

-SensorManager : est un module composé qui modélise les unités de bases d'un nœud capteur .Il est relié au modules suivants : Application, Node et le module Radio de Communication.
-Application : est un module simple représentant la couche application qui permet d'exécuter des applications utilisateurs. Il est relié aux deux modules composés suivants SensorManager et Communication.
-Communication : est un module composé qui permet de modéliser les trois couches de la pile protocolaire : physique, liaison de donné et réseau .Ce module est relié aux modules suivants : Node, Application, Radio du module SensorManager. La figure suivante nous décrit la structure du module Node.

Le module communication est composé de trois modules : MacLayer, NetLayer et Radio qui sont interconnectés entre eux via des liaisons bidirectionnels.

-NetLayer : c'est un module simple modélise la couche réseau d'un nœud capteur permettant de simuler des protocoles de routages implémentés à ce niveau. Il est connecté aux modules MacLayer et Communication.
-MacLayer : module simple permet de représenter la couche Mac (couche liaison de donnée) d'un capteur et simule les protocoles MAC implémentés. Il est relié aux modules NetLayer et Radio.
-Radio : ce module permet de modéliser la couche physique et l'unité transmission / réception .Il représente les trois états possibles d'un capteur SLEEP (veille), BUSY (actif) et DESABLE (désactiver) .Il est connecté vers la couche MAC (MacLayer) et le module Communication.

SensorManager aussi est un module composé de trois modules simples Sensing, MobilityManager et batteryManager.

-Sensing : représente l'unité de captage d'un capteur .Ce module est connecté aux modules SensorManager et BatteryManager.
-BatteryManager : ce module représente l'unité d'énergie dans un capteur. BatteryMannager est connecté au module Radio de SensorManager et Sensing.

5.4 Tests et discussion des résultats

Afin d'évaluer les performances des deux protocoles EAR et TEAR, nous les avons implémenté à la présence des nœuds égoïstes.

5.4.1 Critères de performance

La métrique sélectionnée est le taux de transmission des paquets de données.

5.4.2 Scenario de simulation

La simulation a été réalisée sur des capteurs Mica2 qui se caractérisent par :

-Architecture 8-Bit

-Fréquence 7.3728MHz

-Mémoire de programmation 128Ko

-Mémoire de données 4Ko

-Mémoire de stockage 512Ko

-Module radio CC1000

-Bande de fréquence 315-916MHz

-Débit maximal 38.4Kb/s

Le tableau suivant résume quelques paramètres utilisés :

Paramètre	**Valeur**
Nombre de nœuds du réseau	100
Durée de simulation (seconde)	200
Protocoles de routages	EAR, TEAR
Taux de paquet de données généré par un nœud	1/s
Surface de simulation (m m m)	100 * 100 * 50
Placement des nœuds	Aléatoire
Nombre de stations de base	1
Portée de transmission (m)	-5
Durée d'un round	10s
Type des capteurs	Mica2

Tab.11 : Paramètres de simulation

5.4.3 Discussion des résultats

La figure suivante illustre les résultats obtenus après avoir effectué plusieurs tests :

