



THESE

En vue de l'obtention du grade de Docteur en Sciences

Université Djillali Liabes de Sidi Bel Abbès

Département d'Electronique

Soutenue par Mohammed BELKHEIR

Réseaux AD-HOC : Optimisation de la qualité du service QoS du réseau par conservation d'énergie

Devant le jury :

| | | | |
|-----------------------------|------------|--------------------|----------|
| M. Djebbari Ali | Professeur | Président | UDL-SBA |
| M. Bouziani Merahi | Professeur | Directeur de thèse | UDL-SBA |
| M. Bassou Abdesselam | Professeur | Examineur | U-Bechar |
| M. Bouazza Boubekour Seddik | MCA | Examineur | U-Saida |

Année 2014

Remerciements

Mes vifs remerciements vont à Mon Professeur Monsieur Merah Bouziani, je ne peux à travers cette petite page dévouer mes sincères gratitudee quand à cette grande personne qui m'a soutenu tout au long de mon mémoire de magister et ma thèse de doctorat. Merci ! Pour m'avoir encadré « au sens propre du terme », puis pour m'avoir fait confiance en me confiant ce sujet de thèse et pour m'avoir accompagné, encouragé et conseillé au cours de ces années tant sur le plan technique qu'humain. Sans dieu puis lui, ce travail n'aurait jamais vu le jour.

Un remerciement particulier va aux membres du jury, qui ont accepté d'étudier, rapporté et jugé ce modeste travail.

Mes remerciements vont aussi à tous les membres du laboratoire LTTNS et son président Professeur Ali Djebbari.

Merci à mes collègues, Monsieur Zeyad Al gacem, l'initiateur de ce travail et Monsieur Abdelhalim Zerroug avec son apport positif et ses connaissances dans le domaine de la programmation.

Résumé

Les progrès technologiques réalisés ces dernières années, soutenus par la mobilité des utilisateurs et le développement continu des unités mobiles (Smartphones, PDA, tablettes, capteurs,...), ont vu la naissance de nouveaux types de réseaux baptisés AHWSN (Ad-Hoc and Sensor Wireless Networks) dont les domaines d'applications sont nombreux : domotique, santé, domaine militaire ou bien encore surveillance de phénomènes environnementaux. Des contraintes de déploiement de ces réseaux sont imposées à savoir : la limitation des capacités de traitement, de stockage et surtout d'énergie. La liberté laissée à l'implantation est forte et impose de concevoir complètement l'infrastructure, les mécanismes et les protocoles en fonction de l'application visée. Une autre contrainte prépondérante à qui on doit faire face et qui introduit d'autres métriques à tenir en compte lors du déploiement de tels réseaux est la qualité de service QoS, si nous envisageons une extension voir un remplacement des réseaux filaires par les AHWSN.

Notre travail a été principalement axé sur l'étude et l'introduction de nouveaux mécanismes de routage en vue d'optimiser la consommation d'énergie au niveau de la couche réseau, en se basant sur le protocole OLSR (Optimized Link State Routing) très répandu dans le domaine des réseaux AHWSN. OLSR utilise la technique de relais multipoints (MPRs) visant à optimiser les messages de contrôle lors de l'inondation du réseau.

Notre premier travail consistait sur la modification de l'algorithme de sélection de MPRs, en introduisant l'énergie résiduelle comme critère essentiel de calcul de ces derniers. L'information relative à l'énergie résiduelle d'un nœud sera véhiculée par les messages de contrôle (HELLO et TC) du protocole OLSR et sera utilisée lors du calcul des MPRs et de la construction de la table de routage des nœuds.

La deuxième contribution avait comme objectif principal de pallier au problème d'inactivité des nœuds en vue d'alléger ceux qui ont été longuement sélectionnés comme MPR. Ceci permettra d'équilibrer la charge du réseau et de maintenir un niveau d'énergie acceptable à tous les nœuds afin d'accroître la durée de vie du réseau.

Les différentes simulations effectuées durant notre travail, ont montré clairement que les deux protocoles résultants OE-OLSR et LE-OLSR, ont amélioré considérablement la qualité du service QoS du réseau AHWSN en termes d'optimisation d'énergie et de sa durée de vie.

Mots Clés : AHWSN, Qualité de service, OLSR, MANET, Durée de vie, Energie

Abstract

Technological progress performed these last years, supported by the mobility of the users and the continuous development of mobile units (Smartphones, PDA, tablets, sensors), shown the birth of a new category of networks called AHWSN (Ad hoc and Sensor Wireless Networks). They have various application domains such as: home automations, health care services, military domain and monitoring environments. The deployment of such networks is conditioned by multiple constraints: Limitation of nodes processing capabilities, storage, and energy constraints. Another crucial constraint to take into account is the Quality of Service QoS, which adds several metrics for deploying such networks, if we want that AHWSN goal is to replace the existent wired networks.

The aim of our work is to study and develop new routing mechanisms in order to improve energy management within the third level of OSI model, based on OLSR protocol (Optimized Link State Routing) mainly used in AHWSN networks. OLSR uses the multipoint relays technique (MPRs) to optimize the overhead during the flooding.

Our first contribution to the OLSR protocol was focused on the modification of the MPR selection mechanism, with the introduction of the node residual energy as an essential criterion on the MPR set calculation. To do that, the nodes residual energy information will be transmitted within the routing packets (HELLO and TC) of OLSR protocol and it will be used during MPR calculation algorithm and the built of a node routing table.

The second contribution consists on enhancing the reactiveness of mobile nodes within the network, especially when their residual energy decreases, by giving them the ability to be Multipoint Relays (MPR). This will relieve nodes which have been selected as MPRs for a long time and balance the load over all the nodes of the network. Thus we will keep an acceptable energy level for all nodes and prolong the network lifetime.

Simulations performed during our thesis, demonstrated obviously that the two new protocols (OE-OLSR, LE-OLSR), have significantly improved the QoS of AHWSN networks in terms of energy optimization and lifetime enhancement.

Keywords: *AHWSN, quality of service, OLSR, MANET, lifetime, Energy*

Table des matières

Remerciement

Résumé

Abstract

Table des matières

Table des figures

Liste des Tableaux

Liste des acronymes

Introduction Générale :

| | |
|---|---|
| 1. Contexte Général | 1 |
| 2. Motivations et problématique..... | 3 |
| 3. Contributions et structure de la thèse | 4 |

Chapitre 1 : Concept des réseaux AHWSN : Routage et diffusion 6

| | |
|--|----|
| 1. Introduction | 7 |
| 2. Concept et architecture des réseaux ad-hoc..... | 9 |
| 3. Cas particulier : Réseaux de capteurs (WSN)..... | 12 |
| a. Anatomie des capteurs | 12 |
| b. Architecture des réseaux WSN | 13 |
| 4. Domaines d'application des réseaux AHWSNs..... | 15 |
| 5. Contraintes liées au déploiement des réseaux AHWSN..... | 16 |
| a. Cas des MANET | 17 |
| b. Cas des WSN | 19 |
| 6. Routage de l'information dans les réseaux AHWSN | 22 |
| 6.1 Protocoles proactifs | 23 |
| 6.2 Protocoles réactifs | 25 |
| 6.3 Protocoles réactifs Vs Protocoles proactifs | 27 |
| 6.4 Protocoles hybrides | 28 |
| 6.5 Routage dans les réseaux WSN | 31 |

| | |
|---|-----------|
| 6.5.1 Les Protocoles hiérarchiques..... | 31 |
| 6.5.2 Les protocoles de routage basés sur la localisation | 33 |
| 6.5.3 Les protocoles de routage ‘data-centric’ | 34 |
| 6.5.4 La diffusion dirigée..... | 36 |
| 6.5.5 Le protocole de routage par rumeur..... | 36 |
| 7. Conclusion..... | 38 |
| Chapitre 2 : AHWSN : Qualité de service (QoS) et conservation d’énergie..... | 39 |
| 1. Introduction | 41 |
| 2. Qualité de service à différentes échelles dans les AHWSN | 42 |
| 2.1 Qualité de service dans les AHWSN à l’échelle interne : Différenciation de service au niveau de la couche MAC..... | 43 |
| 2.1.1 Description de la couche MAC IEEE 802.11 | 44 |
| 2.1.2 Différenciation de service basée sur la fonction DCF du protocole 802.11..... | 44 |
| 2.1.3 IEEE 802.11e | 45 |
| 2.2 La Qualité de Service dans les réseaux AHWSN à l’échelle locale | 46 |
| 2.2.1 CEDAR (Core-Extraction Distributed Ad hoc Routing Algorithm) | 47 |
| 2.2.2 Autres protocoles de routage avec QoS..... | 48 |
| 2.2.3 Protocole de réservation de ressources : INSIGNIA | 49 |
| 2.3 La Qualité de Service dans les réseaux AHWSN à l’échelle globale..... | 50 |
| 3. Modèles de qualité de service dans les réseaux AD-HOC..... | 51 |
| 3.1 Flexible quality of service model for MANETs (FQMM) | 51 |
| 3.2 Service differentiation in wireless ad hoc networks (SWAN) | 52 |
| 3.3 Modèle iMAQ..... | 53 |
| 4. Qualité de service QoS : cas des WSN..... | 54 |
| 4.1 Qualité de service liée à l’application | 55 |
| 4.2 Qualité de service liée au réseau | 55 |
| 4.2.1 Modèle orienté-événements | 55 |
| 4.2.2 Modèle orienté-requêtes..... | 56 |

| | | |
|---|--|-----------|
| 4.2.3 | Modèle à flux continu..... | 57 |
| 5. | Techniques de conservation d'énergie dans les réseaux AHWSN..... | 57 |
| 5.1 | Consommation d'énergie d'un nœud dans un réseau AHWSN..... | 58 |
| 5.1.1 | Formes de dissipation d'énergie..... | 58 |
| 5.1.2 | Sources de surconsommation d'énergie..... | 59 |
| 5.1.3 | Consommation d'énergie due au routage..... | 61 |
| 5.2 | Conservation d'énergie..... | 62 |
| 5.2.1 | Techniques du Duty-cycling..... | 63 |
| 5.2.2 | Principaux Algorithmes de routage utilisés pour la conservation d'énergie..... | 69 |
| 5.2.3 | Conservation d'énergie au niveau transport..... | 71 |
| 6. | Conclusion..... | 73 |
| Chapitre 3 : Algorithme d'optimisation de l'énergie dans les réseaux AHWSN | | 75 |
| 1. | Introduction | 77 |
| 2. | Le protocole OLSR (Optimized Link State Routing) | 77 |
| 2.1 | Relais Multipoints (MPRs)..... | 78 |
| 2.2 | Fonctionnement de l'OLSR | 79 |
| 2.3 | Format du paquet OLSR | 80 |
| 2.3.1 | Les messages HELLO..... | 81 |
| 2.3.2 | Les messages TC..... | 83 |
| 2.4 | Détection de voisinage..... | 84 |
| 2.5 | Sélection des Relais Multipoints..... | 86 |
| 2.6 | Gestion de la topologie | 89 |
| 2.6.1 | Les messages MID..... | 90 |
| 2.6.2 | Les messages HNA..... | 90 |
| 2.6.3 | Le calcul de la table de routage..... | 91 |
| 3. | Motivations et défis | 92 |
| 4. | Caractéristiques du simulateur NS-2 | 92 |
| 4.1 | Fonctionnement de NS-2..... | 94 |

| | |
|--|-----|
| 4.2 La mobilité dans NS-2..... | 95 |
| 4.3 Mouvement des nœuds et génération de topologie dans NS-2..... | 98 |
| 4.4 Génération du trafic entre les nœuds mobiles..... | 101 |
| 4.5 Modèles de propagation dans NS-2..... | 102 |
| 4.5.1 Le modèle de propagation en espace libre (Free space model) | 102 |
| 4.5.2 Le modèle de propagation utilisant deux rayons (Two-ray ground reflection model)..... | 102 |
| 4.5.3 Le modèle Shadowing | 103 |
| 4.6 Interprétation des résultats dans NS-2 | 104 |
| 5. Protocole OE-OLSR (Optimized Energy – OLSR)..... | 106 |
| 5.1 Sélection des MPRs dans le protocole OE-OLSR..... | 108 |
| 5.2 Messages de contrôle et algorithme d'inondation dans OE-OLSR..... | 110 |
| 5.2.1 Nouveau message HELLO dans OE-OLSR..... | 111 |
| 5.2.2 Nouveau message TC dans OE-OLSR..... | 112 |
| 5.3 Calcul des routes | 112 |
| 6. Simulation des performances du protocole OE-OLSR..... | 113 |
| 6.1 Métriques d'évaluation..... | 113 |
| 6.1.1 Délai de bout-en-bout..... | 113 |
| 6.1.2 Pourcentage de paquets délivrés | 114 |
| 6.1.3 Nombre de sauts | 114 |
| 6.1.4 Energie Consommée..... | 114 |
| 6.1.5 Nombre des nœuds morts (dead nodes)..... | 114 |
| 6.2 Paramètres de simulation | 115 |
| 6.3 Résultats des simulations et discussions..... | 116 |
| 6.3.1 Nombre de sauts | 116 |
| 6.3.2 Energie totale consommée | 118 |
| 6.3.3 Pourcentage des paquets délivrés (PDR)..... | 119 |
| 7. Discussions et conclusion..... | 120 |

| | |
|--|------------|
| Chapitre 4 : LE-OLSR et la durée de vie du réseau AHWSN..... | 122 |
| 1. Introduction | 123 |
| 2. Notions de la durée de vie du réseau..... | 124 |
| 3. Discussions et motivations | 126 |
| 4. Protocole LE-OLSR « Lifetime Enhanced – OLSR » | 127 |
| 4.1 Algorithme de sélection des MPRs dans le protocole LE-OLSR | 128 |
| 5. Métriques de qualité de service QoS | 130 |
| 5.1 Messages de contrôle (Control Overhead)..... | 130 |
| 5.2 Délai de transmission moyen (Average end to end delay)..... | 130 |
| 6. Environnement de simulation | 130 |
| 7. Impact de MPRs sur la durée de vie du réseau..... | 132 |
| 8. Effet du protocole LE-OLSR sur la QoS du réseau AHWSN..... | 134 |
| 8.1 LE-OLSR et la densité du réseau | 134 |
| 8.1.1 Messages de contrôle (Control overhead) | 134 |
| 8.1.2 Délai de transmission moyen (average end-to-end delay) | 135 |
| 8.1.3 Nombre de nœuds morts (dead nodes) | 135 |
| 8.1.4 Nombre de paquets perdus (packet-loss)..... | 136 |
| 8.2 LE-OLSR et la mobilité du réseau..... | 137 |
| 9. Discussions et conclusion..... | 139 |
| Chapitre 5 : Conclusion générale et perspectives | 141 |
| Synthèse..... | 141 |
| Perspectives | 144 |
| Bibliographie et Références..... | 146 |

Table des figures

| | |
|---|----|
| Figure 1.1 : Architecture d'un réseau ad-hoc | 9 |
| Figure 1.2 : Vue d'ensemble d'un capteur | 12 |
| Figure 1.3 : Architecture d'un WSN | 14 |
| Figure 1.4 : Architecture d'un RCASF | 14 |
| Figure 1.5 : Différents types d'architecture des RCASF | 15 |
| Figure 1.6 : Architecture d'un MANET | 17 |
| Figure 1.7 : Principale source de consommation d'énergie d'un capteur avec une radio CC2500 et un microcontrôleur MSP430 | 21 |
| Figure 1.8 : Optimisation des relais multipoints (MPRs) | 25 |
| Figure 1.9 : Procédure de découverte de route du protocole AODV | 27 |
| Figure 1.10 : Heuristiques dans les protocoles hybrides | 29 |
| Figure 1.11 : Principaux protocoles de routages dans les WSN | 31 |
| Figure 1.12 : Protocoles de routages WSN hiérarchiques | 32 |
| Figure 1.13 : Le routage data-centric | 35 |
| Figure 2.1 : Différents niveaux d'approches de la QoS dans les réseaux AHWSN | 43 |
| Figure 2.2 : Méthode d'accès DCF | 44 |
| Figure 2.3: Modèle FQQM | 52 |
| Figure 2.4: Modèle SWAN | 53 |
| Figure 2.5: Modèle iMAQ | 54 |
| Figure 3.1 : Intérêt de l'implémentation des MPRs | 80 |
| Figure 3.2 : Format du paquet OLSR | 81 |
| Figure 3.3 : Format du message « Hello » | 81 |
| Figure 3.4 : Format des messages "TC" | 83 |
| Figure 3.5 : Exemple d'information de voisinage maintenue par OLSR | 85 |
| Figure 3.6 : Echange des messages HELLO | 86 |
| Figure 3.7 : Diffusion par inondation classique vs inondation par relais multipoints .. | 87 |
| Figure 3.8 : Exemple de sélection des relais multipoints | 88 |
| Figure 3.9 : Optimisation de l'inondation par des relais multipoint. | 89 |
| Figure 3.10 : Format des messages MID | 90 |
| Figure 3.11 : Format des messages HNA | 90 |
| Figure 3.12 Réseau MANET | 91 |
| Figure 3.13 : Processus de simulation dans NS2 | 94 |
| Figure 3.14 : Composants d'un nœud mobile dans NS2 | 96 |
| Figure 3.15: Scénario « wired-cum-wireless » dans NS-2 | 97 |

Table des figures

| | |
|--|-----|
| Figure 3.16 : Modèle de Mobilité dans NS-2 | 99 |
| Figure 3.17: Mouvement d'un nœud selon le modèle <i>Random Waypoint</i> | 100 |
| Figure 3.18 : Format du fichier trace dans NS-2 | 104 |
| Figure 3.18 : Processus du protocole OE-OLSR | 108 |
| Figure 3.19 : Calcul des MPRs dans OE-OLSR..... | 109 |
| Figure 3.20 : Sélection des MPRs « OE-OLSR » Vs « OLSR » | 110 |
| Figure 3.21: Nouveau format du Message HELLO..... | 111 |
| Figure 3.22 : Nouveau format du Message TC..... | 112 |
| Figure 3.23 : Variation du nombre de sauts Vs nombre de nœuds..... | 116 |
| Figure 3.24 : Variation du nombre de sauts Vs Vitesse des nœuds..... | 117 |
| Figure 3.25 : Variation du nombre de sauts Vs Nombre de connexions | 117 |
| Figure 3.26 : Variation de l'énergie totale Vs Nombre de nœuds | 118 |
| Figure 3.27 : Variation de l'énergie totale Vs Vitesse des nœuds..... | 118 |
| Figure 3.28 : Variation de l'énergie totale Vs Vitesse des nœuds..... | 119 |
| Figure 3.29 : Impact du protocole OE-OLSR sur le PDR..... | 120 |
| Figure 4.1 : Evolution du nombre de MPRs | 133 |
| Figure 4.2: Control Overhead et la densité du réseau | 134 |
| Figure 4.3 : Délai de transmission moyen (AVG end-to-end delay) et la densité..... | 135 |
| Figure 4.4 : Nombre de nœuds morts (dead nodes)..... | 136 |
| Figure 4.5 : Packet-loss Vs nombre de nœuds..... | 137 |
| Figure 4.6 : Control overhead Vs mobilité du réseau..... | 138 |
| Figure 4.7 : Délai de transmission moyen Vs mobilité du réseau | 138 |
| Figure 4.8 : Packet-loss Vs mobilité du réseau | 138 |

Liste des Tableaux

| | |
|--|-----|
| Tableau 1.1 : Propriétés des protocoles de routage | 30 |
| Tableau 1.2 : Comparaison des protocoles de routages des WSN..... | 37 |
| Tableau 2.1 : Exigences des applications WSN..... | 57 |
| Tableau 2.2 : Consommation d'énergie liée à une communication point-à-point..... | 61 |
| Tableau 3.1 : Table topologique du nœud A | 91 |
| Tableau 3.2 : Paramètres de simulation d'OLSR et OE-OLSR sous NS-2 | 115 |
| Tableau 4.1 : Paramètres de simulation de LE-OLSR et OE-OLSR | 132 |
| Tableau 4.2 : Nombre de MPRs VS nœuds morts | 133 |

Liste des acronymes

*"Chaque science, chaque étude a son jargon
inintelligible, qui semble n'être inventé que
pour en défendre les approches."
Voltaire, Essais de poésie épique (Chapitre 9)*

| | |
|----------|--|
| AHWSN | Ad-Hoc and Wireless Sensor Networks |
| AODV | Ad-Hoc On demand Distance Vector |
| APDU | Application Protocol Data Unit |
| ATM | Asynchronous Transfer Mode |
| B-MAC | Berkeley MAC |
| BS | Base Station |
| BSC | Base Station Controller |
| CAP | Contention Access Period |
| CBR | Constant Bit Rat |
| CBRP | Cluster Based Routing Protocol |
| CEDAR | Core Extraction Distributed Ad hoc Routing |
| CFP | Contention Free Period |
| CSMA | Carrier Sense Multiple Access |
| CSMA/CA | CSMA with Collision Avoidance |
| CTS | Clear To Send |
| DAD | Duplicate Address Detection |
| DARPA | Defense Advanced Research Projects Agency |
| DCF | Distributed Coordination Function |
| DHCP | Dynamic Host Configuration Protocol |
| DiffServ | Differentiated Services |
| DSDV | Destination Sequence Distance Vector |
| DSR | Dynamic Source Routing |
| ECN | Explicit Contention Notification |
| FEC | Forward Error Correction |
| FFD | Full Function Device |
| FTP | File Transfer Protocol |
| GloMo | Global Mobile Information Systems |
| GPS | Global Positioning System |
| GSM | Global System for Mobile communications |

| | |
|----------|---|
| HCL | High Contention Level |
| HiperLan | High Performance Local Area Network |
| HNA | Host and Network Association |
| HOLSR | Hierarchical Optimized Link State Routing Protocol |
| ICMP | Internet Control Message Protocol |
| IEEE | The Institute of Electrical and Electronics Engineers |
| IETF | The Internet Engineering Task Force |
| INRIA | Institut National de Recherche en Informatique et Automatique |
| IntServ | Integrated Services |
| IP | Internet Protocol |
| ISM | Industrial, Scientific and Medical radio bands |
| ITU | International Telecommunication Union |
| LAN | Local Area Network |
| LEACH | Low-Energy Adaptive Clustering Hierarchy |
| LE-OLSR | Life Enhancement -OLSR |
| LPL | Low Power Listening |
| LQI | Link Quality Indicator |
| MAC | Media Access Control |
| MANET | Mobile Ad-hoc NETWORKS |
| MCU | MicroController Unit |
| MEMS | MicroElectroMechanical Systems |
| MID | Multiple Interface Declaration |
| MOLSR | Multicast OLSR |
| MPR | MultiPoint Relays |
| MSC | Mobile Switching Center |
| NAM | Network Animator |
| NS-2 | Network Simulator 2 |
| NTDR | Near-term DigitalRadio |
| OE-OLSR | Optimized Energy- Optimized Link State Routing Protocol |
| OLSR | Optimized Link State Routing Protocol |
| OQPSK | O_set Quadrature Phase Shift Keying |
| OSI | OSI Open Systems Interconnection |
| OSPF | Open Shortest Path First |
| PAN | Personal Area Networks |
| PCF | Point Coordination Function |

| | |
|-------|--|
| PDR | Packet Delivery Ratio |
| PRNET | Packet Radio Network |
| QOLSR | Quality of Service extension introduced to the OLSR protocol |
| QoS | Quality of Service |
| RERR | Route ERRor |
| RF | Radio Frequency |
| RFC | Request For Comments |
| RREP | Route REPlY |
| RREQ | Route REQuest |
| RSVP | Resource Reservation Setup Protocol |
| RTS | Request To Sent |
| SOLSR | OLSR avec sécurité |
| SURAN | Survivable RAdio Networks |
| TBRPF | Topology Broadcast based on Reverse-Path Forwarding |
| TC | Topology Control |
| TCL | Tool Command Language |
| TCP | Transmission Control Protocol |
| TTL | Time To Live |
| UDP | User Datagram Protocol |
| VINT | Virtual InterNetwork Testbed |
| WSN | Wireless Sensor Networks |
| ZRP | Zone Routing Protocol |

Introduction Générale :

| | |
|---|---|
| 1. Contexte Général | 1 |
| 2. Motivations et problématique..... | 3 |
| 3. Contributions et structure de la thèse | 4 |

1. Contexte Général

La tendance croissante vers les réseaux de communication sans fil affecte de façon drastique les dispositifs électroniques ainsi que les habitudes dans toutes les sphères de la vie. Les réseaux sans fil conventionnels sont gérés par des stations de bases; les unités mobiles doivent interagir avec ces stations de bases selon le modèle classique client/serveur. Pour rendre les réseaux sans fil plus autonomes, les efforts de recherche se focalisent sur les réseaux sans fil complètement plats. Ceux-ci, dénués de toute infrastructure centralisée permettent aux nœuds de communiquer entre eux malgré la couverture restreinte offerte par leur antenne. Dans un scénario de communication à saut multiples, un paquet généré par une source est relayé par plusieurs nœuds intermédiaires jusqu'à destination. Ces réseaux sont dits ad hoc. Un réseau mobile ad hoc, appelé généralement MANET (Mobile Ad hoc NETWORK), consiste en une population relativement dense, d'unités mobiles qui se déplacent dans un territoire quelconque et dont le seul moyen de communication est l'utilisation des interfaces sans fil, sans l'aide d'une infrastructure d'administration centralisée. La topologie du réseau peut changer à tout moment et est imprévisible avec la déconnexion fréquente des unités mobiles. Le caractère aléatoire des MANET pose de sérieux défis lorsque les unités mobiles doivent coopérer pour partager ou accéder à des données et services.

Les défis liés aux réseaux ad hoc sont encore plus importants lorsqu'il s'agit des RCSF (Réseaux de Capteurs Sans Fil) à cause du facteur d'échelle, c'est-à-dire que le nombre de nœuds déployés dans les RCSF est beaucoup plus important comparativement aux MANET. En effet, les avancées récentes dans les technologies de miniaturisation et des systèmes embarqués ont permis le développement à faible coût de systèmes minuscules micro-électromécaniques (MEMS) appelés capteurs, capables de détecter, mesurer et rapporter des données physiques liées à leur environnement. Ces capteurs caractérisés par de faibles ressources (énergie, capacité de calcul, mémoire, etc.) sont munis d'une interface sans fil qui leur permet de collaborer dans l'objectif de réaliser les trois fonctions principales: (a) la capture de données reliées à leur environnement

physique (température, pression, vibration, lumière, mouvement, etc.); (b) le traitement des données collectées; (c) la transmission de ces données à un centre de traitement(CT). Une variante de ces capteurs, plus puissante et plus couteuse dispose de fonctionnalités additionnelles telle que la capacité à se mouvoir pour réaliser des tâches : Ce sont des acteurs. La cohabitation entre capteurs et acteurs donne lieu à plusieurs autres variantes de RCSF. Les réseaux de capteurs et d'acteurs sans fil (RCASF) sont composés de capteurs qui recueillent des informations du monde physique et les rapportent aux acteurs qui prennent des décisions et effectuent les actions pertinentes. De même, avec l'avènement de capteurs d'imagerie, CMOS caméras micros, capables de générer des flux multimédias, la dénomination de réseaux de capteurs multimédias sans fil (RCMSF) est née. Tous ces types de RCSF sont destinés à une multitude d'applications dans les domaines militaire, industriel et domestique, et suscitent les intérêts aussi bien de la communauté scientifique que des milieux industriels. Pourtant le déploiement en grand nombre des capteurs pose plusieurs défis liés aux mécanismes d'adressage et aux techniques de routage des données d'événements détectés.

Dans notre recherche nous avons abordé la contrainte principale d'énergie de ces éléments de réseau livrés à eux au même, tout en essayant d'analyser les différents aspects liés à la caractéristique énergétique due au routage de l'information et proposer des algorithmes permettant d'apporter des améliorations dans la conservation de l'énergie consommée par les éléments du réseau afin d'augmenter la durée de vie de tels réseaux.

A cet effet nous avons pris comme modèle répandu dans ce domaine, le protocole baptisé « OLSR », très répandu dans les réseaux AHWSN, vu son caractère proactif, mais qui présente plusieurs contraintes de consommation d'énergie, faisant objet à une multitude de recherches et publications.

2. Motivations et problématique

Les motivations qui nous ont incités à focaliser notre recherche dans cette optique et le déploiement rapide des réseaux AHWSN ainsi que le progrès observé par ces derniers dans notre monde professionnel et personnel. Plusieurs études et recherches ont abordé ce thème qui est devenu le sujet d'actualité et l'expansion qui a explosé les réseaux filaires.

La mise en œuvre des traitements, de stockage, de détection et de communication dans des dispositifs de petite taille, à faible coût et leur intégration dans les réseaux de capteurs sans fil ouvre la porte à une multitude de nouvelles applications.

La motivation principale de notre travail est l'efficacité dans l'utilisation de ces dispositifs. Cette efficacité est d'une importance vitale étant donné que ces capteurs fonctionnent généralement à batteries limitées en capacités et que dans le cas général, ces dernières ne peuvent pas être remplacées ni rechargées.

Les techniques conçues pour les réseaux traditionnels ne sont pas bien adaptées aux réseaux AHWSN. De nombreuses contraintes doivent être résolues pour les réseaux de capteurs sans fil. Nous nous intéressons, dans cette thèse, aux contraintes posées par le routage et par la gestion de l'énergie dans ce type de réseaux pour prolonger leur durée de vie. Pour cela, notre objectif est de proposer des algorithmes de routage basés sur la conservation de l'énergie en faisant participer des nœuds ayant des batteries pleines comme acteurs principaux par rapport à leurs voisins tout en évitant les zones pauvres en énergie ou en capteurs.

La plupart des solutions proposées pour la diffusion et la couverture de zones dans les réseaux AHWSN s'appuient sur une vue à plat où tous les nœuds sont considérés comme égaux et doivent contribuer ensemble à la gestion du réseau pour qu'ils puissent accomplir leurs tâches. Par ailleurs, les capteurs peuvent apparaître, disparaître (par extinction de leur radio, épuisement de leur énergie ou leur crash), ou se déplacer indépendamment les uns des autres. Ainsi, la topologie du réseau est en constante évolution. De ce fait, l'acheminement de l'information d'un capteur à une station de base distante et vice versa doit se faire par un protocole efficace en énergie.

Afin que ce protocole soit efficace, il devra prendre en considération les contraintes intrinsèques du réseau (topologie en constante évolution), les ressources limitées des capteurs en termes de calcul, de stockage et d'énergie, ainsi que le mode de gestion du médium de communication partagé (bande passante limitée, collisions, ...). L'une des

solutions communément proposées pour la diffusion et la couverture de zones dans les réseaux de capteurs sans fil est d'utiliser une architecture hiérarchisée appelée encore clustering. Cette architecture permet de regrouper les capteurs proches géographiquement en clusters et d'utiliser des schémas de routage différents au sein des clusters et entre les clusters. Ainsi un tel capteur au sein d'un cluster stocke la totalité des informations des capteurs qui font partie de son cluster et seulement une partie des informations qui concernent les autres clusters. Dans cette architecture, seulement les cluster-heads et les nœuds passerelles sont responsables du cheminement de l'information captée par un capteur à la station de base.

3. Contributions et structure de la thèse

Dans notre thèse, nous avons proposé deux algorithmes de routage, une extension du protocole OLSR « Otimized Link State Routing », principalement basés sur la technique des relais multipoints (MPR) afin d'acheminer l'information à destination. Les simulations de ces deux algorithmes ont conclu une nette amélioration en matière de conservation d'énergie dans les réseaux AHWSN. Les deux algorithmes sont bien étalés dans les chapitres 3 et 4 de cette thèse.

Nous avons réparti notre thèse comme suit :

- Le chapitre 1 abordera des généralités sur les réseaux AHWSN ainsi que leurs domaines d'application. Nous avons présenté quelques contraintes essentielles relatives au déploiement de tels réseaux. Il était jugé très utile de présenter les différents protocoles de routage qui ont été développés pour les réseaux AHWSN. Une importance particulière a été attribuée au protocole « OLSR » qui est l'axe principale de notre recherche. Nous avons détaillé son mécanisme de fonctionnement basé sur les relais multipoints ainsi que les différentes limitations de ces protocoles dans la conservation d'énergie.
- Dans le chapitre 2, Nous avons étalé les différents concepts liés à la qualité de service (QoS) des réseaux AHWSN. Ces derniers se présentent comme étant des réseaux sans infrastructures et à forte mobilité, d'où beaucoup de contraintes liées à la qualité de services doivent être étudiées. La principale problématique dans un tel réseau est la conservation d'énergie des nœuds le constituant. Ces derniers sont alimentés par des batteries de capacité limités. Cette contrainte a fait l'objet de plusieurs recherches en incluant la mobilité constante et l'architecture aléatoire de tels réseaux.

- Le chapitre3 quant à lui, décrit principalement notre première contribution au protocole OLSR. Il présente notre plateforme de simulation basée sur le simulateur de réseau NS2 ainsi que les différents éléments qui ont été étudiés pour comparer notre algorithme à celui de l'OLSR basique. Grâce à ce simulateur nous avons pu démontrer les différentes performances de notre algorithme par rapport à celui implémenté dans le protocole OLSR. A cet effet, nous avons défini quelques métriques de qualité de service (control overhead, AVG end to end delay, dead nodes), nous permettant de comparer les performances de chaque protocole.
- Le chapitre4, expose notre deuxième algorithme baptisé LE-OLSR, permettant d'apporter davantage d'amélioration en matière de conservation d'énergie dans un réseau AHWSN. Cet algorithme permet aux différents nœuds du réseau de jouer le rôle de relais multipoints afin de répartir la charge sur l'ensemble du réseau et augmenter de ce fait, sa durée de vie.
- Enfin, nous achevons notre travail par une conclusion ainsi que diverses perspectives de recherches dans cette optique.

Concept des réseaux AHWSN : Routage et diffusion

| | |
|--|----|
| 1. Introduction | 7 |
| 2. Concept et architecture des réseaux ad-hoc..... | 9 |
| 3. Cas particulier : Réseaux de capteurs (WSN)..... | 12 |
| 3.1 Anatomie des capteurs..... | 12 |
| 3.2 Architecture des réseaux WSN..... | 13 |
| 4. Domaines d'application des réseaux AHWSNs..... | 15 |
| 5. Contraintes liées au déploiement des réseaux AHWSN..... | 16 |
| 5.1 Cas des MANET..... | 17 |
| 5.2 Cas des WSN..... | 17 |
| 6. Routage de l'information dans les réseaux AHWSN..... | 22 |
| 6.1 Protocoles proactifs..... | 23 |
| 6.2 Protocoles réactifs..... | 25 |
| 6.3 Protocoles réactifs Vs Protocoles proactifs..... | 27 |
| 6.4 Protocoles hybrides..... | 28 |
| 6.5 Routage dans les réseaux WSN..... | 31 |
| 6.5.1 Les Protocoles hiérarchiques..... | 31 |
| 6.5.2 Les protocoles de routage basés sur la localisation..... | 33 |
| 6.5.3 Les protocoles de routage 'data-centric'..... | 34 |
| 6.5.4 La diffusion dirigée..... | 36 |
| 6.5.5 Le protocole de routage par rumeur..... | 36 |
| 7. Conclusion..... | 38 |

1. Introduction

Les équipements mobiles deviennent de plus en plus petits et puissants en termes de capacité de traitement et de stockage de données. De plus, ils sont dotés d'une multitude de fonctionnalités qui permettent d'assurer différents types d'applications et de services. Parmi les applications et services offerts via un équipement mobile, figurent les services de connexions et les services de données correspondants. Ces derniers représentent le service le plus demandé par les utilisateurs mobiles. Par exemple, les connexions entre deux téléphones mobiles cellulaires sont assurées par les BSC et les MSC; les ordinateurs portables sont connectés à Internet via des points d'accès fixes.

Il y a en outre, des situations spécifiques où les besoins de connexions des utilisateurs ne sont pas assurés par le réseau dans une zone géographique donnée. Dans cette situation, fournir la connectivité est un réel défi. Récemment, de nouvelles alternatives pour fournir les services ont été proposées. Elles sont basées sur le fait d'avoir des stations mobiles interconnectées les unes aux autres grâce à une configuration autonome, créant ainsi un réseau ad hoc flexible et performant. Parallèlement, le réseau ad hoc peut être utilisé pour l'extension d'un réseau filaire. Dans ce cas, les nœuds mobiles peuvent avoir accès à l'Internet à travers une passerelle, pour étendre les services de l'Internet au-delà de l'infrastructure filaire.

Dans le domaine des réseaux ad hoc, les réseaux de senseurs (ou de capteurs) représentent un champ important de recherche. Un réseau de senseurs est composé d'un grand nombre de nœuds mobiles aléatoirement distribués sur le terrain à étudier, dont les tailles et les capacités sont très réduites, et dont l'objectif est de collecter les informations. Le routage ad hoc constitue la base des réseaux de senseurs. Cependant, les solutions proposées dans les réseaux ad hoc sont généralement inadaptées aux spécificités des réseaux de senseurs, vu le type d'application spécifique de ces réseaux et la fonction principale des nœuds qui est de collecter l'information. De plus, les communications dans les réseaux de senseurs sont souvent à un saut et consistent à remonter l'information à une entité centrale.

Historiquement, les réseaux mobiles ad hoc ont été d'abord introduits pour l'amélioration des communications dans le domaine militaire. Dans ce contexte, il n'existe pas d'infrastructure existante pour relier les communications, vue la nature dynamique des opérations et des champs militaires.

Les premières applications dans les réseaux ad hoc sont apparues avec le projet PRNet (Packet Radio Network) [1] en 1972. Ce projet a été inspiré par l'efficacité de la

technologie par commutation de paquet, le partage de la bande passante, le routage store-and-forward, et ses applications dans l'environnement mobile sans fil.

SURAN (Survivable Radio Networks) [2] a été développé par la DARPA en 1983 pour dresser les principaux problèmes du projet PRNet dans le domaine de la scalabilité, la sécurité, la capacité de traitement et gestion d'énergie. Les objectifs étaient de proposer des algorithmes qui peuvent supporter jusqu'à une dizaine de milliers de nœuds, tout en utilisant des mécanismes radio simples, avec une faible consommation d'énergie, et un faible coût. Ce travail a amené à la conception de la technologie LPR (Low-cost Packet Radio) [3] en 1987, dotée d'une couche radio DSSS (Direct Sequence Spread-Spectrum) avec un processeur pour la commutation de paquets intégré (Intel 8086). De plus, une famille de protocoles pour la gestion du réseau a été développée, et une topologie hiérarchique du réseau basée sur un clustering dynamique est utilisée pour remédier au problème de la scalabilité. Des améliorations pour l'adaptabilité de la couche radio, la sécurité et l'augmentation de la capacité ont été proposées. L'évolution des infrastructures du réseau Internet et la révolution de la micro-informatique ont permis de rendre faisables et applicables les idées initiales des réseaux radio de paquets. Le programme GloMo (Global Mobile) [4] initié par la DARPA en 1994 avait comme objectif de supporter les communications multimédia n'importe quand et n'importe où à travers des équipements sans fil.

Tactical Internet (IT) [1] est l'une des implémentations des réseaux sans fil ad hoc grandeur nature développée par l'armée américaine en 1997, utilisant des débits de plusieurs dizaines de kilobits par seconde.

Un autre déploiement a été réalisé en 1999, avec ELB ACTD (Extending the Littoral 1.1. Battle-space Advanced Concept Technology Demonstration) [5] qui permet de démontrer la faisabilité de concepts militaires pour les communications des bateaux en mer aux soldats sur la terre par l'intermédiaire d'un relais aérien. 20 nœuds dans le réseau ont été considérés.

Dans la suite de ce chapitre nous allons aborder le concept des réseaux Ad-hoc et les réseaux de capteurs. Quelques domaines d'application seront étalés démontrant ainsi les différentes contraintes liées au déploiement de tels réseaux.

2. Concept et architecture des réseaux ad-hoc

Les réseaux mobiles ad hoc, aussi appelés MANET (pour Mobile Ad hoc Network), sont des réseaux radio sans infrastructure prédéfinie, aptes à se créer et à s'organiser dynamiquement quand plusieurs équipements se trouvent à portée radio les uns des autres. Une des principales caractéristiques de ces réseaux est que les nœuds sont mobiles, et qu'ils peuvent rejoindre ou quitter le réseau de façon dynamique. La figure 1.1 montre une topologie classique d'un réseau ad hoc. Comme le montre cette figure, les nœuds ne s'appuient pas sur un point d'accès ou une station de base pour communiquer entre eux. Pour se faire, les nœuds utilisent leurs voisins immédiats afin de faire suivre leurs communications. Les nœuds commencent par découvrir leur voisinage et à chaque fois que l'un d'entre eux souhaite communiquer, il envoie son message à ses voisins qui à leur tour l'envoient à leurs voisins et ainsi de suite. Ce processus est répété jusqu'à ce que le message atteigne le nœud destinataire. Ainsi, il est possible de créer de manière spontanée des réseaux à partir d'un ensemble de nœuds suffisamment proches les uns des autres.

Un des paradigmes des réseaux ad hoc est celui de la mise en place rapide d'un réseau de communication dans le cas d'une catastrophe sur des zones dépourvues d'infrastructures ou encore dans le cas où l'infrastructure existante est hors service, voire complètement détruite.

Les exemples les plus réalistes sont les catastrophes naturelles comme les tremblements de terre, les inondations, etc. Les équipes de secours ont besoin de mettre rapidement en place un réseau de communication pour coordonner les recherches, les informations logistiques, voire désenclaver les populations isolées en leur offrant

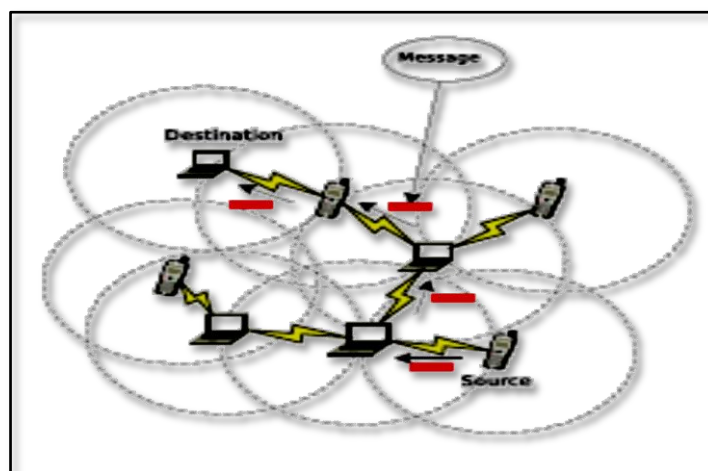


Figure 1.1 : Architecture d'un réseau ad-hoc

rapidement un moyen de communication.

Les nœuds des réseaux ad hoc peuvent être de natures très diverses (ordinateur portable, PDA, caméra sans fil, capteur, téléphone mobile, lecteur MP3, console de jeux, etc.) et avoir des caractéristiques matérielles et logicielles variées (débit de transmission, mémoire, batterie, unité centrale, etc.). Ces nœuds peuvent communiquer en utilisant une ou plusieurs technologies sans fil avec une capacité énergétique limitée : Bluetooth, IEEE 802.11, HiperLAN2 et UWB sont les technologies les plus fréquemment utilisées.

Nous pouvons faire ressortir quatre caractéristiques (contraintes) essentielles qui doivent être prises en considération dans la conception de tout protocole dédié aux réseaux ad hoc [6] :

- **Topologie dynamique.** Les nœuds se déplacent indépendamment les uns des autres et de manière imprévisible. Un nouveau terminal peut intégrer le réseau et en ressortir à n'importe quel moment.
- **Capacités des liens limitées.** Même si les technologies sans fil ont fait d'énormes progrès en termes de bande passante, ils restent néanmoins inférieurs à ceux des technologies filaires. La bande passante varie d'un type de réseau ad hoc à un autre. Par exemple, les performances attendues dans les réseaux de capteurs ne seront pas les mêmes que celles attendues dans les réseaux ad hoc d'entreprise.
- **Autonomie et puissance de calcul limitées.** Comme nous l'avons vu un peu plus haut, les nœuds d'un réseau ad hoc sont de petits dispositifs électroniques qui, d'une part, fonctionnent en mode batterie dans la majorité du temps et, d'autre part, sont limités en puissance de calcul. Il faut aussi noter que ces deux caractéristiques dépendent l'une de l'autre.
- **Protection physique.** Les nœuds d'un réseau ad hoc n'ont pas la même protection physique que les nœuds d'un réseau filaire. En effet, ceux d'un réseau ad hoc sont censés être mobiles et parfois complètement autonomes, c'est notamment le cas des réseaux de capteurs où les nœuds sont souvent lâchés, dans un environnement particulier et parfois hostile, sans aucune surveillance particulière.

L'intérêt principal des réseaux ad hoc est leur capacité à réduire le coût de déploiement. De plus, ils permettent des communications de proche en proche dans des environnements où il n'est pas possible d'installer une infrastructure complète pour des raisons techniques ou fonctionnelles. Après une configuration initiale du terminal, les réseaux ad hoc sont généralement auto-administrés, c'est-à-dire que les utilisateurs eux-mêmes découvrent et utilisent les ressources disponibles dans leur voisinage,

communiquent entre eux, partagent des données, des applications, etc., sans avoir besoin d'une administration centralisée.

Néanmoins, si ce fonctionnement est très appréciable dans un environnement public, il peut représenter un problème dans un contexte sécuritaire. Cette description correspond à un réseau purement ad hoc. En pratique il existe une infinité de variantes mélangeant ad hoc et infrastructure. En effet, selon l'application visée et selon les contraintes liées à l'environnement de déploiement du réseau, on aura des réseaux privilégiant l'approche ad hoc ou l'approche infrastructure.

Voici quelques exemples de réseaux purement ou partiellement ad hoc utilisés dans différents domaines [6] :

- **Réseaux mesh** : Les opérateurs d'un réseau à infrastructure peuvent avoir la possibilité d'étendre la couverture de leur réseau à un moindre coût et ainsi accroître le nombre de clients potentiels. Par exemple, un mobile trop éloigné du réseau de l'opérateur (cellule GSM, point d'accès Wi-Fi, etc.) peut bénéficier du réseau ad hoc et du routage du trafic assuré par les nœuds ad hoc pour communiquer avec l'infrastructure.
- **Réseaux VANETs (pour Vehicular Ad hoc Networks)** : Dans ces réseaux, le but est de fournir de l'information à des véhicules sur les autoroutes. Lorsqu'ils sont suffisamment proches les uns des autres, les véhicules constituent automatiquement un réseau. Ainsi, dès que l'un de ces véhicules est près d'un point d'accès, il commence à recevoir de l'information qu'il diffuse par la suite aux autres véhicules du même réseau ad hoc.
- **Réseaux de capteurs** : Un réseau de capteurs peut être composé d'une centaine ou de milliers de nœuds. Ces appareils, appelés en anglais *motes*, sont des dispositifs électroniques pas très coûteux et limités en ressources : énergie, mémoire et capacité de calcul. Ils sont déployés de façon aléatoire dans des environnements souvent ouverts. Dans la majorité des cas, les capteurs font, indépendamment les uns des autres, des mesures périodiques et envoient les données collectées à un dispositif plus puissant appelé le puits (Sink) ou la station de base, qui agrège les données reçues en calculant, par exemple, leur maximum, moyenne ou médiane.

On peut aussi classer les réseaux ad hoc dans la catégorie des réseaux autonomes et spontanés. Cette catégorie inclut également les réseaux pair-à-pair. En effet, l'une des caractéristiques essentielles d'un réseau autonome est de parvenir à offrir des services

en s'auto-configurant et en coopérant directement sans l'intervention d'une quelconque partie extérieure.

3. Cas particulier : Réseaux de capteurs (WSN)

a. Anatomie des capteurs

Les WSN (Wireless Sensor Networks) sont composés de dispositifs électroniques de petite taille et de faible coût, intégrant un ensemble de fonctionnalités telles que : une unité de calcul, une mémoire, des sondes et une interface sans fil. Cet ensemble appelé capteur interagit avec l'environnement, de concert avec ses pairs pour détecter et contrôler les phénomènes physiques tels que la température, la pression, le bruit, la machinerie, etc. Un capteur est un système embarqué (de l'électronique et un Built-in OS), tel qu'illustré dans la Figure 1.2 (a). Il est composé essentiellement de quatre blocs fonctionnels [7] : l'unité centrale composée d'un microprocesseur et d'un microcontrôleur; le bloc d'émission/réception doté d'une interface radio opérant sur une courte distance; le sous-système de capteurs qui relie le nœud au monde physique est constitué d'un ensemble de capteurs; le sous-système d'alimentation en énergie intègre une batterie ainsi qu'un convertisseur de tension continue.

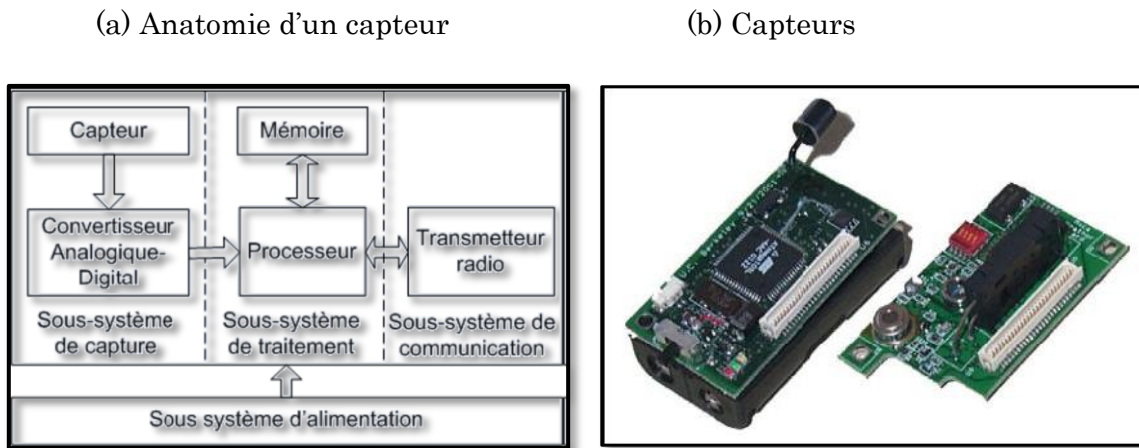


Figure 1.2 Vue d'ensemble d'un capteur

L'unité centrale est le centre d'intelligence du capteur. Elle est responsable du contrôle du capteur, de l'exécution des protocoles de communication et des algorithmes de traitement des signaux sur les données captées. Elle supporte plusieurs modes de

fonctionnement souvent guidés par le souci de l'économie d'énergie : le mode actif, le mode libre et le mode de veille. Le sous-système radio assure la communication avec le monde extérieur. Plusieurs facteurs affectent sa consommation en énergie : la technique de modulation utilisée, le débit d'interface, la puissance d'émission, et le cycle d'activité.

