HAL
open science

Protocoles Localisés pour Réseaux de Capteurs

Karel Heurtefeux

To cite this version:

Karel Heurtefeux. Protocoles Localisés pour Réseaux de Capteurs. Réseaux et télécommunications [cs.NI]. INSA de Lyon, 2009. Français. NNT : . tel-00449801

HAL Id: tel-00449801

https://theses.hal.science/tel-00449801

Submitted on 22 Jan 2010

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Numéro d'ordre 2009-ISAL-0104 Année 2009

Thèse

PROTOCOLES LOCALISÉS POUR RÉSEAUX DE CAPTEURS

présentée devant
L'Institut National des Sciences Appliquées de Lyon

pour obtenir
le grade de docteur

Ecole doctorale : Informatique et Mathématiques de Lyon

Soumis le 26 Septembre 2009

Par
Karel Heurtefeux

Soutenue le 26 Novembre 2009 devant la Commission d'examen
Jury

Diaz Michel	*Directeur de recherche CNRS* Laboratoire d'Analyse et d'Architecture des Systèmes - Toulouse	Président
Dias de Amorim Marcelo	*Chargé de recherche CNRS* Laboratoire d'Informatique de Paris VI - Paris	Rapporteur
Ahmed Toufik	*Professeur des Universités* Laboratoire Bordelais de Recherche en Informatique - Bordeaux	Rapporteur
Li Bo	*Professeur* Northwestern Polytechnical University - Xi'an	Examinateur
Valois Fabrice	*Professeur des Universités* Laboratoire CITI - Villeurbanne	Directeur de thèse

Les travaux présentés dans ce mémoire ont été réalisés au laboratoire CITI sous la direction du Pr. Fabrice Valois, et partiellement financé par le Ministère de la Recherche sous le contrat : ARESA ANR-05-RNRT -01703.

« Dans la vie, rien n'est à craindre, tout est à comprendre. »

Marie Curie

Résumé

Les réseaux de capteurs sont au coeur des efforts de recherche de la communauté internationale depuis plusieurs années. Les domaines d'applications sont variés allant du suivi médical à la traçabilité alimentaire en passant par le bâtiment intelligent ou le monitoring urbain (pollution, bruit, consommation électrique...). Pour que ces réseaux denses, composés de centaines voire de milliers d'entités contraintes en énergie, en puissance de calcul et en communication puissent fonctionner et s'adapter aux différentes applications, il est nécessaire, selon nous, de recourir à l'auto-organisation. L'auto-organisation est un processus duquel émerge une structure globale provenant seulement des multiples interactions locales, sans références à la globalité du réseau. De nombreuses études traitent de l'évaluation de performances des stratégies d'auto-organisation. Mais le réseau est toujours considéré comme entièrement déployé, statique. Nous montrons qu'une analyse plus fine est possible pour caractériser les différentes stratégies d'auto-organisation durant la vie d'un réseau de capteurs sans fil en prenant en compte la dynamique du réseau malgré l'immobilité physique des capteurs. On propose de mettre en évidence les différentes phases de la vie d'un réseau de capteurs et de caractériser un ensemble de protocoles d'auto-organisation sur ces différentes phases ; c'est-à-dire d'en déterminer les comportements. Nous ne concevons pas l'auto-organisation comme une fin en soi, elle doit servir à résoudre des problématiques. Après avoir démontré par une série d'expérimentations dans des environnements réels, l'inadaptation de la mesure du signal reçu (RSSI) pour résoudre le défi de la localisation dans les réseaux de capteurs, nous montrons qu'il est possible de concevoir un protocole d'auto-organisation dédié à la localisation du voisinage : le Protocole de Localisation Qualitative : QLoP. Ce protocole permet de déterminer une distance qualitative en se basant uniquement sur le voisinage à 1 et 2 sauts. Nous montrons dans cette thèse que QLoP possède à la fois de bonnes propriétés pour estimer la proximité d'un noeud mais s'adapte aussi parfaitement aux changements de topologie induite par le déploiement de nouveaux capteurs ou la disparition d'autres. Les propriétés de QLoP, démontrées précédemment permettent de construire une topologie logique, le Relative Neighborhood Graph (RNG), de façon efficace. Cette topologie permet de favoriser les liens les plus robustes et d'acheminer ainsi les paquets même dans un environnement très bruité. Enfin, nous montrons que le choix de la couche MAC ainsi que la topologie influent grandement sur les performances d'un réseau de capteurs. Nous proposerons une solution utilisant les propriétés de QLoP afin de définir une couche MAC appropriée.

Abstract

The context of this is wireless sensors multi-hop networks. We think that these networks can't work efficiently without self-organization. Self-organization is a process in which pattern at the global level of a system emerges solely from numerous interactions among the lower-level components of a system. Previously, the network was still regarded as fully deployed. We show that a better analysis is possible to characterize the different self-organization protocols during the life of a sensor wireless network. After having demonstrated by a series of experiments in real environments the ineffectiveness of Received Strength Signal Indicator (RSSI) to resolve the challenge of localization in Wireless Sensor Network, we show that it is possible to design a self-organization protocol dedicated to the location of the neighborhood : Qualitative Localization Protocol : QLoP. This Protocol is used to determine a qualitative distance based only on the 1 and 2 hop neighborhood. We show that QLoP has good properties to estimate the proximity of a node but also perfectly against topology changes. QLoP allows to build a logical topology, the Neighborhood Graph (RNG) relative effectively. This topology can favour more robust links and route packets even in a very noisy environment. Finally we show that QLoP can conserve energy by adapting the MAC layer to the topology.

Remerciements

J'exprime mes sincères remerciements et toute ma gratitude, en premier lieu, à mon directeur de thèse, Fabrice Valois, qui m'a offert l'opportunité de réaliser cette thèse, de faire ce séjour si enrichissant à l'Université Polytechnique de Xi'an en Chine et qui a su me former et m'orienter avec rigueur et patience durant ces 3 années.

Je remercie Michel Diaz, Directeur de recherche CNRS au Laboratoire d'Analyse et d'Architecture des Systèmes de Toulouse, Marcelo Dias de Amorim, Chargé de recherche CNRS au Laboratoire d'Informatique de Paris VI et Toufik Ahmed, Professeur des Universités au Laboratoire Bordelais de Recherche en Informatique d'avoir accepté d'évaluer mon travail et pour leurs conseils avisés.

Ma gratitude va également envers Li Bo, Professeur à l'Université Polytechnique de Xi'an et son équipe pour son accueil à Xi'an, pour ses qualités humaines et ses connaissances partagées sur les mécanismes de couche MAC. J'espère garder longtemps en exemple son enthousiasme pour la recherche et l'enseignement.

Cette thèse a été réalisée au sein du Centre d'Innovation en Télécommunications et Intégration de Services (CITI), à l'INSA de Lyon, et dans le projet ARES puis SWING de l'INRIA Rhône-Alpes. Je tiens donc à remercier Stéphane Ubeda et Jean-Marie Gorce respectivement l'ancien et le nouveau directeur du CITI ainsi que les enseignants et chercheurs du CITI et du département Télécommunications de l'INSA de Lyon, en particulier Isabelle Augé-Blum pour sa confiance et ses encouragements. Je n'oublie pas non plus les personnels administratifs de l'INSA et bien sur ceux du laboratoire qui font un travail indispensable à la réalisation de toute thèse : Gaelle, Maguy, Joelle et Stéphane.

Mon travail au laboratoire CITI n'aurait pas été possible sans tous mes camarades thésards et ingénieurs de recherche qui ont été présents dans les moments de doute et la période de rédaction de ce manuscrit. C'est avec eux que j'ai eu le plus de discussions scientifiques durant et en dehors des heures de bureau. Je souhaite donc remercier Amira, Anya, Fatiha, Noha, Ioan, Jia Liang, Fei, Rui Feng, Hajer, Virgile, Ibrahim, Thomas, Wassim, Cédric et Loïc.

Je remercie ma famille et mes amis pour leur irremplaçable et inconditionnel soutien. Ils ont également une part importante dans la réalisation de cette thèse.

Enfin, bien sur, je remercie Ochir qui a toujours été présente pour alimenter la réflexion, débattre et écarter les doutes. Elle m'a soutenue et supportée durant toute cette thèse et surtout durant la dernière et longue, interminable ligne droite.

Liste d'acronymes

AOA	Angle Of Arrival
AODV	Ad Hoc On-Demand Distance Vector Routing
BER	Bit Error Rate
BGP	Border Gateway Protocol
CDMA	Code Division Multiple Access
CDS	Connected Dominating Set
CRC	Cyclic Redundancy Check
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
CTS	Clear To Send
DCF	Distributed Coordination Function
DS	Dominating Set
DSR	Dynamic Source Routing
FDMA	Frequency Division Multiple Access
GG	Gabriel Graph
GPS	Global Position System
IEEE	Institute of Electrical and Electronics
IDS	Independent Dominating Set
LMST	Localized Minimum Spanning Tree
MAC	Medium Access Control
MIS	Maximal Independent Set
MPR	Multi Point Relay
MST	Minimum Spanning Tree
OLSR	Optimized Link State Routing
OSI	Open Systems Interconnection
RNG	Relative Neighborhood Graph
RREP	Route Reply
RREQ	Route Request
RSS	Received Strength Signal
RSSI	Received Strength Signal Indication
RTS	Request To Send
SNR	Signal to Noise Ratio
SiNR	Signal to Interference-plus-Noise Ratio
TCP	Transport Control Protocol
TDMA	Time Division Multiple Access
TDoA	Time Difference Of Arrival
ToA	Time Of Arrival
QLoP	Qualitative Localization Protocol
UDG	Unit Disk Graph

Table des matières

Résumé **v**

Abstract **vii**

Remerciements **ix**

Liste d'acronymes **xi**

1 Introduction **9**
1.1 Réseaux de capteurs 9
1.1.1 Définition 9
1.1.2 Applications et scénarios 12
1.2 Problématiques et défis 14
1.3 L'auto-organisation 15
1.4 Besoins, contributions et organisation de la thèse 16
1.4.1 Trois phases dans la vie d'un réseau de capteurs 16
1.4.2 Une approche novatrice de la localisation par l'auto-organisation 17
1.4.3 Des applications au contrôle de topologie et au routage 17
1.4.4 Une approche cross-layer 18
Bibliographie 18

Bibliographie **18**

2 Caractérisation des protocoles d'auto-organisation **21**
2.1 Introduction 21
2.2 État de l'art sur l'auto-organisation 25
2.2.1 Orienté dominant 25
2.2.2 Orienté élagage de liens 28
2.2.3 Évolution d'un réseau de capteurs 33
2.3 Comportement au cours de la vie du réseau 33
2.3.1 Les différentes phases d'un réseau de capteurs 34
2.3.2 Déploiement du réseau 35
2.3.3 Adaptation des topologies logiques : la robustesse 37
2.4 Évolution des propriétés structurelles des différentes structures d'auto-organisation 41
2.4.1 L'effet donut 41

2.5 Conclusion 47
Bibliographie 48

Bibliographie **48**

Liste de publications liées à ce chapitre **53**

3 De l'instabilité du RSSI comme métrique **55**
3.1 Motivations 55
3.2 État de l'art 55
3.3 Expérimentations 59
3.3.1 Matériel 59
3.3.2 Environnements et scénarios 60
3.4 Résultats 62
3.4.1 Scénario « RSSI et distance » 62
3.4.2 Scénario « RSSI et stabilité à long terme » 67
3.5 Conclusion 71
Bibliographie 72

Bibliographie **72**

4 QLoP ou l'auto-organisation appliquée à la localisation **75**
4.1 Motivations 75
4.2 État de l'art 76
4.2.1 Localisations fines 77
4.2.2 Localisations approximatives 78
4.3 Algorithme de localisation qualitative : QLoP 79
4.3.1 Détails de l'algorithme 79
4.3.2 Analyse dans le cas d'une couche physique idéale 81
4.4 Étude des performances de QLoP 84
4.4.1 Comportement du protocole de localisation qualitative sur une topologie régulière 85
4.4.2 Comportement du protocole de localisation qualitative sur des topologies aléatoires 86
4.4.3 Comportement face aux phases de la vie du réseau 89
4.4.4 QLoP face à la ν-distance 92
4.4.5 QLoP face au RSSI 92
4.5 Conclusion 94
Bibliographie 94

Bibliographie **94**

Liste de publications liées à ce chapitre **97**

5 QLoP appliqué au contrôle de topologie et au routage **99**
5.1 Contrôle de topologie . . . 99
5.1.1 RNG-QLoP . . . 100
5.2 Routage en environnement bruité . . . 103
5.2.1 Routage pseudo-DSR . . . 103
5.2.2 Modélisation du canal radio . . . 103
5.2.3 Impacts sur le routage . . . 105
5.3 Consommation énergétique . . . 109
5.4 État de l'art . . . 109
5.5 Conclusion et discussion . . . 110
Bibliographie . . . 110

Bibliographie **110**

Liste de publications liées à ce chapitre **113**

6 Interactions entre l'auto-organisation et les protocoles MAC **115**
6.1 Motivations . . . 115
6.2 État de l'art . . . 116
6.3 Les protocoles MAC pour réseaux de capteurs . . . 119
6.4 Le protocole Aloha . . . 120
6.5 Hypothèses de simulation . . . 122
6.6 Performances de Aloha . . . 124
6.7 L'influence de la topologie . . . 127
6.8 Couche MAC adaptative . . . 134
6.8.1 Principes . . . 134
6.8.2 Évaluation de performances . . . 135
6.9 Conclusion . . . 137
Bibliographie . . . 137

Bibliographie **137**

7 Conclusions et perspectives **139**
7.1 Contributions de la thèse . . . 139
7.2 Perspectives . . . 141
7.2.1 Localisation globale . . . 141
7.2.2 Sécurité . . . 141
7.2.3 Corrélation spatiale . . . 142
Bibliographie . . . 142

Bibliographie **142**

Table des figures

1.1 Capteur sans fil WSN430 développé au laboratoire CITI 10
1.2 Caractéristiques de quelques capteurs les plus courants 11
1.3 Caractéristiques des principales applications 13
1.4 Saut quantitatif : relevé journalier de compteurs d'eau sur une commune de plusieurs milliers d'habitants 14
1.5 Saut qualitatif : compréhension du phénomène de micro-climat sur la montagne Génépi 14
1.6 Exemple d'auto-organisation dans le vivant : le chou romanesco (source : CNRS Photothèque / Stéphane Douady) 16