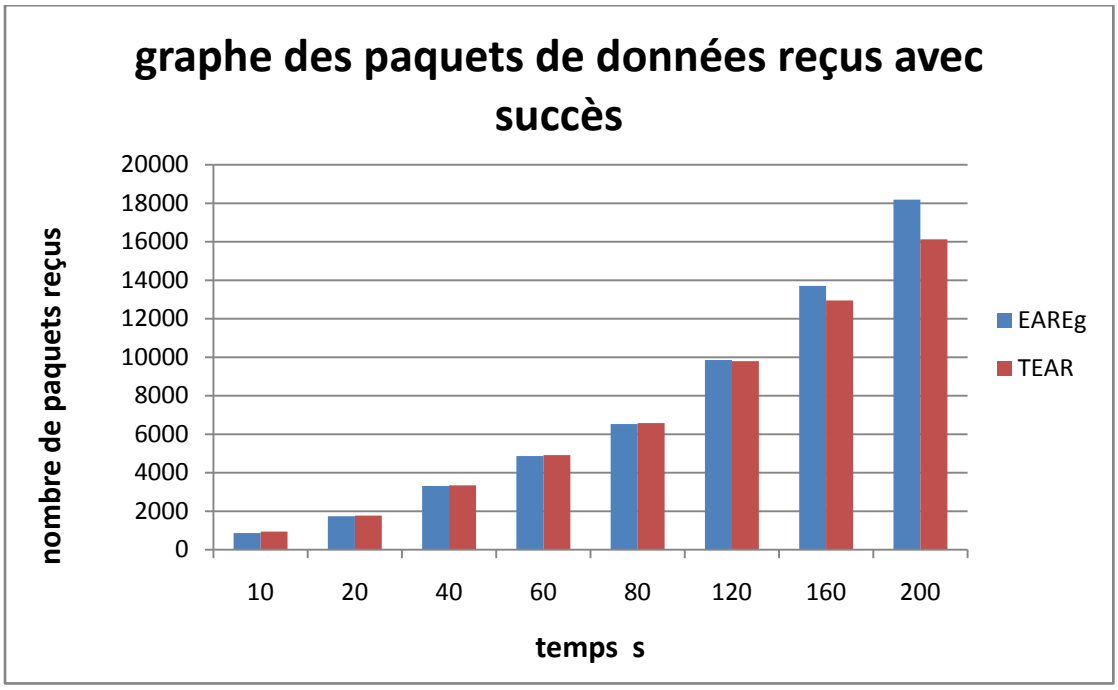

Fig.23 : graphe des paquets de données reçus avec succès

D'après la figure (fig.21) nous constatons que le nombre de paquets de données reçu par la station de base dans le protocole TEAR est plus élevé que celui dans le protocole EAR. À chaque nœud égoïste détecté, ce dernier ne sera pas choisi pour la retransmission des paquets de données.

5.5 Conclusion

Dans ce dernier chapitre, nous avons présenté l'environnement de simulation OMNET++4, ainsi son principe de fonctionnement. Après avoir implémenté le protocole EAR et notre approche protocole, nous avons effectué une comparaison entre ces deux derniers. Les résultats de la simulation obtenus montrent que TEAR augmente le nombre de paquets reçus par la station de base, un nœud égoïste des qu'il sera détecté, il ne participera pas aux prochaines retransmissions des paquets de données.

Conclusion générale

Au cours de ces dernières années la technologie des réseaux de capteurs sans fil n'a cessé de se développer grâce aux progrès dans divers domaines liés à la micro-électronique et aux technologies de la communication sans fil. Ainsi ces reseaux deviennent de plus en plus vulnérables aux différentes attaques malveillantes qui visent à nuire au bon fonctionnement du réseau. D'où la nécessité de leurs implémenter des systèmes de sécurités. En raison de leur limitations(en terme de mémoire, calcul et énergie), l'utilisation des mécanismes de sécurité traditionnels est difficile voir impossible dans ce genre de réseaux, ce qui a conduit a la recherche de nouveaux mécanismes légers tels que la gestion de la confiance entre les nœuds du réseau.

L'objectif de notre travail consistait à améliorer le protocole de routage EAR pour garantir la sécurité du routage en ajoutant un mécanisme léger de gestion de la confiance.

En premier lieu, nous avons présenté un état de l'art détaillé sur les réseaux de capteurs sans fil où nous avons étudié plusieurs aspects liés à ses réseaux, allant de l'architecture d'un capteur , les caractéristiques du réseau formé par un ensemble de ce dernier, jusqu'aux domaines de leurs utilisation en passant par les différentes contraintes imposées par les réseaux de capteurs sans fil. Ensuite, nous nous sommes intéressé a une tache essentielle dans le maintient du bon fonctionnement des réseaux de capteurs sans fil qui est le routage, en commençant par étudier les facteurs à prendre en considération afin de concevoir des protocoles de routages efficaces, ensuite les métriques d'évaluation de performance de ces dernière et enfin leurs classifications selon plusieurs critères.