Il dispose de quatre modes de fonctionnement : émission, réception, libre, veille. Le sous-système de capteurs est responsable de l'observation et de la conversion des phénomènes physiques en signaux électriques; les capteurs peuvent être analogiques ou numériques dépendamment du type de signal qu'ils génèrent sous l'effet du phénomène contrôlé. Ils peuvent mesurer la température, la luminosité, le son, le champ magnétique et capter aussi des images. À son niveau, il existe plusieurs sources de consommation d'énergie : l'échantillonnage du signal reçu, la conversion du phénomène physique en signaux électriques, la mise en forme du signal (filtrage), et la conversion analogique à numérique. L'alimentation est responsable de la fourniture d'énergie aux autres entités, et détermine par ce fait même la durée de vie du capteur. Elle intègre un convertisseur de tension continue responsable de la fourniture en tension constante des autres entités du capteur. La Figure 1.2 (b) montre une vue réelle d'un capteur.

b. Architecture des réseaux WSN

La Figure 1.3 illustre la variante des réseaux ad hoc qui sont les RCSF. Un RCSF est composé de capteurs généralement déployés en grand nombre et munis de transmetteurs sans fil. Chaque capteur est susceptible de collecter des données (traitées ou pas) de l'environnement et de les acheminer vers un centre de traitement par l'intermédiaire d'une passerelle ("sink" ou "gateway") et ceci en un ou plusieurs sauts. La passerelle peut être fixe ou mobile et transmet ensuite ces données à un gestionnaire de tâches au centre de traitement (CT) via Internet ou par satellite. Le CT pourrait être un simple ordinateur central dont le rôle est l'analyse des données rapportées, et la prise de décisions. Le CT effectue certaines opérations sur les données, comme le filtrage et l'agrégation pour en extraire l'information utile. Les capteurs sont déployés en général par centaines ou milliers, avec une densité de nœuds généralement de l'ordre de 20 nœuds/m² [8], d'où la contrainte d'acheminement et routage de l'information. La transmission de l'information entre capteurs peut s'effectuer à l'aide d'un support radio, infrarouge, ou optique.

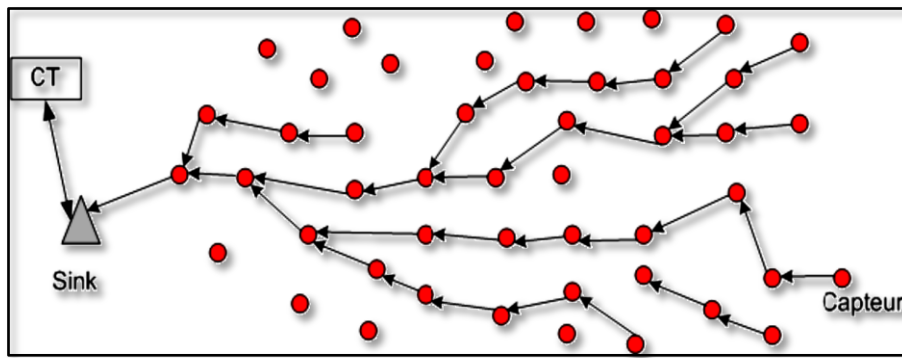


Figure 1.3 : Architecture d'un WSN

Parfois, les capteurs peuvent cohabiter avec des dispositifs plus riches en ressources de toute sorte (puissance de calcul, longue portée de transmission, batterie durable), appelés acteurs [9], ce qui donne lieu à l'architecture de la Figure 1.4 illustrant les réseaux de capteurs et d'acteurs sans fil (RCASF).

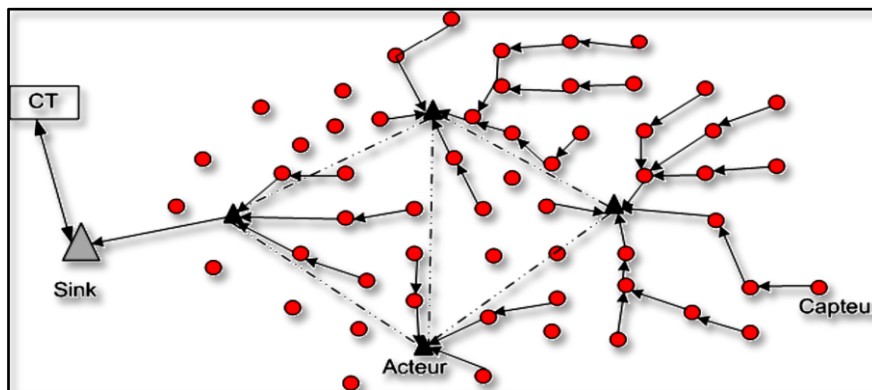


Figure 1.4 : Architecture d'un RCASF

Des coopérations s'établissent entre capteurs et acteurs mais aussi entre acteurs pour faciliter la gestion d'événements à l'aide d'architectures illustrées à la Figure 1.5. Dans l'architecture automatique (Figure 1.5(a)), les capteurs rapportent les événements détectés aux acteurs qui traitent les données rapportées et initient les actions appropriées. Quant à la Figure 1.5(b), elle illustre l'architecture semi-automatique dans laquelle les capteurs rapportent les événements détectés au Sink qui initie les commandes appropriées aux acteurs.

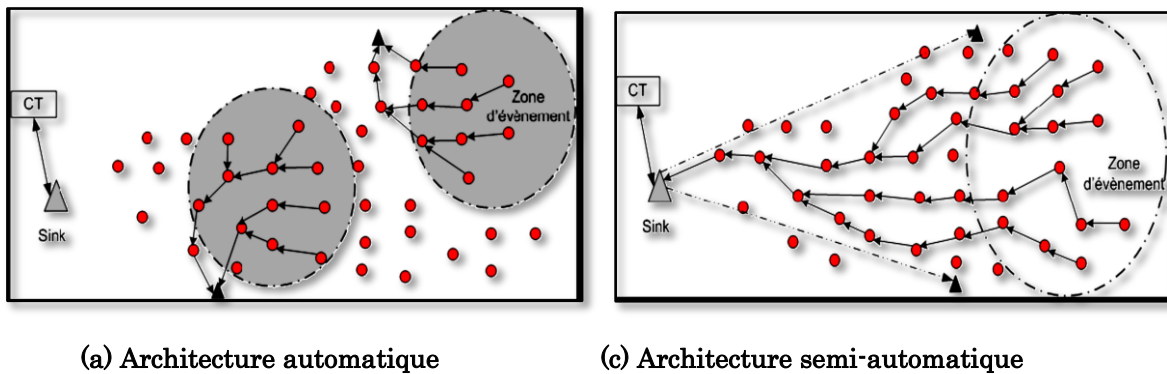


Figure 1.5 : Différents types d'architecture des RCASF

Généralement, dans les WSN, la nature des données collectées et acheminées par les capteurs est beaucoup plus importante que l'identité des capteurs: on dit que les WSN sont *data-centric* [10]. Les données sont requises soit par le Sink, soit par un acteur dans le réseau sur la base d'attributs: on parle alors d'adressage par attributs. Ce type d'adressage permet de trouver des routes de plusieurs sources vers une seule destination. Pour cela, les données des événements détectés sont décrites par une liste de paires attribut-valeur [11].

4. Domaines d'application des réseaux AHWSNs

Les MANET préliminairement pressentis pour les communications militaires connaissent maintenant un plus grand intérêt dans les domaines commercial et de l'éducation. Dans le domaine militaire, il est possible de doter les soldats de dispositifs sans fil afin qu'ils puissent communiquer les uns avec les autres sans l'aide d'une infrastructure centrale vulnérable. Ils peuvent faire l'objet d'installations domestiques comprenant des Laptop, imprimantes, téléphones mobiles, etc. Les MANET peuvent aussi être déployés dans les applications civiles pour permettre la communication entre taxis et polices [12], et aussi dans les opérations de sauvetage d'urgence durant les catastrophes naturelles. Durant des événements spéciaux tels que les jeux Olympiques, la Coupe du Monde de Football, ou dans les aéroports, les MANET peuvent être déployés pour l'extension de la couverture radio à plusieurs usagers. De façon générale, les MANET peuvent être déployés partout où le recours à une infrastructure centralisée pour la communication est difficile.

Quant aux WSN, leur usage permet la gestion et l'analyse de phénomènes complexes sur une large région et sur une longue période de temps. Des données telles que la température, l'humidité, la pression, le bruit ainsi que toute sorte d'informations

liées à la machinerie peuvent être obtenues et traitées moyennant le déploiement de capteurs sans fil. Les WSN sont généralement déployés en grand nombre dans une zone géographique où ils vont capter, mesurer et rapporter certains phénomènes physiques. Dans le domaine militaire, ils peuvent être utilisés pour surveiller le déplacement de troupes ennemies dans un espace donné, ou récolter des données dans une zone dangereuse où l'envoi d'êtres humains serait à risque. À titre d'exemple, les WSN ont été utilisés, sous une forme assez primitive, lors de la guerre froide par les Américains qui ont placé dans l'océan un système appelé SOSUS [13], composé de capteurs acoustiques pour surveiller les sous-marins silencieux russes. Dans le domaine civil, les WSN peuvent être utilisés dans la surveillance des infrastructures, des installations et des zones critiques. Ils peuvent également être utilisés pour surveiller des habitations et contribuer au confort domestique, en transformant les logements en environnements intelligents dont les paramètres (température, pression, humidité, luminosité, etc.) s'adaptent automatiquement au comportement des individus. Dans le domaine de l'environnement, ils peuvent localiser et suivre le mouvement de certains animaux, détecter des feux de forêt ou encore surveiller l'évolution de la densité moyenne de CO₂ dans l'air. CORIE [14] est un exemple réel d'application où des capteurs récoltent des informations sur l'eau de la rivière Columbia (température, salinité, flux et niveau de l'eau, etc.), lesquelles sont utilisées pour gérer les opérations de secours et les interventions sur l'écosystème. Dans le domaine industriel, les capteurs peuvent être placés sur des boîtes de marchandise dans une usine ou un entrepôt pour suivre en temps réel le mouvement des marchandises, ou encore détecter le dysfonctionnement d'une machine en analysant ses émissions acoustiques et vibratoires. Actuellement, il existe quelques applications commerciales assez primitives des WSN, par exemple pour la lecture distante des appareils commerciaux de mesure de la consommation énergétique domestique (les compteurs d'électricité, de gaz, etc.) ou la télémétrie des puits d'une installation pétrolière.

5. Contraintes liées au déploiement des réseaux AHWSN

Même si les MANETs et les WSN présentent des caractéristiques similaires, le facteur d'échelle rend les défis encore plus considérables dans les WSN. Dans cette section, nous exposons les défis liés à l'accessibilité aux données dans les MANET, puis ceux relatifs aux mécanismes d'adressage et de routage avec QoS dans les WSN.

a. Cas des MANET

Les MANET fournissent une solution attrayante pour la mise en réseau dans les situations où l'infrastructure de réseau n'est pas disponible. Ils peuvent communiquer avec des réseaux extérieurs tels que l'Internet à travers une passerelle [15]. La Figure 1.7 illustre l'architecture d'un MANET composé de nœuds mobiles et d'une passerelle vers Internet.

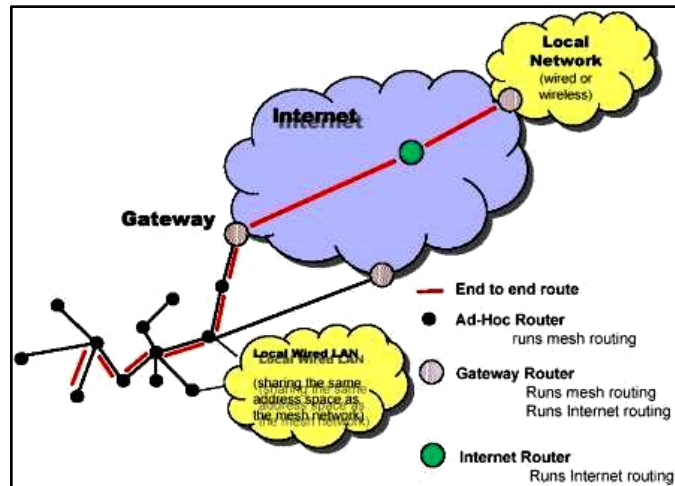


Figure 1.6 : Architecture d'un MANET

Toutefois, les demandes d'accès aux données devront faire face aux problèmes engendrés par les caractéristiques spéciales des MANET, notamment :

- **Le médium sans fil:** les nœuds mobiles communiquent entre eux par l'intermédiaire du médium sans fil ; une seule diffusion peut couvrir tous les voisins à portée radio. Cette nature de la diffusion est un avantage pour le trafic multicast [16], mais pour le trafic unicast, les nœuds entrent en compétition pour avoir accès au médium. En particulier, pour les applications client-serveur, plusieurs sessions simultanées basées sur une communication unicast entre les nœuds et le serveur de données peuvent créer de la congestion, des pertes de paquets ainsi que des interférences lors de la transmission. Cela a aussi pour conséquence d'augmenter la latence d'accès à l'information.
- **La topologie dynamique:** La topologie du réseau connaît des changements fréquents dus à la mobilité des nœuds, la rupture en énergie, et les interférences. Le changement de topologie du réseau provoque aussi des ruptures de routes et induit une surcharge supplémentaire pour l'établissement de nouvelles liaisons. Pour les demandes d'accès aux données, si la route vers le serveur est rompue, la

communication client-serveur sera retardée voire supprimée si une nouvelle route ne peut s'établir à temps. Ce retard ou cette déconnexion est plus susceptible de se produire lorsque plusieurs nœuds sont impliqués dans une interaction client-serveur.

- **La redondance des données** : Si toutes les unités mobiles doivent disposer d'un cache et stocker les mêmes données dans cette dernière, cela relèverait d'un gaspillage d'espace mémoire. Par exemple, on peut imaginer qu'un groupe de travail traitant du même sujet accède pratiquement tout le temps aux mêmes informations et constitue ainsi un scénario typique de gaspillage d'espace, puisque chaque membre du groupe stocke les mêmes informations que ses voisins.
- **La communication multi-saut** : Pour les demandes d'accès aux données, lorsque le nombre de sauts dans une route entre un serveur et un client augmente, cela diminue la fiabilité de la route et, en conséquence augmente le temps de réponse. Ainsi la connexion, si elle est établie entre unités mobiles n'est pas toujours fiable, offrant du coup une qualité de service imprévisible.
- **Des ressources limitées** : Un nœud a généralement des ressources limitées en termes d'énergie, de capacité de calcul, et d'espace de stockage. De ce fait, les nœuds subissent des déconnexions fréquentes, c'est-à-dire que les terminaux dont ils disposent ne restent pas indéfiniment connectés, ceci dans le but d'économiser de l'énergie. En conséquence, la résolution des requêtes d'accès aux données doit être effectuée avec le moins de ressources possibles.
- **La cohérence des données**: La faible bande passante ainsi que le motif de déconnexion des unités mobiles rendent difficiles les mises à jour ainsi que la maintenance de la cohérence des données. La mise en cache par les unités mobiles de données résidant sur un serveur distant apparaît comme une technique efficace pour améliorer les performances de l'accessibilité aux données dans les réseaux filaires. Cela réduit considérablement la latence d'accès aux données et diminue le risque d'usage abusif de la bande passante. Cependant, le schéma classique utilisé dans les réseaux filaires où les usagers sont toujours connectés, ne pourrait pas convenir à un environnement aussi dynamique que celui des MANET, à cause de leur déconnexion fréquente et de leur mobilité incontrôlable. Dans un environnement réel, les données sont généralement mises à jour. Les nœuds du réseau peuvent accéder à des données invalides alors que les originales de celles-ci ont subi une mise à jour. De tels accès aux données invalides consomment inutilement les ressources des nœuds. Pour résoudre ce problème, des mécanismes d'invalidation et de rafraîchissement de

données sont nécessaires, ce qui représente tout de même des opérations coûteuses en bande passante. Plusieurs travaux se sont penchés sur le problème [17-19], mais laissent toujours en suspens la question récurrente de la surcharge de signalisation induite par la mise à jour des données.

Toutes ces caractéristiques intrinsèques aux MANET rendent l'accessibilité aux données, complexe. Pour prévenir la détérioration de cette accessibilité aux données ou services, les mécanismes de conservation et de partage de données utilisent en général des opérations de réplication ou de la mise en cache. Même si ces deux techniques sont attrayantes pour le partage et le stockage des données dans les MANET, aucune investigation relative à une stratégie hybride des deux techniques n'a été menée pour approcher le problème de l'accessibilité des unités mobiles aux données.

b. Cas des WSN

Le nombre croissant de propositions qui essaient de traiter des problèmes liés aux WSN reflète l'intérêt de la communauté scientifique pour cette technologie. La résistance au facteur d'échelle, l'adaptabilité, les contraintes d'énergie et la topologie dynamique sont les facteurs de conception qui doivent être considérés lors du déploiement des WSN [7].

Les WSN diffèrent justement des MANET par ce facteur d'échelle caractérisé par le déploiement d'une multitude de capteurs souvent dans le but de garantir une redondance dans la détection des événements. Dans ce contexte, l'adressage IP ou node-centric qui a été défini pour identifier et localiser un nœud dans les réseaux traditionnels doit être repensé. L'adressage par attribut ou data-centric proposé.

Comme alternative dans les WSN on exploite massivement l'inondation du réseau pour acheminer les requêtes et les données. L'inondation est en générale très gourmande en énergie, car elle affecte plus de nœuds dans le réseau qu'il n'en faut. Le défi à relever revient à cibler lors d'une requête, les capteurs seront susceptibles de garantir des réponses précises dans des délais courts et garantis, sans avoir recours à une inondation massive du réseau. Un mécanisme d'adressage similaire à celui d'IP est nécessaire pour la mise à jour des tables de routage dans chaque nœud, la connaissance partielle ou totale de la topologie du réseau alors que les capteurs sont déployés par centaines. En

outre, la capacité mémoire des capteurs ne peut leur permettre de gérer des mécanismes de fragmentation ou de réassemblage de paquets tels que dans les réseaux IP.

Avec un réseau aussi dense que celui des capteurs, l'allocation d'adresses IP est complexe parce qu'un mécanisme d'allocation centralisé tel que celui du protocole DHCP deviendrait rapidement une source de congestion et de consommation d'énergie, à cause de la signalisation. La récupération d'adresses constitue un problème à gérer, en considérant que la topologie du réseau est dynamique (essentiellement à cause de la défaillance des nœuds). La mise à jour de tout ou d'une partie du réseau est une opération qui nécessite l'identification précise des nœuds destinés à être affectés. Ce problème non encore exploré dans les WSN revêt une importance toute particulière car la reconfiguration des nœuds dans les réseaux traditionnels permet de prolonger l'usage du matériel en réduisant les coûts d'investissement dans l'achat de nouveaux matériels.

L'usage de la localisation géographique des capteurs comme adresses apparaît comme une solution facile pour répondre au problème d'adressage dans ces réseaux, et par la même occasion permet un routage géographique des données d'événements détectés. Cependant l'adoption d'un tel mécanisme d'adressage pose les problèmes de coût de consommation énergétique, et d'efficacité de la localisation dans des environnements fermés.

La mise en œuvre d'un schéma d'adressage devrait aider au routage et à la collecte de données dans les WSN. C'est ce que s'efforce de faire l'adressage par attribut sans pour autant résorber le problème de l'inondation massive du réseau. Dépendamment de la catégorie de routage, le nombre de nœuds impliqués dans l'acheminement des paquets peut être élevé. Dans ce contexte, les ressources énergétiques des nœuds sont fortement sollicitées, diminuant progressivement la durée de vie du réseau. C'est pourquoi tout protocole de routage doit aussi minimiser les dépenses énergétiques des capteurs. Étant prévu que les RCSF devront aussi intégrer des capteurs multimédias (vidéo audio, etc.) [20], les protocoles de routage doivent garantir aussi une certaine QoS pour les applications multimédias et temps réel. Celles-ci produisent généralement un volume considérable de données qui en plus requiert des taux élevés de transmission, et des traitements intermédiaires (compression, décompression, etc.) qui consomment beaucoup d'énergie. En particulier, la transmission d'un flux vidéo en utilisant fréquemment le plus court chemin va absorber l'énergie du nœud sur ce chemin, et ainsi raccourcir la durée de vie du réseau. La plupart des propositions pour le routage dans les WSN sont basées sur un réseau plat homogène où chaque capteur est identique en termes de

capacités physiques. Cependant, les topologies plates ne sont pas toujours les plus adaptées pour traiter la quantité de trafic généré par des applications multimédias [20].

Par conséquent, il est impératif de développer de nouvelles stratégies de routage qui tiennent compte de cette particularité, tout en maximisant la durée de vie du réseau.

Outre ces exigences, ces stratégies doivent satisfaire les contraintes de QoS, ce qui représente un problème ouvert à résoudre dans les WSN.

Ce qui nous intéresse le plus dans notre thèse et le défi énergétique. L'existence des nœuds à faibles ressources dans un WSN impose la conception de protocoles économes en énergie. Comme dans les WSN, il faut préserver l'énergie au niveau des nœuds capteurs. Les protocoles de communication utilisés doivent donc limiter l'utilisation de trafic de contrôle et doivent être localisés et distribués. Aussi les nœuds riches en ressources (actionneurs) peuvent être sollicités plus que les nœuds à ressources limitées (capteurs).

En général, les capacités de traitement et de stockage sont faibles, cependant, la contrainte de conception la plus importante à prendre en compte est la capacité énergétique limitée des nœuds capteurs. Comme le montre la figure 1.7, la consommation d'énergie est dominée par la consommation de la radio du nœud. Il n'est donc pas seulement souhaitable d'envoyer peu de messages mais aussi de minimiser le temps où la radio est allumée. Ainsi les nœuds devraient donc être mis en sommeil le plus longtemps possible sans compromettre les fonctionnalités du réseau.

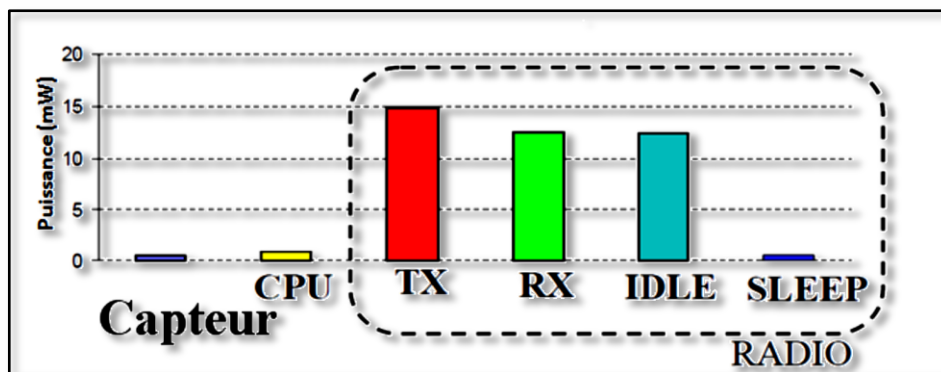


Figure 1.7 : Principale source de consommation d'énergie d'un capteur avec une radio CC2500 et un microcontrôleur MSP430 [21]

Nous ne traitons pas les défis de collaboration et de coordination entre les nœuds dans les réseaux AHWSN. Nous nous concentrerons sur les défis d'énergie, d'hétérogénéité, de la dynamique, d'auto-organisation et de routage dans les AHWSN.

Notre objectif est d'étudier la consommation d'énergie dans le routage de l'information et de proposer des algorithmes permettant l'échange des données relatives à l'énergie résiduelle des nœuds afin qu'elle soit l'une des métriques du routage permettant d'optimiser davantage la durée de vie du réseau.

6. Routage de l'information dans les réseaux AHWSN

La fonction de routage est l'une des plus importantes dans les réseaux de communication, que ce soit dans les réseaux filaires ou dans les réseaux sans fil. Le routage sert à faire communiquer des nœuds distants. C'est un mécanisme qui permet l'établissement et le maintien de routes optimales entre les nœuds d'un réseau. Suivant les besoins et la finalité du réseau, une route optimale est choisie selon différents critères. Il existe des protocoles de routage classiques qui s'appuient sur la longueur de la route afin de choisir la meilleure d'entre elles. D'autres protocoles prennent en considération d'autres critères comme la qualité de service. On retrouve aussi des protocoles de routage qui s'appuient sur des considérations de fiabilité et de sécurité afin de choisir les nœuds qui vont composer une route.

Les protocoles de routage destinés aux réseaux filaires n'ont pas besoin de gérer les contraintes liées à la mobilité. Ces protocoles ne se focalisent pas non plus sur la minimisation des communications sachant que les réseaux filaires sont réputés pour être des réseaux à haut débit. Un autre point très important est le fait que dans les réseaux filaires, le routage est réalisé par des nœuds de confiance appelés routeurs. Ces caractéristiques changent radicalement dès lorsqu'il s'agit des réseaux sans fil ad hoc. En effet, la mobilité qui est une caractéristique de base des réseaux ad hoc, les contraintes liées à la limitation de ressources (bande passante, mémoire, processeur, contraintes d'énergie) et l'absence d'une entité de confiance, ont contraint les chercheurs à concevoir des protocoles de routage spécifiques aux réseaux sans fil ad hoc.

Avant de détailler le fonctionnement des différents protocoles de routage dans les réseaux ad hoc, nous allons tout d'abord présenter leurs différentes catégories. Il existe deux façons de classifier les protocoles de routage dans les réseaux ad hoc. La première classification se base sur la manière dont les informations de routage sont structurées et échangées dans le réseau. Cette classification donne lieu à deux classes de méthodes :

- la méthode du vecteur de distance
- la méthode d'état des liens

Dans la méthode du vecteur de distance, chaque nœud du réseau maintient une table de routage contenant les distances vers tous les nœuds du réseau. À chaque fois qu'un nœud reçoit une mise à jour de routage (table de routage) de la part d'un nœud voisin, il l'examine afin de déduire des routes vers de nouvelles destinations ou bien pour mettre à jour des routes déjà existantes dans sa table de routage. Une fois que ses propres informations de routage sont mises à jour, il les envoie à ses voisins, qui à leur tour font la même chose et ainsi de suite. Un exemple d'un protocole de routage appartenant à cette catégorie est le protocole DSDV. Un inconvénient des protocoles basés sur ce principe est qu'ils convergent très lentement.

Les protocoles basés sur le routage par état de liens essaient de corriger les limitations des protocoles du vecteur de distance. Le fonctionnement de ces protocoles peut être résumé ainsi : chaque nœud du réseau découvre son voisinage (les identités des nœuds à un saut) en diffusant périodiquement des messages appelés messages hello que tous ses voisins potentiels peuvent intercepter; une fois que le nœud a découvert son voisinage, il transmet aux nœuds du réseau un message contenant la liste de tous ses voisins ainsi que le coût nécessaire pour atteindre chacun d'entre eux; ces messages sont enfin utilisés par les nœuds afin d'avoir une vue globale de la topologie du réseau. Le protocole OLSR est l'exemple type des protocoles utilisant ce principe. Cette approche permet une convergence plus rapide que par la méthode du vecteur de distance. Une deuxième méthode de classification des protocoles de routage peut être obtenue en se basant sur le déclenchement des mises à jour des informations de routage. De cette classification il ressort deux approches, l'approche réactive et l'approche proactive.

6.1 Protocoles proactifs

La particularité de l'approche proactive est que les routes sont construites de façon continue même si elles ne sont pas utilisées dans l'immédiat. Nous allons détailler ici deux exemples de protocole de cette catégorie à savoir OLSR et DSDV.

DSDV [22] : Le protocole DSDV (Destination Sequenced Distance Vector Protocol) est une adaptation du protocole RIP (Routing Information Protocol) aux réseaux ad hoc.

Les concepteurs de ce protocole ont rajouté un nouvel attribut (le numéro de séquence) aux entrées de la table de routage qui permet à chaque nœud de distinguer entre les anciennes et nouvelles routes et ainsi éviter la formation des boucles de

routage. Dans DSDV, la structure d'une ligne de la table de routage est définie comme suit : <Destination, Nœud suivant, Nombre de sauts, Numéro de séquence>. Afin de maintenir la cohérence des tables de routage, chaque nœud diffuse périodiquement ou lors d'un changement de topologie des paquets de mise à jour (tables de routage) à ses voisins. À la réception par un nœud d'un paquet de mise à jour, il compare cette information à celles qui existent déjà dans sa table de routage et transmet à son tour un paquet de mise à jour à ses voisins. Si plusieurs paquets de mise à jour sont reçus par un nœud avec des numéros de séquence différents pour la même destination, alors la route avec le plus grand numéro de séquence est sélectionnée. Par contre, si ces paquets ont le même numéro de séquence, alors c'est la route avec la distance (nombre de sauts) la plus courte qui est choisie. En plus d'être lent à converger, le protocole DSDV génère un surcoût considérable en termes de communication ($O(n^2)$ pour un réseau de n nœuds), c'est pourquoi il n'est considéré viable que dans des environnements très particuliers (réseaux relativement statiques et de petite taille).

OLSR [23]: OLSR (Optimized link State Routing Protocol for Ad-Hoc Networks).

Nous allons juste passer en revue le mécanisme de fonctionnement de ce protocole, car il sera étudié en détail lors des simulations dans les chapitres 3 et 4. OLSR est un protocole de routage de nature proactive basé sur un algorithme d'état de liens. Il emploie des échanges périodiques de messages pour maintenir les informations sur la topologie du réseau. C'est une optimisation de la méthode d'état des liens, du fait qu'il utilise des messages compacts et qu'il limite le nombre de retransmissions lors de la diffusion des paquets de contrôle. À cet effet, il se sert de relais multipoint afin de rendre la diffusion des messages de contrôle plus précise et économique. Les relais d'un nœud N sont un sous-ensemble de ses voisins à un saut. Cet ensemble, qui est appelé MPRs du nœud N et noté $MPR(N)$, est choisi de telle façon que les liens avec ces voisins soient bidirectionnels et que tous les nœuds à deux sauts de N soient atteints. Les nœuds n'appartenant pas à l'ensemble MPR du nœud N peuvent lire et traiter les paquets reçus du nœud N , mais ne doivent pas les retransmettre. La figure 1.8 illustre le mécanisme d'optimisation des relais multipoint. La retransmission par les nœuds C et E est suffisante pour assurer la diffusion d'un paquet en provenance de la station N . L'ensemble des stations C et E forme un ensemble de relais multipoint du nœud N . Une diffusion issue du nœud N va donc utiliser uniquement trois transmissions.

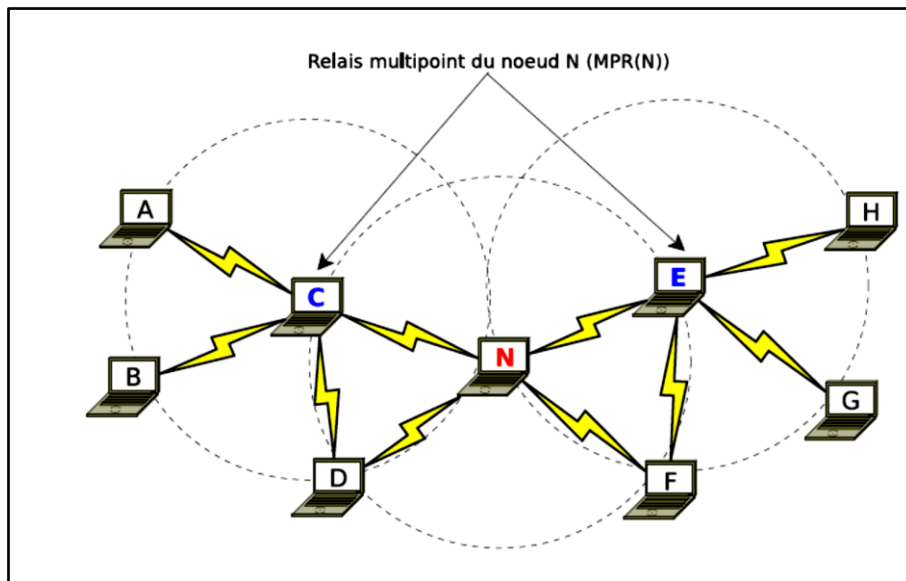


Figure 1.8 : Optimisation des relais multipoints (MPRs)

6.2 Protocoles réactifs

Les protocoles de routage appartenant à cette catégorie, créent et maintiennent les routes selon leurs besoins. Lorsque le réseau a besoin d'une route, une procédure de découverte globale de routes est lancée, et ce, dans le but d'obtenir une information spécifique. Dans ce qui suit, nous allons décrire les protocoles les plus importants de cette classe :

DSR [24] : Le protocole DSR (Routage à Source Dynamique), est basé sur l'utilisation de la technique "routage source". Dans cette technique, la source des données détermine la séquence complète des nœuds à travers lesquels les paquets de données seront envoyés. Un nœud initiateur de l'opération de découverte de routes diffuse un paquet de requête de route dans l'ensemble du réseau. Si l'opération de découverte est réussie, l'initiateur reçoit un paquet réponse de route qui liste la séquence de nœuds à travers lesquels la destination peut être atteinte. Le paquet réponse de route contient donc un champ contenant la séquence des nœuds visités durant la propagation de la requête dans le réseau. Afin d'assurer la validité des chemins utilisés, le protocole DSR exécute une procédure de maintien de routes :

- Quand un nœud détecte un problème dans la transmission (rupture de liens), un message erreur de route est envoyé à l'émetteur original du paquet ;
- Le message d'erreur contient l'adresse du nœud qui a détecté l'erreur et celle du nœud qui le suit dans le chemin ;

- Lors de la réception du paquet erreur de route par le nœud source, le nœud concerné par l'erreur est supprimé du chemin sauvegardé, et tous les chemins qui contiennent ce nœud sont tronqués à ce niveau-là. Par la suite, une nouvelle opération de découverte de routes vers la destination est initiée par l'émetteur.

AODV [25] : Le protocole AODV s'inspire des protocoles DSDV et DSR. Il réduit le nombre de messages diffusés en créant les routes quand cela est nécessaire, contrairement au protocole DSDV qui maintient la totalité des routes. Ceci a pour effet de limiter la répercussion des modifications topologiques aux seules routes en cours d'utilisation.

AODV utilise le principe des numéros de séquence afin de maintenir la cohérence des informations de routage et ainsi utiliser les routes les plus récentes car, à cause de la mobilité des nœuds dans le réseau, les routes changent fréquemment, ce qui rend les routes maintenues par certains nœuds invalides.

De la même manière que dans DSR, AODV utilise une requête de demande de route dans le but de créer un chemin vers une destination donnée. Cependant, AODV maintient les chemins d'une façon distribuée en gérant une table de routage au niveau de chaque nœud appartenant au chemin recherché. Un nœud diffuse une requête de route *RREQ* vers un nœud destination si :

- La destination n'est pas connue au préalable, ou
- La durée de vie du chemin existant vers la destination a expiré ou
- Le chemin est devenu défaillant.

Les nœuds qui reçoivent ces paquets les diffusent à leur tour jusqu'à atteindre la destination ou au moins un nœud qui possède une information de routage récente vers la destination recherchée. Les nœuds situés sur le parcours de la requête conservent, dans leur cache, l'adresse du nœud qui leur a relayé la requête. L'adresse de ce nœud fournit l'adresse du saut suivant vers le nœud source. Cette information est utilisée lors du retour de la réponse de demande de route *RREP* pour permettre d'aiguiller cette réponse jusqu'au nœud source.

Le champ *numéro de séquence destination* du paquet *RREQ*, contient la dernière valeur connue du numéro de séquence associé au nœud destination qui est recopiée de la table de routage. Si le numéro de séquence n'est pas connu, la valeur nulle sera prise par défaut. Le numéro de séquence source du paquet *RREQ* contient, quant à lui, la valeur *du numéro de séquence du nœud source*.

Afin de maintenir l'état correct des routes, une transmission périodique d'un message *hello* est effectuée. Si, par exemple, trois messages *hello* consécutifs ne sont pas reçus à partir d'un nœud voisin, le lien en question est considéré comme étant défaillant et un message d'erreur *RERR* est envoyé à chaque source concernée par ce lien afin de lui permettre de mettre à jour ses informations de routage en relançant de nouvelles procédures de recherche de routes.

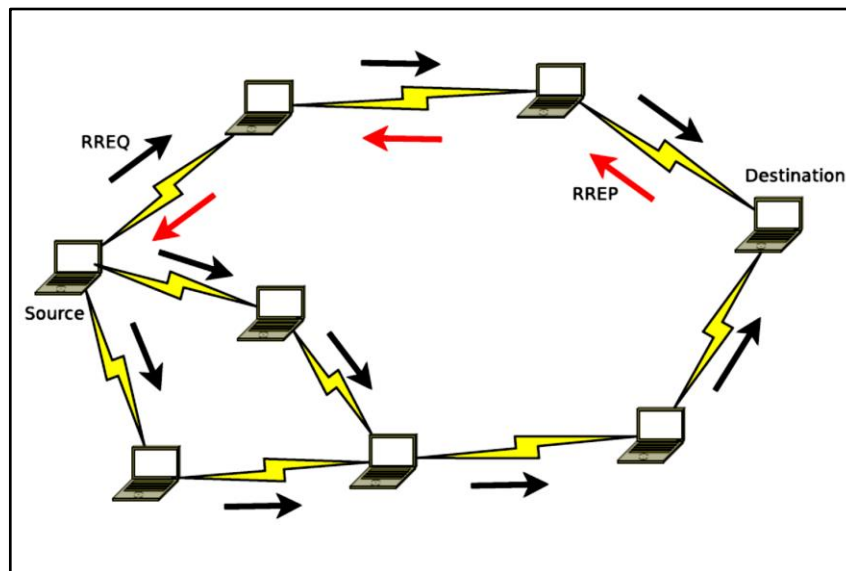


Figure 1.9 – Procédure de découverte de route du protocole AODV

6.3 Protocoles réactifs Vs Protocoles proactifs

Les protocoles proactifs possèdent de bonnes aptitudes en termes de temps de réponse, car quand un nœud souhaite communiquer avec un autre, il trouve immédiatement dans sa table de routage la route adéquate pour atteindre ce nœud. Cependant, un surcoût significatif est engendré par les échanges périodiques de messages de contrôle.

Les protocoles réactifs résolvent plus ou moins le défaut des protocoles proactifs tout en augmentant le temps de réponse. Le surcoût engendré en utilisant l'approche réactive est moindre dans certaines configurations réseau. Néanmoins, il peut demeurer élevé dans d'autres. De manière générale, les protocoles réactifs et proactifs présentent des performances différentes selon les caractéristiques du réseau. Dans le cas d'un réseau dense par exemple et/ou lorsque l'échange des données est intense, le choix d'un protocole proactif s'avère plus judicieux, car un protocole réactif entraîne la diffusion excessive de messages de demande de routes qui risquent de saturer le réseau. En

revanche, dans une configuration opposée, à savoir un réseau à densité faible et/ou à faible trafic, choisir un protocole réactif est plus intéressant, car il ne surchargera pas inutilement le réseau par des flux continuels d'informations de routage entre les nœuds.

6.4 Protocoles hybrides

Afin de tirer profit des avantages des protocoles réactifs et proactifs, des protocoles qui mêlent généralement les deux modes (fonctionnant dans l'un ou dans l'autre mode) suivant des conditions prédéfinies, ont été proposés. Dans ce type de protocoles, on utilise une reconnaissance locale de la topologie réseau jusqu'à un nombre relativement petit de sauts, par un échange périodique de trames de contrôle, autrement dit par une technique proactive. Les routes vers des nœuds plus lointains sont obtenues par un schéma réactif, c'est-à-dire par l'utilisation de paquets de demande de routes qui sont dans la majorité des cas diffusés dans tout le réseau. Parmi les protocoles hybrides, nous nous intéressons particulièrement à **ZRP (Zone Routing Protocol)**[26].

ZRP a été introduit en 1997 par Haas et Pearlman. ZRP définit pour chaque nœud une zone de routage (zone radius), qui inclut tous les nœuds dont la distance minimale (en nombre de sauts) à ce nœud est « d ». Les nœuds qui sont exactement à distance « d » sont appelés nœuds périphériques. Pour trouver une route vers des nœuds situés à une distance supérieure à « d », ZRP utilise un système réactif, qui envoie une requête à tous les nœuds périphériques. Pour cela, ZRP met en œuvre deux types de fonctionnement : IARP (IntrAzone Routing Protocol) et IERP (IntErzone Routing Protocol).

Basé sur un protocole à vecteur de distance, IARP permet, en utilisant une technique proactive, de trouver toutes les routes jusqu'à une distance « d ». IERP quant à lui, permet d'établir les routes vers les nœuds à plus de d sauts d'une façon réactive.

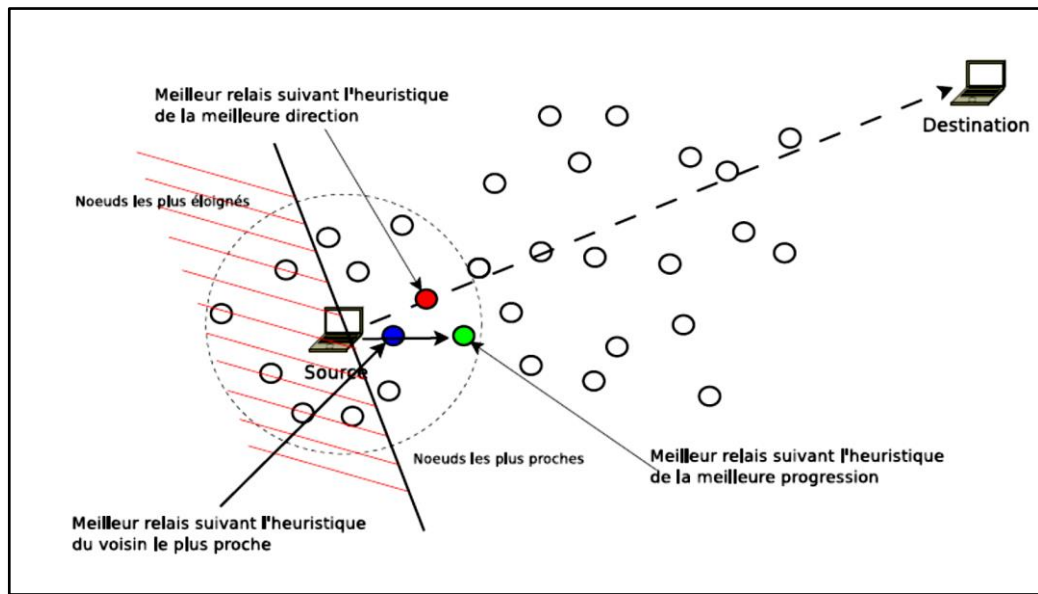


Figure 1.10 – Heuristiques dans les protocoles hybrides

Le processus de recherche de route fonctionne de la façon suivante :

- Si une route est connue, cela signifie que la destination est à moins de « d » sauts. Cette route est la route retournée par le protocole ;
- Si aucune route n'est connue, cela signifie que le nœud est situé à une distance supérieure à « d ». Dans ce cas, le nœud envoie une requête par IERP à tous les nœuds périphériques ;
- Si un nœud périphérique a connaissance d'une route disponible, il renvoie une réponse. Dans le cas contraire, le protocole se poursuit récursivement jusqu'à l'obtention d'une route.

Le tableau ci-après, récapitule l'ensemble des protocoles de routage utilisés dans les réseaux Manets selon leurs spécificités et domaine d'utilisation.

| Protocole | Type | Catégorie | Implication des nœuds | Caractéristique du réseau | Normalisation IETF |
|-----------|-------------|------------------------|-----------------------|-------------------------------------|--------------------|
| DSDV | Proactif | Orienté destination | Uniforme | Faible mobilité faible densité | -- |
| OLSR | Proactif | Orienté Topologie | Non-Uniforme | Trafic de données important | RFC |
| TBRPF | Proactif | Orienté Topologie | Non-Uniforme | Trafic de données important | RFC |
| TORA | Réactif | Orienté destination | Uniforme | Forte mobilité | Draft expiré |
| ABR | Réactif | Orienté destination | Uniforme | Forte mobilité | -- |
| CBRP | Réactif | Hiérarchique de groupe | Non-Uniforme | Faible mobilité | Draft expiré |
| AODV | Réactif | Orienté destination | Uniforme | Trafic de données faible | RFC |
| DSR | Réactif | Orienté Topologie | Uniforme | Trafic de données faible | RFC |
| SHARP | Hybride | Orienté destination | Uniforme | Zone de trafic de données important | -- |
| ZRP | Hybride | -- | Non-Uniforme | -- | Draft expiré |
| DREAM | G. Proactif | Orienté Topologie | Uniforme | Forte mobilité faible densité | -- |
| ZHLS | G. Hybride | Hiérarchique | Non-Uniforme | -- | -- |
| LAR | G. Réactif | Orienté Topologie | Uniforme | Faible mobilité | -- |

Tableau 1.1 : Propriétés des protocoles de routage [27]

6.5 Routage dans les réseaux WSN

La figure suivante résume les principaux protocoles de routage dans les réseaux de capteurs (WSN) [28]

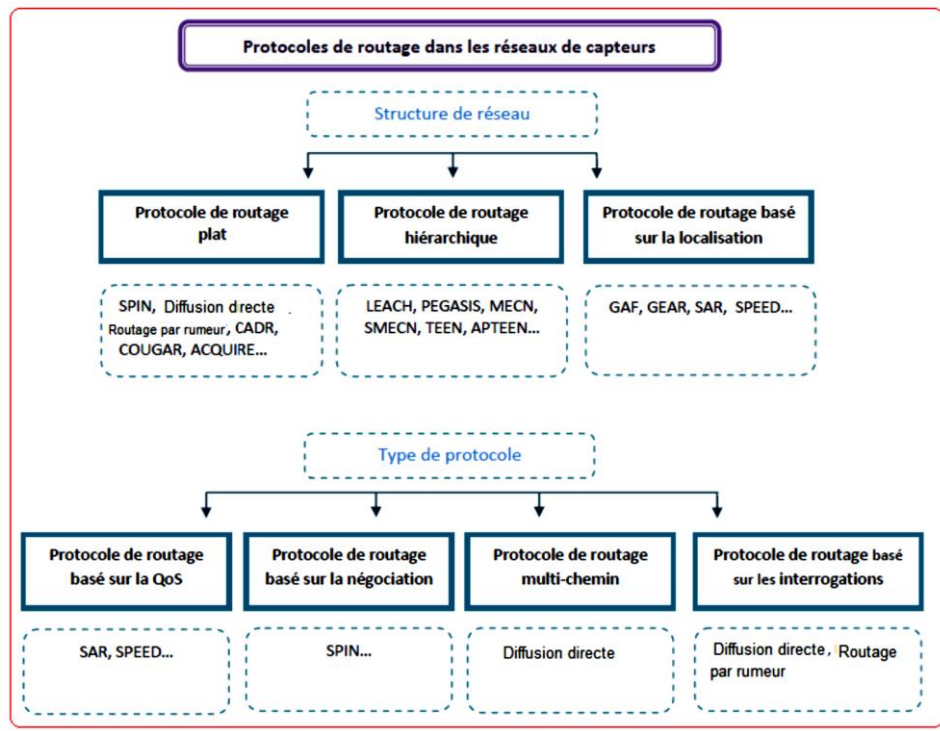


Figure 1.11 : Principaux protocoles de routages dans les WSN

6.5.1 Les Protocoles hiérarchiques

L'objectif principal du routage hiérarchique [29, 30] est de maintenir efficacement la consommation d'énergie des nœuds de capteurs en les impliquant dans la communication multi-hop au sein d'un cluster et en effectuant l'agrégation et la fusion des données afin de diminuer le nombre de messages transmis à la destination. La formation de clusters est généralement fondée sur la réserve d'énergie des capteurs et sur les capteurs qui sont à proximité de cluster-head (voir figure 1.11). LEACH (Low Energy Adaptive Clustering Hierarchical) [28] est l'une de premières approches de routage pour les réseaux de capteurs. L'idée proposée par LEACH a été une inspiration pour de nombreux protocoles de routage hiérarchique, bien que certains protocoles aient été développés de manière indépendante.