2.1 Exemple d'organisation en clusters 22
2.2 MPR : mécanisme de désignation des voisins MPR 26
2.3 CDS : protocole CDS-*règle k* 27
2.4 RNG : mécanisme d'élagage de liens 29
2.5 RNG : topologie logique de 100 nœuds 29
2.6 LMST : mécanisme d'élagage de liens 30
2.7 LMST : topologie logique de 100 nœuds 30
2.8 Graphe de Gabriel : mécanisme d'élagage de liens 31
2.9 Graphe de Gabriel : topologie logique de 100 nœuds 31
2.10 Graphe de Yao : mécanisme d'élagage de liens 32
2.11 Graphe de Yao : topologie logique de 100 nœuds 32
2.12 Graphe de Delaunay : Diagramme de Voronoi (lignes discontinues) et graphe de Delaunay associé 32
2.13 Les 3 phases de la vie d'un réseau de capteurs 34
2.14 Latence des 4 schémas d'auto-organisation orientés dominant 36
2.15 Évolution du degré moyen des topologies LMST et RNG 38
2.16 Évolution de la cardinalité du CDS pour les topologies orientées dominant 38
2.17 Conséquences de la mort de nœuds sur la topologie RNG 39
2.18 Conséquences de la mort de nœuds sur la topologie CDS-IDS 40
2.19 Conséquences de la mort de nœuds sur la topologie CDS-*règle k* 40
2.20 Topologie CDS-*règle k* : allongement de la topologie au cours du temps 42
2.21 Topologie CDS-*règle k* : excentricité du puits au cours du temps 42

2.22 Topologie CDS-*règle k* : évolution des classes de gradient au cours du temps (avec mécanisme d'endormissement) . . . 43
2.23 Topologie CDS-*règle k* : évolution des classes de gradient au cours du temps (sans mécanisme d'endormissement) . . . 44
2.24 Topologie CDS-*règle k* : évolution de l'énergie en fonction du statut des nœuds . 45
2.25 Topologie CDS-*règle k* : évolution de l'énergie au cours du temps en fonction de la distance au puits (avec mécanisme d'endormissement) . . . 45
2.26 Topologie RNG : allongement de la topologie au cours du temps . . . 46
2.27 Topologie RNG : excentricité du puits au cours du temps . . . 46
2.28 Topologie RNG : évolution de l'énergie au cours du temps en fonction de la distance au puits . . . 47
2.29 Effet Donut . . . 47

3.1 Exemple de carte RSSI obtenue par un nœud *sniffer* ^{0} . . . 56
3.2 Division en classes du voisinage à 1 saut afin d'améliorer la précision de localisation 58
3.3 Caractéristiques du WSN430 . . . 60
3.4 Dispositif de mesures avec le capteur WSN430 . . . 60
3.5 Les 3 milieux différents des expérimentations . . . 61
3.6 Scénario « RSSI - distance » . . . 61
3.7 Rapport entre RSSI et distance dans le cas du scénario « appartement » . . . 62
3.8 Phénomène de multi-trajet . . . 63
3.9 Rapport entre écart-type des mesures RSS et distance pour les deux capteurs récepteurs (appartement) . . . 64
3.10 Rapport entre RSSI et distance dans le cas du scénario « bâtiment de bureaux » 65
3.11 Rapport entre écart-type des mesures RSS et distance pour les deux capteurs récepteurs (laboratoire) . . . 65
3.12 Rapport entre RSSI et distance dans le cas du scénario « terrain de football » . . 66
3.13 Rapport entre écart-type des mesures RSS et distance pour les deux capteurs récepteurs (terrain de football) . . . 67
3.14 Emplacement des 6 capteurs dans le scénario « stabilité à long terme du RSSI » . 68
3.15 Évolution du RSSI mesuré par le capteur 3 sur 40 heures . . . 68
3.16 Évolution du RSSI mesuré par le capteur 1 sur 40 heures . . . 69
3.17 Évolution du RSSI mesuré par le capteur 1 sur 40 heures . . . 69
3.18 Différences de stabilité du RSSI selon la disposition des capteurs . . . 70
3.19 Évolution du nombre de paquets nécessaire pour approximer la moyenne . . . 71

4.1 Exemple d'une application de l'algorithme pour un nœud . . . 76
4.2 Exemple d'une localisation approximative : coordonnées virtuelles . . . 78
4.3 Exemple d'une localisation approximative : intersection de signaux . . . 78
4.4 Exemple de localisation qualitative calculée par le nœud 27. . . . 80
4.5 Comparaison de la localisation pour les voisins du nœud 27 obtenue avec l'algorithme de localisation qualitative et en utilisant la position réelle. . . . 81
4.6 Illustration de l'intersection des deux disques $\mathfrak{D}(A, r_A)$ et $\mathfrak{D}(B, r_B)$ . . . 81

4.7 Portion du disque 82
4.8 Dans les cas a) et b), l'aire d'intersection est la même et pourtant la distance est différente 83
4.9 Exemple d'estimation de la distance sur un voisinage de 4 nœuds par le nœud u. 84
4.10 Aire d'intersection des disques par rapport aux distances us, uv et uw 85
4.11 Métrique QLoP par rapport aux distances us, uv et uw 85
4.12 Écart-type entre la métrique QLoP et l'aire d'intersection par rapport à la distance entre us, uv et uw 85
4.13 Algorithme déployé sur une grille 86
4.14 Distance quadratique par classe 87
4.15 Les 3 classes de voisinage logique de l'algorithme 87
4.16 Évolution de la cardinalité des voisinages logiques de proximité en fonction du degré moyen 88
4.17 Évolution de la fiabilité de l'algorithme en fonction du degré moyen 89
4.18 Naissance, vie et mort : impacts sur QLoP 90
4.19 Indice de proximité en fonction de la distance euclidienne sur l'ensemble des capteurs 91
4.20 Évolution de l'erreur de localisation de QLoP en face à l'ajout et à la mort de nœuds 91
4.21 Évolution de la distance quadratique pour QLoP et la pseudo-distance en fonction du degré moyen (topologie UDG) 92
4.22 Évolution de la distance quadratique pour QLoP et la pseudo-distance en fonction du degré moyen (topologie réaliste) 93

5.1 a) Topologie physique, b) Topologie RNG avec informations géographiques (type GPS) c) Topologie RNG avec QLoP (RNG-QLoP) 101
5.2 Évolution de la longueur moyenne des liens de la topologie 102
5.3 Évolution du degré logique moyen des structures RNG-QLoP et RNG classique en fonction du degré physique 102
5.4 Pseudo-DSR sur une topologie à plat et une topologie élaguée avec RNG-QLoP . 104
5.5 Format des paquets utilisés 104
5.6 Influence du modèle radio sur le voisinage : a) graphe de disques unitaires, b) liens avec path-loss et shadowing 105
5.7 Évolution du nombre de paquets RREQ retransmis par nœuds 105
5.8 Évolution du taux de livraison des paquets RREQ 106
5.9 Taux de livraison en fonction du niveau de bruit 107
5.10 La distance face au bruit 108
5.11 Nombre de sauts parcourus par paquet reçu 108
5.12 Communications concurrentes 109

6.1 Influence des mécanismes d'esquive de collisions en termes de performances . . . 116
6.2 Mécanisme RTS/CTS 117
6.3 Blocage en chaîne avec le mécanisme RTS/CTS 119

6.4 Probabilité de collision de deux trames 121
6.5 Aloha : Taux de livraison théorique 121
6.6 Aloha : Débit utile théorique 122
6.7 Aloha : Accès concurrent de 8 nœuds équidistants du nœud destination 122
6.8 Aloha : Accès concurrent de 7 nœuds équidistants du nœud destination et d'un nœud proche 122
6.9 Collision non nécessairement destructrice 123
6.10 Cas a) : débit utile du réseau en fonction des protocoles MAC 123
6.11 Cas a) : taux de livraison du réseau en fonction des protocoles MAC 123
6.12 Énergie moyenne nécessaire pour acheminer un paquet utile 124
6.13 Cas b) : débit utile du réseau en fonction des protocoles MAC 125
6.14 Cas b) : taux de livraison du réseau en fonction des protocoles MAC 126
6.15 Cas b) : seul le capteur 1 proche de la destination est capable de transmettre avec succès 126
6.16 Détails des 3 couches MAC utilisées : CSMA/CA, CSMA et Aloha. 128
6.17 Scénario 1, 2 et 3 : accès de deux nœuds sources vers un même nœud destination par l'intermédiaire de 0, 2 ou 5 nœuds intermédiaires 128
6.18 Scénarios 4, 5 et 6 : transmissions de 2 nœuds sources vers 2 nœuds destinations 129
6.19 Débit moyen pour le scénario 1 129
6.20 Délai moyen pour le scénario 1 130
6.21 Débit moyen pour le scénario 2 131
6.22 Débit moyen pour le scénario 3 132
6.23 Délai moyen pour le scénario 2 132
6.24 Taux moyen de livraison pour le scénario 4 133
6.25 Taux moyen de livraison pour le scénario 5 133
6.26 Taux moyen de livraison pour le scénario 6 133
6.27 Délai moyen pour le scénario 5 133
6.28 Fonctionnement de la couche MAC adaptative 134
6.29 Taux de livraison entre une couche MAC CSMA/CA avec RTS/CTS et une couche MAC adaptative 135
6.30 Évolution de l'énergie moyenne par paquet reçu entre une couche MAC CSMA/CA avec RTS/CTS et une couche MAC adaptative 136
6.31 Évolution de l'énergie moyenne du réseau entre une couche MAC CSMA/CA avec RTS/CTS et une couche MAC adaptative 136

1
Introduction

1.1 Réseaux de capteurs

1.1.1 Définition

La miniaturisation croissante de l'électronique et le progrès des technologies de télécommunication, qui n'ont cessé depuis l'émergence de l'informatique, permettent aujourd'hui de produire à faible coût des capteurs communicants peu consommateurs en énergie. Ces petites entités électroniques, dont l'objectif est de récolter des grandeurs physiques de leur environnement proche (luminosité, mouvement, température, pression barométrique, etc.), et éventuellement de les traiter, constituent les briques de base des réseaux de capteurs (voir figure 1.1). Il existe une foultitude de capteurs sur le marché, allant du capteur cinétique au capteur de champ magnétique ou du capteur de pollution au capteur de mouvement [4]. Cependant, malgré cette diversité apparente, ils restent dotés d'une architecture matérielle similaire. Un capteur est composé :

- d'une unité de capture : elle est chargée de transformer une grandeur physique récoltée dans l'environnement proche en grandeur numérique ;
- d'une unité de traitement : elle est dotée d'un processeur et d'une mémoire ;
- d'une unité de contrôle d'énergie ;
- d'une batterie ;
- d'un module de transmission sans fil.

De par leur contrainte de taille, de consommation et de coût de fabrication, les capacités individuelles de traitement, de stockage et de communication d'un capteur sont très largement inférieures aux PC et aux téléphones cellulaires actuels. Le tableau 1.2 donne les principales

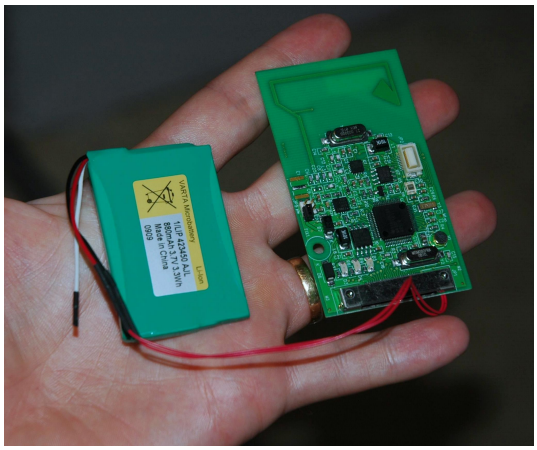

FIGURE 1.1 – Capteur sans fil WSN430 développé au laboratoire CITI

caractéristiques des capteurs actuels.

Nous voyons donc rapidement les contraintes que vont rencontrer les capteurs :

- Une faible puissance de calcul : quand les PCs nouvelle génération peuvent avoir jusqu'à 4 processeurs, chacun cadencé à 3GHz, ou quand les derniers Smartphones peuvent fonctionner jusqu'à 800MHz, un capteur actuel est à peine plus puissant qu'une calculatrice graphique produite dans les années 90, possède une mémoire lente en lecture/écriture et fonctionne parfois encore avec des registres 8 bits.
- Un espace de stockage mémoire limité de quelques kilos à quelques mégaoctets nécessite des algorithmes distribués, localisés et collaboratifs.
- Une puissance radio limitée : l'ordre de grandeur des portées actuellement atteignables par les principaux capteurs est d'une centaine de mètres en extérieur et de quelques dizaines de mètres en intérieur. Cette portée est largement dépendante de la fréquence utilisée et de l'environnement. Elle nécessite un routage multi-saut pour l'acheminement des données vers une entité de collecte, le puits : les capteurs ne peuvent communiquer qu'avec les capteurs de leur voisinage direct qui vont relayer les communications.
- Un débit faible : les composants radio d'un capteur sont limités à quelques centaines de kilo-octets par seconde
- Une réserve d'énergie réduite : même s'il existe des mécanismes de recharge d'énergie (principalement solaire [7]), la durée de vie d'un capteur reste directement liée au niveau de sa batterie. Cette réserve d'énergie est partagée par chaque unité d'un capteur mais l'unité de communication va en consommer près de 95% lors du fonctionnement actif du capteur. Il est donc naturel qu'une forte recherche s'effectue à la fois sur l'augmentation des capacités des batteries [3], sur les dispositifs de transmission radio ultra-basse consommation([8, 9, 13]), les architectures basse consommation [12], et enfin, sur les mécanismes d'endormissement et sur des protocoles de communication spécifiques.