Concevoir un protocole de routage n'est pas une solution complète pour garantir le bon fonctionnement du réseau car ce dernier comme il est déployé souvent dans des environnements hostiles, la sécurité devient cruciale. Les solutions utilisées dans les réseaux traditionnels ne sont pas compatibles avec ce genre de réseaux vu ses caractéristiques. Pour cela d'autres solutions ont été proposées comme dans le cas de la confiance. Pour bien comprendre la notion de la confiance dans les réseaux de capteurs, nous avons donné un aperçu sur les différentes définitions dans divers domaines y compris dans les RCSFs, ses caractéristiques et ensuite nous avons donnez quelques exemples de systèmes de gestion de la confiance existants.

Afin de mieux cerner le concept de gestion de la confiance dans les RCSFs, dans un premier temps, nous avons implémenté à l'aide du simulateur omnet++, le protocole EAR qui est un protocole de routage non sécurisé, ensuite nous avons implémenté sur ce protocole des nœuds égoïstes afin de comparer ses performances en cas de présence de mauvais comportements.
Dans un second temps, nous avons réalisé notre amélioration en implémentant un mécanisme léger de gestion de confiance qu'on a nommé TEAR.

Ces implémentations nous ont permis de faire une étude comparative entre le protocole EAR et TEAR.

Comme perspective nous envisageons d'introduire la notion de la confiance indirecte (basée sur recommandation) pour plus de performance à notre approche.

Bibliographie

[GIL 08] : Gil De Sousa « *Etude en vue de la réalisation de logiciels bas niveau dédiés aux réseaux de capteurs sans fil : microsystème de fichiers* », Thèse, Ecole Doctorale sciences pour l'ingénieur de Clermont-Ferrand, 2008.

[**ANU11]:** Anupama K, Nishad Kamdar, Dhruv Vyas, Ishaan Baokar, Siddharth Sahu, Philip George ; «*Design and Implementation of a Cross Layered Protocol Stack for Sensor Networks in an Indoor Environment* » ; BITS PILANI K K BIRLA GOA CAMPUS GOA INDIA ; 2011.

[AKY01]: I.F. AKYILDIZ, Weilian. SU, Yogesh Sankarasubramaniam and Erdal CAYIRCI, « *Wireless sensor networks: a survey*» Computer Networks 38, pp. 393–422, 2001.

[AKY02]: I.F. Akyildiz, W. Su , Y. Sankarasubramaniam, E. Cayirci, «Wireless sensor networks: a survey» Broadband and Wireless Networking Laboratory, School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332 ; USA ; 2002 .

[TEC10] : Teck Aguilar « *Vers un protocole de routage géographique avec contention et communications coopératives pour les réseaux de capteurs* », thèse, Ecole Doctorale EDITE, 2010.

[WAZ12] : Wazir Zada Khan, N.M.Saad, Mohammed Y Aalsalem «*An Overview of Evaluation Metrics for Routing Protocols in Wireless Sensor Networks*»,4th International Conference on Intelligent and Advanced Systems, 2012.

[SHI10]: Shio Kumar Singh , M P Singh , D K Singh «*Routing Protocols in Wireless Sensor Networks –A Survey* »,International Journal of Computer Science & Engineering Survey (IJCSES) Vol.1, No.2, November 2010.

[ALK04]: Jamal N. Al-Karaki et Ahmed E. Kamal « *Routing Techniques in Wireless Sensor Networks: A Survey*», IEEE wireless communication, vol. 11, no. 6, pp 6-28, Dec 2004.

[MOH11]: Mohamed AISSANI « *optimisation du routage dans les réseaux de capteurs pour les applications temps-reel* », thèse, Université Paris-Est, USTHB, 2011.

[PRE12]: Prabhat Kumar, M.P.Singh et U.S.Triar « *A Review of Routing Protocols in Wireless Sensor Network* », International Journal of Engineering Research & Technology (IJERT), Vol. 1 Issue 4, June – 2012.