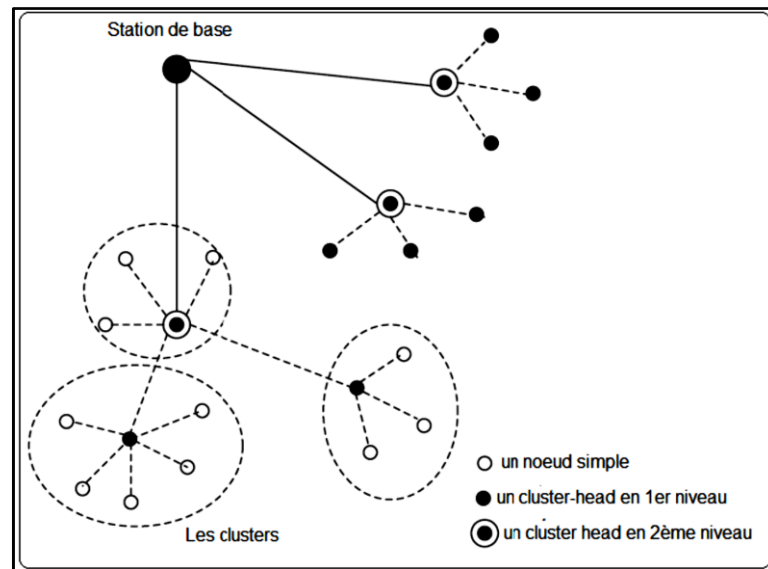


Figure 1.12 : protocoles de routages WSN hiérarchiques

«**LEACH** » [28-29-31] LEACH est l'un des algorithmes de routage hiérarchique le plus populaire pour les réseaux de capteurs. L'idée est de former des clusters de capteurs basés sur les zones où il y a un fort signal reçu, puis utiliser des clusters-heads locaux comme passerelle pour atteindre la destination. Cela permet d'économiser de l'énergie car les transmissions ne sont effectuées que par les cluster-head plutôt que par tous les nœuds capteurs.

«**PEGASIS & Hierarchical-PEGASIS**» **Power-Efficient Gathering in Sensor Information Systems (PEGASIS)** [29] est une version améliorée du protocole LEACH. PEGASIS forme des chaînes plutôt que des clusters afin que chaque nœud transmette et reçoive uniquement des données d'un voisin. Un seul nœud est sélectionné à partir de cette chaîne pour transmettre à la station de base. L'idée de PEGASIS est qu'il utilise tous les nœuds pour transmettre ou recevoir des données avec ses plus proches voisins. Il déplace les données reçues de nœud à nœud, puis les données seront agrégées jusqu'à ce qu'elles atteignent tous la station de base. Donc, chaque nœud du réseau est tour à tour un chef de file de la chaîne, ainsi responsable pour transmettre l'ensemble des données recueillies et fusionnées par la chaîne de nœuds au niveau de la station de base.

«**TEEN et APTEEN**» Les protocoles **Threshold sensitive Energy Efficient sensor Network protocol (TEEN)** et **Adaptive Threshold sensitive Energy Efficient sensor Network protocol (APTEEN)** [32-33] conviennent pour les applications critiques. Dans les deux protocoles, le facteur clé est la valeur de l'attribut mesuré. La caractéristique

supplémentaire d'APTEEN est la capacité de changer la périodicité et les paramètres de TEEN en fonction des besoins des utilisateurs et des applications.

TEEN est conçu pour être sensible à des changements soudains des attributs tels que la température. La réactivité est importante pour les applications critiques dont le réseau fonctionne dans un mode réactif. L'architecture du réseau de capteurs est basée sur un groupement hiérarchique où les nœuds forment des clusters et ce processus va se répéter jusqu'à ce que la station de base soit atteinte.

APTEEN est une extension de TEEN qui fait à la fois la collection des captures périodiques de données et qui réagit aux événements critiques. Quand la station de base forme des clusters, les clusters-head diffusent les attributs, les valeurs des seuils, ainsi que le calendrier de transmission à tous les nœuds. Le cluster-head effectue également l'agrégation de données afin d'économiser l'énergie.

6.5.2 Les protocoles de routage basés sur la localisation

Les protocoles de routage basés sur la localisation [29] utilisent les informations d'emplacement pour guider la découverte de routage et la transmission des données. Ils permettent la transmission directionnelle de l'information en évitant l'inondation d'information dans l'ensemble du réseau. Par conséquent, le coût de contrôle de l'algorithme est réduit et le routage est optimisé. De plus, avec la topologie réseau basée sur des informations de localisation de nœuds, la gestion du réseau devient simple. L'inconvénient de ces protocoles de routage est que chaque nœud doit connaître les emplacements des autres nœuds.

« MECN » [34] **Minimum Energy Communication Network** est un protocole de routage qui cherche à établir et à entretenir une énergie minimale pour les réseaux sans fil en utilisant des GPS de faible puissance. MECN utilise une station de base comme destination de l'information, ce qui est toujours le cas pour les réseaux de capteurs. MECN identifie une région de relais pour chaque nœud. La région de relais se compose de nœuds dans une zone périphérique où la transmission à travers ces nœuds est plus économe en énergie que la transmission directe. L'idée principale de MECN est de trouver un sous-réseau qui a moins de nœuds et qui nécessite moins d'énergie pour la transmission entre deux nœuds quelconques. Cela est effectué en utilisant une recherche localisée pour chaque nœud en prenant en considération sa région de relais.

« GAF » [35] (**Geographic Adaptive Fidelity**) est un protocole de routage basé sur la localisation des nœuds. Il est conçu principalement pour les réseaux mobiles ad hoc, mais peut être applicable aux réseaux de capteurs. La localisation des nœuds dans GAF pourrait être fournie à l'aide d'un GPS ou d'autres techniques de localisation. Il consiste à former des grilles virtuelles de la zone concernée en partitionnant cette zone où les nœuds sont déployés en de petites zones telles que, pour deux grilles adjacentes G_x et G_y , tous les nœuds de G_x peuvent communiquer avec tous les nœuds G_y . Ainsi, ce système de partitionnement GAF assure la fidélité du routage car il existe au moins un chemin entre un nœud et la station de base.

GAF peut augmenter considérablement la durée de vie du réseau. En effet, un seul nœud dans chaque grille reste à l'état actif en faisant passer les autres nœuds de la grille à l'état de sommeil pour une certaine période de temps tout en assurant la fidélité du routage. Cependant, dans certains environnements où les nœuds sont fortement mobiles, la fidélité du routage pourrait être réduite si un nœud actif quitte la grille. Ainsi, le nombre de données perdues sera important.

«GEAR»[36] (**Geographic and Energy Aware Routing**)

Il consiste à utiliser l'information géographique lors de la diffusion des requêtes aux régions cibles car les requêtes contiennent souvent des données géographiques. L'idée est de restreindre le nombre de données dans la diffusion dirigée en prenant en considération uniquement une certaine région, plutôt que d'envoyer les données à l'ensemble du réseau.

Avec le protocole GEAR, chaque nœud maintient le coût pour atteindre la destination en passant par ses voisins. Ce coût est divisé en deux parties : un coût estimé et un coût d'apprentissage. Le coût estimé est une combinaison de l'énergie résiduelle et de la distance jusqu'à destination. Le coût d'apprentissage est un raffinement du coût estimé qu'un nœud dépense pour le routage autour des trous dans le réseau. Un trou se forme quand un nœud n'a pas de voisin proche par lequel il peut atteindre la région cible. S'il n'y a pas de trous, le coût estimé est égal au coût d'apprentissage. Le coût d'apprentissage se propage d'un saut à chaque fois qu'un paquet atteint la destination.

6.5.3 Les protocoles de routage 'data-centric' [37]

Dans de nombreuses applications de réseaux de capteurs, vu le nombre élevé de nœuds déployés, il n'est pas possible d'attribuer des identificateurs globaux à chaque nœud. Cette absence d'identification globale avec le déploiement aléatoire de nœuds de

capteurs font qu'il est difficile de sélectionner un ensemble spécifique de nœuds de capteurs à interroger. Par conséquent, les données sont généralement transmises de chaque nœud de capteurs dans la région de déploiement avec une redondance importante. Cette réflexion a conduit au routage data-centric qui est différent du routage traditionnel où les routes sont créées entre les nœuds adressables gérée dans la couche réseau. Le destinataire envoie des requêtes à certaines régions et attend à recevoir des données provenant des capteurs situés dans les régions sélectionnées. Comme les données sont demandées à travers des requêtes, le nommage est nécessaire pour préciser les propriétés des données.

Comme la montre l'exemple d'une approche data-centric dans la figure 1.13, les données provenant des deux sources sont agrégées au nœud B. Ensuite, la donnée combinée (1+2) est envoyée de B vers la destination.

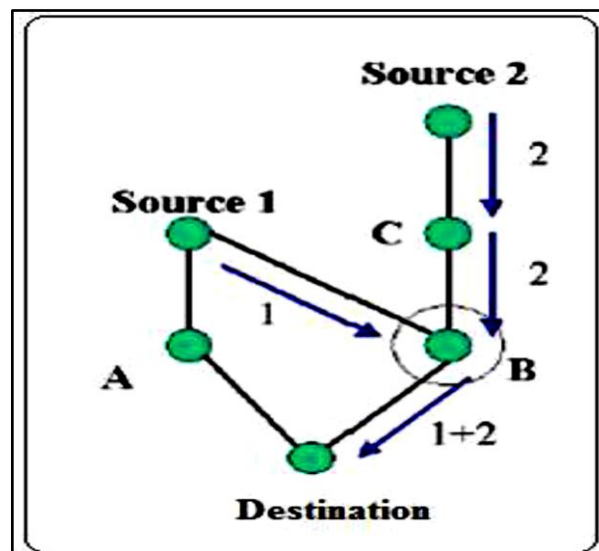


Figure 1.13 : Le routage data-centric

« SPIN » [38] : Un réseau de capteurs sans fil se compose de plusieurs capteurs qui sont déployés dans différentes régions. L'accès aux données d'un événement particulier pour une région ou une zone spécifique peut faire une grande différence. Des mesures peuvent être prises pour l'obtention de données à partir d'un endroit ciblé. Les données sont recueillies auprès de tous les capteurs et transmises de manière redondante sur le réseau, ce qui entraîne une utilisation inefficace de l'énergie. Afin de résoudre ces types de problèmes, les systèmes de routage data-centric ont évolué : la destination envoie des requêtes pour les capteurs du réseau dans un endroit choisi. Les attributs sont utilisés pour demander des données provenant des capteurs.

SPIN (Sensor Protocols for Information via Negotiation) est le premier protocole data-centric qui a été conçu pour les réseaux de capteurs sans fil. Il présente de nombreuses similitudes par rapport à la diffusion dirigée. Il est efficace dans la réduction des données redondantes et économise l'énergie.

La diffusion est le processus de collecte des observations de l'ensemble des capteurs individuel qui sont déployées dans le réseau et où tous les capteurs sont traités comme des nœuds destination. Les tâches confiées à ces capteurs sont de recueillir le point de vue complet de l'environnement sous la forme de données et de renforcer une structure de réseau avec une tolérance aux fautes. La consommation d'énergie durant les calculs et les communications doit être contrôlée afin de prolonger la durée de vie des capteurs au sein du réseau.

6.5.4 La diffusion dirigée [39]

La diffusion dirigée est un protocole important dans le routage data-centric des réseaux de capteurs. L'idée vise à diffuser des données aux nœuds en utilisant un schéma de nommage pour les données. La raison principale derrière l'utilisation d'un tel système est de se débarrasser des opérations inutiles de routage de couche réseau afin d'économiser l'énergie.

La diffusion dirigée suggère l'utilisation de paires attribut-valeur pour les données et les requêtes des capteurs. Afin de créer une requête, un nœud est défini à l'aide d'une liste de paires attribut-valeur comme le nom des objets, l'intervalle, la durée, la zone géographique, etc. Un paquet est diffusé par ce nœud vers la destination à travers ses voisins. Chaque nœud qui reçoit les paquets peut les stocker pour une utilisation ultérieure. Les paquets stockés sont ensuite utilisés pour comparer les données reçues. La requête contient aussi plusieurs champs de gradient. Un gradient est un lien réponse avec un voisin dont le paquet a été reçu et qui est caractérisé par le débit, la durée et la date d'expiration de données. Ainsi, en utilisant les intérêts et les gradients, les routes sont établies entre la destination et les sources. Plusieurs routes peuvent être établies de telle sorte que l'une d'elle est choisie par renforcement. La destination renvoie le message d'intérêt initial à travers la route choisie. Un intervalle plus petit renforce donc le nœud source sur ce chemin pour envoyer des données plus fréquemment.

6.5.5 Le protocole de routage par rumeur

[40] Le routage par rumeur est principalement destiné pour des applications où le routage géographique n'est pas faisable. En général, la méthode (diffusion dirigée) utilise

l'inondation pour envoyer la requête à l'ensemble du réseau où il n'y a pas de critère géographique pour diffuser les tâches. Toutefois, dans certains cas, peu de données sont demandées par les nœuds, donc l'utilisation d'inondation est inutile.

L'idée clé de cette méthode est de trouver les routes pour les requêtes vers les nœuds qui ont observé un événement particulier, plutôt que d'inonder tout le réseau pour récupérer des informations sur les événements survenus. Afin de diffuser un événement sur le réseau, l'algorithme de routage par rumeur emploie des paquets appelés agents. Quand un nœud détecte un événement, il ajoute cet événement à sa table locale, appelée table d'événements et génère un agent. Cet agent parcourt le réseau afin de propager des informations sur des événements locaux pour les nœuds distants. Quand un nœud génère une requête pour un événement, les nœuds qui connaissent le chemin, répondent à la requête en inspectant leur table événement. Par conséquent, il n'est pas nécessaire d'inonder tout le réseau, ce qui réduit le coût de communication. D'autre part, ce routage n'utilise qu'un seul chemin entre la source et la destination au lieu de la diffusion dirigée où les données peuvent être acheminées par des routes multiples.

Le tableau 1.2 représente un comparatif de quelques protocoles de routage dans les réseaux WSN.

| Protocole | Type | Mobilité | Basé sur la négociation | Multi chemin | L'utilisation d'énergie |
|-----------------------|--------------|----------------------|-------------------------|--------------|-------------------------|
| LEACH | Hiérarchique | Station de base fixe | Non | Non | Max |
| PEGASIS | Hiérarchique | Station de base fixe | Non | Non | Max |
| H PEGASIS | Hiérarchique | Station de base fixe | Non | Non | Max |
| TEEN APTEEN | Hiérarchique | Station de base fixe | Non | Non | Max |
| MECN | Hiérarchique | Non | Non | Non | Min |
| GAF | Géographique | Limitée | Non | Non | Limitée |
| GEAR | Géographique | Limitée | Non | Non | Limitée |
| SPIN | Plat | possible | Oui | Oui | Limitée |
| La diffusion dirigée | Plat | possible | Oui | Oui | Limitée |
| Le routage par rumeur | Plat | Très limitée | Non | Non | Min |

Tableau 1.2 : Comparaison des protocoles de routage des WSN

7. Conclusion

Dans cette partie nous avons évoqué la notion des réseaux AHWSN, leurs domaines d'application ainsi que les contraintes liées à la conception et au déploiement de tels réseaux. Nous avons mis l'accent sur la contrainte d'énergie qui demeure l'axe principal de notre recherche dans notre thèse.

Une attention particulière a été attribuée aux protocoles de routage et leurs classifications dans les réseaux AHWSN afin que nous puissions introduire dans ce qui suit la problématique réelle liée principalement à la qualité de service QoS ainsi que l'optimisation de tels réseaux qui demeurent un souci majeur des chercheurs dans ce domaine.

Le chapitre suivant quant à lui, évoquera les différents paramètres liés à la qualité de service des réseaux AHWSN, ainsi que les algorithmes implémentés pour pallier à la contrainte d'énergie des nœuds.

AHWSN : Qualité de service (QoS) et conservation d'énergie

| | |
|--|----|
| 1. Introduction | 41 |
| 2. Qualité de service à différents échelles dans les AHWSN..... | 42 |
| 2.1 Qualité de service dans les AHWSN à l'échelle interne : Différenciation de service au niveau de la couche MAC | 43 |
| 2.1.1 Description de la couche MAC IEEE 802.11 | 44 |
| 2.1.2 Différenciation de service basée sur la fonction DCF du protocole 802.11 | 44 |
| 2.1.3 IEEE 802.11e | 45 |
| 2.2 La Qualité de Service dans les réseaux AHWSN à l'échelle locale | 46 |
| 2.2.1 CEDAR (Core-Extraction Distributed Ad hoc Routing Algorithm) | 47 |
| 2.2.2 Autres protocoles de routage avec QoS..... | 48 |
| 2.2.3 Protocole de réservation de ressources : INSIGNIA | 49 |
| 2.3 La Qualité de Service dans les réseaux AHWSN à l'échelle globale..... | 50 |
| 3. Modèles de qualité de service dans les réseaux AD-HOC | 51 |
| 3.1 Flexible quality of service model for MANETs (FQMM)..... | 51 |
| 3.2 Service differentiation in wireless ad hoc networks (SWAN) | 52 |
| 3.3 Modèle iMAQ..... | 53 |
| 4. Qualité de service QoS : cas des WSN | 54 |
| 4.1 Qualité de service liée à l'application | 55 |
| 4.2 Qualité de service liée au réseau | 55 |
| 4.2.1 Modèle orienté-événements | 55 |
| 4.2.2 Modèle orienté-requêtes..... | 56 |
| 4.2.3 Modèle à flux continu..... | 57 |
| 5. Techniques de conservation d'énergie dans les réseaux AHWSN | 57 |
| 5.1 Consommation d'énergie d'un nœud dans un réseau AHWSN..... | 58 |
| 5.1.1 Formes de dissipation d'énergie | 58 |
| 5.1.2 Sources de surconsommation d'énergie..... | 59 |

| | | |
|-------|--|----|
| 5.1.3 | Consommation d'énergie due au routage..... | 61 |
| 5.2 | Conservation d'énergie..... | 62 |
| 5.2.1 | Techniques du Duty-cycling..... | 63 |
| 5.2.2 | Principaux Algorithmes de routage utilisés pour la conservation d'énergie..... | 69 |
| 5.2.3 | Conservation d'énergie au niveau transport..... | 71 |
| 6. | Conclusion..... | 73 |

1. Introduction

Dans le chapitre précédent, nous avons étalé un état de l'art sur les réseaux AHWSN ainsi que les différentes contraintes liées à leur déploiement. Ces derniers ont incité les chercheurs à étudier et développer plusieurs mécanismes permettant d'en pallier et d'améliorer les différents services apportés par ce type de réseaux. Les travaux menés ont touché les différentes couches de la pile protocolaire de ces réseaux.

Aussi, nous avons évoqué l'aspect primordial du routage de l'information à travers les réseaux AHWSN, qui demeure complètement différent par rapport à celui des réseaux filaires, tout en tenant compte des contraintes de mobilité causée par le déplacement permanent des mobiles constituant le réseau, créant ainsi un changement continue de la topologie du réseau. D'autres contraintes liées aux caractéristiques intrinsèques des mobiles (batterie limitée, capacité de traitement réduite...) ont été abordées.

Tous ses aspects devront être pris en compte lors du développement des mécanismes et algorithmes de routage de l'information dans ces réseaux.

Dans cette partie nous allons présenter les principaux travaux de recherche traitant la qualité de service dans le contexte particulier des réseaux AHWSN.

Dans les réseaux de télécommunication, l'objectif de la qualité de service est d'atteindre un meilleur comportement de la communication, pour que le contenu de cette dernière soit correctement acheminé, et que les ressources du réseau soient utilisées d'une façon optimale.

La qualité de service QoS (Quality of Service) peut être définie comme le degré de satisfaction d'un utilisateur des services fournis par un système de communication. La

La QoS [41] est définie comme la capacité d'un élément du réseau (ex: routeur, nœud ou une application) de fournir un niveau de garantie pour un acheminement des données.

Le RFC 2386 [42] caractérise la QoS comme un ensemble de besoins à assurer par le réseau pour le transport d'un trafic d'une source à une destination. Ces besoins peuvent être traduits en un ensemble d'attributs pré-spécifiés et mesurables en terme de:

- Délai de bout en bout,
- Variance de délai (gigue),
- Bande passante,

- Pertes de paquets.

Suivant le type de l'application, les besoins de QoS sont différents. Par exemple, pour les applications temps réel, comme la voix et la vidéo, le délai de bout en bout d'un paquet doit être limité, autrement le paquet est inutile. Les applications non temps réel, comme le transfert de fichier ou la messagerie, quant à elles se focalisent sur la fiabilité des communications.

Le support de la qualité de service a été largement étudié dans les réseaux filaires. Le réseau ATM (Asynchronous Transfert Mode) a considéré le support de la QoS pour les trafics en plusieurs classes. Des solutions ont été proposées par l'IETF pour améliorer le réseau Internet afin de fournir la QoS aux communications multimédia. Des mécanismes ont été fournis pour gérer efficacement les ressources réseau (bande passante, mémoire tampons) pour répondre aux exigences des applications.

Dernièrement, avec l'émergence des services multimédia temps réel, et les champs variés des applications des réseaux ad hoc, la qualité de service dans les réseaux ad hoc est devenue un thème de recherche qui a suscité beaucoup d'intérêts. Dans ce contexte, des travaux pour l'introduction des applications multimédia dans les réseaux ad hoc ont été proposés. Cependant, il est très difficile de garantir une quelconque qualité de service à une application temps réel dans un réseau ad hoc, car il faut prendre en considération les spécificités de ces réseaux, à savoir : la bande passante limitée, le changement dynamique de la topologie en fonction du temps, ainsi que le manque d'information complète sur l'état du réseau. En outre, la communication entre les stations mobiles étant par voix radio, la qualité du lien sans fil reste peu fiable, et susceptible à des variations suivant la configuration et l'état du réseau.

2. Qualité de service à différentes échelles dans les AHWSN

La QoS dans les réseaux ad hoc peut être envisagée à différentes échelles [43] (voir la Figure 2.1) :

- **Interne** : intégration au niveau de la couche MAC du modèle OSI de chaque nœud du réseau;
- **Locale** : intégration au niveau du protocole de routage, c'est-à-dire dans le voisinage proche des nœuds du réseau;
- **Globale** : intégration de bout en bout entre la source et la destination au sein du réseau.

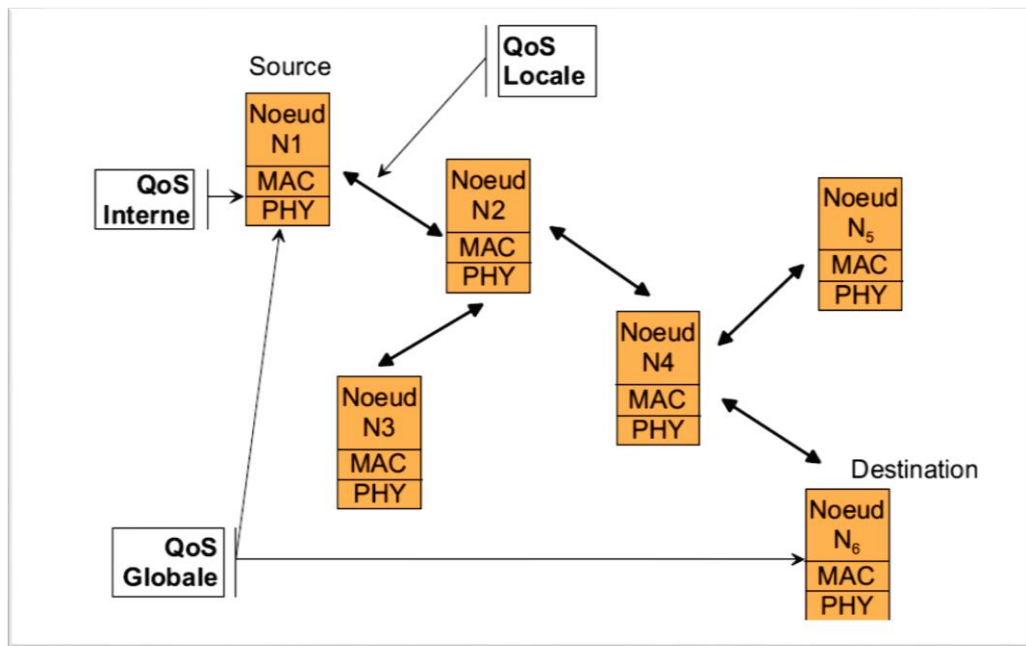


Figure 2.1 : Différents niveaux d'approches de la QoS dans les réseaux AHWSN

2.1 Qualité de service dans les AHWSN à l'échelle interne : Différenciation de service au niveau de la couche MAC

Récemment, des schémas de différenciation de service au niveau MAC ont été proposés. Néanmoins, ils sont souvent basés sur un contrôle centralisé. Dans les réseaux sans fil multi-sauts, un contrôle distribué est nécessaire. Le protocole MACA/PR (Multihop Access Collision Avoidance with Piggyback Reservation) [44] propose de fournir des garanties de bande passante pour les applications temps réel via une réservation. Il permet d'établir des connexions temps réel à un saut seulement. Il utilise un dialogue RTS/CTS (Request To send/ Clear To Send) avec acquittement, et différencie la politique d'accès au médium selon la nature des flux. Pour le trafic prioritaire, une seule demande d'autorisation à transmettre (RTS-CTS) au début du flux est utilisée (jusqu'à perte d'un paquet). Dans chaque paquet, des informations sur l'ordonnancement du paquet suivant sont incluses pour empêcher les voisins d'entrer en collision avec les prochains paquets. Dans la section suivante nous nous intéressons aux mécanismes de différenciation de service proposés pour le protocole IEEE 802.11.

2.1.1 Description de la couche MAC IEEE 802.11

Nous avons utilisé dans notre thèse la couche MAC du standard IEEE 802.11 [45]. Sa méthode d'accès basique est la 'Distributed Coordination Function' (DCF) qui se base sur l'utilisation de CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) pour supporter les transmissions asynchrones de données. La deuxième fonction d'accès, optionnelle, est la PCF (Point Coordination Function) sert à supporter les trafics synchrones, i.e. trafics temps réel. Cette dernière est utilisée en mode infrastructure. Pour les réseaux AHWSN, la première fonction est utilisée.

Le principe de la fonction DCF consiste à écouter le canal pour voir si un autre nœud est en train d'émettre. Le nœud doit s'assurer que le médium est libre pour une certaine durée (DIFS) avant d'émettre. Si le canal est occupé, la transmission est différée d'un temps de Back-off, choisi aléatoirement dans une fenêtre appelée Contention Window (CW). La valeur du Back-off ne sera décrétementée que si le médium est libre. Cependant, si au moins deux stations émettent simultanément, une collision peut apparaître et sa détection par la station émettrice n'est malheureusement pas possible. Pour cela, un acquittement (ACK) est utilisé pour informer la station émettrice que la trame est reçue avec succès.

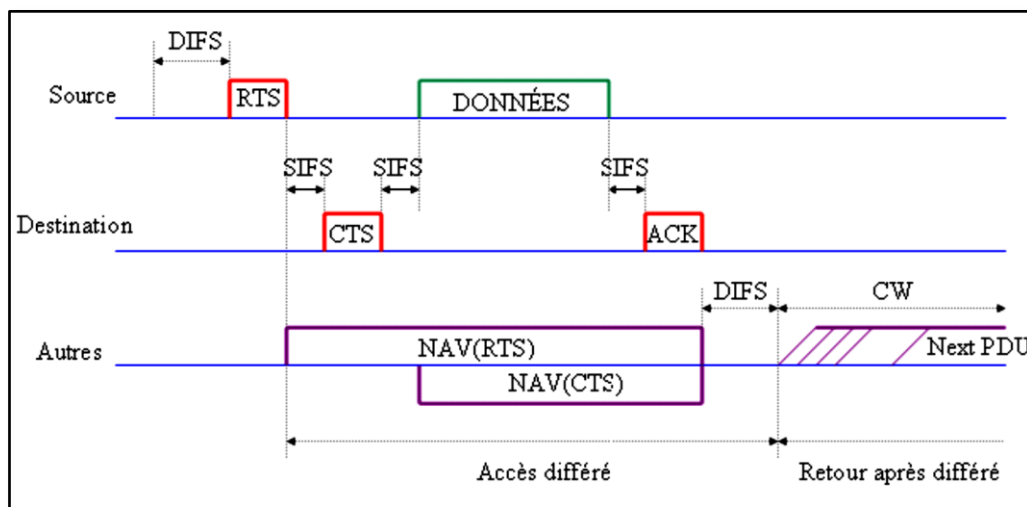


Figure 2.2 : Méthode d'accès DCF

2.1.2 Différenciation de service basée sur la fonction DCF du protocole 802.11

Dans le but d'améliorer la méthode d'accès DCF du protocole 802.11, les techniques suivantes ont été proposées :

Fonction de back-off différente [46] : Le principe est d'attribuer des valeurs de fenêtres de contention (CW) supérieures pour les stations les moins prioritaires et inversement, permettant ainsi de donner plus de chance à une station prioritaire d'accéder au canal.

Différents DIFS [47] : Dans le standard IEEE 802.11 de base les trames ACK ont une priorité sur les trames RTS, en attendant un temps SIFS qui est inférieur à DIFS (pour RTS). Dans cette technique de différenciation, la même idée est utilisée, où chaque station mobile dispose de sa propre valeur de DIFS qui définit son niveau de priorité pour l'accès au médium,

Distributed Fair Scheduling [48] : Dans ce schéma d'accès la valeur du back-off générée avant un envoi, est proportionnelle à la longueur de la trame de donnée et inversement proportionnelle au poids du flux,

BlackBurst [49] : Il impose des conditions telles qu'un intervalle constant pour accéder au lien et la possibilité de bloquer le canal pendant une période de temps, où chaque station a une priorité qui lui permet d'envoyer des trames ayant une taille maximale différente,

Différenciation des valeurs de CWmin de la fenêtre de contention : il utilise des valeurs de CWmin et CWmax différentes, où $CWmin(highprio) < CWmin(lowprio)$, et $CWmax(highprio) < CWmax(lowprio)$.

D'autres approches utilisent une différenciation basée sur les flots ou sur les files au lieu d'une priorité affectée par station mobile. L'étude réalisée dans [50], montre que l'utilisation du paramètre DIFS pour la différenciation de service montre de bons résultats. Un mécanisme de priorité pour la fonction DCF de la couche MAC 802.11 a été étudié dans [51]. Il consiste à différencier les trafics, et introduire une priorité en modifiant les paramètres de la fonction d'accès DCF. Son principe consiste à associer des DIFS ou des temps de back-off plus courts pour les flux prioritaires. Ainsi, les flux prioritaires auront une plus grande probabilité d'accéder au médium que les autres. D'autres paramètres de la fonction DCF peuvent aussi être utilisés pour différencier des services.

2.1.3 IEEE 802.11e

Actuellement en cours d'évaluation, la spécification du draft IEEE 802.11e [52] propose le support de la QoS dans les réseaux sans fil avec une nouvelle fonction de contrôle EDCA (Enhanced Distributed Channel Access), considérée comme la nouvelle version de la fonction DCF, et une fonction de coordination hybride (HCF). EDCA introduit quatre catégories de trafics (TC). Les priorités sont contrôlées par les stations en modifiant le schéma d'accès de base (DCF). Plus flexible que la fonction PCF, HCF est utilisée par les points d'accès pendant la période d'accès contrôlée (CAP), qui peut commencer à n'importe quel moment durant 'la superframe'. Autrement dit, ça lui

permet d'avoir accès au médium pour faire passer un trafic ayant des contraintes de QoS.

2.2 La Qualité de Service dans les réseaux AHWSN à l'échelle locale

La QoS est ici abordée au niveau local, c'est-à-dire dans le voisinage immédiat des nœuds du réseau. Pour cela, les paramètres de QoS sont calculés en lien étroit avec les algorithmes de routage. Les protocoles de routage précédemment exposés ne cherchent qu'à obtenir une route entre la source et la destination; dans le cas de solutions multiples, la route la plus courte en termes de nombre de sauts est le plus souvent choisie. Ce critère peut d'ailleurs être considéré comme un paramètre de QoS, mais de pertinence limitée.

Dans cette approche locale de la QoS, un paramètre supplémentaire de QoS est ajouté aux routes possibles. Ce paramètre est calculé lors de la recherche des routes grâce principalement à l'échange des paquets de contrôle du protocole de routage. La concaténation de ces paramètres locaux donne une idée de la QoS entre la source et la destination.

Contrairement aux protocoles 'au mieux' (Best Effort), le but des protocoles de routage avec support de la qualité de service [53] est de trouver une route ayant suffisamment de ressources pour satisfaire les besoins de QoS d'une communication, tout en optimisant l'utilisation des ressources disponibles.

Les métriques de QoS peuvent être additives, concaves ou multiplicatives. La bande passante est une métrique concave, alors que le délai et la gigue sont des métriques additives. La disponibilité d'un lien, basée sur des critères comme la probabilité de perte du lien quant à elle est une métrique multiplicative.

Une métrique additive A_m est définie comme : $\sum_{i=1}^h (L_i(m))$ où $L_i(m)$ est la valeur de la métrique m sur le lien L_i et $L_i \in P$. h représente la longueur du chemin P . Une métrique concave définit la valeur minimale sur un chemin P et représenté comme :

$C_m = \min(L_i(m), L_i(m) \in P)$. Une métrique multiplicative représente le produit des valeurs des métriques de QoS, elle est définie comme : $M_m = \prod_{i=1}^h L_i(m), L_i(m) \in P$

Pour trouver une route qui satisfait une métrique concave, les ressources disponibles dans chaque lien doivent être au moins égales à la valeur désirée de la métrique.

Trouver un chemin optimal assurant des contraintes multiples peut être un problème NP-Complet, dans le cas où il inclut deux métriques additives ou plus [53].

Contrairement aux réseaux filaires, les changements de topologie dans les réseaux AHWSN exigent de recalculer les routes avec QoS, et répondre assez rapidement sans dégrader leur niveau de QoS. Par conséquent, des ressources additionnelles sont consommées (bande passante, batterie, . . . etc.).

2.2.1 CEDAR (Core-Extraction Distributed Ad hoc Routing Algorithm)

CEDAR [54] est un protocole de routage réactif avec qualité de service basé sur une élection dynamique d'un cœur de réseau stable. Des informations sur les liens stables disposant d'une grande bande passante sont propagées entre les nœuds du cœur. Le calcul des routes est effectué par les nœuds du réseau cœur en utilisant des informations locales.

Utilisé dans des réseaux de petite à moyenne taille (de dizaines à des centaines de nœuds), il est basé sur trois composantes essentielles :

- **Extraction d'un cœur du réseau** : un ensemble de nœud est dynamiquement choisi pour calculer les routes et maintenir l'état des liens du réseau. L'avantage d'une telle approche est qu'avec un ensemble réduit de nœuds les échanges d'informations d'état et de route seront minimisés, évitant ainsi des messages supplémentaires circulant dans le réseau. En outre, lors d'un changement de route, seuls les nœuds du cœur serviront au calcul,

- **Propagation d'état de lien** : le routage avec qualité de service est réalisé grâce à la propagation des informations sur les liens stables avec une grande bande passante. L'objectif est d'informer les nœuds distants sur les liens de grande capacité, alors que les liens de faible capacité restent connus au niveau local (les nœuds n'ont pas une information sur la topologie globale du réseau),

- **Calcul de route** : celui-ci est basé sur la découverte et l'établissement d'un plus court chemin vers la destination satisfaisant la bande passante demandée. Des routes de 'secours' sont utilisées lors de la reconstruction de la route principale, quand cette dernière est perdue. La reconstruction peut être locale (à l'endroit de la cassure), ou à l'initiative de la source.

Au lieu de calculer une route avec un minimum de saut, l'objectif principal de CEDAR est de trouver un chemin stable pour garantir plus de bande passante. Dans ce protocole de routage, les nœuds du cœur du réseau auront plus de trafics à gérer, en plus des messages de contrôle (pour la découverte et la maintenance des routes). En outre, en cas de forte mobilité, la convergence de l'algorithme est difficile à atteindre.

2.2.2 Autres protocoles de routage avec QoS

Ticket-Based QoS Routing [55] est un protocole de routage distribué, qui autorise des informations d'état imprécises durant la phase de calcul de la route. Il permet de réduire la quantité des messages de routage diffusée pour la découverte de la route, en publiant un certain nombre de 'tickets logiques'. Chaque message de découverte (ou d'observation) de route doit avoir au moins un ticket. Quand un message arrive à un nœud, il peut être divisé en plusieurs messages d'observation, qui sont relayés vers les prochains sauts. Chaque message 'fils' contiendra un sous ensemble des tickets de son message 'père'. Evidemment, un message ayant un seul ticket ne peut être divisé. Lors de l'arrivée d'un message de découverte de route à la destination, le chemin saut par saut est connu et les informations de délai ou de bande passante peuvent être utilisées pour effectuer la réservation de ressources pour la route répondant aux besoins de QoS. Le nombre de tickets générés est en fonction de la précision des informations d'états disponibles à la source et les besoins de QoS de la communication. Plus de tickets sont publiés dans le but d'augmenter la chance de trouver un chemin désiré.

Dans les réseaux filaires, une distribution de probabilité, selon des informations sur le délai ou la bande passante, peut être calculée. Cependant, cela reste inapproprié dans les réseaux ad hoc où les liens sans fil sont sujets à des cassures, où les informations d'état sont imprécises. Pour cela, un modèle simple a été proposé pour l'algorithme Ticket Based. Il utilise l'historique et l'estimation des variations du délai, et une formule de lissage pour calculer le délai courant. Pour s'adapter aux changements de topologie, l'algorithme autorise différents niveaux de redondance de route. Il utilise aussi des techniques de réparation et de reroutage pour la maintenance des routes. La réparation des routes se fait en utilisant des reconstructions locales.

Un algorithme de calcul et d'allocation de bande passante de bout en bout basé sur la couche TDMA a été proposé dans [56]. Dans ce cas, un nœud source peut déterminer la disponibilité des ressources pour le support des besoins de QoS vers n'importe quelle destination dans le réseau ad hoc. Cette approche est particulièrement utile pour un mécanisme de contrôle d'admission. Il propose une solution basée sur une heuristique pour connaître les slots libres dans les liens tout au long de la route, et d'assigner ces slots à chaque saut.

Contrairement aux autres protocoles avec QoS, qui essaient de trouver un seul chemin entre la source et la destination, [57] a proposé Multipath QoS Routing Protocol, qui permet de trouver plusieurs routes qui fournissent collectivement suffisamment de ressources. Ce protocole adopte aussi l'idée de distribution de tickets (voir section TBPR).

Ce type de routage est adapté aux réseaux ad hoc ayant une bande passante limitée, où une seule route avec QoS semble être très difficile à assurer.

Une extension du protocole de routage réactif AODV pour le support de la qualité de service a été proposée dans [58]. Elle consiste à étendre les paquets 'route request' et 'route response' durant la phase de découverte de la route. De plus, les informations suivantes sont ajoutées dans la table de routage : bande passante minimale, délai maximum, et la liste des sources qui ont demandé des garanties de délai ou de bande passante. Si un nœud détecte que la QoS demandée n'est pas satisfaite alors il envoie un message à la source ayant initiée cette demande de QoS, pour l'informer.

[59] propose un algorithme de routage qui prend en compte des métriques et des contraintes du niveau réseau et du niveau application pour mieux répondre aux besoins de qualité de service.

Un autre mécanisme utilisé pour le support de la qualité de service est la réservation de ressources. La section suivante détaille le fonctionnement du protocole de signalisation INSIGNIA.

2.2.3 Protocole de réservation de ressources : INSIGNIA [60]

INSIGNIA est un protocole de signalisation spécialement conçu pour les réseaux ad-hoc. Il établit une réservation de bande passante orientée flux dans le but de supporter des services temps réel adaptatifs. Il est basé sur un système de signalisation 'In-band', où les messages de contrôle sont encapsulés comme une option dans les paquets de données IP. Ceci permet de réduire l'over-Head généré par les messages de signalisation, contrairement à une signalisation out-band explicite (comme RSVP par exemple).

Ce protocole supporte deux types de services (temps réel et best effort). Il offre des algorithmes de réservation, restauration et d'adaptation rapides pour répondre aux changements de topologie du réseau et aux dégradations des liens sans fil. La demande de réservation est effectuée lors de l'envoi du premier paquet de données, et est rafraîchie par le passage des paquets de données. Le destinataire informe périodiquement la source de l'état de la route en envoyant des rapports de QoS (QoS Reporting), qui contiennent des statistiques sur la latence, le taux de perte et le débit. Ces informations peuvent donc servir pour la source à réguler son débit d'émission. Dans un cadre général, et dans le but de fournir des services temps réel adaptatifs, [61] propose un modèle de gestion de flots (flow management model), qui consiste en une architecture de contrôle au niveau IP, permettant d'adapter la session de l'utilisateur au

service disponible sans signalisation explicite entre la source et la destination. Il comprend les fonctionnalités suivantes :

- Signalisation in-band (INSIGNIA) se charge d'établir, de terminer, de restaurer et d'adapter les réservations des flots,
- Le module *packet forwarding* classe les paquets entrants. Les messages de signalisation sont remis à INSIGNIA tandis que les paquets sont soit passés aux couches supérieures, soit retransmis vers le destinataire,
- Le module *routingprotocol* s'occupe de la mise à jour de la table de routage selon la topologie du réseau et la met à disposition des autres modules,
- Le contrôle d'admission alloue la bande passante aux flots en se basant sur les débits minimal et maximal spécifiés dans la requête et sur l'utilisation, et la capacité du canal. Il décide entre l'acceptation ou le rejet d'un nouveau flot,
- Le module *packet scheduling* se charge de l'ordonnancement des paquets,
- Le module *MAC* contrôle l'accès au support en tenant compte de la QoS.

L'un des inconvénients d'une telle approche est le fait d'avoir des informations sur les trafics dans chaque nœud ce qui pose des problèmes de capacité des nœuds, et la difficulté de passage à l'échelle avec l'augmentation du nombre de flux. En outre, cette approche n'offre que deux types de service temps réel et best effort.

Finalement, INSIGNIA ne supporte que les applications multimédia adaptatives, et la réservation de ressource ne peut être établie que lorsque le trafic est lancé.

2.3 La Qualité de Service dans les réseaux AHWSN à l'échelle globale

Pour l'approche à l'échelle globale, c'est la totalité du chemin entre la source et la destination qui est ici considérée. Une route est déterminée de manière conventionnelle par un algorithme de routage et elle est caractérisée par des paramètres de QoS de bout en bout ou "End-to-End" comme cela peut être réalisé dans les réseaux filaires classiques [43].

Une fois la route évaluée, la source peut adapter l'émission en jouant sur la taille et la fréquence d'envoi des trames ou en différenciant les flux en fonction d'un niveau de priorité. Cette adaptation peut être fixée une fois pour toutes pour une émission donnée ou bien être dynamique et évoluer au fil de l'émission en fonction du comportement des trames émises et reçues.

Les réseaux AHWSN étant par définition peu stables, il faut donc faire attention à l'estimation des paramètres de QoS dans ce type d'approche, surtout si le choix est

d'avoir un comportement d'émission adaptatif. Les paramètres mesurés sont en effet très bruités et doivent absolument être filtrés pour pouvoir être utilisables.

Il existe de nombreux travaux qui montrent les différentes formes de filtrage pouvant être pertinents dans le cas des réseaux AHWSN. Dans notre thèse, nous avons évoqué cette partie de QoS de bout en bout pour la transmission de l'information, en tenant en compte de la caractéristique d'énergie résiduelle des nœuds, implémentée comme information contenue dans les messages de contrôle du protocole OLSR afin de choisir la route la plus optimisée entre la source et la destination (voir les chapitres 3 et 4 de cette thèse).

3. Modèles de qualité de service dans les réseaux AD-HOC [53]

Les modèles de qualité de service IntServ/RSVP et DiffServ ont été proposés par l'IETF pour fournir des garanties aux besoins des services temps réel dans les réseaux filaires. D'un côté, l'application du modèle IntServ dans les MANET s'avère inadaptée à l'environnement ad-hoc. Ceci est justifié du fait que les capacités des nœuds mobiles sont trop variables et limitées pour supporter un traitement complexe et gérer les réservations ainsi que les états des communications en cours. De plus, une réservation dans les réseaux filaires est différente de celle d'un réseau mobile sans fil, car les liens sont partagés, limités et susceptibles à des variations spatio-temporelles. D'un autre côté, le modèle DiffServ semble le mieux adapté aux réseaux mobiles. Pour résoudre le problème de passage à l'échelle, ce modèle utilise une granularité par classe, où aucune signalisation pour la réservation de ressources n'est utilisée. Cependant, dans ce modèle le cœur du réseau est supposé bien dimensionné, et un administrateur de domaine est nécessaire. Ces deux contraintes restent difficiles à satisfaire.

3.1 Flexible quality of service model for MANETs (FQMM)

Le modèle FQMM [62] repose sur une architecture réseau plate (non hiérarchique), constituée d'une cinquantaine de nœuds mobiles, formant un domaine DiffServ. Il combine les propriétés des modèles filaires IntServ et DiffServ, en offrant une méthode d'approvisionnement hybride : par flux, pour les trafics prioritaires, et par classe pour les autres trafics. Dans le réseau, les nœuds peuvent avoir des rôles différents suivant les trafics existants : nœud d'entrée du trafic, intermédiaire ou de sortie. Les nœuds d'entrée permettent de marquer et classifier les paquets, qui seront ensuite relayés par les nœuds intermédiaires suivant leurs PHB (Per Hop Behavior), jusqu'à arriver au nœud destinataire. Ce modèle repose essentiellement sur la couche IP, où les

fonctionnalités sont séparées en deux grands plans: le plan relayage de données et le plan contrôle et gestion. Les techniques d'ordonnancement et de gestion de mémoires tampons sont étudiées. Dans ce modèle, le protocole de routage est supposé fournir des routes ayant suffisamment de ressources.

L'avantage d'une telle approche est la possibilité d'interfacer le réseau avec l'Internet, vu les mécanismes de qualité de services offerts qui sont proches des protocoles filaires. Cependant, plusieurs mécanismes ainsi que l'interaction avec la couche MAC restent à définir pour s'adapter aux conditions variables du réseau AHWSN.

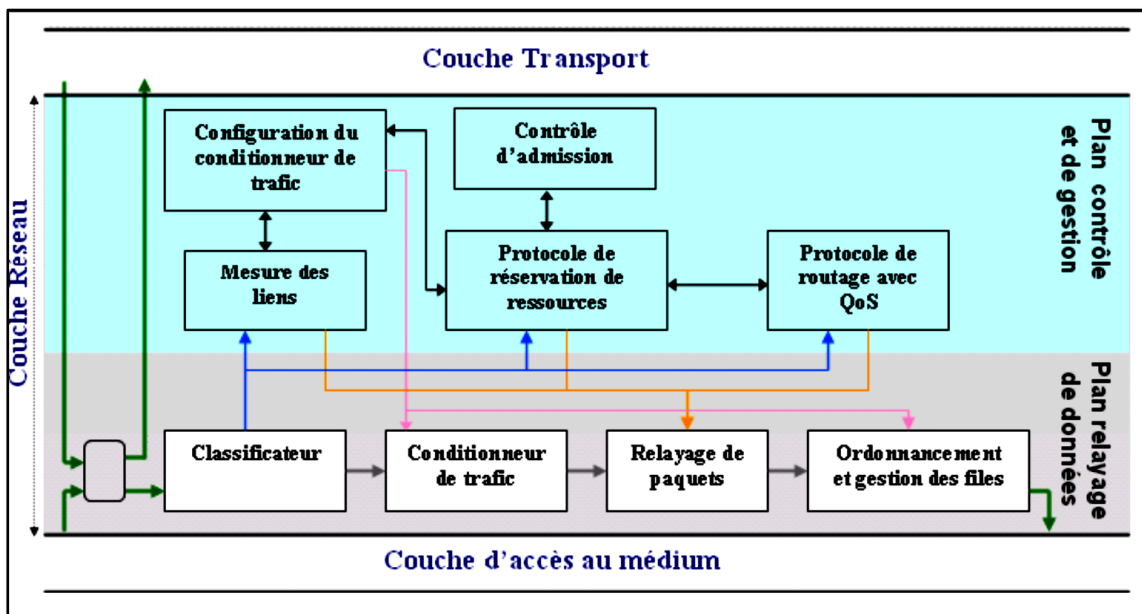


Figure 2.3: Modèle FQMQM

3.2 Service differentiation in wireless ad hoc networks (SWAN)

SWAN [63] est un modèle réseau sans état basé sur des algorithmes de contrôle distribués dans le but d'assurer une différenciation de services dans les réseaux ad hoc. Il offre la priorité (au niveau paquet) aux trafics temps réel en contrôlant la quantité de trafics best effort acceptée par nœud. Pour accepter un nouveau trafic temps réel, le contrôle d'admission sonde la bande passante minimale disponible sur la route (valide et obtenu par un protocole de routage). Une décision à la source est alors prise suivant la bande passante obtenue. Pour maintenir la qualité de service des trafics déjà acceptés, le débit des trafics best effort est régulé en utilisant les mesures de délais au niveau MAC comme paramètre. Un classificateur et un shaper permettent de différencier les deux types de trafic. En cas de congestion, les bits ECN (Explicit Congestion Notification) de l'entête des paquets IP sont positionnés pour permettre à la source de ré-initialiser le

contrôle d'admission. Si la route ne dispose pas d'assez de bande passante, le trafic est supprimé. Ainsi, SWAN permet de fournir une QoS logiciel (soft QoS).

Un flux prioritaire admis n'est pas sûr d'avoir des garanties pendant la durée entière de la communication, et peut à tout moment être violé par d'autres demandes de trafics. Un mécanisme de contrôle de débit des flux best effort n'est pas à lui seul suffisant pour offrir des garanties aux applications temps réel. En outre, dans cette approche, le protocole de routage ainsi que la couche d'accès au médium sont de type best effort.