On doit donc bien comprendre que la force d'un réseau de capteurs ne tient pas à la qualité des capteurs individuellement mais à leur collaboration : l'ensemble du réseau est supérieur à la somme des capteurs qui le composent. Cette collaboration est possible grâce à des protocoles

Motes	MicaZ	Telos	Imote2	WSN430	Wavenis (Wavefront)
Processeur	Atmel ATMega 128L	TI MSP430	Intel PXA271 XScale	TI MSP430	TI MSP430
Vitesse du processeur	16 MHz	8 MHz	13 - 416 MHz	8 Mhz	8 MHz
RAM	4 Ko	2 Ko / 10 Ko	256 Ko	10 Ko	2 Ko
Espace programme	128 Ko	60 Ko / 48 Ko	32 Mo	48 Ko	128 octets
Flash	512 Ko	256 Ko	32 Mo	1 Mo	Néant
Communication série	UART	DIO, SPI, I2C, UART	UART, GPIO	DS2411	SPI, E2P
Batterie	2xAA	2/3A	3x AAA	PoLiFlex	2xAA
Voltage	2.7 V	1.8 - 3.6 V	3.2 - 4.5 V	2.2 V	2.4 - 6 V
Radio	TI CC2420 802.15.4	TI CC2420 802.15.4	TI CC2420	TI CC1100	ASIC RF Wavenis
Fréquence (MHz)	2400-2483	2400-2483	2400-2483	315/433/ 868/915	433/868/915
Débit de données (Kb/s)	250	250	500	250	4,8 - 153
Dimension (mm)	58x32x7	13x26x5	36x48x9	65x40x8	26x20x4.5

FIGURE 1.2 – Caractéristiques de quelques capteurs les plus courants

qui se doivent, nous le montrerons dans cette thèse, d'être localisés et économes en énergie.

Le déploiement de ces entités, qui va permettre de collecter et de transmettre les données mesurées vers un ou plusieurs points de collecte, forme un réseau de capteurs sans fil. Ces réseaux sont composés de centaines voire de milliers de capteurs. La particularité de ces réseaux est directement liée aux contraintes matérielles des éléments qui le composent :

- Nous prenons comme hypothèse l'homogénéité du réseau : il n'y a pas de nœuds dédiés à l'organisation du réseau, ni de « super-nœuds » avec une quantité infinie d'énergie ou une puissance radio supérieure. Cela impose une infrastructure décentralisée : tous les nœuds participent au fonctionnement du réseau.
- Le faible coût du matériel nécessite une redondance des liens pour assurer une connexité du réseau en cas de panne d'un ou plusieurs capteurs. Il impose également un matériel peu coûteux : nous ne pouvons prendre comme hypothèse réaliste la présence par défaut de puce GPS, de plusieurs unités de communication radio ou de plusieurs antennes.
- La faible réserve en énergie et la difficulté pour recharger ou remplacer manuellement les batteries d'un capteur nécessitent de minimiser les calculs et les communications.

Une des forces d'un réseau de capteurs est sa capacité à être déployé rapidement dans des conditions difficiles. La plupart des applications part d'une topologie non maîtrisée, où le positionnement des nœuds est donc aléatoire. Ces conditions de déploiement conduisent à des contraintes supplémentaires :

- L'impossibilité de remplacer manuellement les nœuds va conduire au redéploiement de nouveaux capteurs et à la disparition de capteurs défectueux ou trop anciens. C'est pour cette raison que les protocoles doivent être robustes face aux changements locaux de topologie.
- Une forte densité et une forte cardinalité du réseau interdisent aux capteurs d'avoir une connaissance globale de la topologie du réseau.

À cela, s'ajoute un modèle de trafic qui va de n nœuds vers un ou quelques nœuds destinations et que nous nommons puits (trafic *convergecast*). Enfin, la nature versatile des liens sans fil peut causer des changements topologiques même en l'absence de mobilité ou de défaillance d'un nœud. De plus, l'utilisation du médium radio est partagée, ceci ajouté à une forte densité de déploiement des capteurs, implique une forte contention du canal, du bruit et des interférences.

Nous le voyons donc, les réseaux de capteurs se distinguent des réseaux ad hoc classiques par des contraintes différentes en termes d'énergie, de puissance de calcul, de modèle de communication, de densité et de mobilité.

1.1.2 Applications et scénarios

Le fort potentiel d'application des réseaux de capteurs en fait un domaine de recherche très actif. Ces dernières années ont vu le passage d'applications anecdotiques à de véritables applications à large échelle. La réduction de plus en plus importante de la taille des capteurs, leur coût de plus en plus faible, ainsi que l'étendue du type de capteurs disponibles (thermique, optique, cinétique, chimique, etc.), permettent aux réseaux de capteurs d'envahir de très nombreux domaines d'application.

Dans le projet ARESA [1], nous avons déterminé 3 grandes familles d'applications pour réseaux de capteurs :

- le relevé d'informations dans lequel chaque capteur collecte simplement les données et les envoie périodiquement au puits.
- la détection d'événements où chaque nœud décide s'il envoie des données au puits en fonction des données qu'il a collectées. Cette décision peut nécessiter au capteur un dialogue avec son voisinage.
- le contrôle intelligent dans lequel chaque capteur collecte différentes sortes de données, échange ses informations à travers le réseau et collabore pour former une description de l'état de l'objet ciblé.

Il a également été défini un ensemble de scénarios viables visé par les réseaux de capteurs :

- **Surveillance environnementale.** La télé-relève de compteurs d'eau ou d'électricité, comme le réalise actuellement la société Coronis Systems [2], ou la surveillance de la pollution urbaine en sont de parfaits exemples. Les caractéristiques de ce type d'application sont l'absence de mobilité, un accès difficile aux capteurs, un besoin d'autonomie importante, une topologie aléatoire et à large échelle, une forte densité et un canal radio instable.
- **Bâtiment intelligent.** Il existe déjà des capteurs dans certaines constructions pour mesurer les mouvements internes de la structure et détecter le plus tôt possible d'éventuelles fragilités. Cependant, l'avènement de capteurs sans fil, peu coûteux et compacts permet d'envisager un déploiement plus systématique et plus dense. Les bâtiments intelligents seront capables de détecter un excès d'humidité dans les murs, des fissures ou des contraintes inhabituelles. Dans ces applications les capteurs sont stables et le plus souvent inaccessibles. Cependant, la densité n'est pas nécessairement très importante et la topologie est souvent régulière.

Caractéristiques	Surveillance environnementale	Bâtiment intelligent	Domotique	BAN
Domaine	industriel	industriel, domestique	domestique	personnel
Application	relevé de compteur d'eau	surveillance des contraintes, de la température, de l'humidité	surveillance de la température, de l'humidité, de la luminosité, de présence	surveillance médicale, sport de haut niveau
Accessibilité	limitée à quelques nœuds extérieurs	limitée à quelques nœuds extérieurs	remplaçable	accessible sauf implant
Type de trafic	réactif	réactif et pro-actif	réactif, pro-actif et régulier	pro-actif
Topologie	aléatoire uniforme et large échelle	régulier, pas nécessairement à large échelle	aléatoire	aléatoire
Mobilité	fixe	fixe	mobile	mobile
Problématiques	robustesse, contraintes énergétiques fortes	robustesse, contraintes énergétiques fortes	contraintes énergétiques et d'hétérogénéité des mesures	robustesse et sécurité

FIGURE 1.3 – Caractéristiques des principales applications

- **Domotique.** Faire disparaître une partie du réseau électrique de la maison (interrupteurs sans fil), la surveillance de la température, de la luminosité, ou la détection de présence sont les principales applications visées par la domotique. Ici, les capteurs sont peu mobiles et le plus souvent remplaçables. Le défi de ces applications est l'hétérogénéité des mesures effectuées, impliquant notamment différents intervalles de capture et différents niveaux de fiabilité, l'intégration des capteurs dans un environnement domestique, et l'auto-configuration du réseau pour être accessible à un public néophyte.
- **Body Area Network (BAN).** Avec la miniaturisation des capteurs, il est aujourd'hui concevable de les intégrer sur et à l'intérieur d'un corps humain. Les capteurs peuvent, par exemple, mesurer la température, la pression sanguine, la glycémie ou le rythme cardiaque d'un individu. Naturellement, les contraintes de sécurité et de fiabilité sont très fortes. La forte dynamique et le faible cycle de vie de ces capteurs sont également des caractéristiques essentielles de ces applications.

On peut s'apercevoir que les contraintes ne sont pas de même nature selon les applications (voir figure 1.3). Elles vont nécessiter d'autres approches et vont influencer les protocoles à implémenter. Non seulement les réseaux de capteurs permettent d'obtenir des mesures plus variées dans des domaines plus nombreux mais leur déploiement dense permet une diminution de la granularité qui peut conduire à la compréhension de certains phénomènes jusqu'alors insaisissable : le saut n'est plus seulement quantitatif (davantage de mesures et plus de précision) (voir figure 1.4), il devient qualitatif (meilleure/nouvelle compréhension) (voir figure 1.5). De ce point de vue là, le déploiement sur la montagne du Génépi est un bon exemple [7] : une seule station météo ne permet absolument pas de comprendre le micro-climat dû au permafrost alors qu'un ensemble de capteurs organisés en réseau conduit à l'appréciation de cet élément-clé dans la prédiction des coulées de boue.

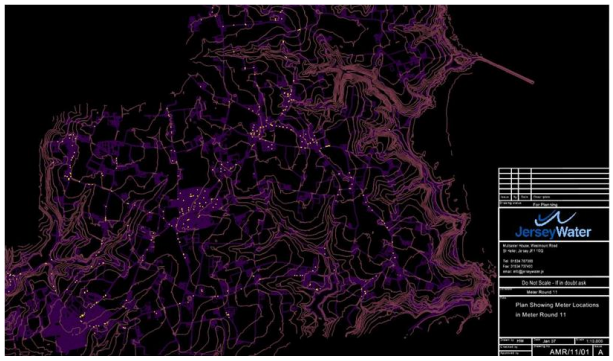

FIGURE 1.4 – Saut quantitatif : relevé journalier de compteurs d'eau sur une commune de plusieurs milliers d'habitants

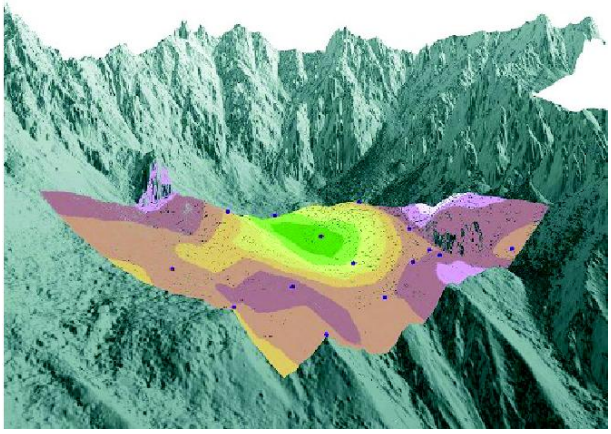

FIGURE 1.5 – Saut qualitatif : compréhension du phénomène de micro-climat sur la montagne Génépi

1.2 Problématiques et défis

Les perspectives d'application des réseaux de capteurs sont enthousiasmantes mais les défis qu'elles posent n'en sont pas moins nombreux et complexes. Parmi les problématiques cruciales, nous pouvons citer :

- Routage : Le récent groupe de travail ROLL (Routing Over Low-power and Lossy networks) constitué à l'IETF (Internet Engineering Task Force) a comme principal objectif la mise en place d'un protocole de routage, efficace et interopérable, fonctionnant sur les réseaux de capteurs [11]. Cela montre à la fois combien cette problématique est d'actualité mais également la prise de conscience de l'impossibilité d'utiliser les protocoles de routage développés pour les réseaux filaires et ad hoc.
- Auto-configuration : Une partie des applications visée appartient au domaine des applications domestiques. Il est donc important que le routage, l'intégration et l'adaptation à l'environnement soient transparents pour l'utilisateur.
- Auto-réparation : Nous venons de le voir, les capteurs sont parfois inaccessibles (intégrés dans un mur, installés chez un particulier, déployés dans une zone dangereuse, etc.) et parfois de conception peu sûre (faible coût de production). Une solution complète doit donc gérer efficacement la perte ou l'ajout d'un nœud dans son réseau.
- Localisation : Il s'agit de concevoir des mécanismes de localisation réalistes vis-à-vis des contraintes et des applications propres aux réseaux de capteurs. Les solutions actuellement proposées reposent sur des solutions, soit imprécises, soit coûteuses en énergie ou en matériel.
- Sécurité : La puissance de calcul limitée des entités d'un réseau de capteurs ouvre de véritables défis pour concevoir des algorithmes de cryptages distribués et des politiques de confiance spécifiques. Il ne s'agit plus de garantir à tout prix la résistance des nœuds pris isolément face aux actes malveillants ou à la défaillance, mais de réfléchir sur la résilience de l'ensemble du réseau (i.e. sa capacité de réaction après une attaque).

- Énergie : Les contraintes en autonomie des réseaux de capteurs imposent de concevoir des protocoles économes en énergie : faible trafic de contrôle, algorithmes localisés, etc. Cela suppose une approche véritablement inter-couche et transverse à tous les points cités précédemment.

1.3 L'auto-organisation

Toutes les problématiques énoncées précédemment doivent pouvoir être adressées en tenant compte des contraintes intrinsèques des réseaux de capteurs. Selon nous, il est indispensable pour cela de recourir à l'auto-organisation. Beaucoup de propositions se basent sur une vue à plat du réseau : chaque capteur étant identique matériellement à ses pairs dans le réseau, il est considéré comme identique par les protocoles de communication fonctionnant dessus. Il est clair, au contraire, que le réseau doit être structuré, auto-organisé, avant de concevoir une solution exploitant un réseau de capteurs. Chaque capteur a ses propres spécificités en dépit de son égalité physique : degré (nombre de voisins), niveau d'énergie, proximité avec ses voisins, etc. La structure prendra en compte ces spécificités. Pour nous, l'auto-organisation n'est donc pas une fin en soi mais une étape indispensable pour faciliter et améliorer l'utilisation des réseaux de capteurs.

Définition. L'auto-organisation est partout. En effet, contrairement à l'intuition, les mécanismes d'auto-organisation ne sont pas rares et on les rencontre régulièrement dans la vie courante, de la théorie politique à la thermodynamique. D'un point de vue scientifique, les mécanismes d'auto-organisation ont été étudiés en premier dans les systèmes biologiques (voir figure 1.6).