[MAL12]: Mallanagouda Patil et Rajashekhar C. Biradar « *A Survey on Routing Protocols in Wireless Sensor Networks*», IEEE, ICON 2012.

[RAM13]: Rama Sundari Battula, O. S. Khanna «Geographic Routing Protocols for Wireless Sensor Networks: A Review », International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 12, June 2013.

[RDE13]: R.Devika, B.Santhi ,T.Sivasubramanian «*Survey on Routing Protocol in Wireless Sensor Network* », International Journal of Engineering and Technology (IJET), Vol 5 No 1 Feb-Mar 2013.

[MAU07]: Mauri Kuorilehto, Mikko Kohvakka,Jukka Suhonen, Panu H¨am¨al¨ainen, Marko H¨annik¨ainen, and Timo D. H¨am¨al¨ainen« *Ultra-Low Energy Wireless Sensor Networks in Practice,Theory, Realization and Deployment* »,Tampere University of Technology, Finland, 2007.

[LUH79] : Luhmann, N «*Trust and power : two works*», Number pts. 1-2 in UMI Books on Demand. Wiley, 1979.

[JOS07] : Jøsang, A., Ismail, R., and Boyd «*A survey of trust and reputation systems for online service provision*». Decision Support Systems, 43(2) :618 – 644. Emerging Issues in Collaborative Commerce. 2007.

[DUE62] : Deutsch, M «*Cooperation and trust : Some theoretical notes*». In Jones, M. R., editor,Nebraska Symposium On Motivation, volume 10, pages 275–320. University of Nebraska Press. 1962.

[GAM00]: Gambetta, D «*Can we trust trust*». Trust Making and Breaking Cooperative Relations, chapter13p :213–237, 2000.

[GRA03]: Grandison, T. W. «*ATrust management for internet applications*». Technical report, 2003.

[AUD07]: Audun Jøsang, Roslan Ismail, Colin Boyd «*A Survey of Trust and Reputation Systems for Online Service Provision*», Information Security Research Centre
Queensland University of Technology Brisbane, Australia, bCollege of Information Technology Universiti Tenaga Nasional (UNITEN), Malaysia, 2007.

[SAK13]: Sakshi Srivastava, Kushal Johari «*A Survey on Reputation and Trust Management in Wireless Sensor Network*», International Journal of Scientific Research Engineering & Technology (IJSRET), Volume 1 Issue3 pp 139-149 August 2012

[MOM 07] : M. Momani, S. Challa, et K. Aboura, « *Modelling trust in wireless sensor networks from the sensor reliability prospective* », Innovative algorithms and techniques in automation, industrial electronics and telecommunications, p. 317–321, 2007.

[THE10]: Theodore Zahariadis, Helen C. Leligou, Panagiotis Trakadas and Stamatis Voliotis «*Trust management in wireless sensor networks*», european transactions on telecommunications, 2010

[MOM10]: Mohammad Momani et Subhash Challa «*Probabilistic Modelling and Recursive Bayesian Estimation of Trust in Wireless Sensor Networks, Bayesian Network*», 2010.

[YAN11]: Yanli Yu, Keqiu Li, Wanlei Zhou, and Ping Li, «*Trust mechanisms in wireless sensor networks: attack analysis and countermeasures*», Journal of Network and Computer Applications, Elsevier, 2011, in press.

[KHT12]: Khorchi karima, Tenboukti Hafidha Ahlem «*Mécanismes de gestion de la confiance pour les réseaux de capteurs sans fil : application au modèle AntMWAC*», Mémoire d'ingénieur, Ecole nationale Supérieure d'Informatique ESI, Algérie, 2012.

[GAN04] : S. Ganeriwal and M. B. Srivastava « *Reputation-Based Framework for High Integrity Sensor Networks*». In 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks, Washington, DC, USA, 2004.

[RAH02]: Rahul C. Shah et Jan M. Rabaey «*Energy Aware Routing for Low Energy Ad Hoc Sensor Networks*», IEEE, Communication/Computation Piconodes for Sensor Networks, 2002.