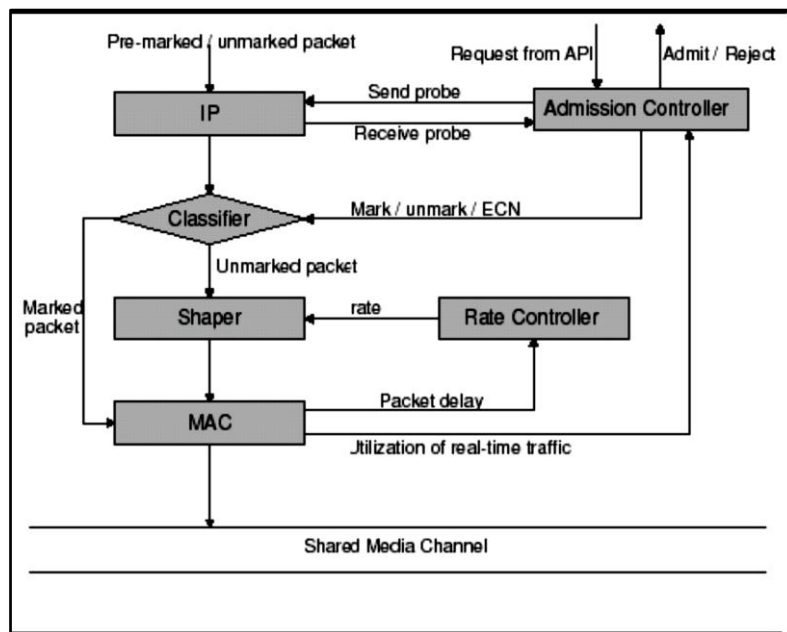


Figure 2.4: Modèle SWAN

3.3 Modèle iMAQ

Le modèle iMAQ [64] fournit le support des transmissions des données multimédia dans un MANET. Le modèle inclut une couche ad hoc de routage et une couche de service logiciel (Middleware). Dans chaque nœud, ces deux couches partagent les informations et communiquent afin de fournir les garanties de QoS aux trafics multimédia. Le protocole de routage est basé sur la prédiction de la position des nœuds (predictive location-based) et orienté QoS. La couche Middleware communique également avec la couche application et la couche réseau et essaye de prévoir le partitionnement du réseau. Pour fournir une meilleure accessibilité aux données, il

réplique les données entre les différents groupes du réseau avant d'effectuer le partitionnement.

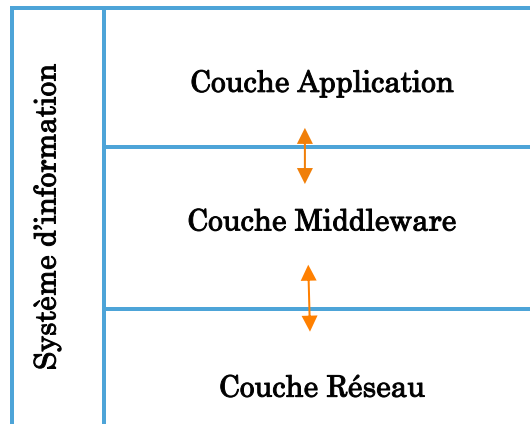


Figure 2.5: Modèle iMAQ

4. Qualité de service QoS : cas des WSN

Bien que les différents modèles de QoS puissent s'appliquer dans un réseau hétérogène incluant des mobiles et des capteurs (AHWSN), ces derniers présentent d'autres contraintes liées à leur conception et déploiement doivent être prises en comptes dans la QoS globale du réseau.

Différentes communautés peuvent interpréter la QoS des WSN de différentes manières. Par exemple, dans les applications impliquant la détection et la poursuite de cibles, beaucoup de facteurs peuvent contribuer à l'échec dans la détection ou l'erreur dans la poursuite. Ceci peut être dû au déploiement et à la gestion du réseau, c'est-à-dire l'endroit où l'événement se produit ne peut être couvert par aucun nœud capteur actif. Intuitivement, nous pouvons définir la couverture ou le nombre de capteurs actifs comme paramètres de mesure de la QoS.

En outre, l'échec peut être provoqué par la fonctionnalité limitée des nœuds capteurs, par exemple, l'exactitude d'observation inadéquate ou un taux de reportage faible des nœuds. De ce fait, on peut définir les erreurs d'exactitude ou de mesure d'observation comme paramètres de mesure de la QoS. De plus, cette dernière peut être induite par la perte de l'information lors de son routage. Il est aussi possible de définir quelques paramètres de transport de l'information pour mesurer la QoS.

Cependant, la séparation dans la définition des paramètres de mesure de la QoS n'est pas absolue puisqu'une seule application, telle que la mesure de performance liée à la détection d'événements, peut impliquer tous ces paramètres. Notre but dans cette section est de nous concentrer sur la façon dont le réseau peut fournir la QoS aux

applications. Pour cela, nous résumons deux approches de la QoS dans les RCSF : QoS spécifique à l'application et QoS liée au réseau.

4.1 Qualité de service liée à l'application

Dans cette optique, on considère des paramètres de QoS tels que la couverture, les erreurs de mesure, et le nombre optimum des nœuds capteurs actifs.

En résumé, les applications imposent des conditions spécifiques au déploiement des nœuds capteurs, le nombre de nœuds actifs, la précision de mesure des nœuds, ...etc, qui sont directement liées à la qualité des applications [65].

4.2 Qualité de service liée au réseau

Dans ce volet, on traite la manière avec laquelle un réseau de communication peut router les données exigeantes en QoS des nœuds capteurs tout en utilisant efficacement les ressources du réseau. Du point de vue de la QoS du réseau, nous ne prenons pas en compte l'application visée, mais plutôt la façon dont les données sont acheminées vers le nœud collecteur ainsi que leurs exigences correspondantes.

Généralement, il existe trois modèles de base d'acheminement des données, à savoir modèle orienté-événements, modèle orienté-requêtes et modèle à flux continus [66]. Notons que ces modèles peuvent coexister dans le même RCSF, donnant ainsi naissance à des modèles hybrides d'acheminement des données. Avant de présenter les exigences des applications en fonction du modèle d'acheminement (Tableau 2.1), nous donnons ci-dessous les quelques facteurs qui les caractérisent :

- Bout-en-bout : l'application peut exiger une performance de bout-en-bout, comme elle peut ne pas l'exiger.
- Interactivité : l'application peut être interactive ou non-interactive.
- Tolérance aux retards : l'application peut être tolérante aux retards des données, comme elle peut ne pas l'être.
- Aspect critique : l'application peut concerner une mission critique, comme elle peut concerner une mission ordinaire.

4.2.1 Modèle orienté-événements

La plupart des applications orientées-événements dans les WSN sont interactives, intolérantes aux retards des données (de type temps-réel), à mission critique, et n'exigent pas la performance de bout-en-bout. Cela signifie que les événements à observer par les nœuds capteurs sont très importants pour le succès de l'application. Cette dernière doit donc détecter ces événements et prend en conséquence une mesure

appropriée aussi rapidement et aussi sûrement que possible. De plus, plusieurs aspects importants devraient être mentionnés. En premier lieu, l'application elle-même n'exige pas une performance de bout-en-bout, c'est-à-dire une extrémité de l'application est représentée par le nœud collecteur, l'autre extrémité n'est pas un seul nœud capteur, mais un groupe de nœuds capteurs situés dans la zone influencée par l'événement. En second lieu, les flux de données de ces nœuds capteurs sont susceptibles d'être fortement corrélés et contenant de ce fait beaucoup de redondances. Troisièmement, le trafic de données généré par un seul nœud capteur peut être d'une intensité très réduite. Cependant, le trafic très dense peut être produit par un ensemble de nœuds capteurs à cause d'un évènement commun ou d'une succession d'évènements. En conclusion, des actions en réponse à l'évènement détecté peuvent devoir être distribuées aux nœuds capteurs ou actionneurs aussi rapidement et aussi sûrement que possible. Ces nœuds capteurs et actionneurs peuvent ne pas être le même ensemble de nœuds qui a informé le nœud collecteur au sujet de cet évènement. Ce modèle d'acheminement de données implique beaucoup d'applications types inhérentes aux WSN exigeant la détection d'évènement et l'estimation du signal de poursuite comme par exemple, la détection et la réponse à une urgence due au dégagement chimique dans un bâtiment.

4.2.2 Modèle orienté-requêtes

La plupart des applications à base de requêtes dans les WSN sont interactives, tolérantes aux retards des requêtes spécifiques, à mission critique, et non exigeantes de la performance de bout-en-bout. Pour économiser l'énergie, des requêtes peuvent être envoyées sur demande. Ce modèle d'acheminement de données est semblable au modèle orienté-événements sauf que la donnée est envoyée par le nœud collecteur contrairement au modèle orienté-événements où la donnée est poussée vers le nœud collecteur. Les applications doivent toujours recevoir ces données désirées aussi rapidement et aussi sûrement que possible. Les aspects importants concernant le modèle orienté-événements sont également appropriés au modèle orienté-requêtes. Notons qu'une requête peut également être utilisée pour contrôler et reconfigurer des nœuds capteurs. Par exemple, si le nœud collecteur veut améliorer le logiciel des nœuds capteurs, reconfigurer le débit d'envoi, ou changer la mission des nœuds, il peut pour cela envoyer une commande pour exécuter ces changements. Notons que les commandes du nœud collecteur forment un flux unidirectionnel et exigent une fiabilité élevée.

4.2.3 Modèle à flux continu

Dans le modèle à flux continu, les nœuds capteurs envoient leurs données sans interruption au nœud collecteur avec un débit préfixé. Une donnée de type temps-réel (voix, image, ou vidéo) exige le respect des délais et impose une certaine largeur de la bande passante. Des pertes de paquets peuvent être tolérées dans une certaine mesure. Il s'agit des applications qui n'exigent pas de la performance de bout-en-bout. Dans un autre contexte, le nœud collecteur peut vouloir rassembler des données périodiques à partir d'une zone du WSN. Dans ce cas, les retards et les pertes des paquets lors du routage sont tolérés.

| Classe | Orienté-événements | Orienté-requêtes | A flux continus |
|---------------------|--------------------|------------------|-----------------|
| Bout-en-bout | Non | Non | Non |
| Interactivité | Oui | Oui | Non |
| Tolérance au retard | Non | Spécifique | Oui |
| Aspect critique | Oui | Oui | Oui |

Tableau 2.1: Exigences des applications WSN

Notons qu'il y a quelques différences entre les WSN et les réseaux traditionnels dans les exigences des applications. Tout d'abord, les applications dans les WSN ne sont pas toujours des applications de bout-en-bout. En second lieu, la bande passante n'est pas la principale préoccupation d'un seul nœud. Cependant, elle peut-être un souci important pour un groupe de nœuds pendant certaines périodes de temps, dues à la nature chargée du trafic de capture. Troisièmement, des pertes de paquets du trafic au niveau d'un seul nœud capteur peuvent être tolérées dans une certaine mesure puisqu'il existe toujours des redondances dans les données.

En conclusion, la plupart des applications des WSN sont à mission critique, ce qui reflète l'importance de ces applications.

5. Techniques de conservation d'énergie dans les réseaux AHWSN

La durée de vie est sans doute la métrique la plus importante dans l'évaluation des performances d'un réseau AHWSN. En effet, dans un environnement contraint, toute ressource limitée doit être prise en compte. Toutefois, la durée de vie du réseau, comme

mesure de la consommation d'énergie, occupe une place exceptionnelle puisqu'elle constitue la borne supérieure de l'utilité de ce réseau [67].

La durée de vie est également considérée comme un paramètre fondamental dans un contexte de disponibilité et de sécurité dans les réseaux AHWSN [68].

Maximiser la durée de vie du réseau revient à réduire la consommation énergétique des nœuds. Malgré les progrès qui ont été faits, la durée de vie de ces dispositifs à piles continue d'être un défi majeur et un facteur clé, exigeant davantage de recherches sur l'efficacité énergétique des plates-formes et des protocoles de communication.

5.1 Consommation d'énergie d'un nœud dans un réseau AHWSN

Les nœuds sont alimentés principalement par des batteries. Ils doivent donc fonctionner avec un bilan énergétique frugal. En outre, ils doivent le plus souvent avoir une durée de vie de l'ordre de plusieurs mois, voire de quelques années, puisque le remplacement des batteries n'est pas une option (cas des WSN) envisageable pour des réseaux avec des milliers de nœud [69].

5.1.1 Formes de dissipation d'énergie

Afin de concevoir des solutions efficaces en énergie, il est extrêmement important de faire d'abord une analyse des différents facteurs provoquant la dissipation de l'énergie d'un nœud.

Cette dissipation d'énergie se fait de manière générale selon plusieurs modes :

- **Le MCU (Micro-contrôleur unit)** : Généralement les MCUs possèdent divers modes de fonctionnement : actif, `_idle_`, et sommeil, à des fins de gestion d'énergie. Chaque mode est caractérisé par une quantité différente de consommation d'énergie. Par exemple, le MSP4303 consomme 3 mW en mode actif, 98 μ W dans le mode `_idle_` et seulement 15 μ W dans le mode sommeil. Toutefois, la transition entre les modes de fonctionnement implique un surplus d'énergie et de latence. Ainsi, les niveaux de consommation d'énergie des différents modes, les coûts de transition entre les modes mais encore le temps passé par le MCU dans chaque mode ont une incidence importante sur la consommation totale d'énergie d'un nœud-capteur.
- **La radio** : la radio opère dans quatre modes de fonctionnement : émission, réception, `_idle_`, et sommeil. Une observation importante dans le cas de la plupart des radios est que le mode `_idle_` induit une consommation d'énergie significative, presque égale à la consommation en mode réception. Ainsi, il est plus judicieux

d'éteindre complètement la radio plutôt que de passer en mode "idle" quand l'on a ni à émettre ni à recevoir de données. Un autre facteur déterminant est que, le passage de la radio d'un mode à un autre engendre une dissipation d'énergie importante due à l'activité des circuits électroniques. Par exemple, quand la radio passe du mode sommeil au mode émission pour envoyer un paquet, une importante quantité d'énergie est consommée pour le démarrage de l'émetteur lui-même [69]. Un autre point important est que les données des constructeurs sous-estiment assez régulièrement ces différentes consommations comme ont pu le montrer les auteurs de [70], en particulier concernant la consommation dans le mode `_idle_`.

- **Le détecteur ou le capteur proprement dit** : il y a plusieurs sources de consommation d'énergie par le module de détection, notamment l'échantillonnage et la conversion des signaux physiques en signaux électriques, le conditionnement des signaux et la conversion analogique-numérique. Étant donné la diversité des capteurs, il n'y a pas de valeurs typiques de l'énergie consommée. En revanche, les capteurs passifs (température, sismiques, ...) consomment le plus souvent peu d'énergie par rapport aux autres composants du nœud-capteur. Notons, les capteurs actifs tels que les sonars, les capteurs d'images, etc. peuvent consommer beaucoup d'énergie.

En outre, il existe d'autres formes de dissipation d'énergie telles que les lectures et les écritures mémoire. Un autre aspect non négligeable est le phénomène d'autodécharge de la batterie. En effet, cette dernière se décharge d'elle-même et perd de sa capacité au fil du temps.

Il est difficile d'apporter ici une étude quantitative et comparative précise de la consommation de chaque composant d'un nœud-capteur en raison du grand nombre de plates-formes commerciales existantes. Cependant, des expérimentations ont montré que c'est la transmission de données qui est la plus consommatrice en énergie. Le coût d'une transmission d'un bit d'information est approximativement le même que le coût nécessaire au calcul d'un millier d'opérations. La consommation du module de détection dépend du type spécifique du nœud-capteur.

5.1.2 Sources de surconsommation d'énergie

Nous appelons surconsommation d'énergie toute consommation inutile que l'on peut éviter afin de conserver l'énergie d'un nœud. Les sources de cette surconsommation sont nombreuses, elles peuvent être engendrées lors de la détection lorsque celle-ci est mal gérée (par exemple par une fréquence d'échantillonnage est mal contrôlée) [71].

La surconsommation concerne également la partie communication. En effet, cette dernière est sujette à plusieurs phénomènes qui surconsomment de l'énergie surtout au niveau MAC où se déroule le contrôle d'accès au support sans fil. Certains de ces phénomènes sont les causes majeures de la perte d'énergie et ont été recensés dans [72] :

- **Les collisions** : elles sont la première source de perte d'énergie. Quand deux trames sont émises en même temps et se heurtent, elles deviennent inexploitables et doivent être abandonnées. Les retransmettre par la suite, consomme de l'énergie. Tous les protocoles MAC essaient à leur manière d'éviter les collisions. Les collisions concernent plutôt les protocoles MAC avec contention.
- **L'écoute à vide (idle listening)** : un nœud dans l'état `_idle_` est prêt à recevoir un paquet, mais il n'est pas actuellement en train de recevoir quoi que ce soit. Ceci est coûteux et inutile dans le cas des réseaux à faible charge de trafic. Plusieurs types de radios présentent un coût en énergie significatif pour le mode `_idle_`. Eteindre la radio est une solution, mais le coût de la transition entre les modes consomme également de l'énergie, la fréquence de cette transition doit alors rester raisonnable
- **L'écoute abusive (overhearing)** : cette situation se présente quand un nœud reçoit des paquets qui ne lui sont pas destinés. Le coût de l'écoute abusive peut être un facteur dominant de la perte d'énergie quand la charge de trafic est élevée et la densité des nœuds est grande.
- **L'overmitting** : un nœud envoie des données et le nœud destinataire n'est pas prêt à les recevoir.
- **L'overhead des paquets de contrôle** : l'envoi, la réception, et l'écoute des paquets de contrôle consomment de l'énergie. Comme les paquets de contrôle ne transportent pas directement des données, ils réduisent également le débit utile effectif.

Le tableau 2.2 présente le coût énergétique, pour un nœud qui n'est pas le destinataire du message du protocole IEEE 802.11, en fonction de la taille des messages. Les terminaux situés à portée d'émission d'un expéditeur reçoivent un message RTS et peuvent entrer dans un mode de conservation d'énergie durant la transmission. Ceci explique les valeurs négatives de m_{AX} et m_X , puisque l'énergie consommée est inférieure à celle du mode *idle*. Le coût fixe, p_{AX} , pour les terminaux non destinataires du message mais à portée d'émission de l'expéditeur est plus important que p_X , avec p_X correspondant au coût associé aux nœuds non-destinataires se trouvant seulement à portée de transmission de l'expéditeur. En effet, ces derniers ne reçoivent pas les messages CTS et ACK. Finalement, les terminaux, se trouvant seulement à portée du destinataire,

reçoivent les messages CTS et ACK, mais ne reçoivent pas de message RTS. Ils ne peuvent donc pas entrer en mode de réduction de consommation d'énergie. Ceci explique pourquoi le coût incrémental m_A est nul. Par conséquent, tous les terminaux écoutent le canal de communication, à l'exception de ceux se trouvant à portée d'émission de l'expéditeur et du destinataire. Seuls ces derniers peuvent économiser de l'énergie en passant en mode veille.

| Noeud | Consommation énergétique ($\mu W.sec$) | m ($\mu W.sec$) | p ($\mu W.sec$) |
|---|---|----------------------|----------------------|
| Expéditeur X | $\epsilon_{exp} = m_{exp} \times taille + p_{exp}$ | $m_{exp} = 1.9$ | $p_{exp} = 454$ |
| Destinataire A | $\epsilon_{dest} = m_{dest} \times taille + p_{dest}$ | $m_{dest} = 0.5$ | $p_{dest} = 356$ |
| Terminal non destinataire à portée de transmission | | | |
| A portée de transmission de l'expéditeur X et du destinataire A | $\epsilon_{AX} = m_{AX} \times taille + p_{AX}$ | $m_{AX} = -0.22$ | $p_{AX} = 210$ |
| A portée de transmission de l'expéditeur X | $\epsilon_X = m_X \times taille + p_X$ | $m_X = -0.04$ | $p_X = 90$ |
| A portée de transmission et du destinataire A | $\epsilon_A = m_A \times taille + p_A$ | $m_A = 0$ | $p_A = 119$ |

Tableau 2.2: Consommation d'énergie liée à une communication point-à-point

5.1.3 Consommation d'énergie due au routage

Cette partie représente l'élément clé de notre recherche dans ce domaine car elle sera axée sur l'optimisation de l'énergie dans les protocoles de routage. Puisqu'il affecte directement la consommation d'énergie, le routage reste l'un des principaux défis des concepteurs de protocoles dédiés aux AHWSN. Les sources de consommation d'énergie au niveau de la couche réseau sont diverses [72] :

- **La longueur des chemins de routage** : le chemin que peut suivre un paquet de données d'une source vers une destination est représenté par le nombre de sauts effectués par ce paquet. Sachant que le coût d'un saut est fonction du carré de la distance séparant les deux nœuds concernés par la communication, l'énergie consommée par un paquet représente alors la somme des énergies consommées par tous les sauts parcourus entre la source et la destination.
- **La qualité des liens** : les retransmissions de paquets au niveau de la couche liaison peuvent accroître le coût énergétique d'une manière significative. Un court chemin avec

beaucoup de retransmissions est plus mauvais qu'un long chemin avec peu de retransmissions.

- **Le mode de communication** : le routage dans les AHWSN diffère de celui utilisé par les réseaux traditionnels; le mode de communication dans les AHWSN est en effet de type "plusieurs vers un", ou de type "un vers plusieurs". Un routage point-à-point est inefficace; il consomme plus d'énergie au niveau des nœuds.

- **Le routage des paquets inutiles** : certaines applications critiques exigent du protocole de routage une fiabilité et un respect des échéances temporelles des paquets de données. Un paquet dont l'échéance temporelle a expiré avant d'atteindre sa destination, est un paquet inutile pour l'application. Continuer à router un paquet dans le réseau dont les chances d'atteindre la destination sont minimales engendrera une consommation d'énergie inutile.

- **Les critères de choix d'un chemin de routage** : la durée de vie d'un AHWSN est souvent relative à l'épuisement de l'énergie d'un certain nombre de nœuds, ayant pour conséquence le partitionnement du réseau et donc l'arrêt total de l'application. La cause principale de ce phénomène est la non-prise en compte de l'énergie des nœuds lors de la sélection des sauts successifs des paquets vers le nœud collecteur du réseau.

5.2 Conservation d'énergie

Comme nous l'avons déjà évoqué, des mesures expérimentales ont montré que, généralement, c'est la transmission des données qui est la plus consommatrice en énergie, et de façon significative, les calculs, eux, consomment très peu. La consommation d'énergie du module de détection dépend de la spécificité du nœud. Dans de nombreux cas, elle est négligeable par rapport à l'énergie consommée par le module de traitement et, par-dessus tout, le module de communication.

Dans d'autres cas, l'énergie dépensée pour la détection peut être comparable, ou supérieure à celle nécessaire à la transmission de données. En général, les techniques d'économie d'énergie se concentrent sur deux parties : la partie réseau (i.e., la gestion d'énergie est prise en compte dans les opérations de chaque nœud, ainsi que dans la conception de protocoles réseau), et la partie détection (i.e., des techniques sont utilisées pour réduire le nombre ou la fréquence de l'échantillonnage coûteux en énergie).

La durée de vie d'un réseau de capteurs peut être prolongée par l'application conjointe de différentes techniques [73]. Par exemple, les protocoles efficaces en énergie visent à réduire au minimum la consommation d'énergie pendant l'activité du réseau. Toutefois, une quantité considérable d'énergie est consommée par les composants d'un

nœud (CPU, radio, etc), même s'ils sont inactifs. Un plan de gestion dédié à l'énergie peut alors être utilisé pour éteindre temporairement les composants du nœud lorsqu'ils ne sont pas sollicités.

5.2.1 Techniques du Duty-cycling

Cette technique est principalement utilisée dans l'activité réseau. Le moyen le plus efficace pour conserver l'énergie est de mettre la radio de l'émetteur en mode veille (low-power) à chaque fois que la communication n'est pas nécessaire. Idéalement, la radio doit être éteinte dès qu'il n'y a plus de données à envoyer et ou à recevoir, et devrait être prête dès qu'un nouveau paquet de données doit être envoyé ou reçu. Ainsi, les nœuds alternent entre périodes actives et sommeil en fonction de l'activité du réseau. Ce comportement est généralement dénommé Duty-cycling. Un Duty-cycle est défini comme étant la fraction de temps où les nœuds sont actifs [69].

Comme les nœuds-capteurs effectuent des tâches en coopération, ils doivent coordonner leurs dates de sommeil et de réveil. Un algorithme d'ordonnancement Sommeil/Réveil accompagne donc tout plan de Duty-cycling. Il s'agit généralement d'un algorithme distribué reposant sur les dates auxquelles des nœuds décident de passer entre l'état actif et l'état sommeil. Il permet aux nœuds voisins d'être actifs en même temps, ce qui rend possible l'échange de paquets, même si les nœuds ont un faible duty-cycle (i.e., ils dorment la plupart du temps).

- **Protocoles Sleep/Wakeup**

Comme mentionné précédemment, un régime sleep/wakeup peut être défini pour un composant donné (i.e. le module Radio) du nœud-capteur. On peut relever les principaux plans sleep/wakeup implantés sous forme de protocoles indépendants au-dessus du protocole MAC (i.e. au niveau de la couche réseau ou de la couche application). Dans le document [74], les protocoles sleep/wakeup sont divisés en trois grandes catégories : à la demande, rendez-vous programmés, régimes asynchrones.

- Les protocoles à la demande utilisent l'approche la plus intuitive pour la gestion d'énergie. L'idée de base est qu'un nœud devrait se réveiller seulement quand un autre nœud veut communiquer avec lui. Le problème principal associé aux régimes à la demande est de savoir comment informer un nœud en sommeil qu'un autre nœud est disposé à communiquer avec lui. À cet effet, ces systèmes utilisent généralement plusieurs radios avec différents compromis entre énergie et performances (i.e. une radio à faible débit et à faible consommation pour la signalisation, et une radio à haut débit

mais à plus forte consommation pour la communication de données). Le protocole STEM (Sparse Topology and Energy Management) [75], par exemple, utilise deux radios ;

- Une autre solution consiste à utiliser une approche de rendez-vous programmés. L'idée est que chaque nœud doit se réveiller en même temps que ses voisins. Typiquement, les nœuds se réveillent suivant un ordonnancement de réveil et restent actifs pendant un court intervalle de temps pour communiquer avec leurs voisins. Ensuite, ils s'endorment jusqu'au prochain rendez-vous ;

- Enfin, un protocole sleep/wakeup asynchrone peut être utilisé. Avec les protocoles asynchrones, un nœud peut se réveiller quand il veut et tant qu'il est capable de communiquer avec ses voisins. Ce but est atteint par des propriétés impliquées dans le régime sleep/wakeup, aucun échange d'informations n'est alors nécessaire entre les nœuds. Quelques régimes sleep/wakeup asynchrones sont proposés dans [76].

• Protocoles du niveau MAC

Plusieurs protocoles MAC pour les réseaux AHWSN ont été proposés, et de nombreux états de l'art et introductions aux protocoles MAC sont disponibles dans la littérature (par exemple, [77]). Nous nous concentrons principalement sur les questions de gestion d'énergie plutôt que sur les méthodes d'accès au canal. La plupart d'entre eux mettent en œuvre un régime avec un faible duty-cycle pour gérer la consommation d'énergie. Nous avons recensés les protocoles MAC les plus communs en les classant en trois catégories : les protocoles fondés sur TDMA, les protocoles utilisant la contention et les protocoles hybrides.

Protocoles MAC reposant sur TDMA

Dans les protocoles MAC fondés sur la méthode TDMA (exemple : [78]) le temps est divisé en trames (périodiques) et chaque trame se compose d'un certain nombre de slots de temps. À chaque nœud est attribué un ou plusieurs slots par trame, selon un certain algorithme d'ordonnancement. Il utilise ces slots pour l'émission/réception de paquets de/vers d'autres nœuds.

Dans de nombreux cas, les nœuds sont regroupés pour former des clusters avec un cluster-head qui est chargé d'attribuer les slots de temps pour les nœuds de son cluster (par exemple, Bluetooth, LEACH, et Energy-aware TDMA-based MAC).

Exemple : un des protocoles TDMA important et efficace en énergie pour les réseaux AHWSN est TRAMA [78]. TRAMA divise le temps en deux parties, une période avec un accès aléatoire et une période avec un accès ordonnancé. La période d'accès

aléatoire est consacrée à la réservation des slots et l'accès au canal est fondé sur la contention. A contrario, la période d'accès ordonnancée est constituée par un certain nombre de slots de temps attribués à un nœud précis.

L'algorithme de réservation des slots est le suivant. Tout d'abord, les nœuds cherchent des informations sur un voisinage à deux sauts, qui sont nécessaires pour établir un ordonnancement sans collisions. Ensuite, les nœuds commencent une procédure d'élection afin d'associer chaque slot à un seul nœud. Chaque nœud aura une priorité pour être le propriétaire d'un slot. Cette priorité est calculée avec une fonction de hachage de l'identifiant du nœud et du numéro du slot. Le nœud avec la plus grande priorité devient le propriétaire du slot. Enfin, les nœuds envoient un paquet de synchronisation contenant la liste des voisins destinataires pour les transmissions suivantes. Par conséquent, les nœuds peuvent se mettre d'accord sur les slots où ils doivent être éveillés. Les slots inutilisés peuvent être annoncés par leurs propriétaires pour être réutilisés par d'autres.

Les protocoles TDMA sont par nature efficaces en énergie, puisque les nœuds n'allument leur radio que lors de leurs propres slots et s'endorment le reste du temps. Toutefois, dans la pratique, les protocoles TDMA ont plusieurs inconvénients qui compensent les avantages en termes d'économie d'énergie [79]. Premièrement, les algorithmes classiques de réservation de slots ont tendance à être complexes, peu flexibles et présentent des problèmes lors du passage à l'échelle. En effet, dans un véritable réseau de capteurs, les changements de topologie sont fréquents (conditions variables du canal, défaillances de nœuds, . . .) et la répartition des slots peut être problématique donc dans de nombreux cas; une approche centralisée peut être adoptée (LEACH). Deuxièmement, ils requièrent une synchronisation très fine et ils sont très sensibles aux interférences. En outre, les protocoles TDMA fonctionnent moins bien que les protocoles avec contention lors d'un trafic faible. C'est pour toutes ces raisons que les protocoles MAC TDMA ne sont pas très fréquemment utilisés dans les réseaux AHWSN.

Protocoles MAC avec contention

Les protocoles avec contention sont les plus populaires et représentent la majorité des protocoles MAC proposés pour les réseaux de capteurs sans fil. Ils assurent le duty-cycle par une intégration étroite des fonctionnalités d'accès au canal avec un régime sleep/wakeup. La seule différence est que, dans ce cas, l'algorithme sleep/wakeup n'est pas un protocole indépendant.

Exemples : un des plus populaires est B-MAC (MAC Berkeley) [80], avec une faible complexité et une faible consommation induite par le système d'exploitation TinyOS. L'objectif de B-MAC est de fournir quelques fonctionnalités de base et un mécanisme efficace en énergie pour l'accès au canal. Il met d'abord en œuvre les caractéristiques de base du contrôle d'accès au canal : un algorithme de backoff, une estimation efficace du canal et des acquittements optionnels. Deuxièmement, pour atteindre un faible duty-cycle, B-MAC utilise un plan sleep/wakeup asynchrone fondé sur l'écoute périodique appelée Low Power Listening (LPL). Les nœuds se réveillent périodiquement pour vérifier l'activité sur le canal. La période entre deux réveils est nommée intervalle de vérification. Après le réveil, les nœuds restent actifs pour un temps de réveil, afin de détecter d'éventuelles transmissions. Contrairement au temps de réveil qui est fixé, l'intervalle de vérification peut être spécifié par l'application. Les paquets B-MAC sont constitués d'un long préambule et d'une charge utile. La durée du préambule est au moins égale à l'intervalle de vérification, afin que chaque nœud puisse toujours détecter une éventuelle transmission au cours de son intervalle de vérification. Cette approche ne nécessite pas que les nœuds soient synchronisés. En fait, quand un nœud détecte l'activité sur le canal, il reste actif et reçoit le préambule en premier puis la charge utile.

Un autre protocole MAC multi-sauts célèbre dans les réseaux de capteurs est S-MAC (Sensor-MAC) [81]. Il adopte un régime de communication avec planification par rendez-vous. Les nœuds échangent des paquets de synchronisation afin de coordonner leurs périodes sleep/wakeup. Chaque nœud peut établir son propre plan ou suivre le plan d'un voisin au moyen d'un algorithme distribué. Les nœuds utilisant le même plan forment un cluster virtuel. Un nœud peut éventuellement suivre deux plans s'ils ne se superposent pas, de sorte qu'il puisse faire un pont de communication entre différents clusters virtuels. Le temps d'accès au canal est divisé en deux parties. Dans la période d'écoute, les nœuds échangent des paquets de synchronisation et des paquets de contrôle pour éviter des collisions. Le transfert de données aura lieu dans le reste de la période. Les nœuds source et destination sont éveillés et communiquent entre eux. Les nœuds qui ne sont pas concernés par cette communication peuvent dormir jusqu'à la prochaine période d'écoute. Pour éviter les latences dans des environnements multi-sauts, S-MAC utilise un plan d'écoute adaptatif.

Les paramètres du protocole S-MAC, i.e. les périodes d'écoute et de sommeil, sont constantes et ne peuvent pas être modifiées après le déploiement. Les auteurs de [82] proposent alors une version améliorée de S-MAC appelée Timeout MAC (T-MAC) et spécialement conçue pour une charge de trafic variable.

Bien que les protocoles MAC fondée sur le duty-cycle soient efficaces en énergie, ils souffrent de la latence du sommeil, i.e., un nœud doit attendre que le récepteur se réveille avant qu'il puisse acheminer un paquet. Cette latence augmente avec le nombre de sauts. En outre, la diffusion de données à partir d'un nœud vers le puits peut connaître un problème d'interruption. En fait, la sensibilité de la radio limite la portée de l'overhearing. Les nœuds en dehors de la portée de l'émetteur ne peuvent donc pas entendre la transmission en cours et se rendorment. C'est pourquoi, dans S-MAC et T-MAC la diffusion de données est limitée à quelques sauts.

IEEE 802.15.4 [83] est un standard à faible débit et à faible puissance pour les réseaux personnels (PAN pour Personal Area Networks). Un PAN est formé d'un PAN coordinator qui gère l'ensemble du réseau et, éventuellement, d'un ou plusieurs coordinateurs qui gèrent les sous-ensembles de nœuds du réseau. D'autres nœuds (ordinaires) doivent s'associer à un coordinateur afin de communiquer.

Les topologies de réseau possibles sont l'étoile (saut unique), le cluster-tree et le mesh (multi-sauts).

Le standard IEEE 802.15.4 prend en charge deux méthodes d'accès aux différents canaux : un mode beacon-enabled et un mode non-beacon enabled. Le mode beacon-enabled fournit un mécanisme de gestion d'énergie sur la base du duty-cycle. Concrètement, il utilise une structure de super-trame qui est délimitée par des balises. D'autres trames de synchronisation sont générées périodiquement par les nœuds coordinateurs. Chaque super-trame consiste en une période active et une période inactive. Dans la période d'activité les dispositifs communiquent avec le coordonnateur auquel ils sont associés. La période active peut être divisée en une période d'accès avec contention (CAP pour Contention Access Period) et une période sans contention (CFP). Au cours de la CAP un algorithme CSMA/CA discrétisé est utilisé pour accéder au canal, tandis que, durant la CFP, un certain nombre de slots garantis (GTS) peuvent être attribués à chaque nœud. Au cours de la période inactive les dispositifs entrent en mode faible puissance pour économiser l'énergie. Dans le mode non-beacon enabled, il n'y a pas de structure en super-trame, i.e. les nœuds sont toujours à l'état actif et utilisent l'algorithme Unslotted CSMA/CA pour l'accès au canal et la transmission de données. Dans ce cas, la conservation d'énergie a lieu au niveau des couches supérieures.

Les protocoles fondés sur la contention sont robustes et garantissent le passage à l'échelle. En outre, ils ont généralement un délai plus faible que ceux reposant sur TDMA et ils peuvent facilement s'adapter aux conditions de trafic. Malheureusement, leur dissipation d'énergie est plus élevée que celle des protocoles TDMA à cause de la

contention et des collisions. Des mécanismes Duty-cycle peuvent contribuer à réduire la surconsommation d'énergie, mais ils doivent être conçus avec soin pour être flexibles et à faible latence.

Protocoles MAC hybrides

L'idée de base des protocoles MAC hybrides (changement du comportement du protocole entre TDMA et CSMA en fonction du niveau de contention) n'est pas nouvelle. Concernant les réseaux WSN, Z-MAC [84] est l'un des protocoles les plus intéressants. Afin de définir le schéma principal du contrôle de transmission, Z-MAC commence par une phase préliminaire de configuration. Chaque nœud construit une liste de voisins à deux sauts par le biais du processus de découverte de voisins. Puis, un algorithme distribué d'attribution des slots est appliqué pour faire en sorte que deux nœuds dans un voisinage à deux sauts ne soient pas affectés au même slot. Par conséquent, on est assuré qu'une transmission d'un nœud avec un de ses voisins à un saut n'interfère pas avec les transmissions de ses voisins à deux sauts.

Z-MAC permet à chaque nœud de maintenir son propre ordonnancement qui dépend du nombre de voisins et évite tout conflit avec ses voisins de contention. Chaque nœud a des informations sur les slots de tous ses voisins à deux sauts et tout le monde se synchronise sur un slot de référence. Après cette phase d'initialisation, les nœuds sont prêts pour l'accès au canal. Les nœuds peuvent être soit en mode faible niveau de contention (LCL pour Low Contention Level), soit en mode haut niveau de contention (HCL pour High Contention Level). Un nœud persiste dans le mode LCL sauf s'il a reçu une notification (ECN pour Explicit Contention Notification). Dans le mode HCL, seuls les propriétaires du slot et leurs voisins à deux sauts sont autorisés à concourir pour l'accès au canal. En LCL (à la fois les propriétaires et les non-propriétaires) peuvent concourir pour transmettre dans n'importe lequel des slots. En revanche les propriétaires ont une priorité sur les autres. De cette façon, Z-MAC peut atteindre un niveau élevé d'utilisation du canal, même en faible contention, car un nœud peut transmettre dès que le canal est disponible.

Les protocoles hybrides tentent de combiner les points forts des protocoles MAC fondés sur TDMA et ceux avec contention tout en compensant leurs faiblesses. Toutefois, ces techniques semblent être complexes pour être réalisables dans un déploiement d'un grand nombre de nœuds.

5.2.2 Principaux Algorithmes de routage utilisés pour la conservation d'énergie

De nombreux algorithmes de routage ont été spécifiquement conçus pour les réseaux AHWSN où la consommation d'énergie est un facteur essentiel. Ce facteur a posé de nombreux défis à la conception et à la gestion des réseaux de capteurs. Ces défis nécessitent une gestion efficace de l'énergie pour toutes les couches de la pile de protocole réseau.

Dans la section précédente nous avons évoqué les différents mécanismes implémentés pour la conservation d'énergie au niveau de la couche MAC. Pour la couche réseau, l'objectif principal de cette partie est de trouver des moyens pour une mise en œuvre efficace de l'énergie et pour une diffusion fiable des données de la source vers la destination, de sorte que la durée de vie du réseau soit maximisée.

Quelques algorithmes ont été développés pour prendre soin du contrôle de la capacité. Certains se concentrent sur l'utilisation effective du temps d'activation des nœuds [85]. L'auteur de [86] a développé un algorithme de diffusion efficace de l'énergie pour les réseaux AHWSN qui porte sur les techniques conservatrices pour diffuser des messages afin que les économies d'énergie puissent être réalisées. Il a souligné également que la technique de routage pour une énergie efficace pourrait améliorer l'efficacité du réseau [48]. Plusieurs paramètres tels que la distance de transmission, le nombre de sauts et le retard ont été pris en compte pour les économies d'énergie dans les réseaux AHWSN. La recherche dans le domaine des protocoles d'énergie efficaces dans ces réseaux est relativement nouvelle. L'objectif principal de tous ces protocoles et algorithmes est de trouver les routes qui sont économes en énergie et donc de maximiser la durée de vie du réseau. Pour atteindre cet objectif, de nombreux protocoles ont été développés. Ces protocoles utilisent des stratégies différentes pour obtenir leurs routes.

Certains de ces protocoles utilisent le clustering, des fonctions, des équations, des arbres de routage optimal, des recherches multi-paths ou un mécanisme efficace pour détourner les trous. Par exemple, le protocole LEACH utilise les clusters-head comme des routeurs pour assurer une communication avec une énergie efficace. Ainsi, l'énergie sera préservée car la communication sera effectuée uniquement entre les clusters-head.

Les algorithmes d'énergie efficace les plus connues sont:

- **L'algorithme de routage « EARLEAHSN »**

L'algorithme Energy Aware Routing for Low Energy Ad Hoc Sensor Networks (EARLEAHSN) [87] utilise un ensemble de sous-chemins optimaux afin d'augmenter la durée de vie du réseau. Ces chemins sont choisis au moyen d'une fonction de probabilité qui dépend de la consommation énergétique de chaque route. La survie du réseau est la

mesure principale de cette approche qui propose d'éviter l'utilisation permanente de la route la plus économe en énergie car cela épuise l'énergie des nœuds sur cette route. Au lieu de cela, l'un des trajets multiples est utilisé avec une certaine probabilité de sorte que la vie entière du réseau se prolonge. Le protocole suppose que chaque nœud est adressable par le biais d'une classe d'adresse qui comprend l'emplacement et les types de nœuds.

- **L'algorithme de routage «EARCBSN »**

L'algorithme Energy-Aware Routing in Cluster-Based Sensor Networks (EARCBSN) [88] propose un algorithme de routage hiérarchique basé sur une architecture à trois niveaux. Les capteurs sont regroupés en clusters avant l'exploitation du réseau. L'algorithme emploie les clusters-head comme des passerelles et ces clusters-head possèdent de l'énergie plus que les autres capteurs et connaissent l'emplacement des tous les capteurs. Le routage nécessite une maintenance d'un cluster-head qui inclut tous les paramètres qui influent sur la décision de routage. Dans cet algorithme, ces paramètres sont l'état du nœud, sa localisation, l'énergie restante et le trafic des messages. Il y a une certaine imprécision dans le modèle d'énergie des passerelles due à la surcharge, la perte des paquets et au retard de propagation des messages [51, 52]. Le nœud passerelle agit comme un gestionnaire de cluster de réseau centralisé qui achemine les routes pour les données des capteurs, qui contrôle la latence dans tout le cluster et qui arbitre les accès entre les capteurs. Le nœud passerelle trace l'utilisation d'énergie de chaque nœud des capteurs et il contrôle aussi les changements dans l'environnement. De plus, il permet de configurer les capteurs et le réseau efficacement afin de prolonger la vie du réseau.

- **L'algorithme de routage « GBR »**

L'algorithme Gradient-Based Routing (GBR) [89] ou le routage par gradient est une version légèrement modifiée de la diffusion dirigée. L'idée de ce protocole est de maintenir le nombre de sauts lorsque le paquet est diffusé à travers le réseau. Ainsi chaque nœud peut découvrir le nombre minimal de sauts jusqu'à la destination. Ce nombre est appelé hauteur du nœud. La différence entre la hauteur d'un nœud et celui de son voisin est considérée comme le gradient sur ce lien. Un paquet est transmis sur un lien avec le gradient le plus grand. Le routage par gradient vise à utiliser certaines techniques auxiliaires telles que l'agrégation des données afin d'équilibrer le trafic de manière uniforme sur le réseau.

Trois techniques différentes pour gérer les données ont été présentées:

- **Stochastic Scheme** : quand il y a deux sauts ou plus avec le même gradient, le nœud choisit l'un d'eux au hasard.
- **Energy-based scheme** : lorsque l'énergie d'un nœud tombe en dessous d'un certain seuil, il augmente sa hauteur afin que les autres capteurs soient découragés d'envoyer des données à ce nœud.
- **Stream-based scheme** : l'idée est de détourner les nouveaux flux à partir de nœuds qui font actuellement partie de la trajectoire des autres filières

Les données s'efforcent alors de parvenir à une répartition égale de la circulation à travers l'ensemble du réseau, ce qui contribue à équilibrer la charge sur les nœuds des capteurs et augmente la durée de vie du réseau. Les techniques employées pour équilibrer la charge de trafic et la fusion de données sont également applicables aux autres protocoles de routage pour des performances améliorées [90].

5.2.3 Conservation d'énergie au niveau transport

Lorsqu'une route a été découverte, le transfert des données est assuré par un protocole de transport. Un protocole de transport dit fiable est responsable de la vérification de la délivrance des données depuis la source vers la destination. Le protocole TCP (Transmission Control Protocol) est le plus communément utilisé pour réaliser cette tâche. Ce protocole, créé pour les réseaux filaires, offre un niveau de performance relativement faible dans les réseaux sans fil. Plusieurs études utilisant des simulations ou expérimentales, quantifient la consommation d'énergie de différentes implémentations du protocole TCP [27].

Les résultats obtenus par Agrawal et al. [91] montrent que les faibles performances de TCP dans un réseau ad hoc multi-sauts sont principalement dues :

- Aux cassures fréquentes des routes,
- Aux délais excessifs lors de l'établissement des routes par les protocoles réactifs,
- A la surcharge du réseau induite par le trafic de contrôle des protocoles de routage.

Par ailleurs, Ahuja et al. [92] observent que les performances du protocole TCP varient en fonction du protocole multi-sauts utilisé. De façon générale, l'utilisation couplée de TCP et d'un protocole proactif offre de meilleures performances comparées à un protocole réactif. Toutefois, les faibles performances de TCP sont principalement dues au fait que TCP réagit de façon inappropriée aux pertes de messages. Les réseaux sans fil souffrent de pertes de paquets dues à un taux d'erreur élevé, résultant des collisions et déconnexions, alors les réseaux filaires sont caractérisés par des pertes moins nombreuses et majoritairement attribuées à la congestion des liens. Il s'ensuit que dans

ces deux types de réseaux, le protocole TCP réagit en faisant appel à des algorithmes de contrôle de congestion inadaptés aux réseaux sans fil. Pour résoudre ce problème, une solution vise à différencier les erreurs dues aux congestions des autres. Holland et al. [93] réalise cette distinction en utilisant un mécanisme

ELN (Explicit Loss Notification) gérant l'envoi de notifications explicites. Ainsi, l'expéditeur n'invoque pas systématiquement des algorithmes de contrôle de congestion.

Zorzi et al. [27] proposent de suspendre la transmission des paquets quand les conditions de communication deviennent difficiles (par exemple, lorsque le taux d'erreur ou le taux de bruit au niveau du canal physique atteint un certain niveau). Ensuite, les transmissions reprennent quand les conditions de communication sont de nouveau satisfaisantes.

D'autres solutions proposent d'adapter le comportement de TCP aux contraintes des environnements sans fil. Plusieurs techniques ont été proposées afin d'améliorer le mécanisme de recouvrement d'erreur. Elles se basent sur une ou plusieurs des approches suivantes :

- L'ajustement dynamique de la taille des fenêtres d'émission de l'expéditeur en fonction des conditions,
- La retransmission rapide des segments manquants,
- Le réajustement dynamique du délai d'attente spécifiant quand un ensemble de paquets doit être renvoyé.

Dans le premier cas, Tsaoussidis et al. [94] observent que le contrôle de la congestion de TCP n'augmente pas assez rapidement la taille des fenêtres de transmission. En fait, la diminution de cette taille est faite rapidement par TCP alors que l'augmentation s'avère être particulièrement lente. Cette technique est efficace dans les réseaux filaires puisqu'elle permet de ne pas aggraver la congestion d'un routeur surchargé. Pour pallier ce problème dans un réseau sans fil, une approche judicieuse vise à augmenter rapidement la taille des fenêtres dès qu'une phase caractérisée par un fort taux d'erreurs prend fin [95]. Dans le deuxième cas, la méthode des SACKs (Selective ACKnowledgment) s'avère la plus adaptée aux réseaux sans fil et réduit efficacement la déperdition énergétique [96]. En effet, cette méthode permet d'identifier de façon précise quels sont les segments de données manquants (non reçus) et limite donc le nombre de retransmissions non nécessaires. Concrètement, le destinataire envoie un SACK correspondant à un accusé de réception dupliqué (c'est-à-dire, envoyé en plus des ACK classiques) lorsqu'il identifie qu'un segment de donnée est manquant. Cet accusé de réception indique quel est le dernier segment de donnée reçu avant le ou les segments

manquants, et le segment immédiatement reçu après le segment manquant. Cette technique permet de notifier rapidement à l'expéditeur que des segments de données sont manquants avant que toutes les données contenues dans une fenêtre ne soient envoyées.

6. Conclusion

Dans ce chapitre, nous avons étalé les principaux aspects liés à la qualité de service (QoS) dans les réseaux AHWSN, si nous voulons que ces derniers soient une continuité des réseaux filaires classiques.

La qualité de service des réseaux AHWSN a été divisée en trois principales échelles : interne, locale et globale, déterminant ainsi les différentes contraintes liées tantôt aux caractéristiques intrinsèques des mobiles, ainsi que le routage des informations au niveau du réseau qui demeure complètement différent par rapport à celui implémenté dans les réseaux filaires (mobilité constante des nœuds).

Bien que les réseaux de capteurs (WSN) forment une section des réseaux AHWSN, nous avons consacré une partie de ce chapitre afin de décrire les différents paramètres liés à la qualité de service lors du déploiement de tels réseaux. Ces paramètres sont liés aux applications de ces capteurs ainsi que la manière dont les informations sont routés à travers le réseau.

Vu que l'axe principale de notre recherche demeure la conservation de l'énergie afin d'optimiser la durée de vie des réseaux AHWSN, nous avons évoqué les différentes techniques et algorithmes qui ont été conçus à cet effet. Une présentation des différentes sources de consommation d'énergie des nœuds a été effectuée, avant de passer en revue les mécanismes déployés à travers toutes les couches du modèle OSI (MAC, Réseau et transport).

Il existe bien évidemment beaucoup d'autres techniques de conservation d'énergie. Par exemple, les paradigmes émanant de l'auto-organisation des systèmes, les mécanismes cross-layers et d'autres protocoles indépendants de niveau réseau ou de niveau applicatif.

Dans la suite de cette thèse, nous allons justement, étaler notre contribution dans le domaine de la conservation de l'énergie au niveau de la couche réseau, en se basant sur un protocole de routage largement utilisé dans le domaine des réseaux AHWSN, en l'occurrence OLSR. La technique utilisée sera de diffuser les informations relatives à

l'énergie résiduelle de chaque nœud et d'utiliser ces informations dans l'élaboration de la table de routage de chaque nœud.