Le préfixe « auto » implique que l'apparition de phénomènes collectifs dans l'ensemble des nœuds en interaction se réalise sans qu'il y ait besoin ni d'un « chef d'orchestre », ni d'une préparation initiale, ni de conditions extérieures faussant les interactions ou la dynamique individuelle. Le terme « organisation » implique que le système possède une certaine structure et des fonctionnalités associées à cette structure. Ce qui signifie que les entités du réseau sont arrangées d'une manière définie et interagissent entre elles de façon identique. De ces fonctionnalités associées découle le fait que le système dans son ensemble réalise un certain but. En d'autres mots, les capteurs interagissent directement les uns avec les autres de façon totalement distribuée mais avec un objectif commun. Pour reprendre la définition de [6], l'auto-organisation est un processus duquel émerge une structure globale provenant seulement des multiples interactions locales, sans référence à la globalité du réseau. C'est de ces interactions au niveau local, qu'apparaissent des propriétés émergentes bien au-delà de la capacité des capteurs pris séparément. Le terme indique également une apparition d'ordre et renvoie aux notions d'entropie [10]. Par exemple, une structure virtuelle (comme un *backbone* de nœuds dominants) ou une topologie logique va émerger d'un ensemble homogène de capteurs. Cette structure va diminuer l'entropie du réseau.

FIGURE 1.6 – Exemple d'auto-organisation dans le vivant : le chou romanesco (source : CNRS Photothèque / Stéphane Douady)

1.4 Besoins, contributions et organisation de la thèse

Nous avons vu que l'auto-organisation était issue d'une observation du vivant. Et comme pour les organismes vivants, cette organisation a un coût. En effet, dans la nature comme dans les réseaux de capteurs, il n'y a pas de violation du second principe de la thermodynamique : la diminution de l'entropie se fait aux dépens d'une consommation en énergie. Une partie de l'énergie des nœuds va donc servir à construire et à maintenir l'organisation. Nous pensons cependant qu'il est indispensable d'avoir une organisation préalable du réseau qui permette de résoudre les défis des protocoles de communication pour réseaux de capteurs et de surmonter les contraintes des réseaux de capteurs décrites précédemment.

Conscient de ce constat, il existe aujourd'hui des propositions de structure auto-organisatrices. Sont-elles toutes équivalentes ? Comment évoluent-elles ? Comment réagissent-elles face à l'apparition de nouveaux capteurs, ou face à la mort de certains ? C'est à ces questions que s'attachera à répondre le deuxième chapitre de la thèse.

1.4.1 Trois phases dans la vie d'un réseau de capteurs

De nombreuses études traitent de l'évaluation de performances des stratégies d'auto-organisation. Mais le réseau est toujours considéré comme entièrement déployé, statique. Comme le montre en particulier [5], une analyse plus fine est possible pour caractériser les différentes stratégies d'auto-organisation durant la vie d'un réseau de capteurs sans fil. En clair, il s'agit de prendre en compte la dynamique du réseau malgré l'immobilité physique des capteurs. On propose de mettre en évidence les différentes phases de la vie d'un réseau de capteurs et de caractériser un ensemble de protocoles d'auto-organisation sur ces différentes phases ; c'est-à-dire d'en déterminer les comportements. Pour être utile, il faut que les protocoles d'auto-organisation soient adaptés aux réseaux de capteurs. Les réseaux de capteurs traversent différentes phases dans leur existence, les protocoles doivent être robustes face à celles-ci. Le fil rouge de cette thèse est l'auto-organisation. Avant de déterminer un protocole d'auto-organisation il convient d'évaluer

un ensemble de protocoles. Un des points vitaux pour les réseaux de capteurs est la robustesse. Comment réagissent ces protocoles à l'ajout de nœuds ? À la disparition de nœuds ?

Nous montrons dans le chapitre 4 qu'il est possible, en partant des conclusions des chapitres 2 et 3, de développer un protocole d'auto-organisation fournissant une localisation relative et qualitative pour un réseau de capteurs : QLoP (Qualitative Localization Protocol).

1.4.2 Une approche novatrice de la localisation par l'auto-organisation

Jusqu'à présent, pour estimer la proximité d'un nœud dans un réseau de capteurs, il y avait deux stratégies :

- la stratégie fine (Time of Arrival, Time difference of Arrival, Angle of Arrival, la combinaison de ces dernières, ou le positionnement GPS) très consommatrice en énergie et surtout très coûteuse en terme de matériel (puce GPS, horloge très précise, etc.)
- la stratégie approximative avec comme principale solution la mesure de la force du signal reçu.

Nous proposons un nouvel algorithme localisé (QLoP), sans GPS, sans ancre et sans spécificité matérielle particulière qui permet de déterminer une distance qualitative des capteurs de son voisinage. L'idée originale de QLoP est d'arriver à fournir une distance qualitative en se basant sur les informations topologiques localisées et de contourner ainsi l'instabilité du canal radio. Pour établir QLoP, en premier lieu, nous prouverons l'inadéquation des mesures de puissance reçu (RSSI) comme métrique pour estimer la proximité. Nous montrons dans le chapitre 3 pourquoi cette mesure est à la fois non fiable et non robuste.

Qui dit auto-organisation dit propriétés émergentes. Le chapitre 5 prouvera qu'il est possible de construire, grâce à QLoP, des topologies logiques et de fournir, grâce à ces topologies, une meilleure robustesse au routage « *DSR-like* » dans des environnements bruités.

1.4.3 Des applications au contrôle de topologie et au routage

Les propriétés de QLoP, démontrées au chapitre précédent, permettent de construire des topologies logiques telles que le Relative Neighborhood Graph (RNG) de façon efficace. Les protocoles de routage dans les réseaux de capteurs doivent prendre en compte les interactions locales, le bruit et les collisions. Actuellement, aucune étude n'existe sur l'utilisation d'une structure logique pour le routage en environnement bruité. Dans ce chapitre, nous proposons d'utiliser le protocole de localisation QLoP afin de fournir un routage plus efficace en environnement bruité.

Les performances relevées mettent en évidence, au niveau réseau, le gain qu'il y a à utiliser les liens les plus courts. Cependant, cette structure n'est utilisée qu'au niveau réseau, pas au niveau MAC. Le chapitre 6 montrera que sans une approche cross-layer il est difficile de concevoir des protocoles d'auto-organisation optimaux.

1.4.4 Une approche cross-layer

Les mécanismes de niveau 2, comme le *CSMA/CA* ou le **RTS/CTS** utilisés dans les normes IEEE 802.11 (WIFI) et 802.15.4, se basent sur la topologie physique, à plat. Nous montrerons d'une part, qu'il y a inévitablement des interactions entre le choix du protocole d'accès au canal radio (couche MAC) et les performances au niveau réseau, et d'autre part, qu'une approche inter-couche en développant un protocole de niveau 2 basé sur cette topologie de niveau 3 est possible. En nous basant sur QLoP, nous définissons une couche MAC adaptative afin d'améliorer la durée de vie du réseau.

Le chapitre 7 conclura en présentant les principaux apports de ce travail et en donnant les perspectives que nous entrevoyons.

La principale contribution de cette thèse est de prouver qu'une solution d'auto-organisation originale dédiée à la localisation est possible. En se basant à la fois sur les conclusions de la caractérisation des protocoles d'auto-organisation durant la vie d'un réseau de capteurs (naissance, fonctionnement normal et mort) et sur un ensemble d'expérimentations, nous montrons qu'il est possible d'appliquer QLoP au routage, au contrôle de topologie et aux politiques d'accès à la couche physique.

Cette thèse a été réalisée au sein du laboratoire CITI de l'INSA de Lyon dans l'équipe SWING et sous la direction du Professeur Fabrice Valois. Elle a été financée par le projet RNRT ARESA dont les partenaires industriels et académiques sont : Coronis Systems, France Telecom R&D, LIG, TIMA et Verimag.

Bibliographie

[1] http://aresa-project.insa-lyon.fr.

[2] http://www-coronis-com.dyn.elster.com.

[3] Candace K. Chan, Hailin Peng, Gao Liu, Kevin McIlwrath, Xiao Feng Zhang, Robert A. Huggins, and Yi Cui. High-performance lithium battery anodes using silicon nanowires. *Nature Nanotechnology*, 3 :31–35, January 2008.

[4] Crossbow Technology. *Environmental Sensor Board MTS 420/400*, 2009.

[5] F. Dai and J. Wu. An extended localized algorithm for connected dominating set formation in ad hoc wireless networks. *Parallel and Distributed Systems*, 15(10) :908–920, October 2004.

[6] Falko Dressler. Self-organization in ad hoc networks : Overview and classification. Technical report, Autonomic Networking Group, Department of Computer Science, 2006.

[7] François Ingelrest, Guillermo Barrenetxea, and Martin Vetterli. Sensorscope, un système clef en main de surveillance de l'environnement. In *13ème Colloque Francophone sur l'Ingénierie des Protocoles (CFIP)*, Les Arcs, France, March 2008.

[8] Texas Instuments. *MSP430 Ultra Low Power Microcontrollers*. Texas Instuments, 2008.

[9] Barbara Laïk, Laurent Eude, Jean-Pierre Pereira-Ramos, Costel Sorin Cojocaru, Didier Pribat, and Emmanuelle Rouvière. Silicon nanowires as negative electrode for lithium-ion microbatteries. *Electrochimica Acta*, 53(17) :5528–5532, 2008.

[10] J.-L. Lu, F. Valois, M. Dohler, and D. Barthel. Quantifying organization by means of entropy. *IEEE Communications Letters*, 12(3) :185–187, March 2008.

[11] A. Tavakoli P. Levis and S. Dawson-Haggerty. Overview of existing routing protocols for low power and lossy networks. Technical report, IETF, 2009.

[12] David Rios-Arambula, Aurélien Buhrig, Gilles Sicard, and Marc Renaudin. On the use of feedback systems to dynamically control the supply voltage of low-power circuits. *Journal of Low Power Electronics*, 2(1) :45–55, April 2006.

[13] Coronis Systems. *Wavecard Modules Radio Ultra Low Power*. Coronis Systems, 2007.

2

Caractérisation des protocoles d'auto-organisation

2.1 Introduction

Les réseaux filaires ainsi que les réseaux sans fil classiques possèdent structurellement une hiérarchie. Celle-ci se manifeste par la présence d'entités dédiées au bon fonctionnement du réseau : routeurs, antennes-relais, point d'accès... Ces entités, situées au coeur du réseau, ont pour seule finalité de l'organiser : assurer le routage des paquets, la couverture radio, la sécurité... afin que les terminaux puissent utiliser ce réseau. Les réseaux de capteurs, par leur nature homogène (tous les capteurs sont considérés comme physiquement identiques), ne possèdent pas d'infrastructure préalable : chaque entité du réseau va potentiellement utiliser les fonctionnalités du réseau et en assurer le fonctionnement. De plus, de par les contraintes énoncées précédemment, les réseaux de capteurs doivent mettre en place des mécanismes d'organisation du réseau sans intervention humaine, efficaces et économes en énergie.

L'auto-organisation se situe dans la continuité naturelle du développement des stratégies de contrôle des réseaux : tout d'abord centralisée puis distribuée et enfin localisée. Il est faux, cependant, de croire que les mécanismes d'auto-organisation existent seulement dans les réseaux ad hoc ou de capteurs. Comme le souligne [27], il existe des mécanismes simples s'apparentant à des processus d'auto-organisation dans le domaine IP (Internet Protocol) : le DHCP (Domain Host Configuration Protocol), qui permet d'obtenir automatiquement une adresse IP, ou le TCP (Transport Control Protocol), qui permet de réduire la congestion sur l'ensemble du réseau à partir d'observations locales.

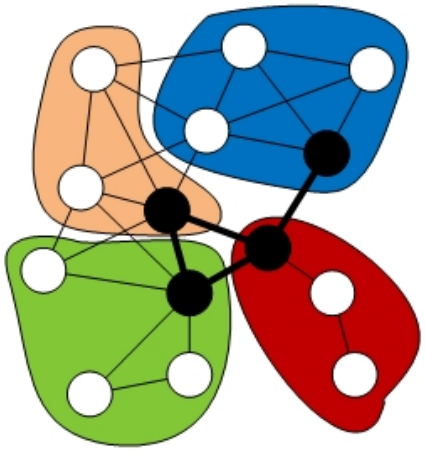

FIGURE 2.1 – Exemple d'organisation en clusters

Selon nous, le fait qu'un réseau soit composé de capteurs matériellement identiques et qu'il soit non hiérarchisé naturellement, n'implique pas nécessairement qu'il doive fonctionner dans cet environnement. Ces hypothèses conduisent à considérer pour chaque problématique : le routage, la localisation ou l'accès au canal radio, un protocole particulier. Au contraire, nous pensons qu'il convient que le réseau s'organise préalablement et que cette organisation fournisse une vue logique sur laquelle s'exécutent les différents protocoles.

De plus, l'auto-organisation n'est pas simplement l'autonomie du réseau, elle est associée aux termes auto-configuration (ensemble des mécanismes générant des configurations appropriées dépendantes de l'environnement), auto-réparation (détection et réparation automatiques des erreurs du réseau liées aux déconnexions ou à la mort de capteurs), auto-gestion (maintenir et gérer le réseau d'après des paramètres préétablis), ou auto-optimisation (similaire à l'auto-gestion mais orientée par rapport à des paramètres optimaux).

Aujourd'hui, nous avons des réseaux de capteurs qui fonctionnent. Des solutions sont mises sur le marché avec succès. Cependant, il reste de nombreux défis à relever : les applications sont encore installées par des professionnels et nécessitent un déploiement manuel. Le routage est encore souvent statique, prédéfini. Nous allons vers des solutions de réseaux plus sécurisés, mais avant même de penser à des attaques ou à des actes malveillants, ne devons-nous pas nous préoccuper de l'impact d'un environnement non pas hostile, mais indifférent ? Le bruit, la volatilité du canal radio, la mort d'un nœud, l'apparition de nouveaux voisins, ne sont pas des scénarios d'attaques hypothétiques par un ennemi invisible, ce sont les conditions réelles d'environnements dans lesquelles doit être déployé un réseau de capteurs.