[MAL05] : C. Mallanda, A. Suri, V. Kunchakarra, S.S. Iyengar, R. Kannan and A. Durresi ; «*Simulating Wireless Sensor Networks with OMNeT++*» ; Department of Computer Science, Louisiana State University, Baton Rouge, LA ; 2005 .

[AND]: András Varga «*The OMNET++ discrete event simulation system* », Department of Telecommunications Budapest University of Technology and Economics ; 1117 Budapest, Hungary .

[RIA09] : Riaz Ahmed Shaikh, Hassan Jameel, Brian J. d'Auriol, Heejo Lee, Sungyoung Lee et Young-Jae Song «*Group-Based Trust Management Scheme for Clustered Wireless Sensor Networks*», IEEE transactions on parallel and distributed systems, vol. 20, no. 11, november 2009.

[FEN11]: Fenye Bao, Ing-Ray Chen, MoonJeong Chang, Jin-Hee Cho «*Trust-Based Intrusion Detection in Wireless Sensor Networks*», IEEE Communications Society, 2011.

[VER11]: L. Vercouter, J.-P. Jamont, A. Balanel «*Mécanismes légers de gestion de la confiance pour des réseaux de capteurs sans fil*», Journées Francophones sur les Systémes Multi-Agents, Valenciennes : France 2011.

[AYM11]: Ayman Tajeddine,Ayman Kayssi ,Ali Chehab «*CENTER: A Centralized Trust-Based Efficient Routing Protocol for Wireless Sensor Networks* », IEEE , 2011.

[SOU10]: Sourendra Sinha, Zenon Chaczko « *T-SNIPER :Trust-aware Sensor Network Information Protocol for Efficient Routing* » , University of Technology, Sydney Australia, 2010.

[GUO12]: Guoxing Zhan, Weisong Shi,Senior, Julia Deng, «*Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs*» Transactions on Dependable and Secure Computing, Volume: 9 , Issue: 2, IEEE 2012.

[ANT08]: Antônio Augusto Fröhlich, Lucas Francisco Wanner «*Operating System Support for Wireless Sensor Networks*», Journal of Computer Science 4 (4): 272-281, ISSN 1549-3636, Science Publications, 2008.

[ZIA09] : Ziane Khodja Lilia «*La structuration et la sécurisation des réseaux de capteurs* », thèse Master 2 Recherche Informatique, IFSIC, 2009.

[MED10] : Medetonhan Shambhalla Eugène William «*Conception d'une architecture hiérarchique de réseau de capteurs pour le stockage et la compression de données*», thèse Pour obtenir le grade de docteur de l'université de Franche-Comté Spécialité Informatique, 2010.

[RAJ09] : Rajashree.V.Biradar, V.C .Patil, Dr. S. R. Sawant, Dr. R. R. Mudholkar, «*CLASSIFICATION AND COMPARISON OF ROUTING PROTOCOLS IN WIRELESS SENSOR NETWORK*», Ubiquitous Computing and Communication Journal, Special Issue on Ubiquitous Computing Security Systems, Volume: Ubiquitous Computing Security Systems, 2009.

[PAR12]: Parul Bakaraniya , Sheetal Mehta «*FEATURES OF WSN AND VARIOUS ROUTING TECHNIQUES FOR WSN: A SURVEY* », ISSN: 2319 -1163, Volume: 1 Issue: 3, IJRET, NOV 2012.

[VVS11] : Vandana Jindal, A.K.Verma, Seema Bawa « *How the two Adhoc networks can be different:MANET & WSNs*», IJCST Vo l. 2, IS Su e4, oC T. – DeC, 2011

[XUA08] : Xuanxia Yao, XueFeng Zheng «*A Secure Routing Scheme for Static Wireless Sensor Networks*», IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application, 2008.

[ABD12] : ABED Mahfoud, BACHA Mehdi, « *Description des comportements d'un réseau de capteurs sans fils à l'aide de SMA* », mémoire de fin d'études, Ecole nationale Supérieure d'Informatique ESI, Algérie, 2012.