Algorithme d'optimisation de l'énergie dans les réseaux AHWSN

| | | |
|-------|---|-----|
| 1. | Introduction..... | 77 |
| 2. | Le protocole OLSR (Optimized Link State Routing)..... | 77 |
| 2.1 | Relais Multipoints (MPRs)..... | 78 |
| 2.2 | Fonctionnement de l'OLSR..... | 79 |
| 2.3 | Format du paquet OLSR..... | 80 |
| 2.3.1 | Les messages HELLO..... | 81 |
| 2.3.2 | Les messages TC..... | 83 |
| 2.4 | Détection de voisinage..... | 84 |
| 2.5 | Sélection des Relais Multipoints..... | 86 |
| 2.6 | Gestion de la topologie..... | 89 |
| 2.6.1 | Les messages MID..... | 90 |
| 2.6.2 | Les messages HNA..... | 90 |
| 2.6.3 | Le calcul de la table de routage..... | 91 |
| 3. | Motivations et défis..... | 92 |
| 4. | Caractéristiques du simulateur NS-2..... | 92 |
| 4.1 | Fonctionnement de NS-2..... | 94 |
| 4.2 | La mobilité dans NS-2..... | 95 |
| 4.3 | Mouvement des nœuds et génération de topologie dans NS-2..... | 98 |
| 4.4 | Génération du trafic entre les nœuds mobiles..... | 101 |
| 4.5 | Modèles de propagation dans NS-2..... | 102 |
| 4.5.1 | Le modèle de propagation en espace libre (Free space model)..... | 102 |
| 4.5.2 | Le modèle de propagation utilisant deux rayons (Two-ray ground reflection model)..... | 102 |
| 4.5.3 | Le modèle Shadowing..... | 103 |
| 4.6 | Interprétation des résultats dans NS-2..... | 104 |

| | |
|---|-----|
| 5. Protocole OE-OLSR (Optimized Energy – OLSR)..... | 106 |
| 5.1 Sélection des MPRs dans le protocole OE-OLSR..... | 108 |
| 5.2 Messages de contrôle et algorithme d'inondation dans OE-OLSR..... | 110 |
| 5.2.1 Nouveau message HELLO dans OE-OLSR..... | 111 |
| 5.2.2 Nouveau message TC dans OE-OLSR..... | 112 |
| 5.3 Calcul des routes | 112 |
| 6. Simulation des performances du protocole OE-OLSR | 113 |
| 6.1 Métriques d'évaluation..... | 113 |
| 6.1.1 Délai de bout-en-bout..... | 113 |
| 6.1.2 Pourcentage de paquets délivrés | 114 |
| 6.1.3 Nombre de sauts | 114 |
| 6.1.4 Energie Consommée..... | 114 |
| 6.1.5 Le nombre des nœuds morts (dead nodes) | 114 |
| 6.2 Paramètres de simulation | 115 |
| 6.3 Résultats des simulations et discussions | 116 |
| 6.3.1 Nombre de sauts | 116 |
| 6.3.2 Energie totale consommée | 118 |
| 6.3.3 Pourcentage des paquets délivrés (PDR)..... | 119 |
| 7. Discussions et conclusion..... | 120 |

1. Introduction

Dans les chapitres précédents, nous avons évoqué les différents principes relatifs aux réseaux AHWSN. Nous avons aussi étalé les travaux de recherches menés afin d'apporter des améliorations aux contraintes du déploiement de tels réseaux.

Ce qui nous intéresse le plus dans notre travail de recherche, est la contrainte de l'optimisation d'énergie de tels réseaux. Nous nous sommes focalisés sur la couche réseau afin d'étudier les différents protocoles de routage développés pour prendre en charge cette contrainte.

A cet effet, nous avons pris comme modèle de référence le protocole OLSR, très répandu dans les réseaux AHWSN et qui a été défini dans la RFC 3626 de l'IETF, où nous allons introduire un nouveau mécanisme de calcul des relais multipoints MPRs, en se basant sur la diffusion de l'information relative à l'énergie résiduelle de chaque nœud via les paquets de contrôle du protocole.

Dans ce chapitre, et afin d'illuminer l'objet de notre travail de recherche, nous allons décrire en détail le protocole OLSR ainsi que le simulateur utilisé lors de notre recherche (NS2). Ensuite, nous allons démontrer les performances apportées au protocole OLSR basique, en implémentant notre nouvel algorithme d'optimisation d'énergie.

2. Le protocole OLSR (Optimized Link State Routing)

Le groupe de travail MANET (Mobile Ad hoc NETwork) [84] à l'IETF (Internet Engineering Task Force) a normalisé le protocole de routage proactif OLSR dans la « RFC 3626 » [97].

Comme son nom l'indique, OLSR est un protocole à état de lien optimisé; il obtient aussi des routes de plus court chemin. Alors que dans un protocole à état de lien, chaque nœud déclare ses liens directs avec ses voisins à tout le réseau (routage classique), dans le cas d'OLSR, les nœuds ne déclarent qu'une sous-partie de leur voisinage grâce à la technique des relais multipoints.

En effet, ce protocole est classé parmi les protocoles proactifs, sa force se résume dans la mise à jour continue des tables de routage, permettant ainsi la vérification périodique des différentes routes, surtout où le réseau demeure fortement mobile et sa topologie est sujette à des variations continues dues aux déplacements des différents éléments le constituant.

Pour se faire, ce protocole est basé sur la notion des relais multipoints (MPR), qui consistent essentiellement, en un nœud donné, à ignorer un ensemble de liens et de voisins directs, qui sont redondants pour le calcul des routes de plus court chemin : plus précisément, dans l'ensemble des voisins d'un nœud, seul un sous-ensemble de ces voisins est considéré comme pertinent. Il est choisi de façon à pouvoir atteindre tout le voisinage à deux sauts (tous les voisins des voisins).

Le protocole OLSR a été mis en application dans de grands projets. La DARPA a choisi OLSR comme protocole de référence pour les réseaux tactiques. D'autres applications dans le domaine civil ont été réalisées. Avec ce grand développement d'OLSR, de nombreuses extensions de ce protocole sont en chantier, on pourra noter par exemple :

- QOLSR : OLSR avec qualité de service (QoS)
- OLSR v6 : OLSR avec auto-configuration
- MOLSR : Multicast OLSR
- SOLSR : OLSR avec sécurité

2.1 Relais Multipoints (MPRs)

L'idée des MPRs est de minimiser la surcharge due à l'inondation des messages de contrôle par la réduction des retransmissions redondantes dans la même région. Chaque nœud choisit un ensemble de nœuds parmi ses voisins distants d'1 saut (1hop) pour retransmettre ses messages. Cet ensemble est baptisée « MPR set ». Les voisins d'un nœud N qui ne sont pas dans l'ensemble du MPR set, reçoivent et analysent les messages broadcast de ce nœud sans les retransmettre.

Chaque nœud dans l'ensemble du groupe de voisins de deux sauts du nœud N (voisin du voisin mais pas le nœud N), doivent avoir un lien symétrique vers l'ensemble MPR(N).

Chaque nœud maintient l'information sur l'ensemble des voisins qui l'a sélectionné comme MPR. Ce groupe est appelé « MPR selector set ». Cette information est obtenue par la diffusion des messages « HELLO ».

2.2 Fonctionnement d'OLSR

L'OLSR est constitué de deux fonctions :

- **Fonctions principales (core)**, nécessaires pour le bon fonctionnement de l'OLSR dans un réseau Ad-hoc.
- **Fonctions auxiliaires**, permettant l'interopérabilité de l'OLSR avec d'autres domaines de routage (non OLSR) ou la redondance de la topologie du réseau

L'IANA a attribué le port 698, utilisant le protocole UDP pour le transfert des messages de contrôle.

Les fonctions principales du protocole sont :

- Format du paquet
- Ecoute du lien (link sensing) – via des messages HELLO
- Détection du voisinage réseau – via des messages MID
- Sélection du MPR
- Diffusion des messages de contrôle de topologie – Messages TC
- Calcul des routes et constitution de la table de routage

Les fonctions auxiliaires du protocole sont :

- interopérabilité avec les interfaces non OLSR
- Notification de la couche liaison (pour mettre à jour les liens physiques)
- Redondance de la topologie
- Redondance du groupe des MPRs

La diffusion d'un message, à tout le réseau, par répétition, peut se faire par l'inondation classique utilisant la règle : « un nœud retransmet un message si et seulement si il ne l'a pas déjà reçu ». La diffusion par relais multipoints, diminue le nombre de retransmissions en utilisant la règle suivante : un nœud retransmet un message si et seulement si :

- 1) il ne l'avait pas déjà reçu, et
- 2) il vient de le recevoir d'un nœud dont il est un relais multipoint.

La figure suivante, donne un exemple de gain en nombre de retransmissions via un graphe simple. Supposons qu'un nœud émette un message, et que pour diffuser cette information au réseau ses voisins répètent cette dernière. Dans l'image, à gauche, où tous les voisins d'un nœud retransmettent, six répétitions (les nœuds en noirs) sont nécessaires. Par contre, en utilisant la retransmission par les relais multipoints seuls (à droite), on économise deux retransmissions.



Figure 3.1 : Intérêt de l'implémentation des MPRs

2.3 Format du paquet OLSR

Afin d'assurer la compatibilité du protocole OLSR avec UDP ainsi qu'IPv4 (V6), le format du paquet est uniforme. Le protocole OLSR définit un format général du paquet, illustré par la figure 3.2. Ce format est unique pour tous les messages circulant sur le réseau. En plus des messages d'échange de trafic de contrôle HELLO et TC (Topology Control), le protocole OLSR propose deux autres types différents de messages : MID (Multiple Interface Declaration) et HNA (Host and Network Association).

Chaque paquet peut contenir plusieurs messages identifiés par un type. Ceci permet d'envoyer plusieurs informations à un nœud en une seule transmission. Selon la taille de MTU (Maximum Transfer Unit), un nœud peut ajouter différents messages et les transmet ensemble. Par conséquent différents types de messages peuvent être émis à la fois, mais traités et retransmis différemment dans chaque nœud. Quand ce dernier reçoit un paquet, il examine les entêtes des messages et en détermine le type selon la valeur du champ « message type ».

Dans OLSR, un message du control individuel est uniquement identifié par une adresse initiale (Originator address) et son numéro de séquence MSN (Message Sequence Number). Le champ « Originator address » indique la source d'un message, par contre le champ MSN nous permet d'éviter le traitement et relayage multiple de ce même message pour un nœud.

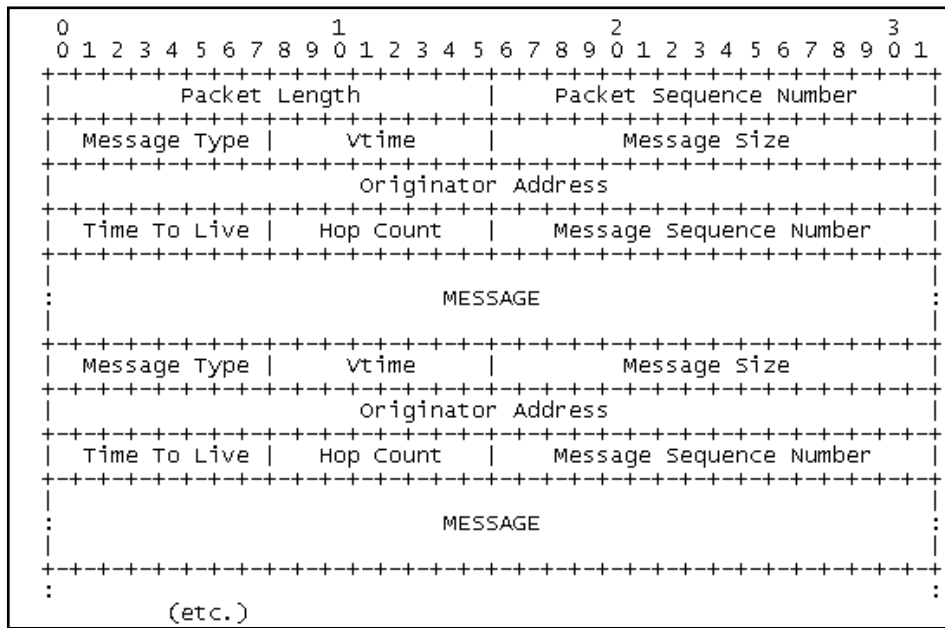


Figure 3.2 : Format du paquet OLSR

2.3.1 Les messages HELLO

Un mécanisme commun est employé pour l'échange des informations relatives à l'état du lien ainsi que la découverte du voisinage d'un nœud via l'échange périodique des messages HELLO.

Le format de ces derniers est comme suit :

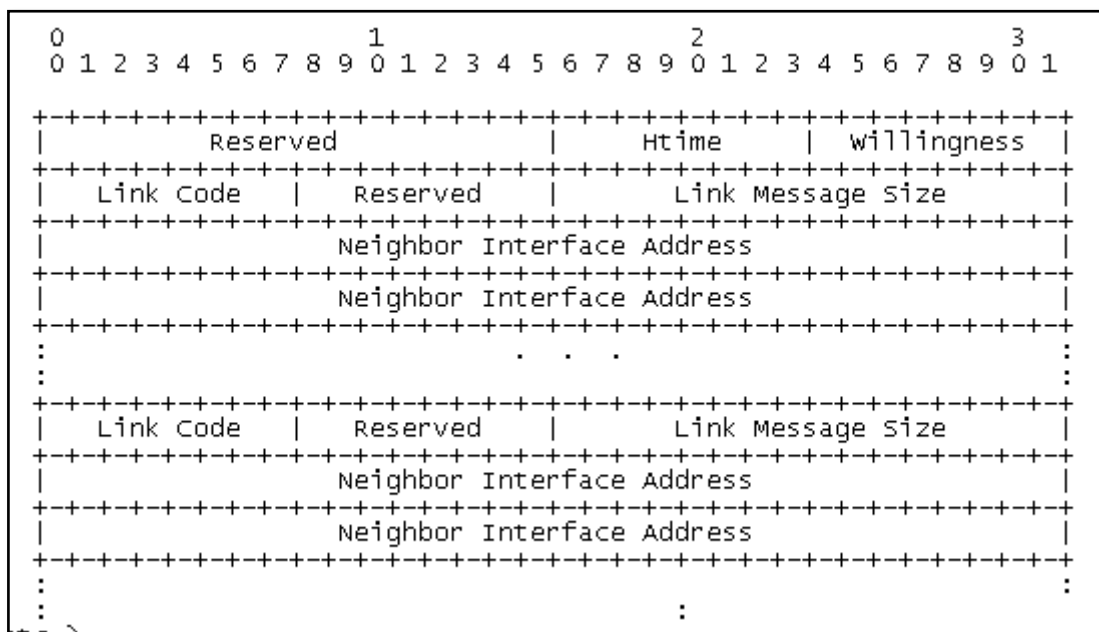


Figure 3.3 : Format du message « Hello »

- **Reserved**

Ce champ doit être rempli par « 0000000000000000 », signifiant que le champ n'est pas encore utilisé, il est réservé pour une future utilisation.

Nota : Ce champ sera utilisé dans notre recherche afin de transmettre les informations relatives à l'énergie résiduelle de chaque nœud.

- **H-Time**

Ce champ spécifie l'intervalle d'émission des messages HELLO, employé par le nœud sur chaque interface particulière, cet intervalle est représenté par sa mantisse (quatre bits les plus forts du champ H-Time et par son exposant (quatre bits les moins significatifs).

- **Willingness**

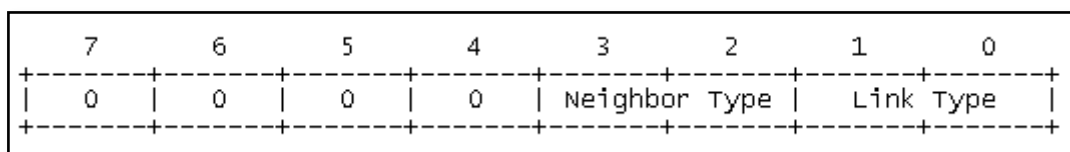
Ce champ spécifie la capacité du nœud à router les paquets vers les destinataires, il est configuré de la manière suivante:

| | |
|--------------|-----|
| WILL_NEVER | = 0 |
| WILL_LOW | = 1 |
| WILL_DEFAULT | = 3 |
| WILL_HIGH | = 6 |
| WILL_ALWAYS | = 7 |

Le champ 'Willingness' peut prendre n'importe quelle valeur entre 0 et 7; d'où WILL_NEVER signifie qu'il est impossible que ce nœud soit sélectionné pour router les paquets vers les autres destinataires, tandis que WILL_ALWAYS veut dire que ce nœud doit toujours être sélectionné pour router les paquets vers les autres destinataires. Aussi ce champ sera communément utilisé dans notre algorithme proposé dans le chapitre 4.

- **Link-Code**

Le champ *Link Code* de taille 8 bits, contient à la fois les informations concernant les liens vers les nœuds voisins et le type de ces derniers.



A travers des valeurs fournies par le champ Link code, un lien peut être soit symétrique ou asymétrique ou perdu.

Aussi, un voisin peut avoir au moins un lien symétrique avec le nœud concerné, comme un voisin peut être désigné dans le groupe des MPRs de ce nœud.

- **Link Message Size**

Le champ de 'Link Message Size' spécifie la taille du message, contenu entre deux champs 'Link Code'.

La génération d'un message HELLO est basée sur les informations contenues dans la base d'information du lien local de chaque nœud. Pour chaque interface, ce message contiendra une liste des liens sur cette interface ainsi qu'une liste de tout le voisinage qui y est associé. La règle retenue afin de rafraichir ces informations est que chaque lien et chaque voisin doivent être listés au moins une fois durant le laps de temps baptisé REFRECH_INTERVAL.

Afin de mettre à jour les changements rapides de la topologie du réseau, un message HELLO est émis au moins une fois durant un intervalle de temps baptisé HELLO_INTERVAL défini par la RFC-3626 par 02 secondes.

Le message HELLO concerne l'information entre l'interface du nœud ainsi que celle du voisin. Donc, il ne doit jamais être transféré par le nœud voisin.

Des algorithmes sont proposés dans la RFC 3626 pour chaque scénario suivant :

- Ecoute et détection de l'état du lien
- Détection du voisinage
- Détection des voisin distants de 02 sauts (02-hop neighbors)

2.3.2 Les messages TC

Les messages « TC » «Topology Control » déclarent les sous-ensembles de voisinage que constituent les relais multipoints. Ils sont diffusés en utilisant une diffusion optimisée par relais multipoints.

Ces messages permettent à chaque nœud de maintenir à jour sa table d'information sur la topologie et ainsi faciliter le calcul de sa table de routage.

Le format des messages TC est comme le suivant :

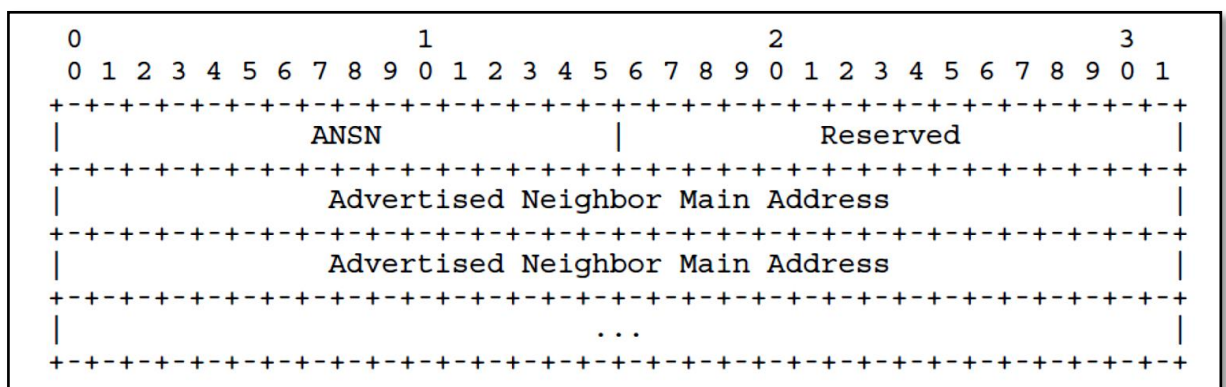


Figure 3.4 : Format des messages TC

- ANSN (Advertised Neighbor Sequence Number)

Les numéros de séquence (Sequence Number), permettent de déterminer les routes les plus récentes ou autrement dit les plus fraîches (fresh routes), un nœud met à jour

cet ensemble de routes chaque fois qu'il détecte un nouveau changement dans son voisinage, puis il incrémente son propre numéro de séquence. Ce numéro est envoyé dans le champ (ANSN) du message TC, et lorsqu'un nœud reçoit ce message, il peut décider si les informations transmises sont plus récentes que de celles qui existent.

OLSR utilise les principes de numéro de séquence afin d'éviter le problème des boucles infinies et des transmissions inutiles des messages sur le réseau, en plus il permet de maintenir la consistance des informations de routage. A cause de la mobilité des nœuds, les routes changent fréquemment ce qui fait que les routes maintenues par certains nœuds, deviennent invalides.

- **Reserved**

Ce champ doit être rempli par « 0000000000000000 », signifiant que le champ n'est pas utilisé, il est réservé pour future utilisation.

- **Advertised Neighbor Main Address**

Ce champ contient l'adresse de l'interface principale du nœud, Cet adresse sera envoyée par le message Topology control (TC).

2.4 Détection de voisinage

Chaque nœud doit détecter toutes les interfaces de ses voisins ayant un lien direct et symétrique avec l'une de ses interfaces. En raison de l'incertitude de la propagation radio, le lien entre deux nœuds voisins peut être unidirectionnel. Les liens doivent donc être vérifiés dans les deux sens avant de les considérer comme valides. Alors, chaque nœud doit diffuser périodiquement un message Hello dans son voisinage direct. Ce message contient les informations relatives aux interfaces reliées à ce nœud : la liste des adresses des interfaces des nœuds voisins avec leurs états de lien. Un lien entre les interfaces d'un nœud et son voisin peut avoir l'un des trois états suivants: « symétrique », « asymétrique », ou « perdu ».

Symétrique : signifie que le lien est validé comme bidirectionnel est qu'il est possible de transmettre des données dans les deux sens.

Asymétrique : signifie que le nœud détecte l'interface de son voisin mais le lien n'est pas encore validé dans l'autre sens.

Perdu : Un lien est dit perdu si ce lien a été déclaré précédemment étant symétrique ou asymétrique mais à ce moment aucun message n'est reçu du nœud voisin via ce lien.

Les informations de voisinage sont maintenues dans une base d'information contenant les voisins directs et leurs interfaces multiples, les voisins à deux sauts, les relais multipoints et les sélecteurs de relais multipoint.

La figure 3.5 montre un exemple de détection de voisinage. Chacun des nœuds possède une seule interface sans fil. Il est nécessaire qu'un nœud possédant plusieurs interfaces, de sélectionner l'adresse d'une de ses interfaces comme son adresse principale.

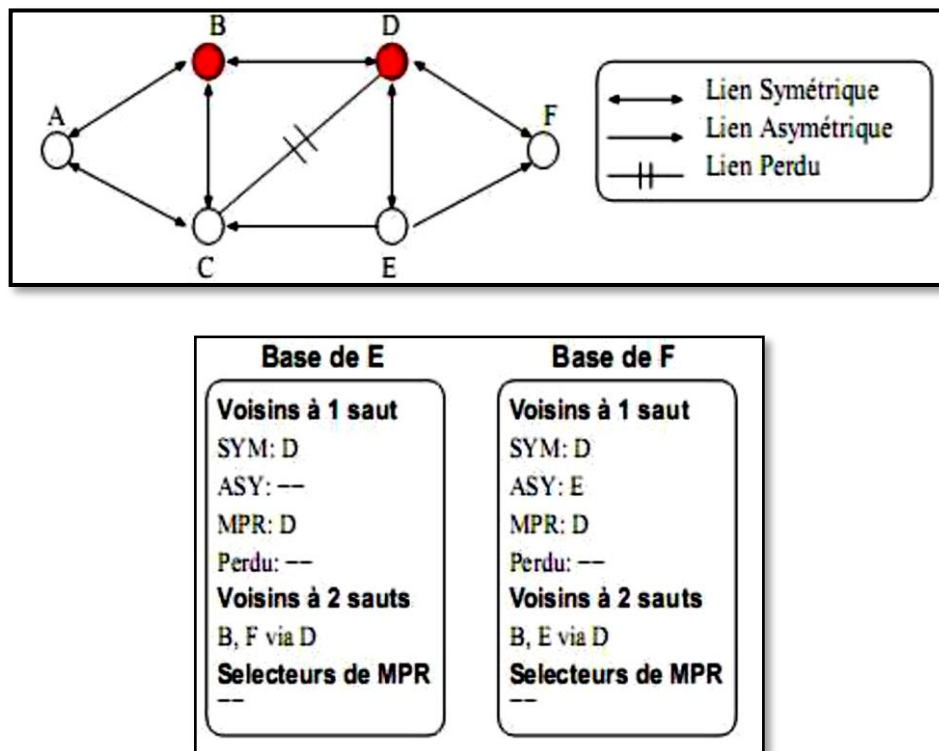


Figure 3.5 : Exemple d'information de voisinage maintenue par OLSR

La Figure 3.6 décrit le processus de découverte des voisins entre deux nœuds A et B. En premier, le nœud A envoie à B un message HELLO qui ne contient aucune information. Une fois B reçoit ce message, il enregistre A comme voisin asymétrique car B ne trouve pas son adresse dans le message. Le nœud B envoie par la suite un message HELLO déclarant qu'il entend A. Ce dernier trouve son adresse dans le message et enregistre B comme voisin symétrique. À son tour, B trouve son adresse dans le message HELLO de A et déclare ce dernier comme voisin symétrique.

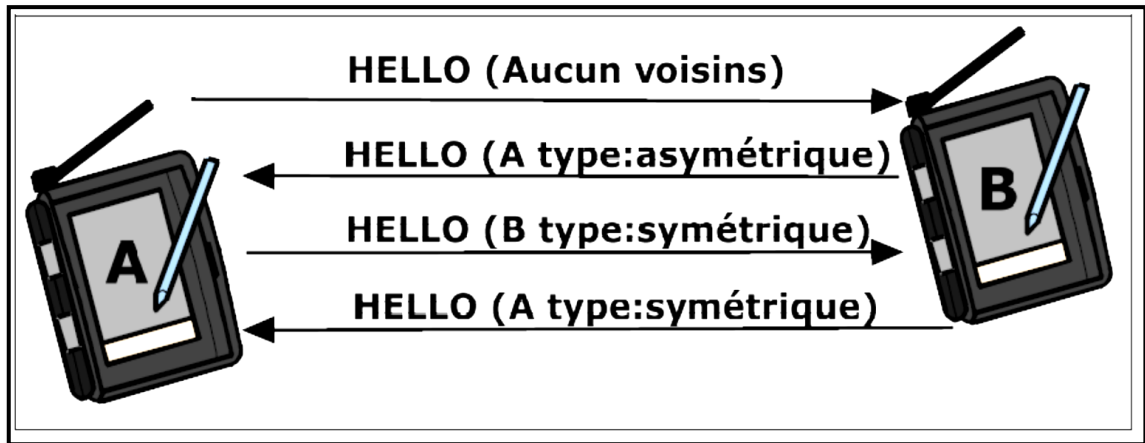


Figure 3.6 : Echange des messages HELLO

L'ensemble des voisins immédiats (ou à 1-saut) d'un nœud s et qui possèdent un lien symétrique avec ce dernier est noté $N1(s)$. Les voisins à 2-sauts d'un nœud s sont définis comme étant l'ensemble suivant :

$$N2(s) = \{y | y \neq s \wedge (\exists x \in N1(s)) [y \in N1(x)]\}$$

Ces deux ensembles $N1(s)$ et $N2(s)$ de chaque nœud s sont construits grâce aux échanges périodiques des messages HELLO. Ceci permet à tous les nœuds d'avoir une vision à 1-saut et à 2-sauts sur la topologie du réseau et ainsi avoir toutes les informations nécessaires pour construire les chemins entre une source et une destination dans la zone à 1-saut et à 2-sauts.

Les messages HELLO sont diffusés sur toutes les interfaces du nœud émetteur et ils sont reçus par tous les voisins qui se trouvent à un saut de ce nœud. Ces messages sont envoyés avec une fréquence déterminée par l'intervalle Hello_Interval (la valeur par défaut est de 2 secondes). Les voisins qui reçoivent ces messages, les traitent et ne les relaient pas. Les messages HELLO permettent également de découvrir les voisins à deux sauts (c'est-à-dire, les voisins des voisins). Les informations de voisinage fournies par ces messages sont valides pendant une durée de vie Neighbor_Hold_time qui est égale à $3 \times \text{Hello_Interval}$. Une approche simple permettant de détecter la non-validité d'un lien OLSR est la perte de 3 Hellos successifs, mais d'autres techniques peuvent être utilisées dans OLSR.

2.5 Sélection des Relais Multipoints

La technique d'inondation est utilisée dans plusieurs algorithmes de routage pour la diffusion des messages à tous les nœuds dans un réseau. Avec cette technique, chaque nœud renvoie une copie du message qu'il reçoit pour la première fois à tous ces voisins immédiats. Ce mécanisme a un impact sur les ressources du réseau en termes de bande

passante et de consommation d'énergie. Or, les réseaux Ad-Hoc ont des ressources limitées et les enjeux de performance sont capitaux.

Dans ce contexte, le protocole OLSR utilise une technique appelée inondation par relais multipoint pour optimiser la diffusion à travers le réseau et ainsi réduire la charge du trafic. Ainsi, chaque nœud « s » sélectionne un sous ensemble de points appelés MPR (Multipoint Relay) parmi ses voisins de $N1(s)$ et qui lui permettent d'être rejoint par tous les nœuds dans $N2(s)$. Or, la connaissance de $N1(s)$ et $N2(s)$ de chaque nœud s permet la diffusion des messages dans tout le réseau. L'échange périodique des messages HELLO permet à chaque nœud dans le réseau de mettre à jour ses ensembles $N1(s)$ et $N2(s)$. C'est ainsi que l'ensemble des relais multipoints est recalculé à chaque changement dans la topologie du réseau.

L'ensemble $MPR(s)$ des relais multipoints d'un nœud s forme un arbre recouvrant et il est défini de la manière suivante :

$$MPR(s) \subseteq N1(s)$$
$$(\forall y \in N2(s)) (\exists x \in MPR(s)[y \in N1(s)])$$

La Figure 3.7 montre la différence entre l'inondation par relais multipoints et l'inondation classique. On remarque que dans le cas classique, il faut 24 retransmissions pour atteindre les nœuds à 3-sauts du nœud s. Alors que dans le cas où on utilise les relais multipoints, seulement 11 retransmissions sont nécessaires pour avoir les mêmes résultats.

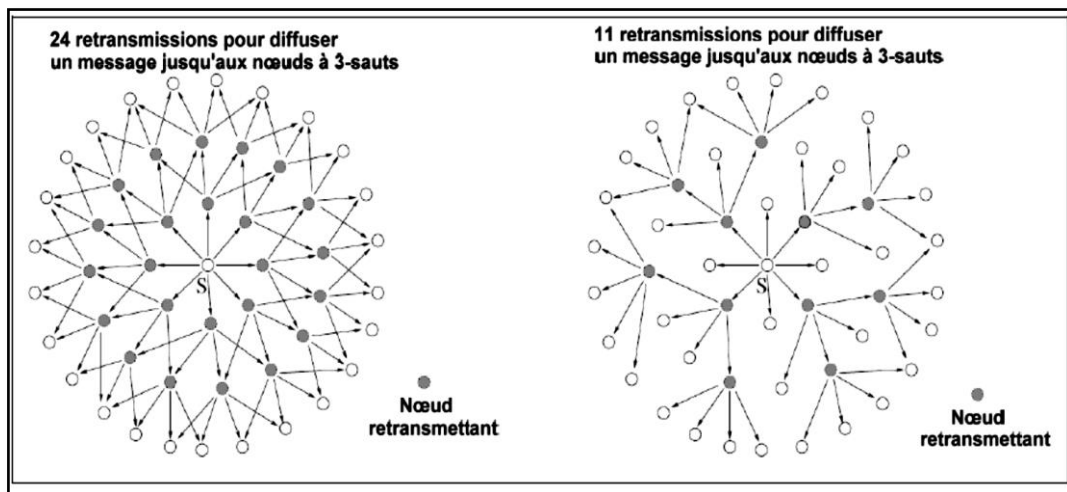


Figure 3.7 : Diffusion par inondation classique vs inondation par relais multipoints

Dans un cas général, pour atteindre le voisinage $N2(s)$ d'un nœud s, il faut $MPR(s)+1$ émissions. Donc pour minimiser le nombre d'émissions possibles dans le réseau et par la suite augmenter les performances, il faut trouver un nombre minimal de relais multipoints pour chaque nœud (c.-à-d., minimum de $MPR(s)$). Or ce problème du

choix des MPR est un problème NP-complet car ceci est équivalent à calculer un sous ensemble dominant dans un graphe. Plusieurs heuristiques ont été proposées à cet effet dans plusieurs articles.

```

Données : Tout nœud  $s$  avec ses voisins  $N_1(s)$  et  $N_2(s)$ .
Résultat : L'ensemble  $MPR(s)$ .

début
   $MPR(s) \leftarrow \emptyset$ ;
  Trouver les nœuds isolés dans  $N_2(s)$  qui sont
  couverts par un seul nœud dans  $N_1(s)$ ;
  pour tout nœud  $y$  dans  $N_2(s)$  isolé faire
    Soit  $x \in N_1(s)$  le seul voisin de ce nœud  $y$ ;
    Ajouter  $x$  à  $MPR(s)$ ;
    Éliminer tous les nœuds dans  $N_2(s)$  couverts par
     $x$ ;
  fin
  tant que  $N_2(s) \neq \emptyset$  faire
    Trouver  $x \in N_1(s)$  tq
    •  $x$  couvre le maximum des nœuds dans  $N_2(s)$ ;
    •  $x$  a le maximum des voisins ;
    Ajouter  $x$  à  $MPR(s)$ ;
    Éliminer tous les nœuds dans  $N_2(s)$  couverts par
     $x$ ;
  fin
fin
  
```

Algorithme 3.1: Sélection des MPR par OLSR (RFC3626)

Dans la suite de cette thèse, seul l'algorithme présenté dans le RFC3626 sera considéré. Cette heuristique de sélection des MPR est présentée dans l'Algorithme 3.1.

La Figure 3.8 présente un exemple d'application de l'algorithme décrit précédemment pour la sélection de l'ensemble des relais multipoints MPR(s) d'un nœud « s ».

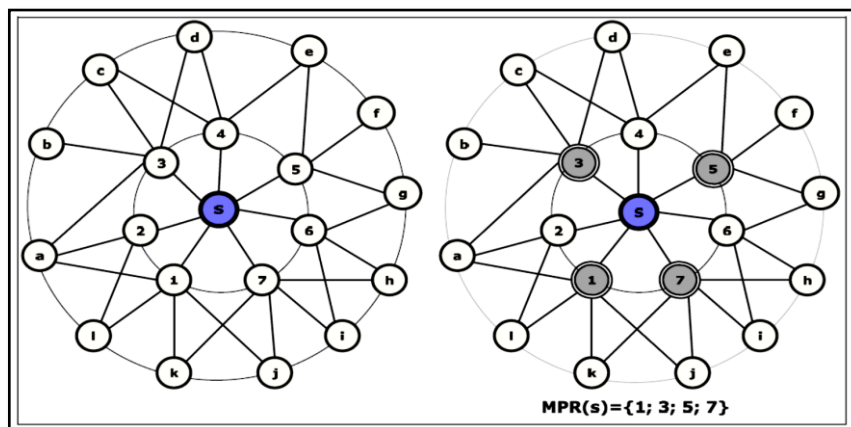


Figure 3.8 : Exemple de sélection des relais multipoints

2.6 Gestion de la topologie

L'Algorithme 3.1 est utilisé par chaque nœud dans le réseau pour construire l'ensemble des relais multipoints. Afin de fournir les informations nécessaires sur la topologie pour construire les routes et ainsi garantir le routage des paquets, Chaque nœud sélectionné comme relais multipoint (MPR) dans le réseau diffuse périodiquement à tous les nœuds du réseau des messages de topologie, appelés Topology Control (TC) avec une fréquence déterminée par l'intervalle TC_Interval. Un message TC contient les nœuds ayant sélectionné le nœud « s » origine du TC comme relais multipoint et un numéro de séquence associé à l'ensemble des sélecteurs de relais multipoint qui sera incrémenté à chaque changement de cet ensemble. Uniquement les nœuds MPRs ont le droit de rediffuser les TCs. La réception de ces messages TCs, permet à chaque nœud dans le réseau de maintenir une base contenant les informations topologiques du réseau qui donne une vision globale (mais non pas entière) de la topologie du réseau. Cette base est constituée d'un ensemble de tuples [T_dest, T_last, T_seq, T_time]. T_dest est l'adresse principale de la destination, qui est accessible en un saut à partir du nœud avec l'adresse principale T_last. En d'autre terme, T_last est un relais multipoint de T_dest. T_seq est un numéro de séquence et T_time spécifie le temps au bout duquel le tuple est expiré. La figure 3.9 montre la base topologique de l'ensemble des nœuds du réseau ad-hoc de la figure 3.4.

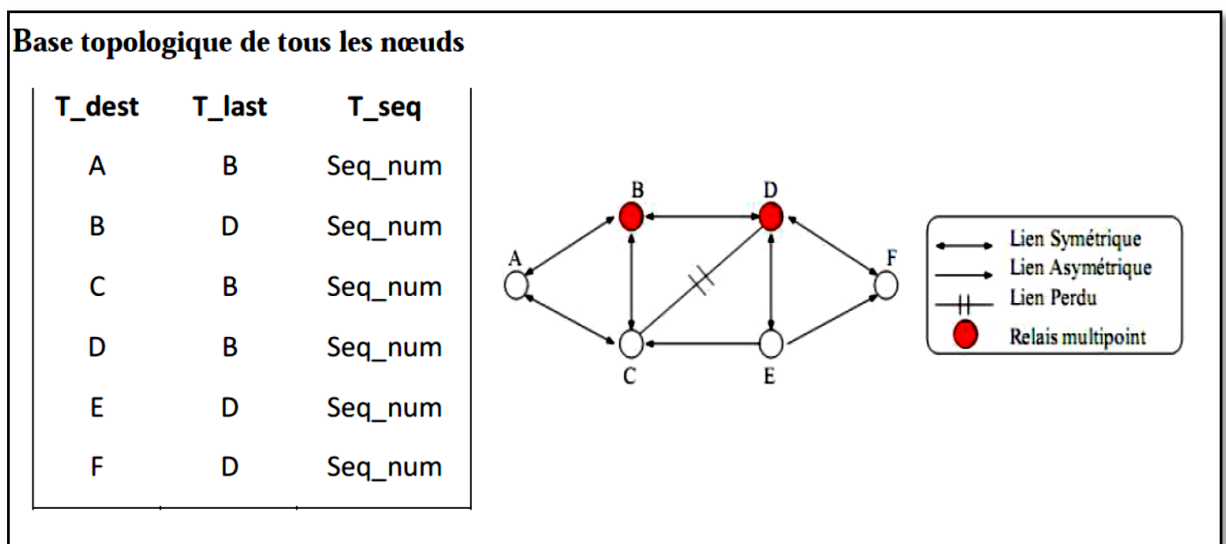


Figure 3.9 : Optimisation de l'inondation par des relais multipoint.

Le protocole OLSR propose deux autres types différents de messages : MID (Multiple Interface Declaration) et HNA (Host and Network Association).

2.6.1 Les messages MID

Les messages MID (Multiple Interface Declaration) sont émis que par un nœud ayant des interfaces OLSR multiples, afin d'annoncer au réseau des informations sur la configuration de ses interfaces. Un message MID contient une liste d'adresses, L'adresse I_if_addr correspond à une des interfaces du nœud, ainsi que I_main_addr est son adresse principale. La diffusion de ces messages se fait par les relais multipoints afin de minimiser le nombre de messages circulants sur le réseau.

Le format des messages MID est comme le suivant :

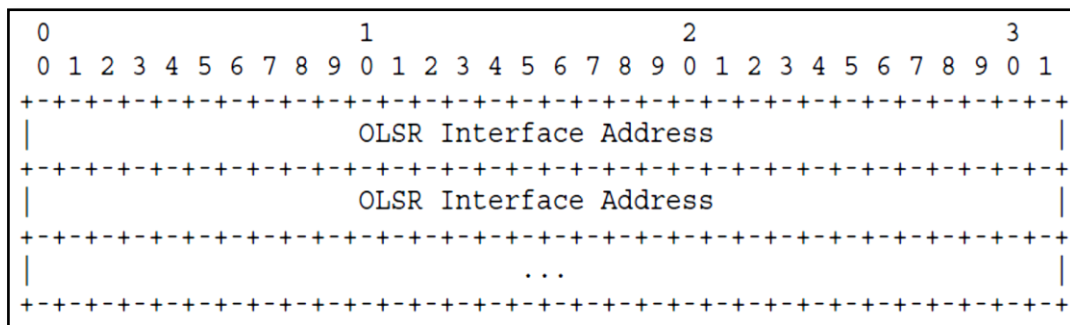


Figure 3.10 : Format des messages MID

2.6.2 Les messages HNA

Les messages HNA (Host and network Association), ne sont émis que par un nœud possédant des interfaces non-MANET multiples, dont le but est de fournir la connectivité d'un réseau OLSR à un réseau non OLSR. Le nœud passerelle émet des messages HNA contenant une liste des adresses des réseaux associés et de leurs masques du réseau (netmasks). Ainsi, les nœuds se trouvant dans les réseaux MANET vont construire des tuples pour tous les nœuds passerelles où chaque tuple contient :

- A_getway_addr : adresse principale du nœud passerelle.
- A_network_addr : adresse de sous réseau.
- A_netmask : adresse du masque du réseau.
- A_time : la durée de tuple.

Le format des messages HNA est illustré dans la figure 3.11 :

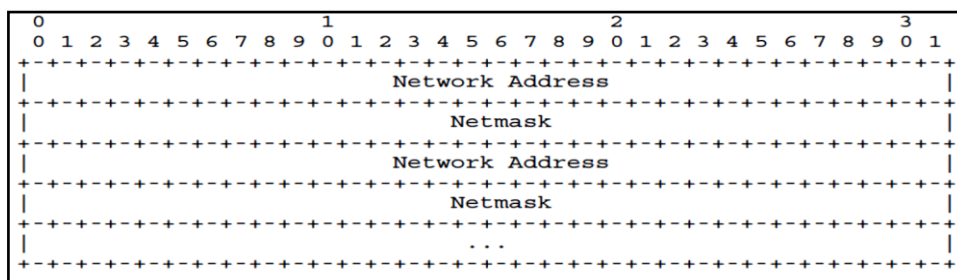


Figure 3.11 : Format des messages HNA

2.6.3 Le calcul de la table de routage

Chaque nœud maintient une table de routage qui lui permet d'acheminer les paquets vers un destinataire. Ces tables sont calculées grâce à l'algorithme du plus court chemin de Dijkstra (Dijkstra, 1959) en se basant sur les informations conservées par les nœuds et celles fournies par les messages de contrôle TC.

Ces tables de routage sont recalculées à chaque changement survenu dans la topologie afin de permettre de mettre à jour les routes vers toutes les destinations dans le réseau.

Le tableau 3.1 illustre la table de routage associée au nœud A de l'exemple de la Figure 3.12:

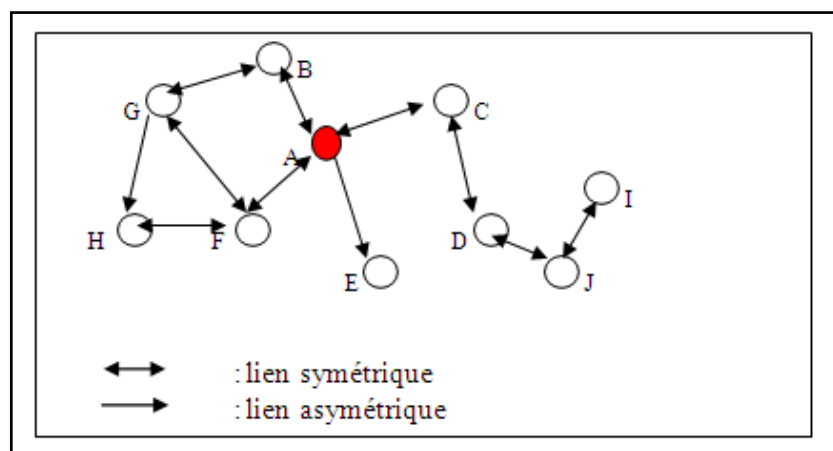


Figure 3.12 Réseau MANET

| Nœuds destinataire | Nœud du dernier saut | Numéro de séquence | Durée de vie |
|--------------------|----------------------|--------------------|--------------|
| B | Direct | 1 | IF A |
| C | Direct | 1 | IF A |
| D | C | 2 | IF A |
| E | Direct | 1 | IF A |
| F | Direct | 1 | IF A |
| G | B | 2 | IF A |
| G | F | 2 | IF A |
| H | F | 2 | IF A |
| I | C | 4 | IF A |
| J | C | 3 | IF A |

Tableau 3.1 : Table topologique du nœud A

3 Motivations et défis

La présentation précédente du protocole de routage OLSR montre que ce dernier offre des fonctionnalités très intéressantes pour les réseaux AHWSN, tout en recherchant des routes optimales en termes de nombre de sauts. Utilisant la technique de sélection des MPR, OLSR diminue au maximum le nombre de messages de contrôle transmis sur le réseau, Aussi, il gère convenablement la topologie du réseau, en diffusant périodiquement des messages TC. Il peut aussi contrôler l'utilisation multiple des interfaces (messages MID) pour chaque nœud et la possibilité de communication entre un réseau MANET et un réseau filaire (messages HNA).

Toutefois, l'OLSR basique montre une vulnérabilité perceptible en termes de sécurité, qui a fait objet de plusieurs thèmes de recherches dans ce domaine. Un autre problème très important est celui de la consommation d'énergie, Le protocole OLSR, ne considère pas la consommation d'énergie comme un critère prépondérant dans la gestion de la topologie du réseau et le calcul des MPRs. Les nœuds du réseau sont généralement alimentés par des piles de capacité limitée, d'où la nécessité de prendre en considération ce paramètre lors du développement d'un protocole de routage à qualité de service. A cet effet, plusieurs travaux de recherche sont apparus avec un objectif : optimiser la consommation énergétique des nœuds à travers l'utilisation de techniques de conservation innovantes afin d'améliorer les performances du réseau et la maximisation de sa durée de vie, d'où notre objet de recherche.

Dans ce qui suit nous allons proposer une nouvelle solution pour optimiser la consommation d'énergie dans le protocole OLSR visant à améliorer la performance de ce protocole en faisant des compromis entre différentes activités aussi bien au niveau du nœud qu'au niveau du réseau.

Ces performances seront quantifiées et démontrées dans les sections suivantes, en se basant sur le simulateur NS2, très répandu dans le domaine des réseaux AHWSN.

4 Caractéristiques du simulateur NS-2

Tester et comparer le fonctionnement des protocoles de routage dans les réseaux AHWSN pose un problème pratique. Cela nécessiterait de posséder un grand nombre d'unités mobiles (ordinateurs portables). En deçà d'une vingtaine d'unités, le routage est une opération simple et il y a fort à parier que les différents protocoles étudiés ne présenteront que des différences de fonctionnement minimales dans ce contexte. Par

ailleurs, il conviendrait dans l'idéal que des utilisateurs manipulent et déplacent ces ordinateurs, sous peine de devoir se restreindre à n'étudier que des réseaux statiques.

Une manière plus pratique et moins couteuse consiste à utiliser un simulateur ; autrement dit un logiciel capable de reproduire les principales caractéristiques d'un réseau ad hoc et le faire évoluer virtuellement.

Un tel logiciel doit donc être capable de simuler :

- Le mouvement d'unités mobiles dans un environnement physique (comportant éventuellement des obstacles);
- La capacité à recevoir et émettre des ondes, à créer des interférences;
- Les diverses protocoles liées à la communication en réseau, notamment au niveau :
 - Physique (forme des ondes, modulation),
 - Liaison de données (protocole de politesse, de gestion de collision, type 802.11, 802.16, etc),
 - Routage (la partie qui nous intéresse),
 - Transport (gestion des échanges du début à la fin, notamment par utilisation de message d'acquittement et par modulation du trafic),
 - Applicatif (création et consommation de flux de données).

Un simulateur adapté doit par ailleurs pré-intégrer les protocoles de routage ad hoc les plus courants, à savoir DSDV, OLSR, DSR, AODV. [98]

Le simulateur NS-2 est un outil logiciel pour évaluer les performances d'un réseau informatique. Il est bâti sur les idées de la conception par objet, de réutilisation du code et de modularité. Il est devenu aujourd'hui un standard de référence dans ce domaine [99]. Il est du domaine public, disponible sur Internet et son utilisation est gratuite. Il est exécutable tant sous Unix que sous Windows.

NS2 est un simulateur à événements discrets développé dans le but de la recherche. Il est orienté objet (écrit en C++ et en oTCL), et il est fourni avec des outils d'analyse complémentaires eux-mêmes écrits en C/C++ ou TCL/Tk. NS-2 fournit un environnement permettant de réaliser des simulations entre autre des protocoles IP, TCP, routage et des protocoles multicast dans les réseaux filaires ainsi que dans les réseaux sans fil, avec support de la mobilité des nœuds. Network Simulator 2 a été originellement développé étant que variante du "REAL network simulator" en 1989, et a considérablement évolué au cours des années. En 1995, NS-2 était développé par le projet VINT (collaboration des chercheurs à UC Berkeley, LBL, USC/ISI et Xerox

PARC). Actuellement, son développement est supporté par le DARPA à travers SAMAN et par la NSF à travers CONSER, tout en incluant de nombreuses contributions extérieures, comme en particulier les codes pour les réseaux sans fil des projets Daedalus de l'UCB et Monarch de la CMU et de Sun Microsystems.