On rencontre de nombreuses façons de faire de l'auto-organisation dans les réseaux sans fil multi-saut : contrôle de topologie par élagage de liens, orienté dominant, table de hachage distribuée [16], clusters (voir figure 2.1), etc.

L'auto-organisation est donc potentiellement bien plus vaste que les seuls ensembles connectés dominants, clusters ou structures d'élagage de liens. L'objectif de ces protocoles reste cependant le même : créer une vue logique plus efficace que la vue physique.

Dans ce chapitre, nous avons choisi de ne traiter que les deux plus grandes familles d'auto-organisaton : les protocoles de contrôle de topologie par élagage de liens et les protocoles orientés dominant. Les premiers sélectionnent un sous-ensemble de nœuds dans le réseau, tandis que les seconds sélectionnent un sous-ensemble de liens. Nous n'étudions pas l'organisation en clusters qui consiste à diviser le réseau en régions organisées autour d'un chef de cluster (ou *clusterhead*). Si tous les membres du cluster sont à un saut, il est aisé de voir que l'on retrouve la problématique des ensembles maximaux indépendants présente dans les protocoles orientés dominant. Si les nœuds d'un cluster sont organisés de façon non localisée on retrouvera les problématiques des réseaux mais de façon réduite. De manière générale, dans le cas d'un réseau homogène, la division du réseau en régions ne peut pas, selon nous, répondre seule aux problématiques de routage dans un réseau de capteurs. Il existe cependant des solutions hybrides alliant clustering et dorsale virtuelle [37]. De notre point de vue, l'utilisation de table de hachage distribuée, venue des réseaux filaires pair-à-pair, ne convient pas à des réseaux sans fil étendus et contraints en énergie. Le coût d'une communication radio est élevé dans ce type de réseau et impose des communications localisées, incompatibles avec la distribution et l'interrogation de tables de hachage sur l'ensemble d'un réseau de capteurs.

Les motivations pour organiser un réseau sont nombreuses. Les ensembles dominants sont classiquement utilisés pour adresser un ensemble de problématiques présentes dans les réseaux de capteurs. Nous présentons ici les plus importantes.

Inondation. L'algorithme de l'inondation classique est simple : un nœud retransmet le paquet s'il ne l'a pas déjà relayé. Le but est atteint si le réseau est connexe et que les liens sont fiables : tous les nœuds du réseau recevront le paquet. Cependant, cette simplicité a un revers : une grande redondance, et donc une consommation excessive. L'ensemble dominant connecté se présente comme une solution pour réduire le nombre de retransmissions tout en garantissant l'objectif initial, à savoir atteindre tous les nœuds du réseau. Dans ce cas-là, l'inondation n'est effectuée que par les nœuds dominants. De nombreuses études cherchent donc à minimiser le nombre de nœuds dominants dans le réseau, afin de réduire d'autant le nombre de retransmissions [29, 1, 42, 40]. Cependant, le calcul de l'ensemble dominant de taille minimale (MCDS pour Minimum Connected Dominating Set) est un problème NP-difficile (classe des problèmes au moins aussi difficile que l'ensemble des problèmes de NP). Ce calcul doit en outre être effectué, dans le cas des réseaux de capteurs, de façon distribuée, voire localisée. Le compromis est à trouver entre cardinalité de l'ensemble dominant et quantité d'information nécessaire à l'élection des nœuds dominants.

Routage. Le routage dans les réseaux de capteurs est une problématique importante. Les protocoles de routage des réseaux filaires ne sont pas adaptés aux réseaux de capteurs. L'approche « vecteur de distance » (de RIP (Routing Information Protocol) [20] par exemple), qui consiste à partager l'ensemble de sa table de routage avec ses voisins, est à la fois bien trop lente à converger, limitée en nombre de sauts et consommatrice en énergie. Dans le routage à « état de lien » (de OSPF v.2 (Open shortest path first) [23] par exemple) chaque routeur doit avoir la connaissance de l'ensemble de la topologie pour exécuter un algorithme de plus court chemin et construire sa table de routage. On peut facilement imaginer le nombre de mises à jour nécessaires lors du déploiement de 50 nouveaux capteurs dans une topologie de plusieurs milliers

d'autres. Dans ce type de réseau, les informations indispensables pour le routage doivent être réduites et localisées afin de s'adapter rapidement à la topologie. L'un des principaux avantages du routage sur un ensemble dominant est qu'il est supporté par seulement une partie des nœuds du réseau. Seuls ces nœuds maintiennent des informations de routage et eux seuls auront à les mettre à jour en cas de modification de la topologie [8, 37].

Énergie. L'ensemble dominant connecté, qu'il serve à relayer les messages lors d'une inondation ou au routage des paquets de données, va être beaucoup plus sollicité que les autres nœuds du réseau. De nombreuses propositions existent pour intégrer dans l'élection d'un nœud dominant une métrique en lien avec l'énergie [35, 44]. Cela va éviter d'« affamer » les nœuds dominés et permettre de répartir la charge du routage sur plus de nœuds. En outre, la présence d'un ensemble dominant connecté rend simple la mise en place d'un mécanisme d'endormissement des nœuds dominés [12]. Ce dernier mécanisme nécessite néanmoins la mise en place de méthodes d'ordonnancement d'activité.

Agrégation. Le but de l'agrégation est de réduire la charge des données remontées au puits et diminuer l'énergie consommée. L'idée est d'exploiter la corrélation spatiale ou temporelle des données afin d'éliminer les données redondantes. Pour cela, l'agrégation de données se base généralement sur une structure hiérarchique, comme des arbres logiques. Un nœud reçoit des données de ses fils, les agrège avec ses propres données et les transmet à son père et ainsi de suite, jusqu'au puits. La structure dominante connectée peut aisément se transformer en une structure d'agrégation de données : l'ensemble des nœuds dominants ou seulement un sous-ensemble constituera des points de rendez-vous. [19] propose, par exemple, d'utiliser une structure dominante et un modèle adaptatif auto-régressif et moyenne mobile (A-ARMA pour Adaptative-AutoRegressive Moving Average) pour effectuer une agrégation temporelle par chacun des nœuds et spatiale par les nœuds dominants.

Les protocoles d'auto-organisation basés sur l'élagage de liens sont, quant à eux, traditionnellement utilisés sur l'ensemble des problématiques suivantes.

Énergie. Le contrôle de topologie dans les réseaux de capteurs est souvent associé à la problématique d'assignation de puissance de transmission. Si l'on considère qu'il est possible, pour chacun des capteurs, d'ajuster sa puissance de transmission en fonction de la distance de ses voisins, le contrôle de topologie va permettre une importante réduction d'énergie. En effet, la plupart des protocoles d'élagage de liens ont pour objectif de sélectionner les liens les plus courts tout en maintenant la connectivité. De nombreuses études ont donc été réalisées afin de définir une puissance de transmission pour chacun des nœuds afin de réduire le coût énergétique total du graphe, [31, 14, 26].

Inondation. Parallèlement aux préoccupations énergétiques, certains auteurs s'intéressent aux gains possibles en utilisant des protocoles d'élagage de liens pour les problématiques d'inondation. Les protocoles RNG (Relative Neighborhood Graph) et LMST (Local Minimum Spanning Tree) associés à un protocole d'élimination de voisins (NES pour Neighbor Elimination Scheme) sont utilisés dans [5] pour améliorer des mécanismes d'inondation. Une étude comparative avec le protocole centralisé BIP (Broadcast Incremental Power) [41] est présentée : les deux protocoles distribués restent compétitifs en termes de consommation d'énergie.

Débit. En réduisant la puissance de transmission, il est possible de réduire la contention du canal et les interférences et d'augmenter ainsi le débit d'un réseau. Par simulation, [21] montre qu'il est possible de doubler le débit par rapport à une topologie sans contrôle de puissance de transmission.

Sécurité. [11] modifie le protocole de contrôle de topologie LMST pour intégrer une métrique telle que la réputation plutôt qu'une métrique liée à la distance ou à l'énergie. En utilisant le mécanisme d'élagage de lien pour éviter les capteurs corrompus, il montre ainsi qu'il est possible de créer une topologie à la fois connexe et sécurisée en utilisant des protocoles localisés de contrôle de topologie.

Cependant, si celle-ci est parfois souhaitable pour réduire le bruit ou augmenter la robustesse aux interférences, l'élagage des liens entraîne, de facto, une réduction de la redondance des chemins, leur allongement, l'apparition de liens critiques et la fragilisation des routes créées. C'est pourquoi certaines propriétés comme un facteur d'allongement borné ou le degré constant de la topologie créée sont recherchées [4, 43]. Ces topologies peuvent plus efficacement être utilisées pour un routage minimisant le nombre de sauts.

2.2 État de l'art sur l'auto-organisation

Nous nous concentrons dans cet état de l'art sur deux grandes familles de protocoles d'auto-organisation dans le domaine des réseaux de capteurs : les protocoles **orientés dominant** et les protocoles **orientés élagage de liens**. Nous verrons que les objectifs de ces topologies virtuelles sont multiples mais l'idée générale est la même : s'affranchir de la topologie physique en créant une vue logique supérieure à la vue physique.

2.2.1 Orienté dominant

Un ensemble dominant est un ensemble de nœuds tel que tous les nœuds du réseau sont, soit dans cet ensemble, soit voisins d'un nœud de cet ensemble. On dit que cet ensemble dominant est connecté si et seulement s'il existe au moins un chemin entre chaque nœud qui le compose. La propriété de connexité de l'ensemble dominant va permettre de garantir que chaque nœud dominant (i.e. appartenant à l'ensemble dominant) recevra le paquet et sera ainsi capable de le retransmettre.

Nous présentons maintenant quatre protocoles d'auto-organisation orientés dominant : MPR (MultiPoint Relay), MPR-DS (MultiPoint Relay-Dominating Set), CDS-*règle k* (Connected Dominating Set-*règle k*) et CDS-IDS (Connected Dominating Set-Independent Dominating Set). Ils reflètent selon nous l'ensemble des principales familles d'ensembles dominants connectés existant dans la littérature.

Multipoint Relay

[29] présente l'algorithme Multipoint Relay et une heuristique de complexité $\log n$ qui calcule l'ensemble MPR pour un réseau de cardinalité n. Dans cet article, les auteurs développent cet ensemble dominant connecté afin de réduire le nombre de retransmissions lors d'une inondation

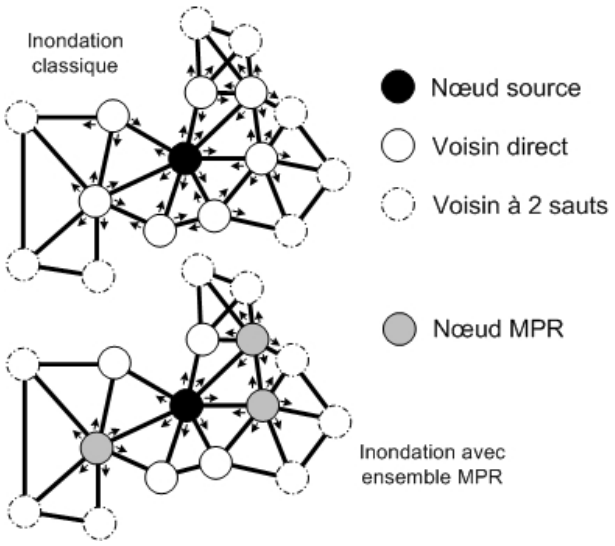

FIGURE 2.2 – MPR : mécanisme de désignation des voisins MPR

du réseau. Un nœud source sélectionne dans son voisinage direct un sous-ensemble de nœuds couvrant l'ensemble de ses voisins à 2 sauts (voir figure 2.2). Plus formellement, soit E, un ensemble de nœuds. Si $N(E)$ est l'ensemble des nœuds de E ou voisins de E, alors $N_1(E) = N(E) - E$ et $N_2(E) = N(N(E)) - N(E)$ sont respectivement l'ensemble des voisins à un saut et l'ensemble des voisins à deux sauts de E. Un ensemble MPR M d'un nœud x est donc un sous-ensemble de $N_1(x)$ tel que $N_2(x) \subset N(M)$. [7] et [24] proposent deux algorithmes différents pour calculer l'ensemble MPR d'un nœud : MPR glouton et MPR Min-id.

Le MPR glouton fonctionne de la manière suivante :

Algorithme 1 Algorithme du MPR glouton

1. Trouver dans le voisinage à deux sauts les nœuds qui ne sont connectés que par un seul voisin direct et intégrer dans le sous-ensemble MPR les voisins connecteurs.
2. Intégrer dans le sous-ensemble MPR en priorité les voisins directs couvrants le plus de voisins à 2 sauts non encore couverts.

Dans le cas de l'algorithme MPR Min-id, les voisins sont explorés et ajoutés ou non à l'ensemble MPR par ordre croissant de leur identifiant. L'avantage de ce dernier algorithme est la possibilité pour un nœud de savoir de lui-même s'il appartient à l'ensemble MPR d'un voisin. Néanmoins, [1] montre que le calcul de l'ensemble MPR pour le MPR Min-id est d'une complexité cubique (en $O(m^3)$), contre une complexité quadratique (en $O(m^2)$) pour le MPR glouton (avec m le degré maximal d'un nœud). Cet article montre également qu'il est bien moins efficace que le second en termes de cardinalité de l'ensemble MPR.

Pour construire un ensemble qui soit connecté et dominant, chacun des nœuds retransmettants (ou nœuds MPR) désigne à son tour ses nœuds MPR dans son propre voisinage. La désignation de voisins MPR est donc localisée puisqu'elle ne nécessite qu'une connaissance du voisinage à deux sauts, mais la construction de l'ensemble dominant est distribuée car elle est dépendante de la source et se propage à travers le réseau.