La mise en œuvre d'une simulation se fait via une étape qui décrit la topologie du réseau (la mobilité) et le comportement de ses composants (le trafic), puis vient l'étape de simulation proprement dite et enfin l'interprétation des résultats en utilisant un langage approprié. Dans notre cas, un script en java pour l'extraction de données, et des outils pour la visualisation de ces résultats (Figure 3.13).

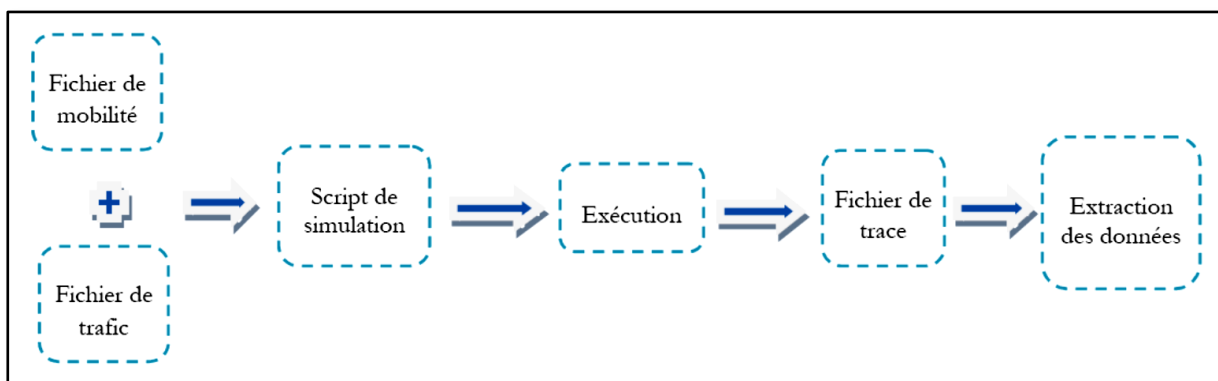


Figure 3.13 : Processus de simulation dans NS2

4.1 Fonctionnement de NS-2

NS2 est un simulateur à événements discrets : l'ensemble des changements d'état du système simulé se produit en des instants (sans durée) repartis sur un axe temporel. Par ailleurs, les simulations ne se font pas en temps réel. Le simulateur gère un temps propre sur lequel sont placés les différents événements. Le traitement de ces derniers se fait dans l'ordre de placement sur l'axe temporel de la simulation et permet de séparer le passé (les événements déjà traités), le présent (l'évènement en cours de traitement) et le futur (les événements restant à traiter). Les événements traités provoquent l'apparition de nouveaux événements dans le futur, ce qui reproduit les relations de causalité. La dissociation entre temps réel et temps de simulation, si elle a l'inconvénient d'empêcher une visualisation "directe" du fonctionnement du réseau, garantit néanmoins l'indépendance de la simulation vis-à-vis de la rapidité et de la puissance de calcul de l'ordinateur sur lequel elle est effectuée.

L'utilisation de NS-2 pour un scénario donné nécessite schématiquement trois étapes :

- **La création du fichier de paramétrage** : Ce fichier se présente sous la forme d'un script écrit dans le langage interprété en TCL. Il décrit les différents aspects du scénario:
 - le nombre et le déplacement des unités mobiles (appelées nœuds),
 - le choix des différents protocoles pour chaque couche de chaque nœud,
 - le nombre, le type et la durée de divers transferts de données entre ces nœuds,
 - Les caractéristiques intrinsèques de chaque nœud (énergie résiduelle...etc)
- **La simulation proprement dite** : Elle reproduit en interne le fonctionnement du scénario décrit précédemment et génère un *fichier de traces*. Ce dernier contient l'information jugée utile, écrite dans un format standardisé.
- **L'analyse du fichier de trace** : Cette analyse peut être effectuée au moyen d'analyseurs syntaxiques ou d'outil de visualisation (comme le logiciel NAM, fournit avec NS2). Le contenu du fichier de trace consiste en une liste d'évènements datés se produisant chronologiquement, à raison d'un évènement par ligne. Les évènements répertoriés dans le fichier de trace sont, à quelques exceptions près, de deux types : d'une part ceux concernant le déplacement des nœuds, d'autre part ceux concernant le parcours des différents types de paquets. C'est ce dernier type d'information qui s'avère le plus intéressant du point de vue de l'analyse du routage. Il permet de connaître, à chaque fois qu'un paquet passe d'un nœud à un autre ou passe - au sein d'un même nœud - d'une couche à une autre, le contenu de ses en-têtes et des informations caractéristiques (identifiants, taille, etc...).

4.2 La mobilité dans NS-2

L'apport de la mobilité passe par l'ajout d'un nouveau type de nœuds définis dans la classe « *MobileNode* ». Les caractéristiques de la mobilité telles que le mouvement des nœuds, les mises à jour de localisation ou les limites de la topologie sont implémentées en C++. Par contre, les composants réseaux comme le nœud mobile lui-même (classificateur, couche liaison...) sont implémentés en OTcl.

Comme l'objectif étant de simuler des réseaux entièrement mobiles, il a fallu mettre en place des protocoles de routage. Dans notre cas ce qui nous intéresse est l'implémentation du protocole OLSR dans NS-2. Lorsqu'un nœud mobile est créé dans une simulation, le simulateur crée un objet « *MobileNode* », un agent de routage et la pile réseau qui sera décrite plus loin. Ensuite ces composants sont interconnectés et la pile est connectée au canal. Ces composants sont illustrés dans la **Figure 3.14 [100]**.

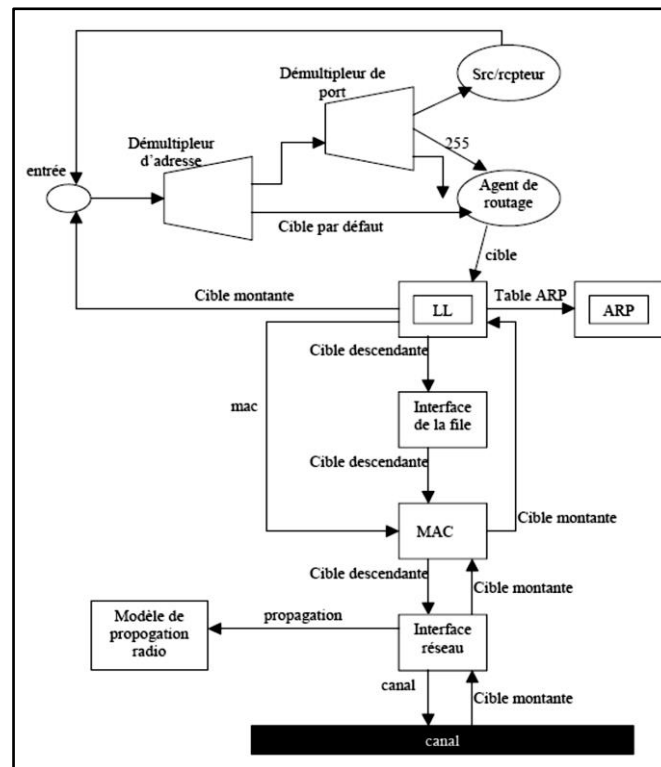


Figure 3.14 : Composants d'un nœud mobile dans NS2

Une caractéristique forte des nœuds mobiles est bien sûr de pouvoir se déplacer. NS-2 a été conçu pour exécuter des déplacements en 3D, mais actuellement la troisième dimension n'est pas utilisée ($Z=0$). Il existe deux mécanismes pour permettre à l'utilisateur de simuler un mouvement aux nœuds mobiles :

- **Indiquer le point d'origine** : la destination et la vitesse explicitement pour chaque nœud mobile. Les mises à jour sont déclenchées chaque fois que l'on exige la position du nœud mobile à un moment donné. Cette solution est plutôt faite pour des petites simulations.
- **Générer des mouvements aléatoires** : à l'appel d'une procédure, le nœud mobile démarre à partir d'une position aléatoire et exécute des déplacements. Le nœud mobile exécute des mises à jour de routage pour changer de destination et de vitesse.

Indépendamment des méthodes utilisées pour générer les mouvements des nœuds mobiles, il faut définir une topographie ; L'espace est considéré comme étant une grille dont il faut donner les frontières (valeurs de x abscisses et y ordonnées).

Dans ce qui suit, nous étalons plus en détail les composants réseaux d'un nœud mobile :

- **L'objet LinkLayer** est le même que celui utilisé par les nœuds unicast, avec un module ARP en plus. Ce module est implémenté dans le style BSD. Il traite des

demandes de l'objet LinkLayer en utilisant une table de correspondance entre l'adresse IP et l'adresse MAC. Il se sert d'un buffer pour mettre les paquets pour lesquels il ne connaît pas de correspondance.

- L'interface de file d'attente a été décrite par un nouvel algorithme de priorité : **PriQueue**. Cette gestion de file d'attente donne priorité aux paquets de routage.
- La couche MAC implémente uniquement la norme 802.11
- On arrive aux interfaces réseaux. L'objectif est de simuler l'interface matérielle qu'un nœud mobile puisse utiliser pour accéder au canal. Ces interfaces sont implémentées dans les fichiers `wirelessPhy.{cc,h}`. Ces interfaces sont soumises aux collisions et enregistrent l'intensité du signal, la longueur d'onde...
- Le modèle de propagation radio utilisé est l'atténuation espace-Friss ($1/r^2$) pour les courtes distances et Two Ray Ground ($1/r^4$) pour les grandes distances. L'antenne simulée est une antenne omnidirectionnelle.

Les limitations de ce modèle se sont vite ressenties. Effectivement, le modèle original de la mobilité permet des simulations de réseaux locaux sans fil et de réseaux ad-hoc uniquement. C'est pourquoi une première extension a été ajoutée au modèle, toujours fondée sur le travail des chercheurs de CMU, qui permet de faire des simulations impliquant des nœuds filaires et des nœuds sans fil à la fois. Cette extension, appelée « **wired-cum-wireless** », utilise le modèle de base de la mobilité décrit ci-dessus. L'objectif est donc de relier des réseaux locaux sans fil par un réseau filaire. Il se pose immédiatement un problème pour le routage ; Le routage des nœuds filaires s'effectue d'après la topologie grâce au concept de liaison, alors que dans la mobilité le concept de liaison n'existe pas. Un nouveau type de nœud est alors créé pour assurer la liaison entre le réseau filaire et le réseau sans fil. Ce nœud est appelé *BaseStationNode* (représenté dans la Figure 3.15).

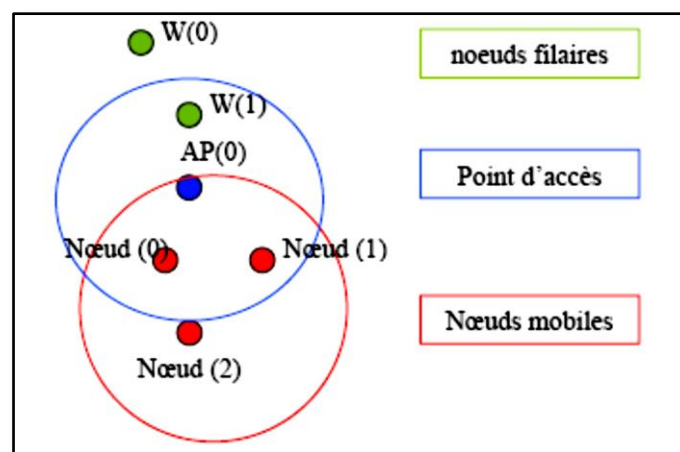


Figure 3.15: Scénario « wired-cum-wireless » dans NS-2

Ce nœud est un hybride entre un nœud hiérarchique et un nœud mobile. L'introduction de tel point d'accès a un impact sur l'adressage. Chaque domaine de nœuds mobiles à une adresse unique de domaine et un domaine est défini comme l'ensemble des nœuds mobiles qui sont attachés au point d'accès du domaine. Les nœuds mobiles doivent donc supporter le routage hiérarchique (excepté le SRNode). Un paquet destiné à un correspondant situé en dehors du domaine sans fil sera transmis au point d'accès, si toutefois il existe un chemin jusqu'à celui-ci.

Pour s'apercevoir de la portée et du niveau de simulation qu'il est possible de faire, voici la liste attributs d'un nœud mobile, qui doivent être paramétrés lors des simulations :

- Type d'adressage : plat ou hiérarchique
- Type du routage ad hoc
- Type de l'objet LinkLayer
- Type du protocole utilisé par la couche MAC
- Type de propagation radio
- Interface de la file d'attente
- Type de support physique
- Type de l'antenne
- Type du canal
- Activer ou non les fonctionnalités de routage filaire
- Activer ou non le protocole MIP sur le nœud
- Type de modèle d'énergie / énergie initiale
- Activer ou non un agent de trace sur le nœud
- Activer ou non un agent de trace de routage sur le nœud
- Activer ou non les traces des mouvements des mobiles

4.3 Mouvement des nœuds et génération de topologie dans NS-2

Les nœuds dans les réseaux Ad-Hoc sont mobiles. L'évaluation des performances des protocoles dans les réseaux Ad-Hoc nécessite donc des tests dans des conditions réelles. Or, dans NS-2 il est possible d'intégrer des modèles de la mobilité des nœuds pour rendre les simulations proches de la réalité. Un modèle de mobilité permet de générer un scénario de mouvement des nœuds.

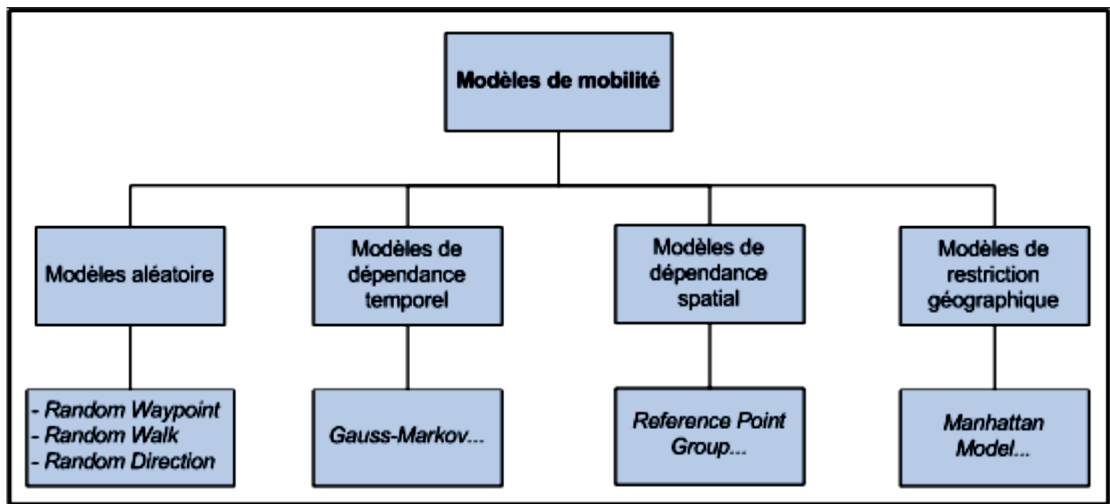


Figure 3.16 : Modèle de Mobilité dans NS-2

La Figure 3.16, donne une classification des modèles de mobilité les plus connus [101]. On peut distinguer quatre catégories : modèles de mobilité aléatoire, modèles de mobilité de dépendance temporelle, modèles de mobilité de dépendance spatiale et modèles de mobilité de restriction géographique. Or, le modèle aléatoire et en particulier « *Random Waypoint Mobility Model* » [102], a été retenu dans notre simulation et est souvent utilisé dans plusieurs travaux de simulations d'analyse des performances des protocoles de routage dans les réseaux Ad-Hoc. Dans ce modèle de mobilité, les nœuds sont placés d'une manière aléatoire dans une zone carrée. Le mouvement de chaque nœud est indépendant. Chaque nœud choisit un point de destination de manière aléatoire et il se déplace vers ce point avec une vitesse uniforme choisie entre 0m/s et V_{max} . Une fois que le nœud arrive à la destination, il marque une pause de temps donné et se déplace de nouveau vers une autre destination choisie aléatoirement avec d'autres paramètres de vitesse (Figure 3.17).

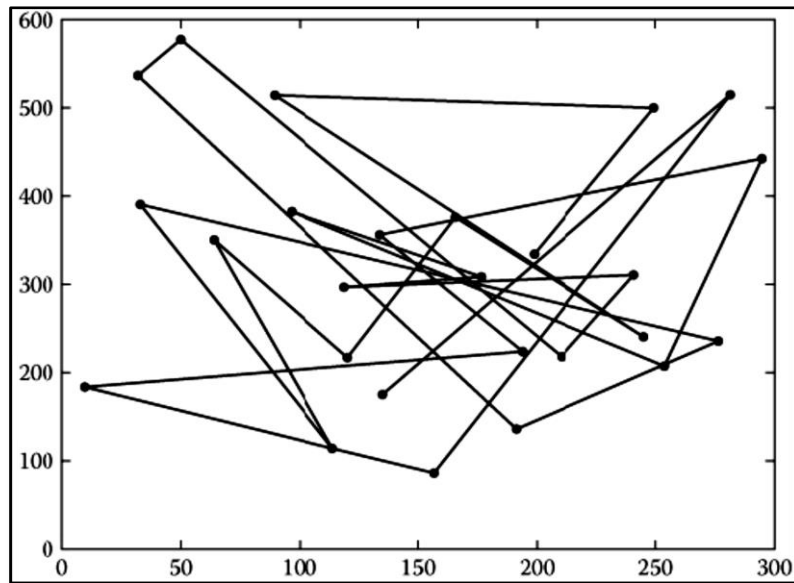


Figure 3.17: Mouvement d'un nœud selon le modèle *Random Waypoint*.

Au lieu de spécifier et contrôler chaque position et mouvement de nœud, nous utilisons dans notre simulation un outil baptisé « *setdest* » pour générer le nombre requis de nœuds ainsi que leurs mouvements. Cet outil utilise le modèle *Random Waypoint*. La syntax utilisée est :

```
# setdest -v 1 -n $numnodes -p $pt -M $maxspeed -t $simtime -x $maxx -y $maxy
```

Dans notre simulation, et pour nous permettre de générer plusieurs scénarios en fonction, de nombre des nœuds, vitesse...etc, nous utilisons un patch comme suit :

```
#!/bin/csh

#####
# Script for the original version of setdest
#####
unset noclobber

set outdir = scenario
set maxspeed = 1
set maxx = 780
set maxy = 780
set simtime = 300
set pt = 2

foreach numnodes( 20 40 60 100 )

foreach scen( 1 )

echo scen $scen : setdest -v 1 -n $numnodes -p $pt -M $maxspeed -t $simtime \
-x $maxx -y $maxy
time ./setdest -v 1 -n $numnodes -p $pt -M $maxspeed -t $simtime \
```

```
-x $maxx -y $maxy \  
>$outdir/scen-${maxx}x${maxy}-${numnodes}-${pt}-${maxspeed}-${scen}  
echo  
end  
end
```

Ceci veut dire que pour chaque nombre de nœuds allant de 20 à 100, les nœuds se déplacent dans un carré de 780*780m avec une vitesse de 1m/s, et ce pour une durée de 300 secondes, avec une pause entre chaque mouvement de 2 secondes.

4.4 Génération du trafic entre les nœuds mobiles

Dans un réseau Ad-Hoc, différents types de communication pourraient être établies entre les nœuds. Pour émuler ce type de communication dans NS-2, on utilise des applications de trafic à débit constant CBR (Constant Bit Rate) et qui modélisent la couche application sur des agents de transport UDP (User Datagrammes Protocol). On génère les scénarios de trafic aléatoires grâce à la modification d'un script « *cbrgen.tcl* » en TCL fourni sous NS-2 (*~ns/indep-utils/cmu-scen-gen*).

Le script utilisé dans notre cas pour chaque simulation est comme suit :

```
#ns cbrgen.tcl [-type cbr|tcp] [-nn nodes] [-seed seed] [-mc connections] [-  
rate rate] >output.tcl
```

Où « *nn* » désigne le nombre de nœuds dans la simulation, « *seed* » est un paramètre aléatoire fixé à 1, « *mc* » est le nombre de connexions maximales qu'on crée entre les nœuds mobiles et « *rate* » désigne le nombre de paquets par seconde émis entre la source et la destination ou plus exactement le débit binaire utilisé. Par défaut la taille d'un paquet est de 512 octets.

Un exemple de génération de trafic de type CBR dans nos simulations est illustré dans ce qui suit :

```
# nodes: 60, max conn: 8, send rate: 0.5, seed: 1.0  
#  
#  
# 1 connecting to 2 at time 2.5568388786897245  
#  
set udp_(0) [new Agent/UDP]  
$ns_ attach-agent $node_(1) $udp_(0)  
set null_(0) [new Agent/Null]  
$ns_ attach-agent $node_(2) $null_(0)  
set cbr_(0) [new Application/Traffic/CBR]  
$cbr_(0) set packetSize_ 512  
$cbr_(0) set interval_ 0.5  
$cbr_(0) set random_ 1  
$cbr_(0) set maxpkts_ 10000  
$cbr_(0) attach-agent $udp_(0)  
$ns_ connect $udp_(0) $null_(0)  
$ns_ at 2.5568388786897245 "$cbr_(0) start"  
#
```

Ceci exprime un trafic généré dans un réseau de 60 nœuds de type CBR avec un maximum de 8 connexions pour chaque nœud et un débit de 2 paquets par seconde.

4.5 Modèles de propagation dans NS-2

NS-2 permet également de choisir parmi les modèles de propagation suivants, qui influenceront en particulier sur la manière dont seront atténués les signaux en fonction de la distance [103] :

4.5.1 Le modèle de propagation en espace libre (Free space model)

Ce modèle considère le cas idéal où il y a un seul chemin de propagation entre l'émetteur et le récepteur et qu'il est en vue directe.

L'équation suivante permet de calculer la puissance du signal reçu en environnement libre à une distance d de l'émetteur.

$$Pr(d) = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 d^2 L}$$

Où P_t est la puissance d'émission, G_t et G_r les gains respectifs des antennes de l'émetteur et du récepteur. L (avec $L \geq 1$) est la perte du système, et λ est la longueur d'onde. Ce modèle de propagation représente les zones de communication comme un cercle autour de l'émetteur.

Si un récepteur est dans ce cercle il reçoit tous les paquets, s'il est en dehors il n'en reçoit aucun.

4.5.2 Le modèle de propagation utilisant deux rayons (Two-ray ground reflection model)

En environnement réel, il est peu probable que le seul chemin de propagation soit le chemin direct. Le modèle two-ray-ground considère donc à la fois le chemin direct et une réflexion sur le sol. Ce modèle donne des résultats plus justes que le modèle de propagation en espace libre quand la distance est assez grande. La puissance reçue à une distance d est calculée de la manière suivante :

$$P_r(d) = \frac{P_t G_t G_r h_t^2 h_r^2}{d^4 L}$$

Où ht et hr sont les hauteurs des antennes de transmission et de réception. Afin que NS-2 soit cohérent avec le modèle de propagation en espace libre, L a été ajouté à l'équation.

L'équation précédente présente une décroissance de la puissance reçue en fonction de la distance plus rapide que celle du premier modèle. Cependant, pour des distances courtes, le modèle à deux rayons ne donne pas de bons résultats. Le modèle de propagation en espace libre est donc utilisé à la place de celui-ci quand d est suffisamment petit.

4.5.3 Le modèle Shadowing

Les modèles de propagation en espace libre ou utilisant deux rayons calculent de manière déterministe la puissance reçue en fonction de la distance. Ils représentent tous deux la zone de communication comme un cercle idéal. Dans la réalité, la puissance reçue à une certaine distance varie de manière aléatoire, à cause des effets de propagation par des chemins multiples. En fait, les deux modèles précédents calculent la puissance moyenne reçue à une distance d .

Le modèle "shadowing" est composé de deux parties. La première est le modèle d'atténuation en fonction de la distance, qui calcule la puissance moyenne reçue à une distance d , notée $Pr(d)$. Il utilise une distance courte comme référence, notée d_0 . $Pr(d)$ est calculé relativement à $Pr(d_0)$ de la manière suivante :

$$\frac{Pr(d_0)}{Pr(d)} = \left(\frac{d}{d_0}\right)^\beta$$

β est appelé l'exposant d'atténuation en fonction de la distance, et est généralement déterminé de façon empirique par des mesures en environnement réel. Les grandes valeurs de β correspondent à une obstruction plus forte et donc à une décroissance plus rapide de la puissance reçue en fonction de la distance.

$Pr(d_0)$ peut être calculé à partir de l'équation ci-dessous, en prenant par exemple $d_0 = 1$ mètre. L'atténuation en fonction de la distance est souvent mesurée en dB.

$$\left[\frac{Pr(d)}{Pr(d_0)} \right]_{dB} = -10 \beta \log\left(\frac{d}{d_0}\right)$$

La seconde partie du modèle shadowing reflète les variations de la puissance reçue à une distance donnée. C'est une variable suivant une loi log-normale, c'est-à-dire dont la

distribution mesurée en dB est gaussienne. L'ensemble du modèle shadowing est représenté par :

$$\left[\frac{P_r(d)}{P_r(d_0)} \right]_{dB} = -10 \beta \log\left(\frac{d}{d_0}\right) + X_{dB}$$

Où X_{dB} est la variable aléatoire gaussienne dont la moyenne est zéro et l'écart type sigma dB. Sigma dB est appelée shadowing déviation, et est également obtenue par des mesures en environnement réel. L'équation ci-dessus est aussi connue sous le nom de « log-normal shadowing model ».

Le « shadowing model » étend le cercle idéal de communication à un modèle statistique plus riche; les nœuds ne peuvent communiquer qu'avec une certaine probabilité lorsqu'ils sont vers la limite de portée.

Dans notre simulation, nous avons implémenté le modèle à deux raies two-ray-ground.

4.6 Interprétation des résultats dans NS-2

NS-2 fournit plusieurs types de support pour analyser les résultats d'une simulation. D'une part, NS-2 inclut des classes pour suivre à la trace les fluctuations des paquets, pour calculer et enregistrer diverses statistiques sur l'ensemble des paquets ou uniquement pour un certain flux. L'utilisateur a le choix de mettre en place ce système de suivi pour chaque simulation. D'autre part, NS-2 travaille de pair avec l'outil de visualisation NAM qui permet de visualiser l'ensemble de la topologie dans une fenêtre graphique.

Dans un souci de regrouper tous les formats de trace de simulation sans fil qui ont émergé et pour être le plus exact que possible, un nouveau format de fichier de sortie a été mis en place. La figure qui suit illustre le format du fichier résultant de la simulation.

```
r -t 0.000982269 -Hs 29 -Hd -1 -Ni 29 -Nx 0.00 -Ny 0.00 -Nz 0.00 -Ne 99.999941 -Nl MAC -Nw --- -Ma 0 -Md ffffffff -Ms 1e -
Mt 800 -Is 30.255 -Id -1.255 -It OLSR -Il 48 -If 0 -Ii 0 -Iv 32 -P olsr -Pn 1 -Ps 0 [-Pt HELLO -Po 30 -Ph 0 -Pms 0]
r -t 0.000982269 -Hs 28 -Hd -1 -Ni 28 -Nx 0.00 -Ny 0.00 -Nz 0.00 -Ne 99.999941 -Nl MAC -Nw --- -Ma 0 -Md ffffffff -Ms 1e -
Mt 800 -Is 30.255 -Id -1.255 -It OLSR -Il 48 -If 0 -Ii 0 -Iv 32 -P olsr -Pn 1 -Ps 0 [-Pt HELLO -Po 30 -Ph 0 -Pms 0]
r -t 0.000982269 -Hs 27 -Hd -1 -Ni 27 -Nx 0.00 -Ny 0.00 -Nz 0.00 -Ne 99.999941 -Nl MAC -Nw --- -Ma 0 -Md ffffffff -Ms 1e -
Mt 800 -Is 30.255 -Id -1.255 -It OLSR -Il 48 -If 0 -Ii 0 -Iv 32 -P olsr -Pn 1 -Ps 0 [-Pt HELLO -Po 30 -Ph 0 -Pms 0]
r -t 0.000982269 -Hs 26 -Hd -1 -Ni 26 -Nx 0.00 -Ny 0.00 -Nz 0.00 -Ne 99.999941 -Nl MAC -Nw --- -Ma 0 -Md ffffffff -Ms 1e -
Mt 800 -Is 30.255 -Id -1.255 -It OLSR -Il 48 -If 0 -Ii 0 -Iv 32 -P olsr -Pn 1 -Ps 0 [-Pt HELLO -Po 30 -Ph 0 -Pms 0]
r -t 0.000982269 -Hs 25 -Hd -1 -Ni 25 -Nx 0.00 -Ny 0.00 -Nz 0.00 -Ne 99.999941 -Nl MAC -Nw --- -Ma 0 -Md ffffffff -Ms 1e -
Mt 800 -Is 30.255 -Id -1.255 -It OLSR -Il 48 -If 0 -Ii 0 -Iv 32 -P olsr -Pn 1 -Ps 0 [-Pt HELLO -Po 30 -Ph 0 -Pms 0]
```

Figure 3.18 : format du fichier trace dans NS-2

Ce format de fichier semble plus complexe, mais il est beaucoup plus facile à lire que le précédent. Effectivement, chaque valeur notée dans le fichier est précédée de sa signification. En plus des informations contenues dans l'ancien format (type d'événement, temps, source, récepteur...), il contient des informations sur :

- Sur la position des nœuds (-Nx, -Ny, -Nz)
- Sur l'énergie des nœuds (-Ne)
- Sur le prochain saut (-Hs, -Hd)
- Au niveau MAC : type Ethernet, adresses Ethernet...
- Au niveau applicatif: type de l'application, type du protocole, caractéristiques particulières suivant ces types

Le fichier trace résultant de la simulation demeure toujours volumineux et difficile à interpréter manuellement. Dans notre cas, et afin d'extraire les résultats qui nous permettront de distinguer les diverses performances des protocoles implémentés, nous avons développé un script en langage java. Ce script, permettra une grande facilité dans l'extraction des données résultantes du fichier trace. Le résultat, sera ensuite stocké dans un fichier texte .txt puis interprété par des outils graphiques dans EXCEL.

Un autre fichier résultant de la simulation pourra être interprété par l'outil de visualisation NAM (Network Animator). Ce dernier permet le suivi des états d'un grand nombre de nœuds, une analyse de l'échange de messages et des interactions dynamiques pour des trafics concurrents. Les outils de visualisation permettent à l'utilisateur d'accéder rapidement à une quantité importante d'informations et d'identifier visuellement les modèles de communication, leur permettant ainsi de mieux comprendre les interactions et les causalités. Basé sur le langage TCL/TK, NAM permet également de donner une représentation graphique du réseau décrit dans le fichier de simulation TCL tout en animant les liens entre les nœuds du réseau, le modèle théorique du NAM a été non seulement créé pour lire un large ensemble de données d'animation, mais aussi suffisamment extensible pour être utilisé quelque soit le type de réseau simulé (fixe ou mobile ou mixte), ce qui permet de visualiser tout type de simulation possible. Généralement les scénarios simulés génèrent des fichiers avec l'extension .nam, la visualisation de ces scénarios avec NAM se fait à l'aide de la commande :

```
./nam <FichierNAM>.nam
```

Ou l'exécution de cette commande à travers le script par l'ajout de l'instruction :

```
Proc finish {} {exec ./nam <FichierNAM>.nam & exit }
```

5 Protocole OE-OLSR (Optimized Energy – OLSR)

Cette partie décrira en détail notre premier apport au protocole OLSR, en implémentant le paramètre de l'énergie résiduelle des nœuds comme facteur de sélection des MPRs ainsi que le calcul de la table de routage des paquets dans le réseau AHWSN.

Comme a été déjà stipulé, nous avons profité des champs réservés dans les paquets de contrôle du protocole OLSR basique afin de transmettre l'information relative à l'énergie des nœuds. Ensuite, l'heuristique de calcul des MPRs dans chaque nœud a été modifiée afin de tenir compte de l'énergie des nœuds dans la décision du choix d'un nœud comme MPR. Dans le paquet de contrôle « TC », l'information de l'énergie permettra de se décider de la route à emprunter pour acheminer l'information utile [104].

La partie qui suit, détaillera les différents travaux de simulations réalisées dans notre publication [104].

Il est important de définir certaines terminologies qu'on utilisera dans la suite de cette section. Soit S un nœud donné du réseau :

On dit qu'un nœud $X \in N_1(S)$, ou $N_1(S)$ signifie tous les nœuds autour du nœud S d'une distance de 1-saut.

On dit aussi $N_2(S)$: tous les nœuds visibles par le nœud S , mais à travers un ou plusieurs nœuds de $N_1(S)$, donc ils sont distants de deux sauts (2-sauts).

Les nœuds $D(S)$: tous les nœuds visibles par le nœud S distants de 1-saut, mais ils ne sont pas utilisés pour relier des nœuds de $N_2(S)$.

Notre algorithme appliqué sur le protocole OLSR est comme suit :

1. Effacer les tables de routage dans les nœuds MPRs.
2. Sélectionner les nœuds MPRs en utilisant la méthode suivante :
 - a. Envoyer les messages HELLO en spécifiant le degré de l'énergie soit supérieur ou inférieur par rapport à deux seuils de référence. Ceci déterminera la valeur du champ « willingness » qui désigne la capacité d'un nœud à transmettre les messages en provenance des autres nœuds voisins.
 - b. Lire les messages HELLO des voisins et les comparer avec les seuils de référence.
 - i. Si l'énergie résiduelle est supérieure ou égale à 80% de l'énergie initiale, le nœud sera sélectionné comme MPR.
 - ii. Si l'énergie résiduelle est inférieure ou égale à 10% de l'énergie initiale, le nœud sera sélectionné comme mort (dead).

3. Après la sélection des nœuds MPRs, Les messages TC (Topology Control) seront échangés entre ces derniers afin de définir la topologie du réseau.
4. Après avoir identifié la topologie du réseau, on calcule les tables de routage de la manière suivante :
 - a. Effacer toutes les entrées des tables de routage existantes
 - b. L'énergie résiduelle sera comparée aux seuils qui sont déjà définis :
 - i. Si l'énergie résiduelle est supérieure ou égale à 80% ; ajouter à la table de routage, les voisins qui possèdent un lien symétrique avec ce nœud.
 - ii. Si l'énergie résiduelle est inférieure ou égale à 10% ; sélectionner ce nœud comme un nœud mort (dead) et il ne sera jamais sélectionné pour construire la table de routage.
4. Sélectionner les nœuds de routage et construire les tables de routage en se basant sur l'énergie résiduelle comme premier critère. Ensuite, sélectionner les voisins à 2-sauts via ceux à 1-saut aptes à construire les tables de routage.

Le principe du protocole OE-OLSR est le suivant :

- Sélectionner les nœuds possédant une énergie résiduelle suffisante pour jouer le rôle de MPR, responsables à transmettre les informations utiles via le réseau.
- Garantir la transmission des données à travers les nœuds ayant une énergie résiduelle suffisante, signifiera aussi une bonne répartition de la charge du réseau.

Ce processus peut être illustré par l'organigramme suivant :

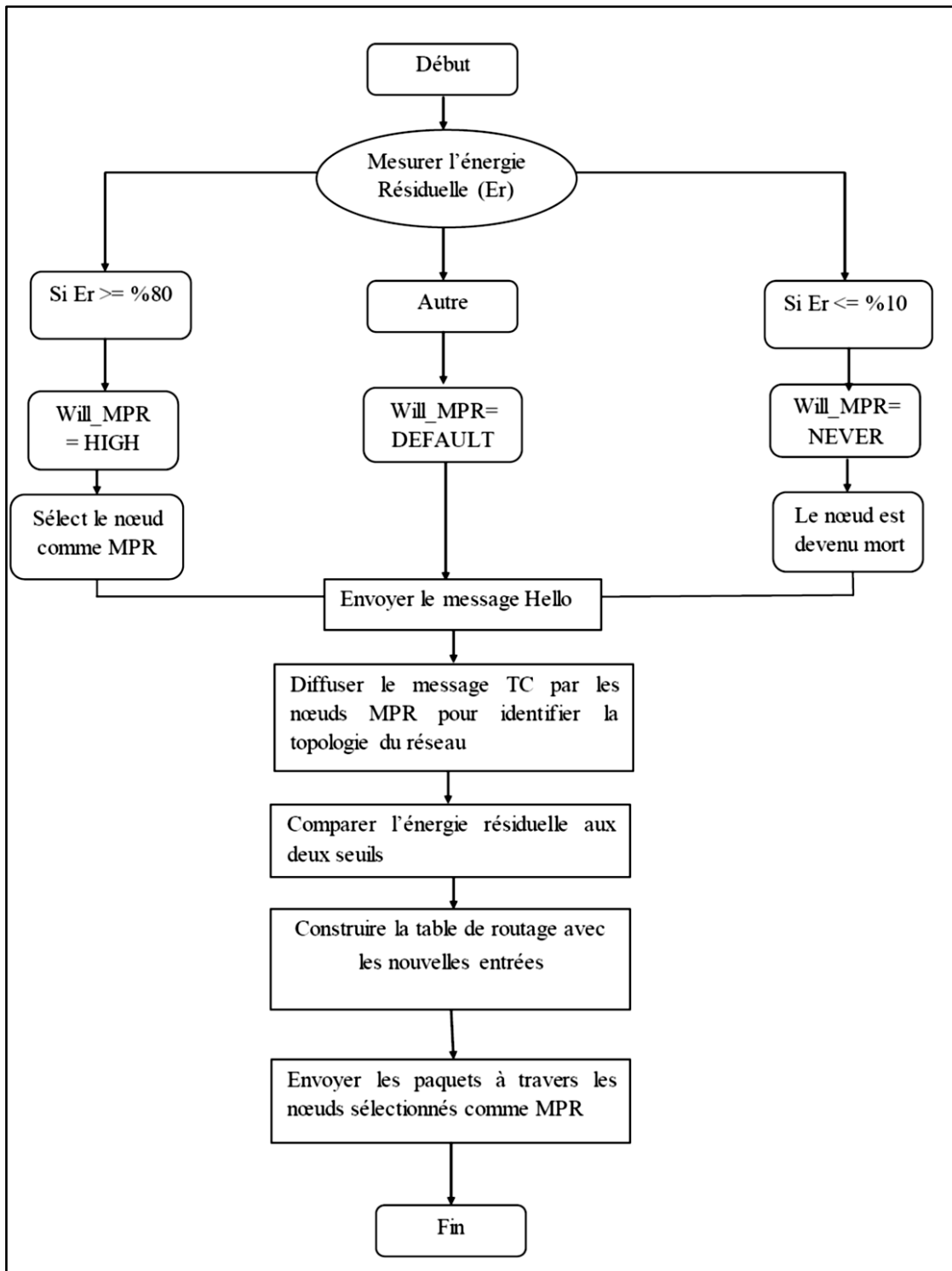


Figure 3.18 : processus du protocole OE-OLSR

5.1 Sélection des MPRs dans le protocole OE-OLSR

Le protocole OE-OLSR implémente un nouvel algorithme de sélection des MPRs. Ce dernier est basé en partie sur l'algorithme classique décrit dans la RFC 3626, avec comme objectif de déterminer à la fois les nœuds possédant une énergie résiduelle

supérieure à 80% de la valeur initiale, ainsi que les nœuds qui ont une énergie résiduelle moins de 10%.

La figure 3.19 décrit l'heuristique de sélection des MPR dans le protocole OE-OLSR. Pour tout nœud S dans le réseau, on commence au préalable par identifier tous ses voisins à 1-saut et à 2-sauts ($N_1(S)$ et $N_2(S)$). Ensuite, On recherche tous les nœuds X dans $N_1(S)$ qui possèdent une énergie résiduelle plus de 80%. Ces nœuds seront ajoutés à ceux sélectionnés comme MPRs.

```
Données : Tout nœud  $s$  avec ses voisins  $N_1(s)$  et  $N_2(s)$ .  
Résultat : L'ensemble  $MPR(s)$ .  
  
Début  
   $MPR(s) \leftarrow \emptyset$  ;  
  Trouver les nœuds isolés dans  $N_2(s)$  qui sont  
  couverts par un seul nœud  $N_1(s)$  ;  
  Pour tout nœud  $y$  dans  $N_2(s)$  isolé faire  
    soit  $x \in N_1(s)$  le seul voisin de ce nœud  $y$   
    et d'énergie résiduelle  $\geq 80\%$  ;  
    Ajouter  $x$  à  $MPR(s)$  ;  
    Eliminer tout les nœuds dans  $N_2(s)$  couverts par  $x$  ;  
  Fin  
  Tant que  $N_2(s) \neq \emptyset$  faire  
    Trouver  $x \in N_1(s)$  tq  
    o  $x$  a d'énergie résiduelle  $\geq 80\%$  ;  
    o  $x$  couvre le maximum des nœuds dans  $N_2(s)$  ;  
    o  $x$  a le maximum des voisins ;  
    Ajouter  $x$  a  $MPR(s)$  ;  
    Eliminer tous les nœuds dans  $N_2(s)$  couverts par  $x$  ;  
  fin  
fin
```

Figure 3.19 : Calcul des MPRs dans OE-OLSR

La figure 3.19 illustre bien que pour sélectionner les nœuds MPRs, le protocole commence à chercher les nœuds possédant l'énergie résiduelle supérieure ou égale à 80%. Dans le cas où plus d'un nœud satisfait cette condition et afin d'éviter la redondance, OE-OLSR sélectionnera le nœud qui peut relier le maximum des nœuds appartenant à $N_2(S)$. Ensuite, et si on trouve plus d'un nœud pouvant relier le même

nombre de nœuds de $N2(S)$, le nœud reliant le maximum de nœuds dans $D(S)$ sera élu comme MPR.

La figure 3.20 illustre une comparaison entre l'algorithme de sélection des MPRs relatif à OE-OLSR et l'heuristique classique définie dans la RFC 3626. Les nœuds 1, 3, 5 et 7 sont déclarés MPRs dans l'algorithme classique, mais ce n'est pas le cas dans le protocole OE-OLSR.

Les nœuds ayant l'énergie résiduelle supérieure ou égale 80% sont colorés en vert, ceux qui ont l'énergie résiduelle inférieure ou égale 10% en rouge, et le reste en blanc.

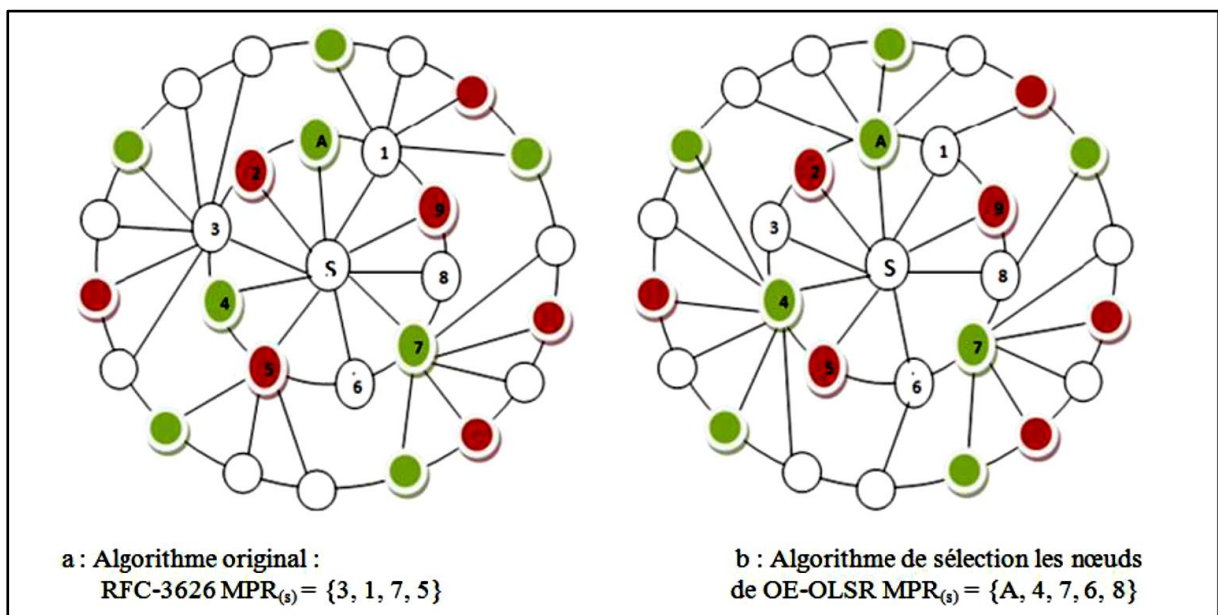


Figure 3.20 : Sélection des MPRs « OE-OLSR » Vs « OLSR »

L'algorithme de sélection des MPRs dans OE-OLSR se base sur le choix des nœuds qui sont bien chargés. Dans le cas où il nous est impossible d'atteindre des nœuds isolés qui appartiennent à $N2(S)$, on peut utiliser les nœuds possédant l'énergie résiduelle supérieure à 10% pour les joindre. Toutefois, il est impossible de sélectionner des nœuds qui ont l'énergie résiduelle inférieure ou égale à 10%, sauf pour recevoir leurs propres données. Les nœuds possédant une énergie résiduelle moins de 10% ont été déclarés comme des nœuds morts, ils ne seront jamais utilisés pour construire la table de routage.

5.2 Messages de contrôle et algorithme d'inondation dans OE-OLSR

Une fois que l'ensemble des MPRs a été identifié ainsi que celui des nœuds morts dans le réseau, il faut définir un mécanisme pour diffuser les informations sur la topologie du réseau.

Le protocole OE-OLSR utilise les mêmes mécanismes d'inondation que le protocole classique OLSR (RFC 3626). Les seules modifications concernent le format et le contenu

des messages HELLO et TC. Ces derniers devront être modifiés pour transmettre l'information de l'énergie résiduelle de chaque nœud dans le réseau.

En effet dans OE-OLSR, il faut que chaque nœud S dans le réseau insère dans ses messages HELLO ses MPRs ainsi que l'état de son énergie résiduelle en la comparant aux seuils décrits précédemment. On notera les valeurs :

- HIGH : si l'énergie résiduelle est supérieure ou égale à 80%,
- LOW : si elle est inférieure ou égale à 10% ou
- DEFAULT : si elle est comprise entre 10% et 80%.

De la même manière, chaque nœud émettant des messages TC, devra transmettre à travers ces derniers, l'état de son énergie résiduelle.

Du moment où les informations sur la topologie sont échangées entre les nœuds selon les nouvelles spécifications des messages de contrôle dans OE-OLSR, chaque nœud procédera au calcul des chemins les plus courts et optimaux vers une destination donnée, en se basant sur l'algorithme de Dijkstra. Deux options s'imposent sur chaque nœud pour calculer ses routes:

- Les nœuds MPRs seront sélectionnés parmi tous les nœuds qui ont l'énergie résiduelle supérieure ou égale à 80%.
- Le calcul des tables de routage ne tient compte que des nœuds qui ont l'énergie résiduelle supérieure à 10%.

5.2.1 Nouveau message HELLO dans OE-OLSR

Chaque nœud doit diffuser dans son message HELLO l'état de son énergie, pour être tenu en compte dans l'algorithme de sélection des MPRs ainsi que pour calculer les tables de routage. Donc tout nœud doit savoir l'état de l'énergie de ses voisins.

| | | | |
|-----------------------------|----------|-------------------|-------------|
| Reserved | | Htime | Willingness |
| Link code | Reserved | Link Message Size | |
| Neighbors interface address | | | |
| Neighbors interface address | | | |

a. Message HELLO dans OLSR

| | | | |
|-----------------------------|----------|-------------------|-------------|
| Reserved | Energie | Htime | Willingness |
| Link code | Reserved | Link Message Size | |
| Neighbors interface address | | | |
| Neighbors interface address | | | |

b. Message HELLO dans OE-OLSR

Figure 3.21: Nouveau format du Message HELLO

Le champ « **Energie** » dans le message HELLO peut prendre trois valeurs possibles :

- HIGH: Si l'énergie résiduelle du nœud est supérieure ou égale à 80% ;
- DEFAULT: Si l'énergie résiduelle est inférieure à 80% et supérieure à 10% ;
- LOW: Si l'énergie résiduelle est inférieure ou égale à 10% ;

5.2.2 Nouveau message TC dans OE-OLSR

Les messages HELLO sont droppées par les nœuds MPRs, mais les messages TC sont diffusés à travers le réseau entier en utilisant le processus d'inondation optimisée d'OLSR par l'intermédiaire des MPRs. A cet effet, nous avons inséré l'état de l'énergie résiduelle dans les messages TC.

| | |
|----------------------------------|----------|
| ANSN | Reserved |
| Advertised Neighbors Main Adress | |
| Advertised Neighbors Main Adress | |
| ----- | |

a. Message TC dans OLSR

| | | |
|----------------------------------|---------|----------|
| ANSN | Energie | Reserved |
| Advertised Neighbors Main Adress | | |
| Advertised Neighbors Main Adress | | |
| ----- | | |

b. Message TC dans OE-OLSR

Figure 3.22 : Nouveau format du Message TC

Le champ « **Energie** » dans le message TC peut prendre les mêmes valeurs que dans les messages HELLO.

5.3 Calcul des routes

Chaque nœud dans le réseau calcule sa table de routage en se basant sur les informations de voisinage et de topologie rafraîchies périodiquement. L'algorithme de Dijkstra est utilisé pour le calcul du plus court chemin en nombre de sauts, vers tous les nœuds du réseau.