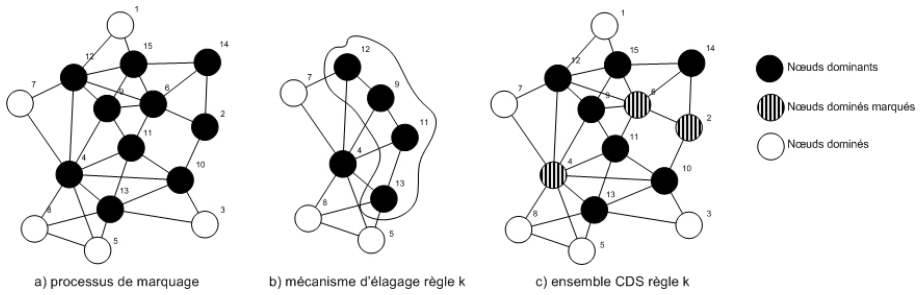

FIGURE 2.3 – CDS : protocole CDS-*règle k*

Ce protocole est utilisé dans le protocole de routage OLSR (Optimized Link State Routing) [7] standardisé par l'IETF.

Multipoint Relay Dominating Set (MPR-DS)

Le Multipoint Relay-Dominating Set (MPR-DS) [1] utilise le même mode d'élection que le MPR. Cependant, afin de ne pas être dépendant d'un nœud qui va initier la construction de l'ensemble dominant, il base l'élection des nœuds dominants sur l'identifiant ce qui lui permet d'être entièrement localisé et non orienté source. Un nœud du réseau va appartenir à l'ensemble dominant s'il respecte une des deux règles détaillées dans l'algorithme suivant.

Algorithme 2 Algorithme de MPR-DS

1. Le nœud est un minimum local : son identifiant est plus petit que tous ses voisins directs.
2. Le nœud est désigné MPR par le voisin de plus petit identifiant.

Ce protocole va donc appartenir à la famille des protocoles à désignation de voisins. C'est par ses voisins qu'un nœud est en mesure de savoir s'il est ou non dans l'ensemble dominant.

Connected Dominating Set *règle k*

Le CDS-*règle k* [42] permet la construction localisée d'un CDS en deux phases : le **processus de marquage** et l'**élagage de la règle k**. Le processus de marquage suit l'algorithme suivant.

Soit E l'ensemble des liens du graphe. Un nœud u se marque s'il a deux voisins directs v et w tel $(w, u) \in E$, $(u, v) \in E$ et $(w, v) \notin E$. Énoncé plus simplement, un nœud se considère comme *marqué* s'il possède deux voisins non connectés entre eux.

Lors de la phase suivante, la règle k s'exécute sur chacun des nœuds marqués.

Soit $V_+(u)$ l'ensemble des voisins marqués de u et d'identifiant supérieur, $V_d(u)$ le voisinage dominant défini par w tel que $(w, u) \in E$ et $V_a(u)$ le voisinage absorbant défini par v tel que $(u, v) \in E$. On calcule l'ensemble des composantes connexes $V_{c_1}, V_{c_2}, ..., V_{c_i}$ du graphe induit par $V_+(u)$, $G[V_+(u)]$. S'il existe au moins une composante connexe V_{c_i} telle que $V_d(u) - V_{c_i} \subseteq V_d(V_{c_i})$ et $V_a(u) - V_{c_i} \subseteq V_a(V_{c_i})$, alors le nœud m se démarque (voir figure 2.3).

En définitive, le CDS-*règle k* définit un ensemble connecté dominant de plus fort poids dans le voisinage.

Connected Dominating Set - Independent Dominating Set

La construction du CDS-IDS proposée par Wan, Alzoubi et Frieder [40] peut se résumer en 3 étapes :

1. Construction de l'arbre couvrant
2. Construction de l'ensemble indépendant dominant (IDS)
3. Construction de l'arbre dominant

Un ensemble dominant indépendant est un ensemble dominant dans lequel chacun des nœuds est non adjacent avec les autres nœuds de l'ensemble. Un nœud appartenant à un IDS est donc, par définition, éloigné d'au moins deux sauts et d'au plus trois d'un autre nœud dominant. La particularité de l'IDS construit par les auteurs est que chaque nœud est à exactement 2 sauts d'un autre nœud de l'ensemble. Ils utilisent pour cela la notion de *rang*. Ce rang est calculé grâce à la distance en nombre de sauts à la racine de l'arbre et à l'identifiant unique du nœud, et va ainsi créer un ordonnancement total parmi les nœuds. L'IDS est ensuite construit de la racine vers les feuilles de la façon suivante :

Algorithme 3 Construction de l'IDS

1. La racine fait partie de l'IDS et envoie un message *BLACK*.
2. Les nœuds qui reçoivent un message *BLACK* se déclarent gris et envoient un message *GREY*.
3. Si un nœud reçoit un message *GREY* de l'ensemble de ses voisins de rang inférieur, il se déclare noir et envoie un message BLACK.

Les nœuds déclarés « noir » appartiendront à l'IDS. Pour construire un CDS, les nœuds noirs désignent un parent de rang inférieur, en partant à nouveau de la racine vers les feuilles. Les parents de nœuds IDS seront considérés comme dominants. Ils formeront, avec les nœuds IDS, l'ensemble dominant connecté.

On le voit, cette topologie se distingue des autres en ceci qu'elle est entièrement distribuée : la construction de l'IDS et du CDS ne se réalise qu'après une phase de découverte du réseau qui va permettre de classer les nœuds selon leur hauteur dans l'arbre couvrant. Cette connaissance quasi globale du réseau va permettre une meilleure sélection de l'ensemble dominant connecté. [40] montre que, contrairement aux autres topologies, la cardinalité du CDS-IDS va être bornée à 8 fois la cardinalité du CDS de taille minimale (MCDS) dans le pire cas.

2.2.2 Orienté élagage de liens

Dans un réseau de capteurs, du fait de l'absence d'infrastructure centralisée, de la fluctuation du canal radio et de la dynamique, le réseau n'a pas de topologie fixe. Le rôle des protocoles de contrôle de topologie va donc être de déterminer une topologie appropriée pour adresser les grandes problématiques des réseaux de capteurs.

Nous présentons ici 4 des algorithmes de contrôle de topologie les plus connus. Nous prenons des antennes omnidirectionnelles comme hypothèse.

Relative Neighborhood Graph

Le *Relative Neighborhood Graph* [38] (RNG) T d'un graphe $G = (V, E)$ est défini par $T = (V, E')$ où E' est l'ensemble des arêtes qui obéissent à cette règle : une arête reliant deux sommets u et v de G appartient à T si et seulement si il n'existe pas de sommets w plus proches à la fois de u et de v. Plus formellement, $\forall u, v \in V : (u, v) \in E' ssi \nexists \ \ w \in V : max d(u, w), d(v, w) < d(u, v)$ où $d(u, v)$ est la distance euclidienne entre les deux nœuds u et v. En résumé, RNG enlève la plus grande arête dans tout triangle du graphe (voir figure 2.4).

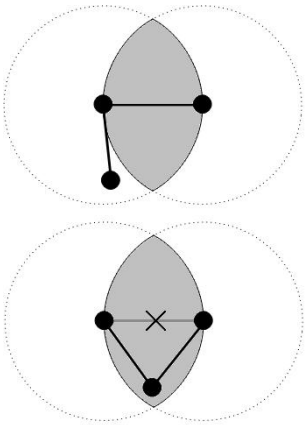

FIGURE 2.4 – RNG : mécanisme d'élagage de liens

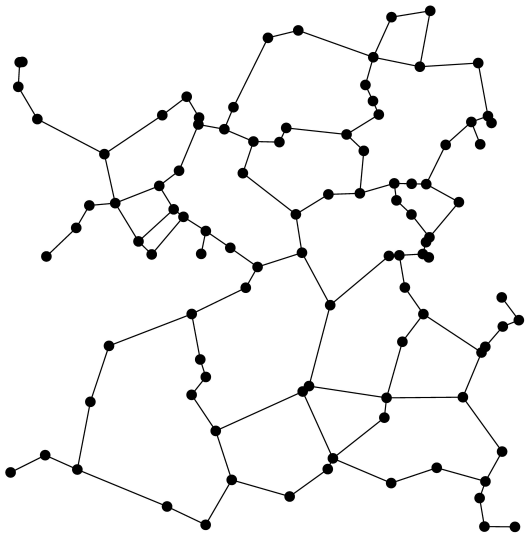

FIGURE 2.5 – RNG : topologie logique de 100 nœuds

Le RNG est un algorithme localisé dans le sens où seule la connaissance du voisinage direct permet la construction de la topologie logique. Cependant, la construction originale de RNG est basée sur la connaissance de la position des nœuds voisins ou de la distance qui sépare un nœud de ses voisins à 1 saut ainsi que du rayon de transmission.

[4] a montré que l'arbre couvrant minimal (MST pour Minimum Spanning Tree) était un sous-graphe de RNG. Cela implique que RNG respecte les propriétés de connexité du graphe initial : si le graphe G est connexe le graphe T l'est également (voir figure 2.5). Cependant, [3] montre que le facteur d'étirement d'une topologie RNG est en $O(|V|-1)$. Le facteur d'étirement d'un graphe est défini par :

$$\alpha = max \frac{d_T(u, v)}{d_G(u, v)}$$

avec $d_T(u, v)$ et $d_G(u, v)$ la longueur en nombre de sauts du chemin dans les graphes T et G entre deux sommets u et v.

Intuitivement, cela signifie qu'une topologie RNG peut donc rendre deux nœuds, voisins dans la topologie physique, très éloignés dans la topologie logique. Le degré moyen d'une topologie RNG est d'environ 2.5.

Les protocoles d'élagage de liens sont très souvent utilisés dans les protocoles de routage

géographique [30]. Ils permettent d'obtenir un graphe planaire (les arêtes d'un tel graphe ne se croisent pas), qui va être l'étape préliminaire au choix du prochain saut dans ce type de routage. RNG est également utilisé dans [5] en combinaison avec le mécanisme d'élimination de voisins (NES) [36] pour réduire le nombre de retransmissions lors d'une inondation.

On peut également citer l'utilisation de la topologie RNG pour la maximisation de la surface couverte par chaque capteur [32].

Local Minimum Spanning Tree (LMST)

Étant donné un graphe non orienté et connexe, un arbre couvrant est un sous-ensemble de ce graphe qui est à la fois un arbre et qui connecte tous les sommets. Si l'on associe un poids à chaque arête, le poids du graphe sera la somme des poids des arêtes qui le composent. L'arbre est dit minimal si son poids est plus petit ou égal à celui de tous les autres arbres couvrants du graphe. Ici, le poids d'une arête sera sa taille soit la distance euclidienne qui sépare les deux sommets qu'elle connecte. L'arbre couvrant minimum local (LMST) a été proposé par [17]. Dans ce protocole, chaque nœud calcule l'arbre couvrant minimal (MST) de son voisinage. Pour ce faire, les auteurs utilisent l'algorithme de Prim [28] :

Algorithme 4 Algorithme de Prim

1. $F \leftarrow \emptyset$ (ensemble des arêtes qui définit le sous-graphe).
2. Tant que F n'est pas couvrant, on ajoute à F une des arêtes de poids minimal qui le relie à un sommet extérieur.

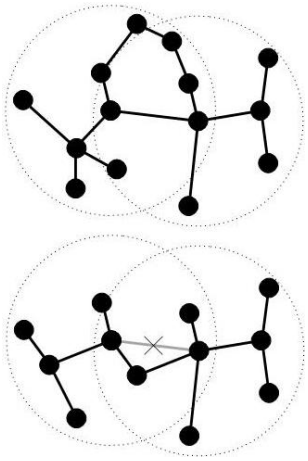

FIGURE 2.6 – LMST : mécanisme d'élagage de liens

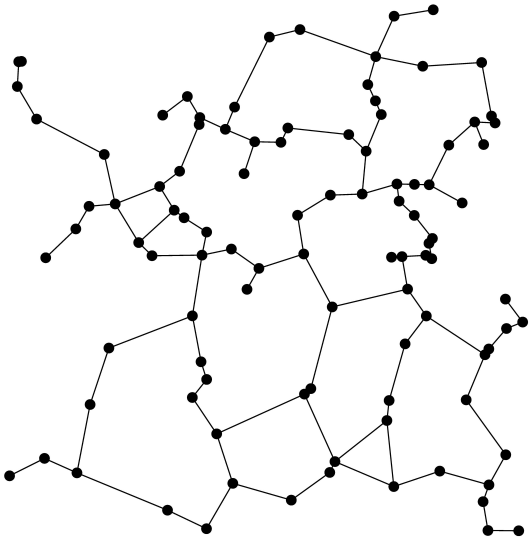

FIGURE 2.7 – LMST : topologie logique de 100 nœuds

Un lien entre deux nœuds u et v appartient au LMST si et seulement si v est voisin de u dans le MST du voisinage de u et si u est voisin de v dans le MST du voisinage de v (voir figure 2.6). La topologie LMST (voir figure 2.7) préserve la connexité du graphe initial tout en ne nécessitant pas de connaissance globale du réseau. Il est à noter cependant qu'une

connaissance très précise de la distance entre les nœuds est indispensable pour la construction d'une topologie LMST. De plus, tout comme la topologie RNG, l'élagage de liens effectué par LMST peut allonger les chemins entre deux nœuds de façon importante : le facteur d'étirement est en $O(|V|-1)$.

Graphe de Gabriel

Le graphe de Gabriel (GG) est introduit par [10] : soit $\mathfrak{D}(u,v)$ le disque de diamètre uv. Une arête appartiendra au graphe de Gabriel si et seulement si $\mathfrak{D}(u,v)$ ne contient aucun autre sommet (voir figure 2.8). Il est aisé de montrer qu'une topologie RNG est un sous-graphe d'une topologie GG : la zone d'exclusion d'un GG est incluse dans la zone d'exclusion d'un RNG. Les topologies GG vont donc également conserver la connexité du réseau. Cependant, le facteur d'allongement de la topologie GG est compris entre $\sqrt{|V|}/2$ et $4\pi\sqrt{2|V|-4}/3$. La figure 2.9 illustre un graphe de Gabriel sur une topologie de 100 nœuds.

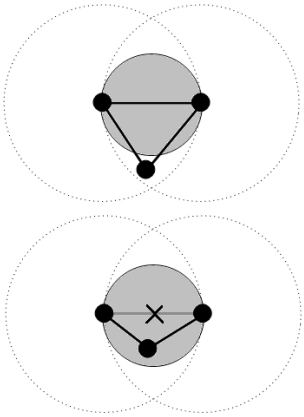

FIGURE 2.8 – Graphe de Gabriel : mécanisme d'élagage de liens

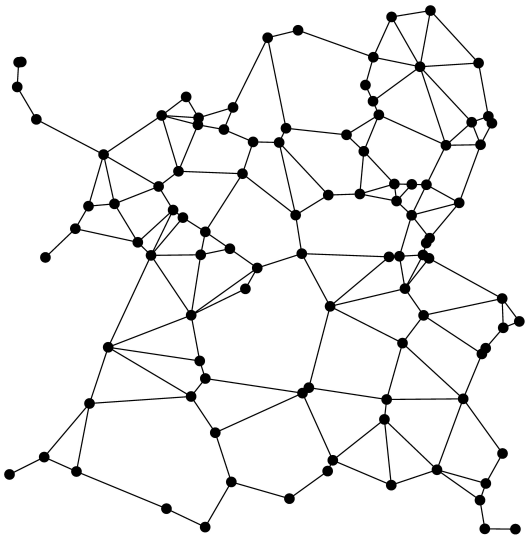

FIGURE 2.9 – Graphe de Gabriel : topologie logique de 100 nœuds

Graphe de Yao

[43] définit le Yao Graph de la façon suivante : on suppose une partition de l'espace autour de chaque nœud du réseau en secteur d'angle fixé. Chaque nœud se connecte au nœud voisin le plus proche dans chaque secteur (voir figure 2.10). À la condition que chaque secteur ait un angle $\Theta < \pi/3$, le graphe résultant sera connexe avec un facteur d'étirement égal à $\frac{1}{1-2sin(\Theta/2)}$ (voir figure 2.11). La zone d'exclusion d'un graphe de Yao (dans le cas d'un angle $< \pi/3$) est incluse dans la zone d'exclusion du graphe RNG, une topologie RNG est donc un sous-graphe des topologies produites par cet élagage de liens.

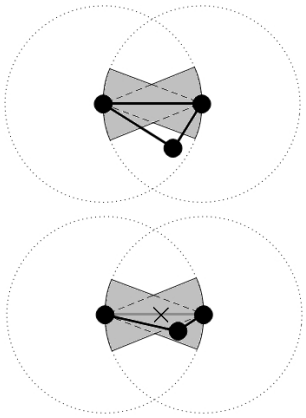

FIGURE 2.10 – Graphe de Yao : mécanisme d'élagage de liens

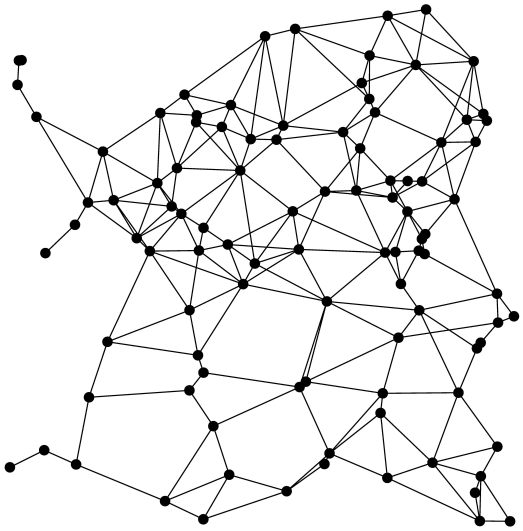

FIGURE 2.11 – Graphe de Yao : topologie logique de 100 nœuds

Graphe de Delaunay

On définit une région de Voronoï comme l'ensemble des points du plan plus proches d'un nœud du réseau que des autres. Intuitivement, cela signifie que chaque nœud x du réseau est au coeur d'une région telle qu'un point de cette région est plus proche du nœud x que de n'importe quel autre nœud du réseau. Le diagramme de Voronoï est l'union des régions de Voronoï. Le graphe de Delaunay est le dual du diagramme de Voronoï, c'est-à-dire que toutes les paires de nœuds dont les régions de Voronoï sont adjacentes sont reliées entre elles (voir figure 2.12). [9] détermine un algorithme dont la complexité en temps dans le pire cas est en $O(n \log n)$. Cet algorithme, basé sur la méthode de la ligne de balayage, a été démontré comme asymptotiquement optimal.

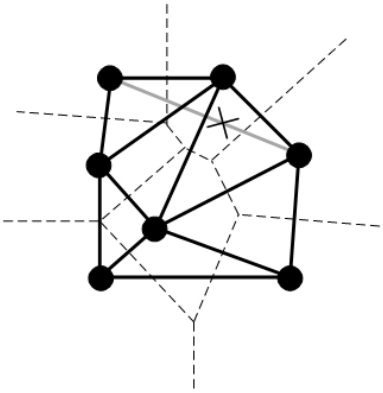

FIGURE 2.12 – Graphe de Delaunay : Diagramme de Voronoi (lignes discontinues) et graphe de Delaunay associé

Comme nous l'avons vu précédemment, de nombreux protocoles de routage garantissent la

livraison du paquet lorsqu'ils fonctionnent sur une topologie planaire. Cependant, à la fois pour RNG, GG ou LMST le facteur d'étirement de ces protocoles orientés élagage de liens n'est pas borné par une constante. Cela a pour conséquence un allongement imprévisible des chemins. Le graphe de Delaunay est donc utilisé dans le routage pour ses propriétés de graphe planaire et de *spanner* (i.e. graphe avec un facteur d'étirement borné) [4]. Le coût de la construction d'un tel graphe de manière distribuée est également traité [18].

2.2.3 Évolution d'un réseau de capteurs

Nous le voyons, les protocoles d'auto-organisation, à la fois orientés dominant ou orientés élagage de liens, se basent en grande partie sur la théorie des graphes : ils sont conçus et testés sur des graphes de disques unitaires (UDG pour Unit Disk Graph). L'évaluation de leurs propriétés reste le plus souvent réalisée avec des métriques directement héritées de cette théorie : cardinalité empirique et théorique de l'ensemble dominant [1], degré moyen de la topologie logique [18], facteur d'étirement et degré moyen des nœuds dominants [36].

Il existe cependant des études sur les performances « réseau » de ces protocoles. [36] étudie le taux d'accessibilité des nœuds et, par-là même, met en évidence le hiatus entre métriques de la théorie des graphes et performances dans un réseau sans fil. En partant du constat que l'auto-organisation réduisait le nombre de liens radio utilisés dans le réseau, [33] s'intéresse à l'impact de l'auto-organisation sur la capacité. [13] étudie la « robustesse » des protocoles MPR, MPR-DS et CDS-*règle k* mais en se limitant à une étude sur le pourcentage de nœuds touchés par une inondation.

Avant d'évaluer les protocoles d'auto-organisation déployés sur les réseaux de capteurs, il convient de déterminer tout d'abord la dynamique propre des réseaux de capteurs. Les problématiques de déploiement sont réduites aux problématiques de placement des capteurs sur le terrain. Pourtant, si le fonctionnement de la plupart des protocoles a été observé sur des topologies statiques, il est probable que ceux-ci aient un comportement différent sur des topologies dynamiques.

Quel est, par exemple, l'impact de la mort ou de la naissance d'un capteur dans l'organisation du réseau ? Cet impact est-il le même selon les protocoles qui organisent ce réseau ? Comment évolue structurellement un réseau organisé selon telle topologie logique ? C'est à ces questions que nous répondrons dans la suite de ce chapitre.

2.3 Comportement au cours de la vie du réseau

Il n'existe, à notre connaissance, que deux études [15, 22] qui prennent en compte, quoique partiellement, les différentes phases de vie d'un réseau de capteurs dans des conditions réalistes. [15] propose une analyse du comportement d'un protocole de clustering durant la phase de déploiement d'un réseau asynchrone. Toutefois, seule cette phase est étudiée et seulement sur ce protocole. Le temps de convergence est calculé, ainsi que l'effet d'un réveil synchrone et asynchrone. Il n'y a de résultat ni durant le fonctionnement normal ni durant la phase de mort et reconstruction du réseau. Enfin, [22] est plus focalisé sur le compromis entre l'efficacité énergétique et la rapidité de la dissémination de données dans le réseau.

Nous proposons ici de définir les trois phases que traversera inévitablement un réseau de capteurs, d'en examiner à la fois les caractéristiques et le comportement des différents protocoles d'auto-organisation durant celles-ci.

2.3.1 Les différentes phases d'un réseau de capteurs

Quand on observe dans sa globalité un réseau de capteurs sans fil, il apparaît des phases distinctes avec des caractéristiques particulières : la **naissance**, le **fonctionnement normal** et la **mort** (voir figure 2.13).

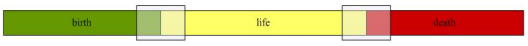

FIGURE 2.13 – Les 3 phases de la vie d'un réseau de capteurs

La phase de **naissance** correspond à l'arrivée progressive des nœuds, à la fois durant le déploiement initial du réseau de capteurs et durant le re-déploiement de nouveaux nœuds. Il en résulte une phase où les nœuds découvrent leur voisinage. Chaque nœud diffuse des paquets `hello` pour indiquer sa présence, transmettre des informations sur son état, et diffuser sa table de voisinage. Des incohérences dans ces tables de voisinage apparaissent alors. En effet, à cause du déploiement progressif, les capteurs ont généralement une vision partielle de leur voisinage physique durant l'envoi de leurs premiers messages : seule une fraction des capteurs présents dans le voisinage se sont déjà déclarés. Cela conduit à des erreurs durant le processus d'élection des nœuds dominants ou le processus de sélection de liens. Par exemple, un voisin à 1 saut peut être considéré comme un voisin à 2 sauts. Nous observons ces incohérences ainsi que le temps nécessaire avant la stabilisation de la structure logique. Nous déterminons ainsi la latence entre la naissance physique d'un réseau et sa naissance logique suivant son schéma d'auto-organisation.

La phase de **fonctionnement normal** commence dès que la structure organisée est stabilisée. Cette phase correspond à ce que nous pouvons attendre de l'auto-organisation. Nous mettons en évidence les particularités d'une auto-organisation durant cette phase en observant soit la cardinalité de la structure dominante (dans le cas de protocoles orientés dominant), soit le degré moyen du réseau (dans le cas de protocoles à sélection de liens). Cette phase peut intégrer des processus d'endormissement des capteurs. La phase de fonctionnement normal se termine quand il y a trop de modifications dans le réseau pour que la structure soit maintenue.

Alors, commence la troisième et dernière phase : la **mort**. Lorsqu'un ou plusieurs nœuds disparaissent, la reconstruction de la structure logique, globale ou localisée va être nécessaire. Là encore, les capteurs n'ont pas immédiatement la perception de la disparition d'un voisin, et cela a pour conséquence une certaine inertie. Cette dernière phase peut être assimilée à un processus de maintenance et d'auto-réparation.

Notre objectif est de mettre en évidence le comportement des protocoles d'auto-organisation durant l'évolution du réseau au cours du temps. Pour cela, nous prendrons 6 protocoles d'auto-organisation : 4 orientés dominant et 2 orientés élagage de liens.

Selon nous, la *qualité* d'un protocole est sa capacité à être performant sur un ensemble de propriétés. L'auto-organisation n'étant pas une fin en soi, elle est entreprise pour répondre à

un objectif. Nous avons énoncé précédemment quelles pouvaient être les différentes motivations pour qu'un réseau s'auto-organise. Les « bonnes » propriétés d'un protocole vont dépendre de ces objectifs. Par exemple, dans le cas d'un protocole de contrôle de topologie, selon que la structure logique est utilisée pour réduire la gestion du voisinage au minimum ou pour router les paquets avec un nombre de sauts minimal, le facteur d'allongement va s'opposer au degré moyen de la topologie logique. En effet, pour le premier objectif, un faible degré moyen va primer sur un facteur d'allongement important. Il est donc important d'établir des métriques cohérentes avec les objectifs du protocole d'auto-organisation. Les protocoles LMST et RNG sont conçus pour réduire le voisinage tout en conservant la connexité du réseau. Le degré logique moyen d'une telle structure est donc une des métriques importantes. Cette réduction importante du degré va entraîner un allongement important. Il est donc également crucial de s'intéresser au diamètre d'une topologie logique et à l'excentricité d'un nœud puits (i.e. le plus long des plus courts chemins entre le puits et les autres nœuds du réseau). Dans le cas d'un protocole d'auto-organisation orienté dominant, même si un allongement de la topologie logique est également observable, c'est la cardinalité de l'ensemble dominant qui va être particulièrement significative. En effet, la réduction de l'ensemble dominant permet de réduire d'autant les retransmissions dans le cas d'une inondation ou de réduire le nombre de capteurs prenant en charge le routage des paquets de données. Les réseaux de capteurs étant très contraints en énergie, la consommation énergétique va donc également être une métrique importante.

Cependant, c'est l'observation de ces métriques dans le temps qui va donner une indication supplémentaire et originale de la qualité d'un protocole. La latence, c'est-à-dire la durée d'instabilité de la structure logique, est mesurée. Afin de comprendre les conséquences de la disparition d'un nœud, nous observons le nombre de changements qu'entraîne cette disparition ainsi que leur distance par rapport au nœud mort. Cette métrique est utile pour comprendre pourquoi, en dépit de protocoles localisés, il est possible d'avoir des reconstructions non locales. Selon nous, ces métriques permettent de caractériser les différentes auto-organisations durant l'évolution d'un réseau de capteurs sans fil (naissance, vie et mort).

2.3.2 Déploiement du réseau

Les résultats présentés par la suite proviennent de simulations avec un intervalle de confiance de 95%. Nous utilisons un simulateur à évènements discrets : JIST-SWANS [2]. La modélisation de la couche physique prend en compte l'évanouissement du canal, les interférences et les collisions. Cela implique que le voisinage n'est pas nécessairement persistant et que des pertes de paquets peuvent subvenir. La cardinalité du réseau varie entre 50 et 200 nœuds distribués en suivant une loi aléatoire et uniforme. La puissance d'émission permet de contrôler la densité du réseau. L'objectif est d'observer les environnements influençant la construction de la topologie logique. Chaque capteur est considéré comme fixe et son identité est déterminée par un identifiant unique.