Une entrée de la table de routage possède le format suivant : [R_dest, R_next, R_dist] où R_dest est l'adresse du nœud destinataire à atteindre après R_dist sauts en passant d'abord par le voisin direct R_next. Désormais R_next est pris seulement en fonction du lien symétrique, mais aussi en fonction de l'énergie résiduelle, car si cette dernière demeure inférieure à 10%, le nœud ne sera jamais sélectionné comme R_next.

6. Simulation des performances du protocole OE-OLSR

Le simulateur NS-2 fournit une plateforme de simulation pour plusieurs protocoles ad-hoc. Par défaut, ce simulateur intègre DSR et AODV mais malheureusement pas le protocole OLSR. Cependant, il existe des extensions pour NS-2 afin d'implémenter le protocole OLSR. Notre choix a été basé sur UM-OLSR (version, 2008.8)[105]. Ce package permet d'intégrer OLSR (RFC-3626) dans le simulateur NS-2, il est sous une licence GNU et il a été utilisé dans plusieurs articles afin d'expérimenter le protocole OLSR. Ce package est compatible avec la version 2.29 de NS-2. Ceci explique notre choix de la version de NS-2 utilisée comme plateforme de simulation.

Le développement de la version du protocole OE-OLSR pour NS-2 a été basé sur le package UM-OLSR. En effet, nous avons intégré UM-OLSR dans NS-2 sous une machine Windows 2003 (XP) en utilisant le logiciel Cygwin, un émulateur de l'environnement Linux. Ensuite, nous avons modifié le protocole UM-OLSR développé sous le langage C++, en modifiant les champs « reserved » des paquets de contrôle HELLO et TC. Enfin, la validation de notre implémentation a été effectuée grâce à des modèles de topologie bien déterminés.

Après l'implémentation et la simulation en envisageant différents paramètres réseau et différents scénarios, l'interprétation des résultats a été effectuée via un programme développé en JAVA, afin de nous faciliter la tâche de lecture des fichiers résultats, très volumineux et complexes. Ces résultats seront tracés par Excel afin d'analyser sous format graphique la performance de notre protocole OE-OLSR par rapport à OLSR basique.

6.1 Métriques d'évaluation

6.1.1 Délai de bout-en-bout

Synonyme de latence ou temps de réponse, le délai de transmission de bout en bout est le temps écoulé entre l'émission et la réception d'un paquet. On distingue trois types de délai à travers le réseau :

- **Délai de propagation (D_p)** : Il est fixe car il ne dépend que du support de transmission. Il désigne le temps effectué par la transmission d'un bit via le média de transmission.
- **Délai de traitement (D_t)** : Il correspond au temps utilisé par un routeur pour le traitement d'un paquet, i.e, le temps effectué pour traiter un paquet de l'interface d'entrée et le mettre dans la file d'attente de l'interface de sortie. Il

varie en fonction de la vitesse du CPU, de son utilisation, du mode de commutation utilisé, de l'architecture du routeur et de la taille du paquet.

- **Délai de mise en file d'attente (Df)** : Il s'agit du temps que le paquet passe dans la file d'attente de la sortie du routeur. Il dépend du nombre et de la taille des paquets déjà dans la file, de la bande passante de l'interface et du mécanisme de file d'attente.

Le délai de bout en bout correspond donc à la somme de ces trois délais observés à travers le chemin de la source à la destination.

$$\boxed{\text{Délai de bout en bout} = D_p + D_t + D_f}$$

6.1.2 Pourcentage de paquets délivrés

Le pourcentage de paquets délivrés ou PDR (Packet Delivery Ratio), est une métrique qui permet de calculer le nombre total des paquets délivrés à une destination par rapport au nombre des paquets transmis. En effet ce paramètre mesure l'efficacité du protocole réseau implémenté pour router l'information de la source à la destination d'une manière fiable.

6.1.3 Nombre de sauts

Le nombre de nœuds qu'un paquet traverse d'un nœud source à la destination. Ce paramètre permet de déterminer les performances des protocoles par rapport aux chemins optimaux empruntés.

6.1.4 Energie Consommée

Désigne l'énergie totale consommée pour transmettre tous les paquets aux destinataires. Pour assurer une performance optimale d'un réseau, l'énergie consommée devra être plus petite que possible.

L'énergie consommée $E(P, n_a)$ pour transmettre un paquet du nœud n_a au nœud n_b est donnée par la relation suivante :

$$\boxed{E(P, n_a) = E_{tx}(P, n_a) + E_{rx}(P, n_b) + (N - 1).E_0(P, n_i)}$$

Ou, E_{tx} , E_{rx} est la quantité d'énergie consommée pour transmettre le paquet du nœud source n_a , à la destination n_b , respectivement. N représente le nombre de sauts qu'un paquet traverse d'un nœud source à la destination. Donc, le plus petit nombre de sauts signifie une minimisation de la quantité d'énergie consommée.

6.1.5 Nombre des nœuds morts (dead nodes)

Le nombre des nœuds qui se déchargent après le temps de simulation. Un nombre faible des nœuds morts, signifie l'augmentation de la durée de vie des réseaux.

6.2 Paramètres de simulation

Les tableaux suivants présentent le récapitulatif des paramètres de simulation en mode dynamique. Ces paramètres sont utilisés dans le script de simulation de NS-2 écrit en TCL.

| Paramètres | Valeurs |
|-------------------------------|--|
| Type de canal | <i>Sana fil (wireless)</i> |
| Modèle de propagation radio | <i>Two Ray Ground</i> |
| Type d'interface réseau | <i>IEEE 802.11</i> |
| Type de file d'attente | <i>DropTail/ Priority Queue</i> |
| Longueur de la file d'attente | <i>50 Paquets</i> |
| Couche liaison | <i>Link Layer (LL)</i> |
| Type d'antenne | <i>Omnidirectionnal Antenna</i> |
| Modèle de mobilité | <i>Random WayPoint</i> |
| Type de Trafic | <i>Constant Bit Rate (CBR)</i> |
| Trafic | <i>2 Paquets de 512 octets par seconde</i> |
| Intervalle des messages HELLO | <i>Par défaut (02 Secondes)</i> |
| Intervalle des messages TC | <i>Par défaut (05 secondes)</i> |
| Temps de simulation | <i>100 secondes</i> |

| Paramètres | Variation du nombre de nœuds | Variation de la vitesse des nœuds | Variation du nombre de connexions |
|------------------------|------------------------------|-----------------------------------|-----------------------------------|
| Surface | <i>870m x 870m</i> | <i>870m x 870m</i> | <i>870m x 870m</i> |
| Nombre de nœuds | <i>20, 40, 60, 80, 100</i> | <i>40</i> | <i>40</i> |
| Vitesse des nœuds | <i>3m/s</i> | <i>1, 3, 5, 8, 10 m/s</i> | <i>3m/s</i> |
| Temps de la simulation | <i>100s</i> | <i>100s</i> | <i>100s</i> |
| Type de trafic | <i>CBR</i> | <i>CBR</i> | <i>CBR</i> |
| Nombre de connexions | <i>14</i> | <i>14</i> | <i>10, 12, 14, 16, 18</i> |
| Débit | <i>2 paquets/s</i> | <i>2 paquets/s</i> | <i>2 paquets/s</i> |
| Energie initiale | <i>100 joules</i> | <i>100 joules</i> | <i>100 joules</i> |
| Protodocle de routage | <i>OLSR et OE-OLSR</i> | <i>OLSR et OE-OLSR</i> | <i>OLSR et OE-OLSR</i> |

Tableau 3.2 : Paramètres de simulation d'OLSR et OE-OLSR sous NS-2

6.3 Résultats des simulations et discussions

Comme nous l'avons déjà évoqué, nous avons utilisé des métriques comme critères d'évaluation des deux protocoles. En effet, ces métriques relatent les performances en matière de qualité de service (QoS) du réseau. Le calcul de ces critères sera effectué par le fichier Java développé en se basant sur le fichier trace (.tr) résultant qui demeure très complexe.

6.3.1 Nombre de sauts

Comme nous l'avons précédemment cité, il s'agit du nombre de sauts qu'un paquet effectue de la source à la destination. Une minimisation de nombre de sauts signifie une optimisation de l'énergie résiduelle.

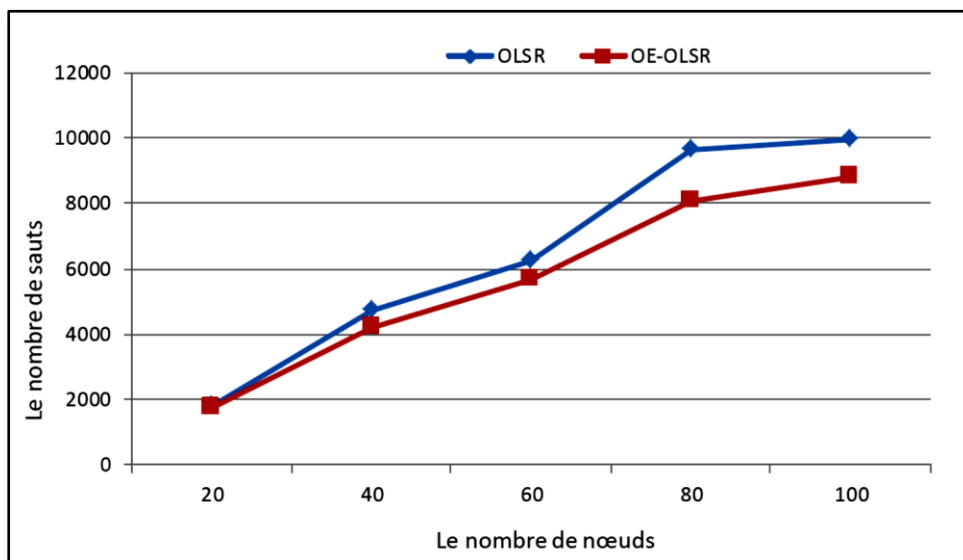


Figure 3.23 : Variation du nombre de sauts Vs nombre de nœuds

La figure 3.23, illustre l'évolution du nombre de sauts des deux protocoles en fonction du nombre de nœuds constituant le réseau. L'apport de notre mécanisme décrit précédemment qui a été implémenté sur le protocole OLSR basique en tenant en compte l'énergie résiduelle des nœuds dans le processus du choix des MPRs a réduit les sauts entre la source et la destination, surtout lorsque le nombre de nœuds s'accroît. Dans un réseau constitué d'un nombre petit de nœuds, les deux protocoles ont le même effet. Ceci est explicite car les chemins sélectionnés pour router l'information sont minimales.

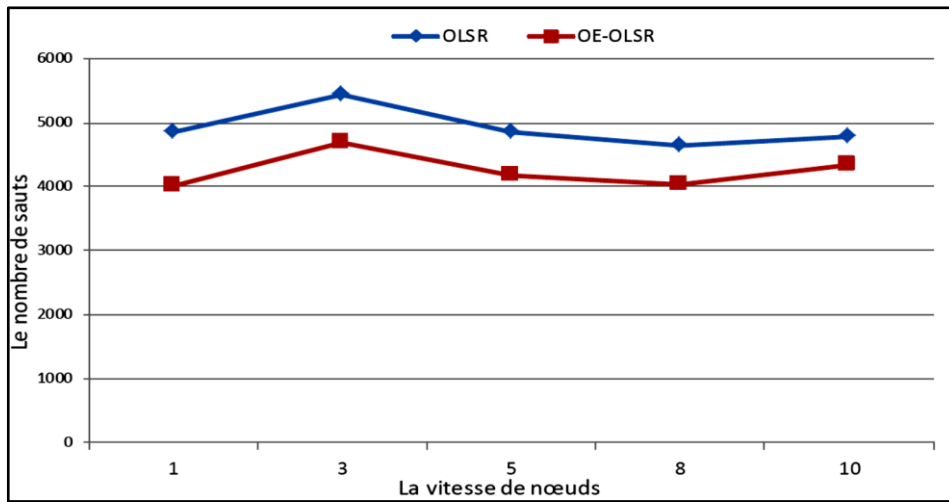


Figure 3.24 : Variation du nombre de sauts Vs Vitesse des nœuds

La figure 3.24 illustre l'impact des deux protocoles étudiés sur le nombre de sauts en fonction de la mobilité du réseau. L'avantage de l'implémentation de l'énergie résiduelle des nœuds comme facteur de choix des MPRs et du calcul des routes demeure nettement meilleur par rapport au protocole OLSR basique. Le nombre de sauts a été nettement réduit, ce qui explique que le protocole OE-OLSR agit d'une façon plus efficace sur le réseau AHWSN.

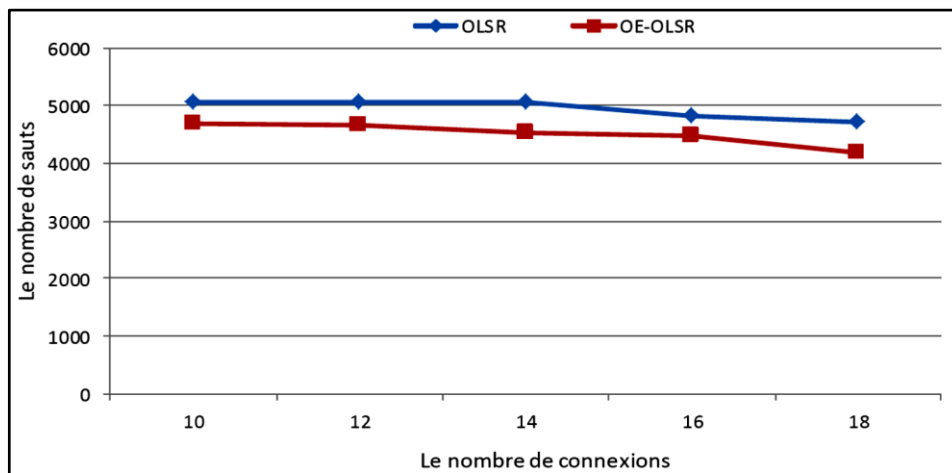


Figure 3.25 : Variation du nombre de sauts Vs Nombre de connexions

De même que pour le nombre de connexions entre les nœuds, le protocole OE-OLSR agit nettement meilleur que l'OLSR basique. Ceci est dû au fait que les nœuds utilisant OOE-OLSR sélectionnent des routent optimales dans le réseau en tenant en compte du facteur de l'énergie résiduelle de leurs voisins de transit.

6.3.2 Energie totale consommée

Comme a été déjà décrit dans le point 6.1.4, il s'agit de l'énergie totale consommée pour transmettre tous les paquets aux destinataires. Le protocole est performant si cette énergie est minimale. Il y a une relation étroite entre le nombre de sauts et l'énergie totale consommée.

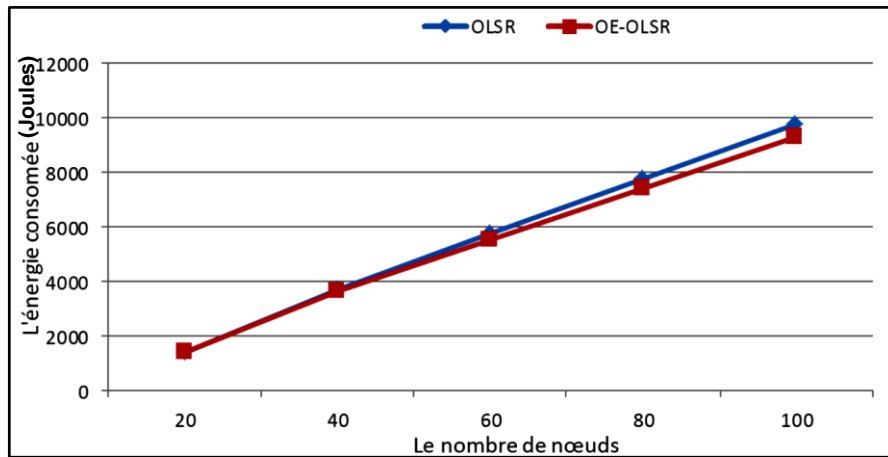


Figure 3.26 : Variation de l'énergie totale Vs Nombre de nœuds

La variation de l'énergie consommée est presque linéaire entre les deux protocoles, avec une légère amélioration du protocole OE-OLSR quand le nombre de nœuds augmente. Toutefois, l'amélioration est nettement visible dans le cas de la mobilité et la connectivité du réseau.

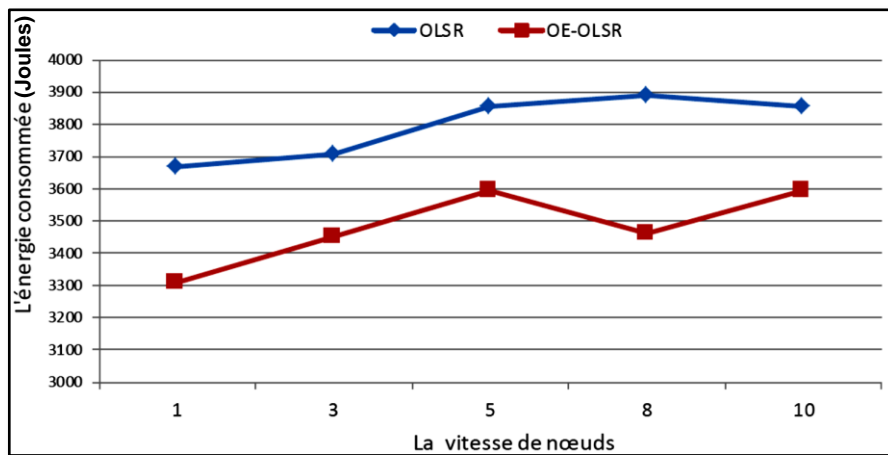


Figure 3.27 : Variation de l'énergie totale Vs Vitesse des nœuds

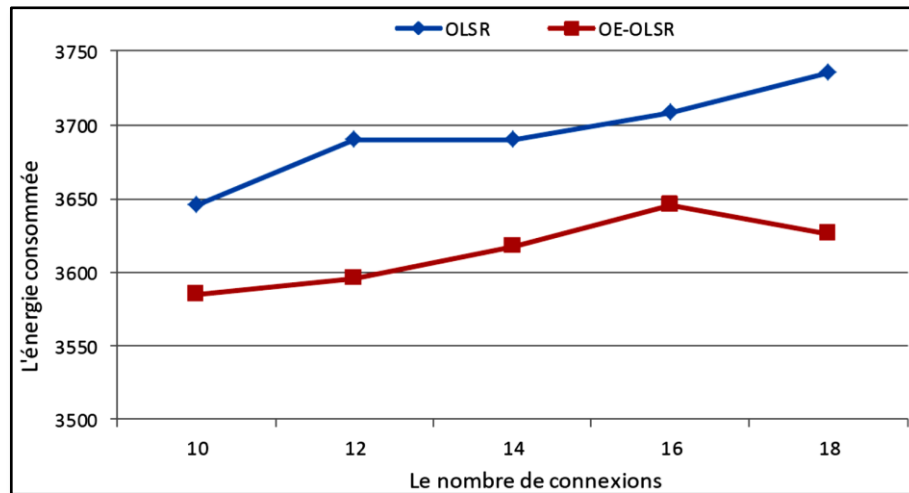


Figure 3.28 : Variation de l'énergie totale Vs nombre de connexions

Les deux figures précédentes illustrent clairement la nette amélioration du protocole OE-OLSR, comparé à celui de l'OLSR. L'énergie totale consommée demeure un facteur prépondérant de la qualité de service QoS d'un réseau AHWSN. En effet, elle caractérise la durée de vie du réseau. Une consommation minimale de l'énergie signifie une conservation de la charge des batteries des nœuds ce qui augmente davantage la durée de vie du réseau.

6.3.3 Pourcentage des paquets délivrés (PDR)

Cette métrique est essentielle dans la qualité de service QoS du réseau AHWSN. En effet, elle mesure le ratio des paquets reçus par les nœuds destinataires à ceux émis par les nœuds sources. Dans le cas idéal, un PDR est égale 1 signifie que tous les paquets émis sont bien reçus.

Dans ce qui suit, nous allons étudier l'effet de l'introduction de l'énergie résiduelle des nœuds dans le processus du choix des MPRs et de la construction de la table de routage des nœuds sur le PDR.

Les différentes simulations effectuées, illustrent clairement que le protocole OE-OLSR a un impact positif sur le PDR, comparé à celui de l'OLSR, et ce dans les trois cas « densité », « mobilité » et « connectivité ». Ceci est dû principalement au fait que les routes sélectionnées pour transmettre l'information de la source vers la destination sont optimales et maintenues durant toute la durée de la simulation.

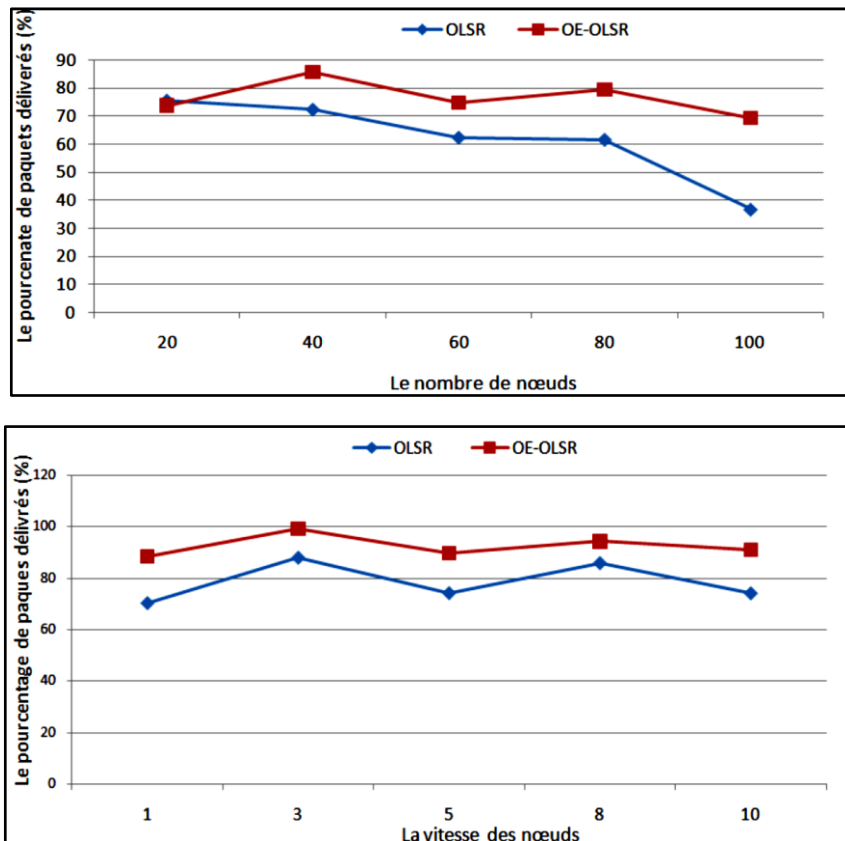


Figure 3.29 : Impact du protocole OE-OLSR sur le PDR

7. Discussions et conclusion

Dans ce chapitre, nous avons étudié en détail le mécanisme implémenté par le protocole OLSR (RFC3626) dans la sélection des relais multipoints pour assurer l'inondation de l'information dans le réseau ainsi que le processus de calcul de la table de routage des nœuds.

Aussi, une explication du choix de la version du simulateur NS-2 a été détaillée durant ce chapitre. NS-2 demeure beaucoup plus adapté à simuler des environnements mobiles avec des paramètres beaucoup plus proches à la réalité.

Les différentes simulations effectuées durant notre travail qui a été conclu par une publication [105], ont montré clairement que toutes les métriques de qualité de service QoS étudiées ont vu une nette amélioration avec l'implémentation du nouveau protocole OE-OLSR.

Bien que le protocole OLSR tel qu'il a été initialement conçu implémente un processus d'inondation très efficace basé sur la technique des relais multipoints (MPR), il nécessite davantage d'amélioration en tenant en compte d'autres critères permettant d'accroître la qualité de service ainsi que la durée de vie du réseau.

Une des améliorations a été représentée dans ce chapitre, où nous avons introduit le critère de l'énergie résiduelle des nœuds constituant le réseau dans le processus de sélection des MPR et le calcul de la table de routage, tout en se basant sur le champ « reserved » des messages HELLO et TC. Pour avoir plus d'efficacité, le processus de choix des MPRs a été modifié d'une manière à inclure l'énergie résiduelle des nœuds. Cette efficacité a clairement été conclue par les simulations effectuées.

Le facteur d'énergie dans un réseau AHWSN demeure très important et critique dans la conception d'un tel réseau. Le choix d'un protocole de routage devra impérativement tenir compte de ce critère. Les différentes simulations effectuées ont montré clairement l'efficacité du protocole OE-OLSR, mais une constatation a été effectuée est du fait qu'à un certain moment tous les nœuds se déchargent d'une manière rapide, surtout à la fin de la simulation.

Dans le chapitre suivant nous allons détailler notre deuxième apport au protocole OLSR, permettant d'équilibrer la charge sur l'ensemble des nœuds constituant le réseau. Nous allons montrer à travers d'autres simulations que l'implémentation de ce mécanisme accroîtra davantage la durée de vie du réseau AHWSN, qui demeure notre préoccupation majeure durant cette thèse.

LE-OLSR et la durée de vie du réseau AHWSN

| | |
|--|-----|
| 1. Introduction | 123 |
| 2. Notions de la durée de vie du réseau..... | 124 |
| 3. Discussions et motivations | 126 |
| 4. Protocole LE-OLSR « Lifetime Enhanced – OLSR »..... | 127 |
| 4.1 Algorithme de sélection des MPRs dans le protocole LE-OLSR | 128 |
| 5. Métriques de qualité de service QoS | 130 |
| 5.1 Messages de contrôle (Control Overhead)..... | 130 |
| 5.2 Délai de transmission moyen (Average end to end delay)..... | 130 |
| 6. Environnement de simulation | 130 |
| 7. Impact de MPRs sur la durée de vie du réseau..... | 132 |
| 8. Effet du protocole LE-OLSR sur la QoS du réseau AHWSN..... | 134 |
| 8.1 LE-OLSR et la densité du réseau | 134 |
| 8.1.1 Messages de contrôle (Control overhead) | 134 |
| 8.1.2 Délai de transmission moyen (average end-to-end delay) | 135 |
| 8.1.3 Nombre de nœuds morts (dead nodes) | 135 |
| 8.1.4 Nombre de paquets perdus (packet-loss)..... | 136 |
| 8.2 LE-OLSR et la mobilité du réseau..... | 137 |
| 9. Discussions et conclusion..... | 139 |

1. Introduction

Dans le chapitre précédent, nous avons détaillé une technique qui a été implémenté sur le protocole OLSR afin d'apporter des améliorations sur la qualité de service QoS d'un réseau AHWSN. Il s'agit essentiellement d'introduire l'énergie résiduelle des nœuds du réseau comme critère de choix des relais MPRS ainsi que dans la construction de la table de routage.

A travers les différentes simulations effectuées, nous avons constaté une nette amélioration de la qualité de service en implémentant le nouveau protocole proposé OE-OLSR.

Dans ce chapitre nous allons détailler un autre travail visant principalement la durée de vie du réseau. Cette dernière demeure sans doute la métrique la plus importante dans l'évaluation des performances d'un réseau de capteurs. En effet, dans un environnement contraint, toute ressource limitée doit être prise en compte. Toutefois, la durée de vie du réseau, comme mesure de la consommation d'énergie, occupe une place exceptionnelle puisqu'elle constitue la borne supérieure de l'utilité de ce réseau.

La durée de vie est également considérée comme un paramètre fondamental dans un contexte de disponibilité et de sécurité dans les réseaux AHWSN.

Maximiser la durée de vie du réseau revient à réduire la consommation énergétique des nœuds. Malgré les progrès qui ont été faits, la durée de vie de ces dispositifs à piles continue d'être un défi majeur et un facteur clé, exigeant davantage de recherches sur l'efficacité énergétique des plates-formes et des protocoles de communication.

2. Notions de la durée de vie du réseau

Un réseau ne peut accomplir son objectif que tant qu'il est « en vie », mais pas au-delà. La durée de vie prévue est critique dans tout déploiement de réseau de capteurs. Le but des scénarios applicatifs classiques consiste à déployer des nœuds dans un domaine sans surveillance pendant des mois ou des années.

La vie d'un réseau de capteurs correspond à la période de temps durant laquelle le réseau peut, selon le cas : maintenir assez de connectivité, couvrir le domaine entier, ou garder le taux de perte d'information en-dessous d'un certain niveau. La vie du système est donc liée à la vie nodale, même si elle peut en différer. La vie nodale correspond à la vie d'un des nœuds du réseau. Elle dépend essentiellement de deux facteurs : l'énergie qu'il consomme en fonction du temps et la quantité d'énergie dont il dispose.

Selon la discussion de [106], la quantité prédominante d'énergie est consommée par un nœud capteur durant la détection, la communication puis le traitement des données.

Il existe différentes définitions de la durée de vie d'un réseau AHWSN (fondées sur la fonctionnalité désirée). Elle peut être définie par la durée jusqu'au moment où le premier nœud meurt. Elle peut également être définie par le temps jusqu'au moment où une proportion de nœuds meurt. Si la proportion de nœuds morts dépasse un certain seuil, cela peut avoir comme conséquence la non couverture de sous-régions et/ou le partitionnement du réseau. Les définitions possibles et proposées dans la littérature sont les suivantes :

1. La durée jusqu'à ce que le premier nœud épuise toute son énergie [107] ;
2. La durée jusqu'à ce que le premier cluster Head épuise toute son énergie [108] ;
3. La durée jusqu'à ce qu'il reste au plus une certaine fraction de nœuds survivants dans le réseau [109] ;
4. Demi-vie du réseau : la durée jusqu'à ce que 50% des nœuds épuisent leurs batteries et s'arrêtent de fonctionner [107] ;
5. La durée jusqu'à ce que tous les capteurs épuisent leur énergie [110] ;
6. La durée jusqu'à ce que le réseau soit partitionné : apparition de la première division du réseau en deux (ou plus). Cela peut correspondre aussi à la mort du premier nœud (si celui-ci tient une position centrale) ou plus tard si la topologie du réseau est plus robuste [107] ;
7. k-couverture : la durée pendant laquelle la zone d'intérêt est couverte par au moins k nœuds [111] ;

8. 100%-couverture :

- La durée pendant laquelle chaque cible est couverte par au moins un nœud [112] ;
- La durée pendant laquelle l'ensemble de la zone est couverte par au moins un nœud [113] ;

9. α -couverture

- La durée cumulée, au bout de laquelle au moins une portion α de la région est couverte par au moins un nœud [114] ;
- La durée pendant laquelle la couverture tombe en-dessous d'un seuil prédéfini α [115] ;
- La durée de fonctionnement continu du système avant que la couverture ou la proportion de paquets reçus (PDR pour Packet Delivery Ratio) tombent en-dessous d'un seuil prédéfini [116] ;

10. La durée pendant laquelle un pourcentage donné de nœuds possèdent un chemin vers la Station de Base [116].

11. L'espérance de l'intervalle complet pendant lequel la probabilité de garantir simultanément une connectivité et une k-couverture est au moins α [111] ;

12. La durée jusqu'à la perte de la connectivité ou de la couverture [117] ;

13. La durée jusqu'à ce que le réseau ne fournisse plus un taux acceptable de détection d'événements [110] ;

14. La durée pendant laquelle le réseau satisfait continuellement les besoins de l'application [118].

Finalement, nous constatons bien que plusieurs définitions convergent puisque certaines d'entre elles ne sont que des relaxations des autres et la majorité suggèrent que la durée de vie du réseau dépend de la consommation d'énergie de ses nœuds. Toutefois, il peut s'avérer judicieux d'introduire une métrique pour affiner ou choisir une de ces définitions telle que la fiabilité, la couverture, la robustesse, etc.

Ce que l'on peut également constater c'est que la définition même de la durée de vie va dépendre de l'application dévolue au réseau AHWSN.

L'emplacement des nœuds défaillants est également important. Si la proportion de nœuds dépourvus d'énergie est située dans une certaine partie critique du réseau, par exemple, reliant le nœud central (Station de Base) et le reste du réseau, cela peut avoir comme conséquence le dysfonctionnement précoce du réseau entier. Il convient de noter que la simulation de la durée de vie du réseau peut être un problème statistique difficile.

De toute évidence, plus ces durées sont longues, meilleur est le fonctionnement du réseau. De manière plus générale, il est possible de chercher à estimer le complémentaire de la fonction de répartition des durées de vie des nœuds (avec la probabilité qu'un nœud survive un temps donné), ou la survie relative d'un réseau (à quel moment tel pourcentage de nœuds est encore opérationnel).

Notons toutefois que des corrélations vont s'instaurer entre les consommations des différents nœuds, ces corrélations pouvant être positives et liées à une densité importante d'événements dans une partie de la zone de surveillance ou du phénomène d'overhearing ou bien négatives en raison du routage.

Toutes ces métriques peuvent bien sûr être évaluées avec un ensemble d'hypothèses sur les caractéristiques d'un nœud donné en terme de consommation d'énergie, sur la « charge » courante que le réseau est appelé à traiter (par exemple, où et quand les événements se produisent) et aussi sur le comportement du canal radio.

Plusieurs protocoles ont été proposés pour améliorer les performances des réseaux en matière de conservation d'énergie et augmenter la durée de vie des réseaux AHWSN.

Dans notre thèse, nous nous sommes intéressés à la partie routage de l'information. Cette partie demeure une suite des travaux présentés dans le chapitre 3.

3. Discussions et motivations

Dans le chapitre précédent, nous avons étalé les différentes modifications effectuées sur le protocole OLSR basique (RFC3626) afin de tenir en compte l'énergie résiduelle des nœuds comme critère de sélection des MPRs ainsi que pour la construction de la table de routage. A travers les différentes simulations effectuées, le protocole résultant OE-OLSR demeure plus efficace en termes de QoS que l'OLSR basique. Toutefois, et à la fin de la simulation, nous avons constaté un certain comportement aléatoire du réseau et une diminution progressive de l'énergie des nœuds qui ont principalement joué le rôle de MPRs. A un certain moment de la simulation, aucun nœud ne peut être sélectionné comme MPR à cause de sa faible énergie. Ce phénomène cause une diffusion importante des paquets de contrôle à travers tout le réseau, affecte principalement la stabilité du réseau et diminue remarquablement sa durée de vie.

Ceci nous a amenés à chercher un autre mécanisme afin de faire participer tous les nœuds du réseau pour jouer le rôle de MPR. L'objectif principal est de répartir la charge sur tous les nœuds et non pas de choisir un certain nombre limité de nœuds pour

jouer le rôle de MPRs, ce qui causera la diminution rapide de leur énergie résiduelle et les rendra inactifs à la fin de simulation.

Dans OLSR, les nœuds sont sélectionnés comme MPR selon deux principaux critères : « *WILLINGNESS* » et « *REACHIBILITY* », qui signifient la capacité et le degré de voisinage du nœud. Un nœud est sélectionné comme MPR selon son aptitude (énergie résiduelle) et sa visibilité par les autres nœuds.

Pour se faire, nous nous sommes axés sur un ensemble défini dans le protocole OLSR, baptisé « *Mprselset()* » qui est un attribut du nœud. *Mprselset()* permet d'identifier le nombre de nœuds dans le réseau qui ont sélectionné ce dernier comme MPR. Cela signifie que si cet ensemble est vide, le nœud en question n'a pas été sélectionné comme MPR.

L'objet de notre travail est de se baser sur les paramètres cités ci-dessus afin de répartir la charge sur l'ensemble des nœuds constituant le réseau, permettant ainsi, de pallier au comportement aléatoire observé lorsque l'énergie résiduelle avoisine le seuil inférieur déterminé dans le protocole OE-OLSR. Ceci permettra à un nœud qui n'a pas joué le rôle de MPR et qui possède une énergie résiduelle suffisante de l'être.

4. Protocole LE-OLSR « Lifetime Enhanced – OLSR »

Dans cette section, nous allons présenter les différentes modifications apportées sur le protocole OE-OLSR décrit dans le chapitre précédent afin d'accroître la durée de vie du réseau AHWSN. Le nouveau protocole résultant et baptisé « LE-OLSR » [119].

Le protocole OE-OLSR, a permis d'introduire l'énergie résiduelle du nœud comme critère de construction des routes pour acheminer l'information de la source vers la destination. Ceci-dit, l'information emprunte la route la plus optimisée en matière d'énergie. Toutefois, quand l'énergie résiduelle du nœud atteint le niveau minimum fixé, ce dernier ne peut être sélectionné comme MPR. Après un certain temps, aucun MPR n'est présent dans le réseau. Cette situation cause un surcroît considérable des paquets de contrôle et cause une dégradation de la durée de vie du réseau.

Le protocole LE-OLSR, propose une nouvelle heuristique afin de donner la chance à un nœud qui n'a pas été sélectionné comme MPR, dû à sa contrainte d'énergie résiduelle afin de l'être. Ceci permettra de distribuer la charge sur tous les nœuds du réseau et alléger ceux qui ont été longuement sélectionnés comme MPR.

Pour se faire, nous allons introduire un nouveau paramètre baptisé « *Dynamic_threshold* ». Si un nœud n'a pas été sélectionné comme MPR durant une

longue durée, son énergie est nettement meilleure par rapport à celui qui a été longuement sélectionné comme MPR. Donc, nous allons réduire graduellement ce paramètre afin de donner la chance à tous les nœuds d'être MPR. A cet effet, la charge sera uniformément distribuée sur l'ensemble des nœuds et permettra d'accroître la durée de vie du réseau AHWSN.

Ceci-dit, les principaux objectifs visés sont :

- Réduction des paquets de contrôle
- Equilibre de la charge du réseau
- Prolongement de la durée de vie du réseau, surtout lorsque la capacité de batterie des nœuds devient trop faible.

4.1 Algorithme de sélection des MPRs dans le protocole LE-OLSR

Chaque nœud dans le réseau maintient à jour une table de ses voisins qu'ils l'on sélectionné comme MPR. Cette table est nommée « Multipoint Relay Selector Set » (MPR Selector Set). Cette information peut être extraite à travers les différents messages « HELLO », périodiquement reçus des voisins (RFC3626). Quand cette table est vide, cela signifie que le nœud en question n'a pas été sélectionné comme MPR.

Contrairement au protocole OE-OLSR, dans notre cas nous allons utiliser le champ « WILLINGNESS » du message hello pour transmettre l'information relative au seuil de l'énergie résiduelle du nœud.

La nouvelle heuristique de calcul des MPRs est définie comme suit :

```
dynamic_thresh_ = 10.0
Energy_level = (energy/initenergy_)*100;
if (energy_level<=dynamic_thresh_)
  willingness()=OLSR_WILL_NEVER;
  else if (energy_level<=30.0)
    willingness()=OLSR_WILL_LOW;
    else if (energy-level<=60.0)
      willingness()=OLSR_WILL_DEFAULT;
else willingness()=OLSR_WILL_HIGH;
```

La valeur du champ "Willingness" fera partie du message HELLO

Une fois le message HELLO reçu, le nœud exécutera les opérations suivantes :

- *Populating the 1-hop neighbor set*
- *Populating the 2-hop neighbor set*
- *MPR computation*
- *Populating of the MPR selector set*
- *Decreasing of the dynamic_thresh_ value by 1 if the MPR selector set of the node is empty : “if mprselset().size()=0 then dynamicthresh_ = dynamicthresh_ - 1;”*

En effectuant les opérations ci-dessus, le nœud informera son voisinage qui est capable de jouer le rôle de MPR.

La « Willingness » d'un nœud demeure le paramètre prépondérant dans le calcul des MPRs. Dans notre travail, cette dernière indique exclusivement l'état de la batterie d'un nœud (dans notre cas l'énergie initiale est de 100 Joules). Le champ « Willingness » d'un nœud peut avoir les valeurs de 0 à 7, et spécifie la capacité d'un nœud afin de transmettre le trafic vers d'autres nœuds voisins. Par défaut, un nœud a une valeur WILL_DEFAULT. WILL_NEVER indique que le nœud en question ne puisse router des paquets en provenance d'autres nœuds, à cause de ses ressources limitées (batterie faible). WILL_ALWAYS indique que ce nœud devra toujours être sélectionné comme MPR à cause de ses ressources stables (alimenté par une source permanente, une position stratégique couvrant plusieurs nœuds du réseau...).

Dans notre travail nous avons divisé le champ Willingness (0-100) sur 4 niveaux :

- De 100 à 60 → Willingness = WILL_HIGH
- De 60 à 30 → Willingness = WILL_DEFAULT
- De 30 à 10 → Willingness = WILL_LOW
- Inférieur à 10 → Willingness = WILL_NEVER

A noter que les valeurs 60-30-10 ont été prises arbitrairement. Nous pouvons supposer d'autres valeurs en maintenant toujours les 04 niveaux décrits précédemment.

5. Métriques de qualité de service QoS

Dans un réseau AHWSN, nous avons besoin de diffuser des messages de contrôle afin de maintenir les fonctionnalités du réseau en matière de sa topologie, ou de publier de nouveaux services. Cependant, ce phénomène d'inondation des messages est assez gourmand en termes de ressources réseau. Par conséquent, l'optimisation de la diffusion de ces messages de contrôle demeure très importante et affecte directement les performances du réseau [120].

De la même manière que dans le cas OE-OLSR, nous avons utilisé des métriques usuelles afin de comparer les performances des deux protocoles en termes de qualité de service QoS.

5.1 Messages de contrôle (Control Overhead)

C'est le nombre total des paquets de routage (HELLO et TC) pour chaque paquet de donnée délivré.

Nous avons déjà vu que la plus grande partie de l'énergie des nœuds est consommée dans la transmission des paquets. Ceci-dit, tant que le nombre des messages de contrôle est minime, l'énergie consommée est conservée et la durée de vie du réseau est prolongée.

5.2 Délai de transmission moyen (Average end to end delay)

Cette métrique a déjà été définie dans le chapitre 3 (section 6.1.1). Un minimum de délai signifie que le paquet transmis a emprunté la route la plus optimale. Cette métrique demeure très importante dans la décision de la performance d'un protocole de routage [121]

6. Environnement de simulation

Comme suite au chapitre précédent, les paramètres de simulations ont été conservés. Nous avons implémenté OLSR et LE-OLSR sur NS-2. Les nœuds mobiles se déplacent selon le modèle « Random Waypoint Mobility Model » décrit dans le chapitre 3 (section 4.3). La couche MAC utilisée est définie par la norme IEEE 802.11 avec un débit de 2 paquets/seconde. Le trafic data utilisé est de type CBR.

Le temps de la simulation a été ajusté à 300 secondes, ceci nous permettra d'observer le comportement du réseau quand les nœuds atteignent un niveau d'énergie

| | Simulation Parameter | Value |
|------------------|---------------------------|---------------------|
| Configuration | <i>Transmission Area</i> | <i>870 x 870</i> |
| | <i>Nodes Number</i> | <i>20,60,80,100</i> |
| | <i>Node Speed</i> | <i>1 m/S</i> |
| | <i>Simulation time</i> | <i>300s</i> |
| Traffic | <i>Traffic Type</i> | <i>CBR</i> |
| | <i>Connections number</i> | <i>8</i> |
| | <i>Packet rate</i> | <i>2 packets</i> |
| Energy | <i>Initial energy</i> | <i>100 joules</i> |
| | <i>Rx Power</i> | <i>1.1 w</i> |
| | <i>Tx Power</i> | <i>1.65 w</i> |
| | <i>Idle Power</i> | <i>0.3w</i> |
| | <i>Sleep Power</i> | <i>0.042w</i> |
| Routing protocol | <i>OE-OLSR, LE-OLSR</i> | |
| Mac layer | <i>802.11</i> | |
| Physical layer | <i>CP Threshold</i> | <i>10.0 dB</i> |
| | <i>CS Threshold</i> | <i>1.559e-11</i> |
| | <i>RX Threshold</i> | <i>3.652e-10</i> |
| | <i>Bandwidth</i> | <i>2 MHZ</i> |
| | <i>Frequency</i> | <i>914 MHZ</i> |

Tableau 4.1 : Paramètres de simulation de LE-OLSR et OE-OLSR

7. Impact des MPRs sur la durée de vie du réseau

Afin de bien expliquer notre approche, nous avons étudié l'évolution du nombre de MPRs dans le temps. Comme nous l'avons expliqué précédemment, maintenir un nombre suffisant de relais multipoints permet de limiter les messages de diffusion et accroître davantage la durée de vie du réseau.

Nous avons simulé un réseau composé de 100 nœuds avec les paramètres décrit précédemment et nous avons calculé le nombre de MPRs en fonction du temps.

Le tableau 4.2 représente quelques valeurs du fichier trace entre 120 et 300 secondes. En effet, nous avons comparé le nombre de MPRs dans le réseau par rapport à celui des nœuds morts (dead nodes), ou dont l'énergie résiduelle devient au-dessous de 5%.

| Simulation Time (S) | LE-OLSR | | OE-OLSR | |
|---------------------|---------|------------|---------|------------|
| | MPRs | Dead nodes | MPRs | Dead nodes |
| 120 | 64 | 0 | 65 | 0 |
| 180 | 40 | 12 | 40 | 20 |
| 210 | 30 | 47 | 14 | 87 |
| 250 | 20 | 72 | 0 | 93 |
| 280 | 5 | 85 | 0 | 100 |

Tableau 4.2 : Nombre de MPRs VS nœuds morts

Ceci illustre clairement notre approche. En effet, l’apport au protocole OLSR agit principalement à la fin de la simulation où l’énergie résiduelle des nœuds s’affaiblit considérablement. Notre heuristique permet de maintenir un nombre suffisant de MPRs afin de transmettre efficacement l’information et limiter les messages de diffusion envoyés périodiquement par tous les nœuds du réseau afin de connaître sa topologie et de calculer les chemins de routage.

La figure 4.1 représente le résultat ci-dessus sous une forme graphique.

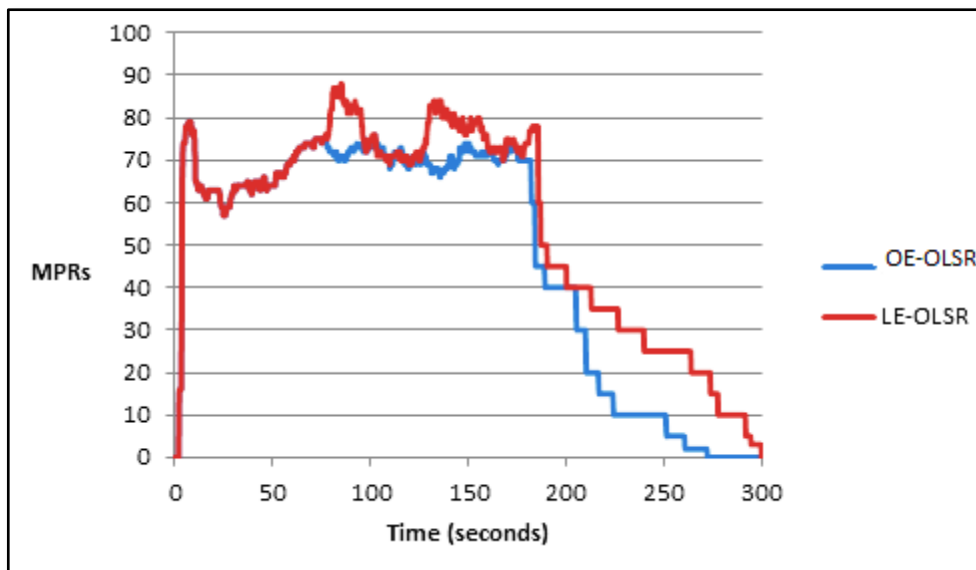


Figure 4.1 : Evolution du nombre de MPRs

Un réseau implémentant OLSR comme protocole de routage, incite les nœuds à envoyer des messages de contrôle « HELLO » chaque 02 secondes afin de découvrir leur voisinage. Le non maintien d’un nombre suffisant de MPRs signifie que ces messages seraient diffusés et inondent le réseau en entier. Ceci explique aussi, l’optimisation en termes de messages de contrôle (control overhead).

8. Effet du protocole LE-OLSR sur la QoS du réseau AHWSN

Dans cette partie, nous allons étaler les différentes simulations effectuées durant notre travail afin de comparer le protocole LE-OLSR par rapport à OE-OLSR et son apport sur la qualité de service QoS du réseau.

8.1 LE-OLSR et la densité du réseau

Dans cette section, nous allons simuler l'implémentation du protocole LE-OLSR, en le comparant à celui de OE-OLSR, en augmentant progressivement le nombre de nœuds du réseau (20, 60, 80, 100)

8.1.1 Messages de contrôle (Control overhead)

La figure 4.2 illustre l'effet de la densité du réseau sur les messages de contrôle.

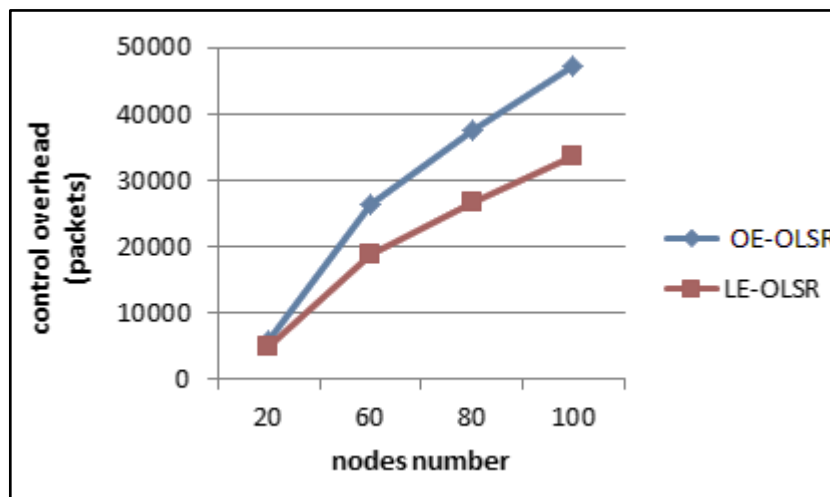


Figure 4.2: Control Overhead et la densité du réseau

Comme nous l'avons évoqué précédemment (5.1), cette métrique consiste à déterminer le nombre de paquets de routage à savoir les messages « HELLO » et « TC » diffusés périodiquement afin de transmettre un paquet de données entre la source et la destination. Ces messages de contrôle consomment énormément d'énergie des nœuds, vu leur nombre important et leur périodicité, sachant que la plus grande partie de l'énergie est consommée durant la transmission.

Il demeure clair que le protocole LE-OLSR diminue significativement l'inondation des messages de contrôle. Ceci donne l'opportunité aux nœuds du réseau d'optimiser l'énergie consommée et d'accroître la durée de vie du réseau.

8.1.2 Délai de transmission moyen (average end-to-end delay)

Le délai de transmission se réfère au temps écoulé pour transmettre le paquet de données d'un nœud source vers sa destination. Comme nous l'avons déjà expliqué, ceci est tributaire de plusieurs paramètres du réseau, à savoir le nombre de sauts ainsi que le délai de passage dans les files d'attente des routeurs du réseau...etc.

La figure 4.3. Illustre l'impact de la densité du réseau sur cette métrique

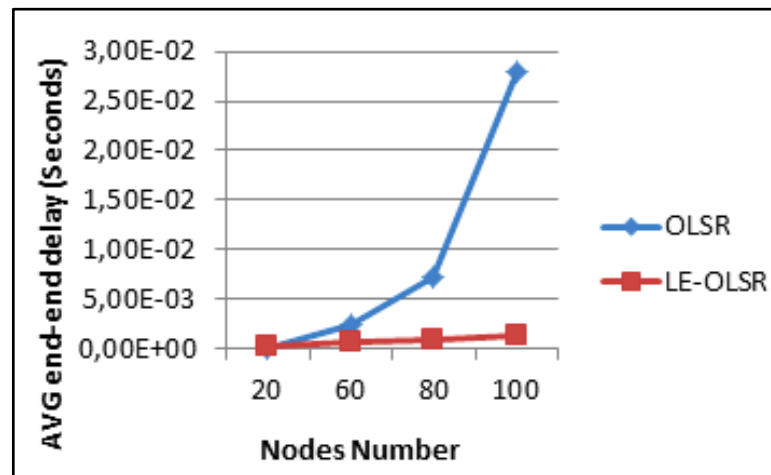


Figure 4.3 : Délai de transmission moyen (AVG end-to-end delay) et la densité

Un réseau implémentant le protocole OLSR, diffuse les messages TC chaque 05 secondes. Ces derniers véhiculent l'information sur la topologie du réseau qui sera utilisée par les nœuds afin de construire leurs tables de routage.

Comme ces messages demeurent sous la responsabilité exclusive des MPRs, un nombre suffisant de ces derniers, permettra de transmettre efficacement les informations de routage afin de choisir le chemin optimal. Ceci optimisera davantage la consommation de l'énergie des nœuds et accroîtra la durée de vie du réseau AHWSN.

8.1.3 Nombre de nœuds morts (dead nodes)

Dans notre simulation, un nœud est considéré comme mort si son énergie devient résiduelle inférieure à 5%. Cette métrique demeure très importante afin de savoir si la charge du réseau a été uniformément distribuée sur l'ensemble des nœuds constituant le réseau. Afin d'avoir une information fiable pour extraire le nombre des nœuds morts à partir du fichier trace résultant, nous avons utilisé un temps de référence de 185 secondes.

La figure 4.4 illustre l'effet de la densité du réseau sur le nombre des nœuds morts pour les deux protocoles LE-OLSR et OLSR

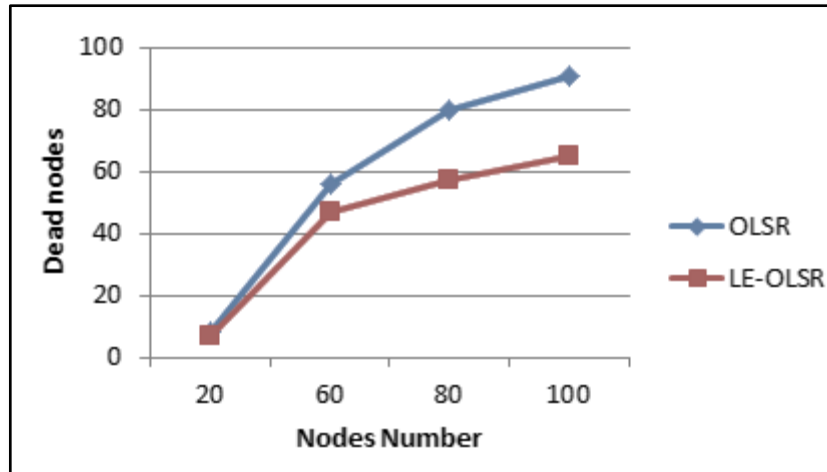


Figure 4.4. : Nombre de nœuds morts (dead nodes)

Il est clair que le nombre de morts est beaucoup moindre dans le cas du protocole LE-OLSR. Ceci est le résultat de tout ce qui a été expliqué précédemment.

8.1.4 Nombre de paquets perdus (packet-loss)

Le script java que nous avons développé pour nous permettre d'extraire les différentes informations à partir du fichier trace résultant, permet aussi de calculer le nombre de paquets reçus.

Le paramètre packet-loss est une métrique importante afin de déterminer la performance du protocole dans la transmission des paquets de données de la source vers la destination et éviter les retransmissions qui sont dues aux pertes de paquets dans le réseau. Ces retransmissions épuisent considérablement l'énergie des nœuds et diminuent la durée de vie du réseau.

$$\text{Packet-loss} = \text{N}^\circ \text{ de paquets émis} - \text{N}^\circ \text{ de paquets reçus}$$

Une valeur moindre du packet-loss signifie une bonne performance du protocole de routage implémenté.

La figure 4.5, illustre l'évolution de cette métrique en fonction de la densité du réseau.

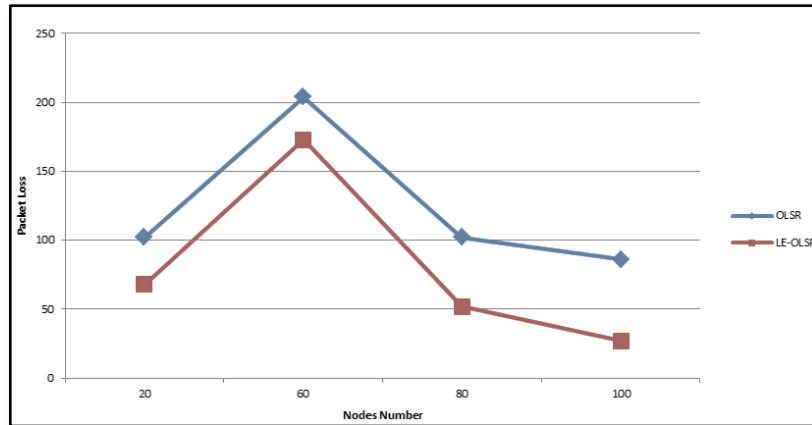


Figure 4.5 : Packet-loss Vs nombre de nœuds

Le résultat de la simulation exprime clairement que le protocole LE-OLSR minimise considérablement le nombre de paquets perdus, d'où une qualité de service meilleure, comparée à celle du protocole OLSR.

8.2 LE-OLSR et la mobilité du réseau

Les résultats des simulations précédentes ont montré clairement l'apport positif de notre modification au protocole OLSR à la qualité de service du réseau AHWSN et sa durée de vie, en se focalisant sur la densité du réseau.

Dans cette section, nous allons présenter les différents résultats obtenus suite à un comportement autre du réseau. Il s'agit de la mobilité des nœuds, en augmentant progressivement leurs vitesses (1, 3, 5, 8 m/s). Un réseau AHWSN suppose que les nœuds se déplacent en permanence avec des trajectoires aléatoires et des vitesses variables.

Le modèle de mobilité retenu « Random Waypoint Model » [102], semble le plus réaliste afin de simuler un réseau mobile.

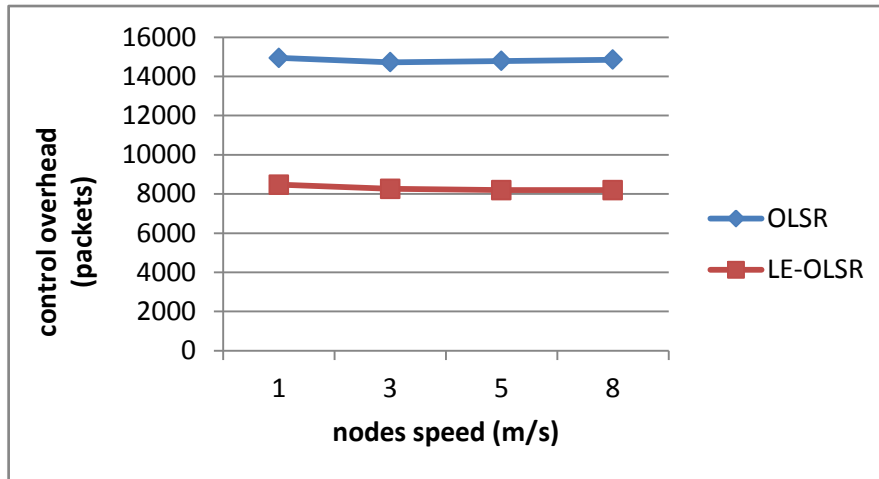


Figure 4.6 : Control overhead Vs mobilité du réseau

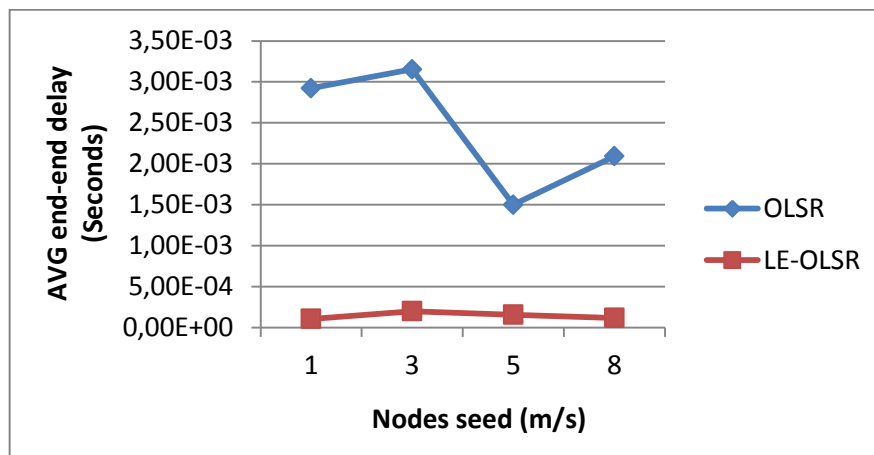


Figure 4.7 : Délai de transmission moyen Vs mobilité du réseau

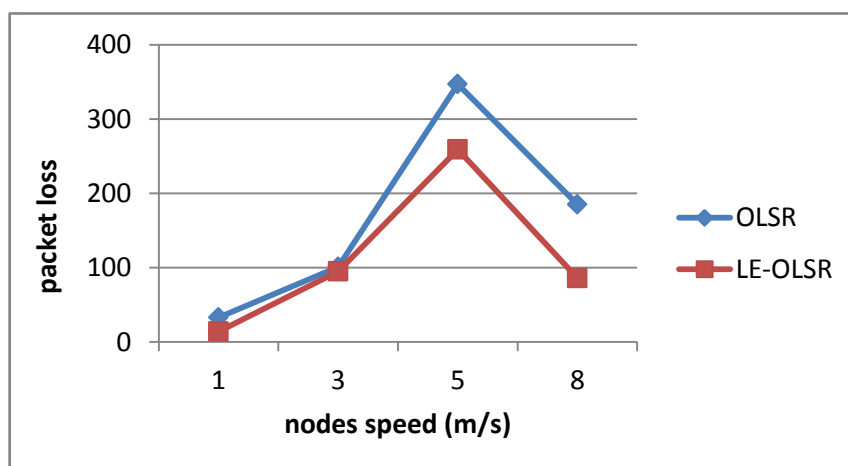


Figure 4.8 : Packet-loss Vs mobilité du réseau

A travers toutes les simulations effectuées, il demeure clair que la qualité de service QoS obtenue dans le cas du protocole LE-OLSR est nettement meilleure que celle

du protocole OLSR basique. Aussi, cette qualité est transparente par rapport à la densité ou la mobilité du réseau. Tout cela, soutient davantage notre hypothèse préalable qui était de maintenir un nombre de MPRs suffisant afin de pallier au comportement aléatoire du réseau AHWSN lorsque l'énergie des nœuds diminue progressivement.

Toutes les explications données dans la section 8.1, s'appliquent tantôt pour la densité du réseau que pour sa mobilité. Ceci-dit, le protocole LE-OLSR demeure transparent par rapport au changement des caractéristiques physiques du réseau AHWSN, car son objectif principal est de répartir la charge sur l'ensemble des nœuds afin d'optimiser leur consommation d'énergie et augmenter la durée de vie du réseau.

9. Discussions et conclusion

Dans ce chapitre nous avons étalé notre travail, publié dans [119], relatif au protocole LE-OLSR et son apport sur la qualité de service d'un réseau AHWSN.

Ce protocole intervient principalement lorsque l'énergie résiduelle des nœuds atteint un niveau bas, afin d'équilibrer la charge du réseau et de maintenir un nombre suffisant de relais multipoints, responsables de router l'information. Pour se faire l'heuristique choisie se base principalement sur l'ensemble « MPRSet » qui est l'un des attributs du nœud mobile et qui détermine le nombre de nœuds qui ont sélectionné ce dernier comme MPR.

A travers les simulations effectuées, le maintien d'un nombre suffisant de MPRs, limitera l'inondation inutile des messages de contrôle à travers le réseau entier. Car la plus grande énergie consommée demeure dans la transmission des paquets.

En effet, dans le but de construire l'information sur la topologie du réseau, chaque nœud qui est sélectionné comme MPR, est responsable d'échanger des messages TC « Topology control ». Chaque nœud maintient une table de routage qui lui permet de router les données, destinées aux autres nœuds du réseau. Cette table est construite à travers les informations contenues dans des bases appelées « Local link information base » et « topology set », construites par chaque nœud à travers les échanges des messages HELLO et TC. Après chaque changement des informations contenues dans ces deux bases, la table de routage est recalculée de nouveau afin de mettre à jour les routes vers toutes les destinations du réseau. Ceci-dit, le nombre de MPRs possède un impact direct afin de construire cette table de routage dans le but de choisir le chemin optimal entre la source et la destination.

Ceci a bien été confirmé par les simulations effectuées, où nous avons démontré que les différentes métriques de la QoS ont été améliorées, spécialement dans le cas où le nombre des nœuds devient important ou le réseau demeure fortement mobile.

Les simulations effectuées ont démontré une optimisation entre 30% à 57% en termes de nombre de paquets de contrôle « control-overhead », ce qui explique que l'énergie totale consommée est nettement optimisée.

En conclusion, notre nouveau protocole LE-OLSR, permet une nette optimisation à un réseau AHWSN dense et fortement mobile, ainsi les paquets sont acheminés à travers des routes optimales en termes d'énergie entre la source et la destination. Ceci éliminera davantage les congestions et la charge sera uniformément distribuée à travers le réseau.

Conclusion générale et perspectives

Les réseaux AHWSN ont connu au cours de ces dernières années un formidable essor aussi bien dans l'industrie que dans le milieu universitaire, surtout avec l'avènement du monde des Smartphones et des tablettes. Cela est principalement attribuable à l'ampleur sans précédent des possibilités qu'offre cette technologie en matière de densité et de mobilité. Toutefois, Ces réseaux doivent aussi faire face à d'importants défis de conception en raison de leurs capacités de calcul et de stockage limitées et surtout de leur dépendance à l'égard d'une énergie limitée fournie par une batterie.

L'énergie est une ressource critique et constitue souvent un obstacle majeur au déploiement des réseaux AHWSN qui prétendent à l'omniprésence dans le monde de demain.

Ceci a mené les chercheurs à étudié profondément dans diverses travaux, les différents aspects liés au déploiement de ces réseaux, en proposant des solutions pour faire face aux contraintes intrinsèques et extrinsèques de ces réseaux, et en développant des protocoles de communication tenant compte de ces aspects à travers toutes les couches du modèle OSI.

Notre thèse a porté essentiellement sur l'optimisation de l'énergie dans les réseaux AHWSN, notamment au niveau routage de l'information, tout en proposant des mécanisme pouvant apporter des améliorations en termes de conservation d'énergie et d'optimisation de la durée de vie du réseau AHWSN.

La QoS est défini essentiellement comme un ensemble de conditions et de critères qui doivent être satisfaites par un réseau durant le transport d'un flux de données d'une source vers une destination. Le réseau est appelé à garantir un ensemble d'exigences des utilisateurs en termes de transmission de bout en bout, consommation d'énergie et de délai qui demeurent les métrique les plus prépondérantes dans un réseau AHWSN.

Synthèse

Dans la première partie de notre thèse, avons évoqué la notion des réseaux AHWSN, leurs domaines d'application ainsi que les contraintes liées à la conception et

au déploiement de tels réseaux. Nous avons mis l'accent sur la contrainte d'énergie qui demeure l'axe principale de notre recherche dans notre thèse.

Une attention particulière a été attribuée aux protocoles de routage et leurs classifications dans les réseaux AHWSN afin que nous puissions introduire la problématique réelle liée principalement à la qualité de service QoS ainsi que l'optimisation de tels réseaux qui demeurent les axes principaux des chercheurs dans ce domaine, si on veut que ces réseaux remplacent les réseaux filaires existants.

La qualité de service des réseaux AHWSN a été divisée en trois principales échelles : interne, locale et globale, déterminant ainsi les différentes contraintes liées tantôt aux caractéristiques intrinsèques des mobiles, ainsi que le routage des informations au niveau du réseau qui demeure complètement différent par rapport à celui implémenté dans les réseaux filaires (mobilité constante des nœuds).

Bien que les réseaux de capteurs (WSN) forment une section des réseaux AHWSN, nous avons consacré une partie du chapitre 2 afin de décrire les différents paramètres liés à la qualité de service lors du déploiement de tels réseaux. Ces paramètres sont liés aux applications de ces capteurs ainsi que la manière dont les informations sont routés à travers le réseau.

Vu que l'axe principale de notre recherche demeure la conservation de l'énergie afin d'optimiser la durée de vie des réseaux AHWSN, nous avons évoqué les différentes techniques et algorithmes qui ont été conçus à cet effet. Une présentation des différentes sources de consommation d'énergie des nœuds a été effectuée, avant de passer en revue les mécanismes déployés à travers toutes les couches du modèle OSI (MAC, Réseau et transport). Il existe bien évidemment beaucoup d'autres techniques de conservation d'énergie. Par exemple, les paradigmes émanant de l'auto-organisation des systèmes, les mécanismes cross-layers et d'autres protocoles indépendants de niveau réseau ou de niveau application.

Dans le chapitre 3, nous avons détaillé notre contribution dans le domaine de la conservation de l'énergie au niveau de la couche réseau, en se basant sur un protocole de routage largement utilisé dans le domaine des réseaux AHWSN, en l'occurrence OLSR.

Dans ce chapitre, nous avons étudié en détail le mécanisme implémenté par le protocole OLSR (RFC3626) dans la sélection des relais multipoints pour assurer l'inondation de l'information dans le réseau ainsi que le processus de calcul de la table de routage des nœuds.

Aussi, une explication du choix de la version du simulateur NS-2 a été détaillée durant ce chapitre. NS-2 demeure beaucoup plus adapté à simuler des environnements mobiles avec des paramètres beaucoup plus proches à la réalité.

Les différentes simulations effectuées durant notre travail qui a été conclu par une publication [105], ont montré clairement que toutes les métriques de qualité de service QoS étudiées ont vu une nette amélioration en implémentant le nouveau protocole OE-OLSR.

Bien que le protocole OLSR tel qu'il a été initialement conçu implémente un processus d'inondation très efficace basé sur la technique des relais multipoints (MPR), nous avons montré qu'il nécessite davantage d'amélioration en tenant en compte d'autres critères permettant d'accroître la qualité de service ainsi que la durée de vie du réseau.

Une des améliorations a été représentée dans ce chapitre, où nous avons introduit le critère de l'énergie résiduelle des nœuds constituant le réseau dans le processus de sélection des MPR et le calcul de la table de routage, tout en se basant sur le champ « reserved » des messages HELLO et TC. Pour avoir plus d'efficacité, le processus de choix des MPRs a été modifié d'une manière à inclure l'énergie résiduelle des nœuds. Cette efficacité a clairement été conclue par les simulations effectuées.

Le facteur d'énergie dans un réseau AHWSN demeure très important et critique dans la conception d'un tel réseau. Le choix d'un protocole de routage devra impérativement tenir compte de ce critère. Les différentes simulations effectuées ont montré clairement l'efficacité du protocole OE-OLSR, mais une constatation a été effectuée est du fait qu'à un certain moment tous les nœuds se déchargent d'une manière rapide, surtout à la fin de la simulation.

Dans le chapitre 4 nous avons étalé notre travail, publié dans [119], relatif au protocole LE-OLSR et son apport sur la qualité de service d'un réseau AHWSN.

Ce protocole permet de pallier à la contrainte discutée dans le chapitre 3 et intervient principalement lorsque l'énergie résiduelle des nœuds atteint un niveau bas, afin d'équilibrer la charge du réseau et de maintenir un nombre suffisant de relais multipoints, responsables de router l'information. Pour se faire l'heuristique choisie se base principalement sur l'ensemble « MPRSet » qui est un des attributs du nœud mobile et qui détermine le nombre de nœuds qui ont sélectionné ce dernier comme MPR.

A travers les simulations effectuées, le maintien d'un nombre suffisant de MPRs, limitera l'inondation inutile des messages de contrôle à travers le réseau entier. Car la plus grande énergie consommée demeure dans la transmission des paquets.

En effet, dans le but de construire l'information sur la topologie du réseau, chaque nœud qui est sélectionné comme MPR, est responsable d'échanger des messages TC « Topology control ». Chaque nœud maintient une table de routage qui lui permet de router les données, destinées aux autres nœuds du réseau. Cette table est construite à travers les informations contenues dans des bases appelées « Local link information base » et « topology set », construites par chaque nœuds à travers les échanges des messages HELLO et TC. Après chaque changement des informations contenues dans ces deux bases, la table de routage est recalculée de nouveau afin de mettre à jour les routes vers chaque destination du réseau. Ceci-dit, le nombre de MPRs possède un impact direct afin de construire cette table de routage dans le but de choisir le chemin optimal entre la source et la destination.

Ceci a bien été confirmé par les simulations effectuées, où nous avons démontré que les différentes métriques de la QoS ont été améliorées, spécialement dans le cas où le nombre des nœuds devient important ou le réseau demeure fortement mobile.

La densité et la mobilité des nœuds doivent avoir une grande influence sur les performances du protocole de routage. Une densité faible peut causer des déconnexions fréquentes du réseau et une densité forte accentue quant à elle, le problème de la congestion, et une dégradation des performances.

Les simulations effectuées ont démontré une optimisation entre 30% à 57% en termes de nombre de paquets de contrôle « control-overhead », ce qui explique que l'énergie totale consommée est nettement optimisée.

En conclusion, notre nouveau protocole LE-OLSR, permet une meilleure optimisation à un réseau AHWSN dense et fortement mobile, ainsi les paquets sont acheminés à travers des routes optimales en termes d'énergie entre la source et la destination. Ceci éliminera davantage les congestions et la charge sera uniformément distribuée à travers le réseau. La QoS dans un réseau est un compromis de plusieurs paramètres. Notre contribution a nettement amélioré les critères étudiés, au détriment d'un problème des nœuds isolés du réseau et leur connectivité.

Perspectives

Les travaux que nous avons effectués dans cette thèse nous ouvrent de nombreuses perspectives de recherche. Nous les structurons selon nos réflexions comme suit :

- Dans notre travail le choix des seuils de décision sur l'énergie résiduelle des nœuds ainsi que celui des nœuds morts était arbitraire. Nous pouvons

envisager des seuils dynamiques et simuler les performances des protocoles résultants.

- D'autres déploiements de réseaux AHWSN, dans des environnements variés peuvent rendre l'étude expérimentale encore plus passionnante, ils apporteront de riches enseignements pour le développement de modèles exacts et le dimensionnement de protocoles. En vue de l'arrivée massive des réseaux urbains et domotiques, des études de cohabitation avec d'autres normes seront du plus grand intérêt pour la fiabilité et la robustesse des futures solutions.
- Concernant le routage, en tenant compte de l'énergie résiduelle des nœuds, nous pensons que c'est une problématique attrayante aussi bien d'un point de vue théorique que pratique. Les premiers résultats de nos mécanismes d'équilibrage de charge nécessitent une consolidation par des expérimentations afin d'étayer les hypothèses que nous avons retenues. D'autres études avec des scénarios diversifiés nous semblent intéressantes.
- Il y a lieu de considérer des réseaux avec des topologies irrégulières, des nœuds avec des énergies résiduelles différentes, d'implémenter diverses modèles de propagation et de mouvements aléatoires dans la même simulation pour se rapprocher de la réalité.
- Nous envisageons également de généraliser les méthodes présentées afin de tenir compte d'une répartition non uniforme des énergies voire des trafics à écouler, ainsi que d'autres aléas tels que les pannes potentielles des nœuds, etc.
- Enfin, De part les observations sur le partage de charge dans la couche réseau, nous pensons que la combinaisons des stratégies d'optimisation de l'énergie à travers toutes les couches du modèle OSI avec des techniques d'agrégations, de réduction de données ou de data-gathering apportera des gains considérables en terme d'économie d'énergie et de la durée de vie du réseau AHWSN.

Bibliographie et Références

- [1] A.Freebersyser, B.Leiner, "A DoD perspective on mobile ad hoc networks", Ad Hoc Networking, Addison Wesley, pp. 29-51, 200;
- [2] J.Westcott, G.Lauer, "Hierarchical routing for very large networks", Proc. IEEE, MILCOM '84, pp. 214-218, 21-24.
- [3] W.Fifer, F.Bruno, 'The low-cost packet radio', Proceedings of the IEEE 75 (1), pp 33-42, (1987)
- [4] B.Leiner, R.Ruth, A.R. Sastry, "Goals and challenges of the DARPA GloMo program", IEEE Personal Communications 3 (6), pp 34-43, 1996
- [5] Althouse, E: Extending the Littoral Battlespace (ELB). "Advanced Concept Technology Demonstration (ACTD)", NATO Information Systems Technology Panel Symposium on Tactical Mobile Communications, June 1999
- [6] Boussad AIT-SALEM. Sécurisation des Réseaux Ad hoc : Systèmes de Confiance et de Détection de Répliques. Thèse de doctorat. P12. 12/07/2011
- [7] I.F.Akyildiz, S.Weilian, Y.Sankarasubramaniam, et E.Cayirci, "A survey on sensor networks," IEEE Communications Magazine, vol. 40, pp. 102-14, 2002.
- [8] C.Intanagonwiwat, R.Govindan, D.Estrin, J.Heidemann, et F.Silva, "Directed diffusion for wireless sensor networking," IEEE/ACM Transactions on Networking, vol. 11, pp. 2-16, 2003.
- [9] I.F.Akyildiz, I.H.Kasimoglu, "Wireless sensor and actor networks: research challenges," Ad Hoc Networks, vol. 2, pp. 351-367, 2004.
- [10] J.N.Al-Karaki, A.E.Kamal, "Routing techniques in wireless sensor networks: a survey," IEEE Wireless Communications, vol. 11, pp. 6-28, 2004.
- [11] B.David, E.Deborah, "Rumor routing algorithm for sensor networks," in Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications, Atlanta, Georgia, USA, , pp. 22-31. 2002
- [12] M.Robert, J.John, K.Frans, L.Jinyang, D.Douglas, "CarNet: a scalable ad hoc wireless network system," in Proceedings of the 9th workshop on ACM SIGOPS European workshop: beyond the PC: new challenges for the operating system, Kolding, Denmark , , pp. 61-65. 2000
- [13] C.Chee-Yee, S.P.Kumar, "Sensor networks: evolution, opportunities, and challenges," in Proceedings of the IEEE, vol. 91, pp. 1247-1256, 2003.
- [14] CMOP, "Projet CORIE," tiré de: <http://www.ccalmr.ogi.edu/>, 2009.

- [15] E.P.Charles, T.M.Jari, W.Ryuji, N.Anders, J.T.Antti, "Internet connectivity for mobile ad hoc networks," *Wireless Communications and Mobile Computing*, vol. 2, pp. 465-482, 2002.
- [16] J.Wieselthier, G.Nguyen, et A.Ephremides, "Resource-Limited Energy-Efficient Wireless Multicast of Session Traffic," in *Proceedings of the 34th Annual Hawaii International Conference on System Sciences*, IEEE Computer Society, 2001.
- [17] W.Zhijun, K.D.Sajal, C.Hao, "A Scalable Asynchronous Cache Consistency Scheme (SACCS) for Mobile Environments," *IEEE Transaction on Parallel and Distributed Systems*, vol. 15, pp. 983-995, 2004.
- [18] L.Sunho, L.Wang-Chien, C.Guohong, R.D.Chita, "Cache invalidation strategies for internet-based mobile ad hoc networks," *Computer Communications*, vol. 30, pp. 1854-1869, 2007.
- [19] L.Wenzhong, E.Chan, W.Yilin, C.Daoxu, "Cache Invalidation Strategies for Mobile Ad Hoc Networks," in *Proceedings of the International Conference on Parallel Processing*, pp. 57-57. 2007
- [20] F.A.Ian, M.Tommaso, R.C.Kaushik, "A survey on wireless multimedia sensor networks," *Computer Networks*, vol. 51, pp. 921-960, 2007.
- [21] S.Plancoulaine, A.Bachir, D.Barthel. Wsn node energy dissipation,. France Telecom R&D, Technical Report. July 2006
- [22] E.Perkins, P.Bhagwat. "Highly dynamic destination sequenced distance-vector routing (dsv) for mobile computers". In *Proceedings of the conference on Communications architectures, protocols and applications*, pp 234–244, 1994.
- [23] *Optimized link state routing protocol (olsr)*, 2003
- [24] J.David, M.David A, B.Josh. "Dsr : The dynamic source routing protocol for multi-hop wireless ad hoc networks". *Ad Hoc Networking*, edited by Charles E. Perkins, Chapter 5, pp 139–172. Addison-Wesley, 2001.
- [25] C.Perkins, E.Belding-Royer, S.Das. "Ad hoc on-demand distance vector (aodv) routing", 2003.
- [26] J.Haas, R.Pearlman. "Zrp : a hybrid framework for routing in ad hoc networks". pp 221–253, 2001.
- [27] F.Sailhan. « Localisation De Ressources Dans Les Réseaux Ad Hoc ». Thèse de doctorat, pp 26. Avril 2010
- [28] M.Ali, S. K. Ravula, "Real-time support and energy efficiency in wireless sensor networks". Technical report, IDE0805, January 2008.

- [29] K.Akkaya, M.Younis, "A Survey on Routing Protocols for Wireless Sensor Networks". *Journal of Ad Hoc Networks*, Vol. 3, No. 3, May 2005, pp. 325-349.
- [30] J.N. Al-Karaki, A.E. Kamal, "Routing techniques in wireless sensor networks: survey. *Wireless Communications*". IEEE, December 2004.
- [31] W.Heinzelman, A.Chandrakasan, H.Balakrishnan, "Energy-efficient communication protocol for wireless sensor networks ". In the Proceeding of the Hawaii International Conference System Sciences, Hawaii, January 2000.
- [32] A. Manjeshwar, D. P. Agrawal, "TEEN: A Protocol for Enhanced Efficiency in Wireless Sensor Networks". 1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing, San Francisco, CA, April 2001.
- [33] N. V. Subramanian, "Survey on Energy-Aware Routing and Routing Protocols for Sensor Networks". Technical Report, Computer Science, University of North Carolina, Charlotte. 2004.
- [34] V.Rodoplu, T. H. Ming, "Minimum energy mobile wireless networks". IEEE *Journal of Selected Areas in Communications*, Vol. 17, No. 8, , pp. 1333-1344. 1999.
- [35] Y.Xu, J.Heidemann, D.Estrin, "Geography-informed Energy Conservation for Ad hoc Routing". In Proceedings of the 7th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM'01), Rome, Italy, pp.70-84. July 2001
- [36] Y.Yu, D.Estrin, R.Govindan, "Geographical and Energy-Aware Routing: A Recursive Data Dissemination Protocol for Wireless Sensor Networks," UCLA Compute Science Department Technical Report, UCLA-CSD TR-01-0023, May 2001.
- [37] B.Krishnamachari, D.Estrin, S.Wicker, "Modelling Data-Centric Routing in Wireless Sensor Networks". USC Computer Engineering Technical Report CENG 02-14, 2002.
- [38] H.Qi.P.T.Kuruganti, Y.Xu, "The Development of Localized Algorithms in Wireless Sensor Networks". Published on 202 SENSORS ISSN, pp 1424- 8220.
- [39] C.Intanagonwiwat, R.Govindan, D.Estrin, "Directed diffusion: A scalable and robust communication paradigm for sensor networks". In the Proceedings of the 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'00), Boston, MA, August 2000.

- [40] B.Krishnamachari, D.Estrin, S.Wicker, "Modeling Data Centric Routing in Wireless Sensor Networks". In the Proceedings of IEEE INFOCOM, New York, NY, June 2002.
- [41] QoS Forum. "QoS protocols and architectures". White paper of QoS Forum, <http://www.qosforum.com>
- [42] E.Crawley, R.Nair, B.Rajagopalan, H.Sandick, "A Framework for QoS-based Routing in the Internet", IETF RFC2386
- [43] JP.Chanet. "Algorithme de routage coopératif à qualité de service pour des réseaux ad hoc agro-environnementaux". Thèse de Doctorat pp 76. Avril 2007
- [44] C.R.Lin, M.Gerla, 'MACA/PR : "An Asynchronous Multimedia Multihop Wireless Network". In Proceedings of IEEE INFOCOM '97, Apr. 1997
- [45] The Institute of Electrical and Electronics Engineers, Inc. "IEEE Std 802.11 – Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. The Institute of Electrical and Electronics Engineers".
- [46] J.Deng, RS.Chang. "A priority scheme for IEEE 802.11 DCF access method", IEICE Transactions in Communications, vol 82-B, n 1, 1999
- [47] I.Aad, C.Castelluccia, "Differentiation mechanisms for IEEE 802.11", IEEE Infocom 2001, Anchorage - Alaska, April 22-26h, 2001
- [48] N.H.Vaidya, P.Bahl, S.Gupta, "Distributed fair scheduling in wireless LAN", In Sixth Annual International Conference on Mobile Computing and Networking, Boston, USA August 2000
- [49] J.L.Sobrinho, A.S.Krishnakumar, "Quality-Of-Service in Ad hoc Carrier sense multiple access Wireless networks", IEEE Journal on Selected Preas in Communications, pp. 1353-1368, August 1999
- [50] I.Aad, C.Castelluccia, "Priorities in WLANs," Computer networks, vol. 41/4 pp 505 - 526, February 2003
- [51] I.Aad, C.Castelluccia, "Differentiation mechanisms for IEEE 802.11", IEEE Infocom 2001, Anchorage - Alaska, April 22-26h, 2001
- [52] IEEE 802.11 WG, Draft Supplement to STANDARD FOR Telecommunications and Information Exchange Between Systems-LAN/MAN Specific Requirements – Part 11 : Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications : Medium Access Control (MAC) Enhancement for Quality of Service (QoS), IEEE 802.11e/Draft 3.0, May 2002

- [53] R.MERAIHI, "Gestion de la qualité de service et contrôle de topologie dans les réseaux ad hoc", Thèse de doctorat ENST Paris, page24,.
- [54] R.Sivakumar, P.Sinha,V. Bharghavan, "CEDAR : a Core-Extraction Distributed Ad hoc Routing algorithm", INFOCOM '99, Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies Proceedings, IEEE , Volume : pp 202 -209 vol.1 1999
- [55] S.Chen, K.Nahrstedt, "Distributed quality-of-service routing in ad hoc networks", IEEE Journal on Selected Areas in Communications 17 (8), pp 1488-1504, (1999)
- [56] Z. J. Haas, al., eds., "Special Issue on Wireless Ad Hoc Networks", IEEE J. on Selected Areas in Communications, Vol. 17, No. 8. August 1999
- [57] C.R.Lin, M. Gerla, 'MACA/PR: An Asynchronous Multimedia Multihop Wireless Network'. In Proceedings of IEEE INFOCOM '97, Apr. 1997
- [58] C.E.Perkins, E.M.Royer, S.R.Das, "Quality of service for ad hoc on-demand distance vector routing" IETF Internet Draft,
- [59] N.Nikaein, C.Bonnet, Y.Moret, I. A. Rai, "2LQoS- Two-Layered Quality of Service Model for Reactive Routing Protocols for Mobile Ad Hoc Networks", Orlando, 2002
- [60] S.B. Lee, A. T. Campbell. 'INSIGNIA: "In-band signaling support for QoS in mobile ad hoc networks". In 5th Int. Workshop on Mobile Multimedia Communication (MoMuc'98), Berlin, Germany, October 1998
- [61] S.B.Lee, A.Gahng-Seop, X.Zhang, A.T.Campbell, 'INSIGNIA : "An IP-Based Quality of Service Framework for Mobile Ad Hoc Networks", Journal of Parallel and Distributed Computing (Academic Press) , Special issue on Wireless and Mobile Computing and Communications, Vol. 60 No. 4 pp. 374-406, April 2000
- [62] H.Xiao, K.G. Seah, A.Lo, K. C. Chua, "A flexible quality of service model for mobile ad-hoc networks", Vehicular Technology Conference Proceedings, , IEEE: 51st, Volume : 1, pp: 445 -449. 2000, VTC 2000-Spring Tokyo
- [63] G-Seop Ahn, Andrew, T.Campbell, A.Veres, Li-H Sun, "SWAN : Service Differentiation in Stateless Wireless Ad Hoc Networks", Proc. IEEE INFOCOM' 2002,
- [64] K.Chen, S.H.Shah, K.Nahrstedt, "Cross Layer Design for Data Accessibility in Mobile Ad Hoc Networks," Journal on Wireless Communications, vol. 21, pp. 49-75, 2002

- [65] M.Aissani, "Optimisation du routage dans les réseaux de capteurs pour les applications temps-réel". Thèse de doctorat, université USTHB. Mars 2011.
- [66] S. Tilak, N.Abu-Ghazaleh, W.Heinzelman, "A taxonomy of wireless micro-sensor network communication models," Proc. of the ACM SIGMOBILE Mobile Computing and Communication Review (MC2R), Vol. 6(2), pp. 28-36, April 2002.
- [67] I.Dietrich, F.Dressler. "On the lifetime of wireless sensor networks". ACM Transactions on Sensor Networks, 5(1), pp:1-39, 2009.
- [68] M.Khan, J.Misic. "On the lifetime of wireless sensor networks". In Y. Zhang, J. Zheng, and H. Hu, editors, Wireless Networks and Mobile Communications, volume 6, BocaRaton, FL, 2008.
- [69] R.Kacimi, "Techniques de conservation d'énergie pour les réseaux de capteurs sans fil". Thèse de Doctorat, Université de Toulouse. Septembre 2009
- [70] H.Philipp, T.Braun. "Calibrating wireless sensor network simulation models with real-world experiments". In Proceedings of the 8th International IFIP-TC6 Networking Conference (NETWORKING'09), volume 5550, pp 1_13, Singapore, May 5-6 2009.
- [71] C.Alippi, G. Anastasi, C.Galperti, F.Mancini, M.Roveri. "Adaptive sampling for energy conservation in wireless sensor networks for snow monitoring applications". In Proceedings of the 4th IEEE International Conference on Mobile Adhoc and Sensor Systems, pp 1_6, Pisa, Italy, October 2007.
- [72] M. Ali, A. Böhm, M. Jonsson. "Wireless sensor networks for surveillance applications - A comparative survey of MAC protocols". In Proceedings of the 4th International Conference on Wireless and Mobile Communications (ICWMC '08), pp 399-403, Washington, DC, USA, 2008. IEEE Computer Society.
- [73] G. Anastasi, M. Conti, M. Di Francesco, A. Passarella. "Energy conservation in wireless sensor networks : A survey". Ad Hoc Networks, 7(3) :537_568, 2009.
- [74] T. Armstrong. "Wake-up based power management in multi-hop wireless networks", Term Survey Paper, University of Toronto. 2005.
- [75] C.Schurgers, V.Tsiatsis, MB. Srivastava. "STEM : Topology management for energy efficient sensor networks". In Proceedings of the IEEE Aerospace Conference, volume 3, pp 78_89, Big Sky, Montana, USA, 2002.
- [76] R.Zheng, JC. Hou, L.Sha. "Asynchronous wakeup for ad hoc networks." In Proceedings of the 4th ACM international symposium on Mobile ad Hoc networking & computing (MobiHoc'03), pp 35_45, New York, NY, USA, 2003. ACM.

- [77] K. Langendoen. "Medium access control in wireless sensor networks". In Hongyi Wu and Yi Pan, editors, *Medium Access Control in Wireless Networks*, pp 535-560. Nova Science Publishers, May 2008.
- [78] V. Rajendran, K. Obraczka, J. J. Garcia-Luna-Aceves. "Energy-efficient collision-free medium access control for wireless sensor networks". In *Proceedings of the 1st international conference on embedded networked Sensor Systems (SenSys '03)*, pp 181-192, New York, NY, USA, 2003.
- [79] I. Rhee, A. Warrier, M. Aia, J. Min, L. Sichitiu. "Z-MAC: a hybrid MAC for wireless sensor networks". *IEEE/ACM Transactions on Networking*, 16(3) pp: 511-524, 2008.
- [80] J. Polastre, J. Hill, D. Culler. "Versatile low power media access for wireless sensor networks". In *Proceedings of the 2nd international conference on embedded networked Sensor Systems*, pp 95-107, New York, NY, USA, 2004.
- [81] W. Ye, J. Heidemann, D. Estrin. "Medium access control with coordinated adaptive sleeping for wireless sensor networks". *IEEE/ACM Transactions on Networking*, pp: 493-506, 2004.
- [82] T. Van Dam, K. Langendoen. "An adaptive energy-efficient MAC protocol for wireless sensor networks". In *Proceedings of the 1st international conference on embedded networked Sensor Systems*, pp 171-180, New York, NY, USA, 2003.
- [83] IEEE standard for information technology part 15.4 : "Wireless LAN medium access control (MAC) and physical layer (PHY) specification for low rate wireless-personal area networks". (LR-WPANs), 2003.
- [84] I. Rhee, A. Warrier, M. Aia, J. Min, Mihail L. Sichitiu. "Z-MAC : a hybrid MAC for wireless sensor networks". *IEEE/ACM Transactions on Networking*, 16(3), pp:511-524, 2008.
- [85] M.Kubisch, H.Karl, A.Wolisz, L.C.Zhong, J. Rabaey, "Distributed Algorithms for Transmission Power Control in Wireless Sensor Networks". In *Proc. IEEE. pp.558-563. INFOCOM, 2003*
- [86] N.Li, J.C. Hou, "BLMST: "a decentralized, power-efficient broadcast algorithm for wireless sensor networks". Accepted for publication in *ACM Baltzer Wireless Networks (WINET)*, 2005.
- [87] M.Younis, M.Youssef, K.Arisha, "Energy-Aware Routing in Cluster-Based Sensor Networks". In *Proceedings of the 10th IEEE/ACM International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems*, 2002.

- [88] R.Shah and J.Rabaey, "Energy Aware Routing for Low Energy Ad Hoc Sensor Networks". In the Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC), Orlando, FL, March 2002.
- [89] C.Schurgers, M.B.Srivastava, "Energy efficient routing in wireless sensor networks". In the MILCOM Proceedings on Communications for Network-Centric Operations: Creating the Information Force, McLean, VA, 2001.
- [90] Y. Yaser, "Routage pour la Gestion de l'Energie dans les Réseaux de Capteurs Sans Fil", Thèse de doctorat, Université de Haute Alsace. Juillet 2010.
- [91] S.Agrawal, S. Singh. "An experimental study of TCP's energy consumption over a wireless link". In Proc. of EPMCC, 2001.
- [92] A.Ahuja, S.Agarwal, J.PSingh, R. Shorey. "Performance of TCP over different routing protocols in mobile ad hoc networks". In Proc. of IEEE VTC, 2000.
- [93] G.Holland, N.Vaidya. "Analysis of TCP performance over mobile ad hoc networks". In Proc. of IEEE/ACM MOBICOM, 1999.
- [94] V.Tsaoussidis, H.Badr, X.Ge, al. "Energy/throughput tradeoffs of TCP error control strategies". In Proc. of IEEE ISCC 2000.
- [95] V.Tsaoussidis, H.Badr, R.Verma. "Wave and wait: An energy-saving transport protocol for mobile IP-devices". In Proc. of IEEE ICNP, 1999.
- [96] H.Singh, S. Singh. "Energy consumption of TCP reno, newreno, and SACK in multihop networks". In Proc. of ACM SIGMETRICS, 2002.
- [97] T.Clausen, P.Jacquet, "Optimized Link State Routing Protocol: OLSR", Request for Comments: 3626, October 2003.
- [98] Collaboration between researchers at UC Berkeley, LBL, USC/ISI, and Xerox PARC, "The ns Manual", on line at: <http://www.isi.edu/nsnam/ns/>, 2009.
- [99] E.Cizeron, "Routage Multichemins et Codage à Description Multiple dans les Réseaux Ad Hoc". Thèse de Doctorat, Université de Nantes, Septembre 2009.
- [100] N. Miontavant, « La mobilité dans les réseaux IP ». Rapport de DEA Informatique, université Louis Pasteur de Strasbourg. 2001
- [101] S.K. Sarkar, TG Besavaraju, C.Puttamadappa, « Ad Hoc Mobile Wireless Networks », Auerbach Publications, 2008
- [102] T.Camp, J. Boleng, V. Davies, « A survey of mobility models for ad hoc network research ». Wireless Communications & Mobile Computing (WCMC) Vol. 2. 2002.

- [103] M.Daoud, "Analyse du protocole AODV". DEA de coopération dans les sciences de traitement de l'information, Université Paul Sabatier, Année 2005/2006.
- [104] M.Belkheir, Z.Qacem, M.Bouziani, A.Ghelamellah, « An Energy Optimization Algorithm for Mobile Ad Hoc Network», International Journal of Soft Computing And Software Engineering (JSCSE), Oct 25, 2012.
- [105] F.J.Ros, "UM-OLSR" → <http://masimum.dif.um.es/?Software:UM-OLSR>, University of Murcia (Spain), Janvier 2006.
- [106] F.Akyildiz, W.Su, Y.Sankarasubramaniam, E.Cayirci. "Wireless sensor networks: a survey". Computer Networks, 38(4) : 393_422, 2002.
- [107] K. Holger, A. Willig. "Protocols and Architectures for Wireless Sensor Networks". Wiley, 2005.
- [108] S.Soro, WB. Heinzelman. "Prolonging the lifetime of wireless sensor networks via unequal clustering". In Proceedings of 19th IEEE International Parallel and Distributed Processing Symposium (IPDPS'05), Denver, Colorado, USA, April 2005.
- [109] K.Hellman, M.Colagrosso. "Investigating a wireless sensor network optimal lifetime solution for linear topologies". Journal of Interconnection Networks, 2006.
- [110] D. Tian, ND. Georganas. "A coverage-preserving node scheduling scheme for large wireless sensor networks". In Proceedings of the 1st ACM international workshop on Wireless Sensor Networks and Applications (WSNA'02), New York, NY, USA, 2002.
- [111] W.Mo, D.Qiao, Z.Wang. "Mostly-sleeping wireless sensor networks : Connectivity, k-coverage, and alpha-lifetime". In Proceedings of the the 43rd Annual Allerton Conference on Communication, Control, and Computing, Monticello, IL, USA, 2005.
- [112] M. Cardei, MT.Thai, Y.Li, and W.Wu. "Energy-efficient target coverage in wireless sensor networks". In Proceedings of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'05), Miami, USA, March 2005.
- [113] M.Bhardwaj, AP.Chandrakasan. "Bounding the lifetime of sensor network via optimal role assignments". In Proceedings of the 21st Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '02), New York, USA, June 2002.
- [114] H.Zhang, JC.Hou. "Maintaining sensing coverage and connectivity in large sensor networks". Ad Hoc & Sensor Wireless Networks, 2005.
- [115] K.Wu, Y.Gao, F.Li, Y.Xiao. "Lightweight deployment-aware scheduling for wireless sensor networks". Mobile Networks and Applications, 2005.
- [116] B.Crbunar, A.Grama, J.Vitek, Octavian. Crbunar. "Redundancy and coverage detection in sensor networks". ACM Transactions on Sensor Networks, 2006.
- [117] K.Sha, W.Shi. "Modeling the lifetime of wireless sensor networks". Sensor Letters, 2005.

- [118] S.Kumar, A.Arora, TH.Lai. "On the lifetime analysis of always-on wireless sensor network applications". In Proceedings of the 2nd IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS'05), Washington, DC, USA, 2005.
- [119] M.Belkheir, Z.Qasem, M.Bouziani, A.Zerroug, "Ad hoc and Sensor Networks Lifetime Enhancement by Energy Optimization, Ad-hoc and Sensor networks, April 2014.
- [120] S.Mahfoudh, P.Minet, "Energy-aware routing in wireless ad hoc and sensor networks", IWCMC'10, Proceedings of the 6th International Wireless Communications and Mobile Computing Conference, 2010.
- [121] M.Tokekar, R D. Joshi, "Extension of Optimized Linked State Routing Protocol for Energy Efficient", International Journal on Ad Hoc Networking Systems (IJANS), Vol.1 No.2, October 2011, pp. 23-37