Le temps de construction de la topologie logique (naissance) est différent selon les schémas d'auto-organisation orientés dominant (voir figure 2.14). Alors que les nœuds découvrent leur voisinage en moins de 1.8 seconde, la topologie logique du MPR va mettre dix fois plus de temps avant de devenir stable. En revanche, les autres schémas seront plus rapides, achevant la

construction de leur ensemble dominant en moins de quelques secondes.

Le degré moyen des nœuds va avoir un impact non négligeable dans le temps de construction des structures logiques basées sur une construction en arbre : la hauteur de l'arbre parcourant le réseau étant d'autant plus réduite que le degré moyen est élevé par rapport à un même graphe de degré moindre, le temps de parcours et d'élection des nœuds dominants s'en trouve réduit. Pour le MPR-DS et le CDS-*règle k*, ce temps de construction reste identique car l'élection des nœuds dominants est purement locale.

L'énergie consommée est directement liée au temps par l'utilisation de `hello` périodiques. Une latence importante signifie qu'un nombre important de paquets est nécessaire. On note que la construction de la topologie pour le CDS-*règle k* va nécessiter une phase où près de 80% des nœuds seront présélectionnés comme dominants avant de prendre leur statut de « dominés ». Ce passage d'un statut à l'autre, s'il n'est pas préjudiciable en termes de latence peut, en revanche, être coûteux en énergie.

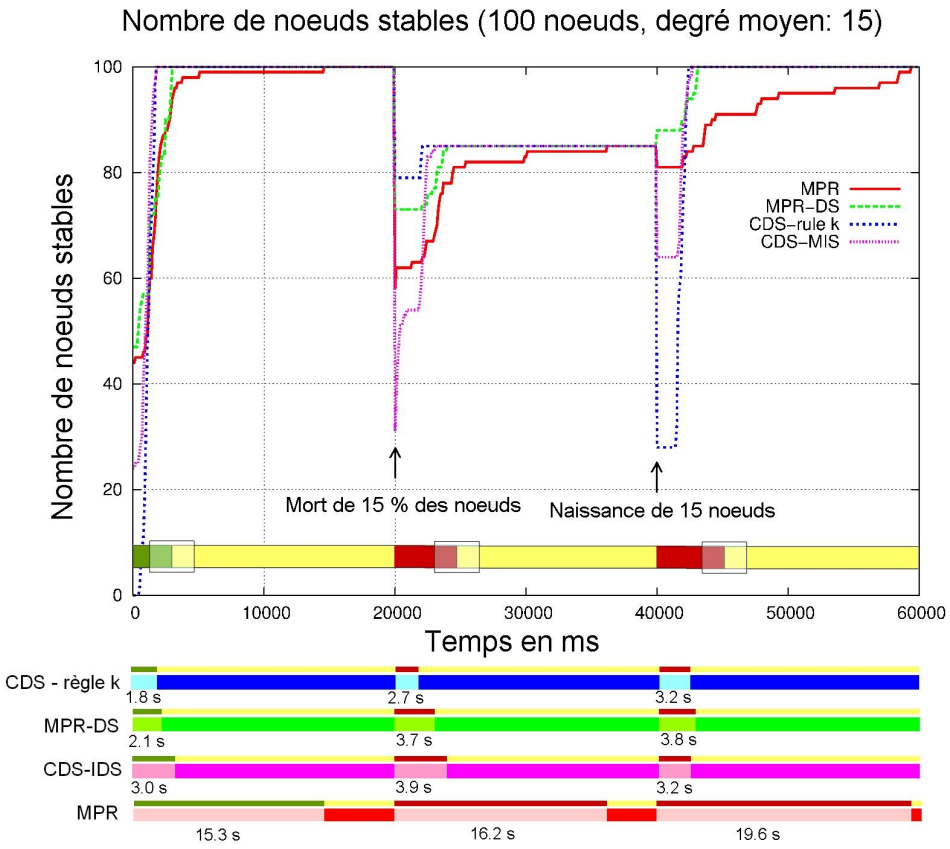

FIGURE 2.14 – Latence des 4 schémas d'auto-organisation orientés dominant

La construction des topologies de sélection de liens est beaucoup plus rapide. La naissance logique du réseau, c'est-à-dire à la construction de la topologie logique, correspond exactement à sa naissance physique, c'est-à-dire la découverte de l'ensemble du voisinage de chaque capteur. Ainsi, la naissance logique est très rapide : aux alentours de 1.8 seconde. Les deux protocoles sont

donc très proches. La vitesse à laquelle les nœuds déterminent leurs voisins logiques, ceux avec qui ils gardent un lien, est seulement liée à la périodicité d'envoi des paquets `hello` (voir figure 2.15). La qualité des protocoles de sélection de liens durant la phase de fonctionnement normal est déterminée par la qualité des liens sélectionnés et la connectivité du réseau. RNG et LMST garantissent la connectivité du réseau. Cependant, LMST est légèrement plus performant : pour un degré moyen constant de 18, il garde seulement 2.2 voisins logiques tandis que RNG en sélectionne 2.4. Cela est parfaitement en accord avec les résultats théoriques.

2.3.3 Adaptation des topologies logiques : la robustesse

Une des attentes des réseaux de capteurs est leur capacité à être déployés dans des conditions difficiles, rapidement. Cela signifie que sans robustesse le réseau perd son principal intérêt. Pour mesurer la robustesse, nous enlevons un pourcentage variable de nœuds du réseau, parmi les dominants, les dominés (dans le cas des protocoles orientés dominant) ou indistinctement (dans le cas des deux stratégies). Nous étudions ensuite les conséquences de cette manipulation sur l'organisation du réseau : l'aspect localisé ou étendu des modifications et leur intensité. Si la perte de quelques capteurs dans un réseau entraîne une réorganisation limitée au voisinage des capteurs morts et ne concerne qu'un faible nombre de nœuds, la robustesse sera considérée comme forte. À l'inverse, si le nombre de capteurs perturbés par ces changements topologiques est important ou si les conséquences sont étendues dans l'espace, la robustesse sera considérée comme faible.

Pour les topologies orientées dominant, la perte d'un nœud dominant a plus de conséquences que la perte d'un nœud dominé quelque soit la stratégie choisie. On remarque cependant des différences notables entre elles quant à l'importance des conséquences. Le CDS-IDS est très peu résistant à la perte de capteurs notamment pour les degrés moyens et faibles, mais il retrouve rapidement une structure stable. Le MPR est plus résistant en termes de changements de topologie mais ne retrouve une structure stable que très lentement après la perte des nœuds. Le MPR-DS et le CDS-*règle k* se comportent convenablement face à la perte de nœuds : leur structure est changée localement et elle se stabilise rapidement.

Il est intéressant de noter qu'à taille égale, un réseau avec un degré moyen supérieur sera plus robuste quelque soit le protocole d'auto-organisation utilisé. La raison de la faiblesse structurelle du MPR et du CDS-IDS est à chercher dans la construction en arbre de l'ensemble dominant. Si cette structure permet une faible cardinalité de l'ensemble dominant pour le CDS-IDS [40], l'initialisation de la construction par un nœud « source » entraîne une grande fragilité : si un nœud dominant proche de la source change d'état, c'est toute la branche de l'arbre qui est potentiellement à reconstruire. Ainsi d'après les différentes simulations effectuées, le nombre de changements lors de la perte de nœuds MPR est relativement important. Lorsque l'on supprime un nœud de l'arbre, le nombre moyen de nœuds affectés est de 3 et la portée moyenne de 1.70 saut. Un comportement similaire est constaté pour le protocole CDS-IDS avec une moyenne de 13 nœuds dont le statut est modifié et une portée de 1.70 saut. Cela signifie que la perte d'un seul nœud dominant va entraîner une modification topologique importante de l'arbre, à la fois en termes de nombre de nœuds modifiés mais également en termes de distance par rapport au nœud mort. Là encore, la construction en arbre de l'ensemble dominant est mise en cause.

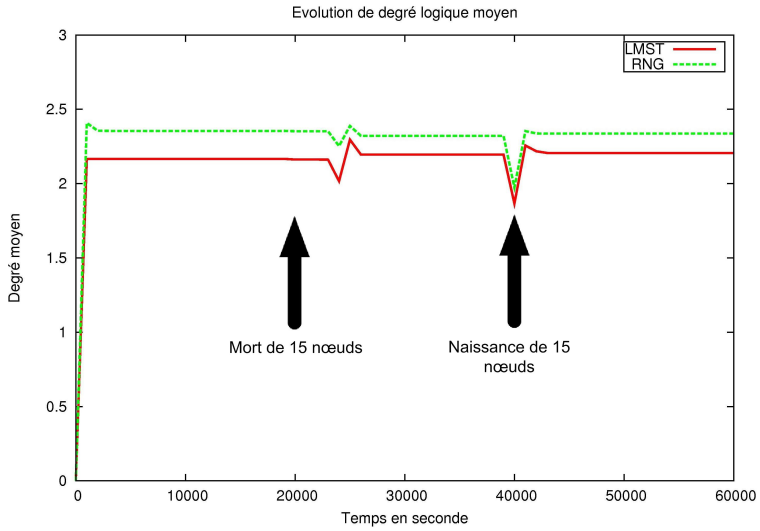

FIGURE 2.15 – Évolution du degré moyen des topologies LMST et RNG

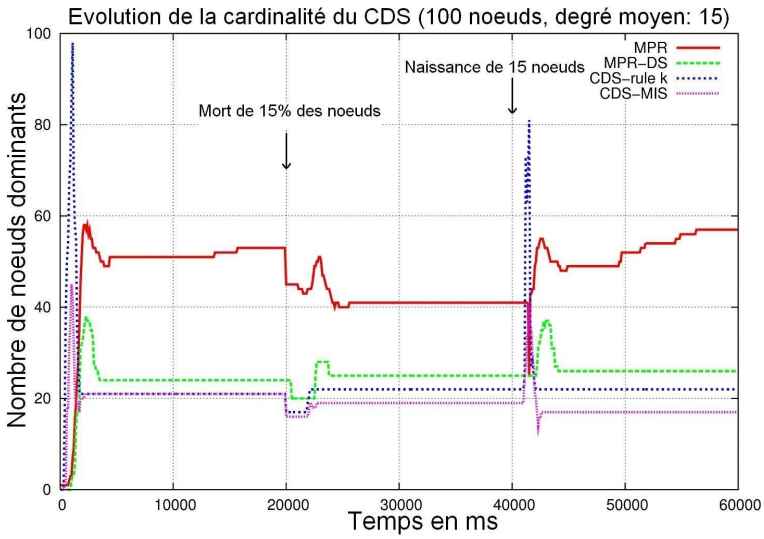

FIGURE 2.16 – Évolution de la cardinalité du CDS pour les topologies orientées dominant

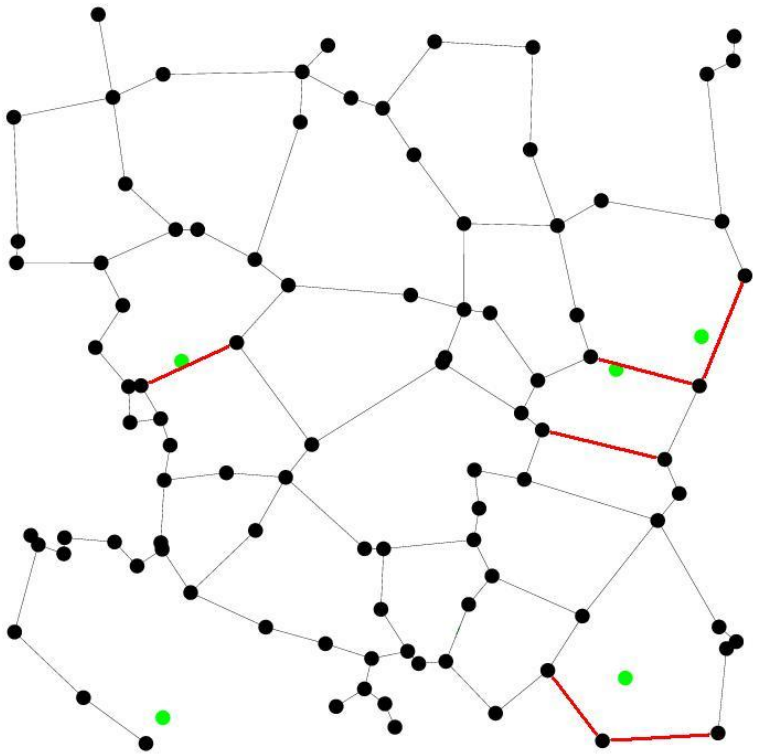

FIGURE 2.17 – Conséquences de la mort de nœuds sur la topologie RNG

De plus, la cardinalité très faible d'un ensemble dominant organisé avec le protocole CDS-IDS suggère une plus grande importance des nœuds dominants causée par la faible redondance. L'efficacité de la sélection des nœuds dominants se transforme en fragilité quand un de ces nœuds disparaît.

Le protocole CDS-*règle k* se comporte de façon très satisfaisante dans les deux aspects tandis que le protocole MPR-DS subit un changement de topologie non négligeable mais uniquement localisé à 1 saut du nœud perdu. (1.1 nœud changeant en moyenne sur un rayon moyen de 1.1 saut pour le CDS-*règle k* et 2.4 nœuds changeants en moyenne sur un rayon moyen de 1.08 saut pour le MPR-DS).

Le comportement des protocoles d'élagage de liens est différent. Les incohérences sont plus rares car seul le voisinage à 1 saut est concerné et il n'y a pas de mécanisme d'élection. En conséquence, les perturbations dues à la perte d'un nœud sont très limitées et totalement localisées. De plus, le degré moyen du réseau joue un rôle mineur dans la robustesse car la topologie LMST ou RNG est peu sensible à la puissance de transmission. Le nombre moyen de changements d'une topologie organisée selon RNG est égal à 1.7. La propagation de la perte d'un nœud est purement locale et donc égale à 1 saut dans la topologie physique. Cela signifie que seules les arêtes contenues dans le voisinage du nœud mort sont potentiellement perturbées (voir figure 2.17). Le comportement est similaire pour le protocole LMST en termes de nombre de changements (1.8) et de propagation.

Les deux figures 2.18 et 2.19 illustrent ces résultats. Elles représentent les modifications dans

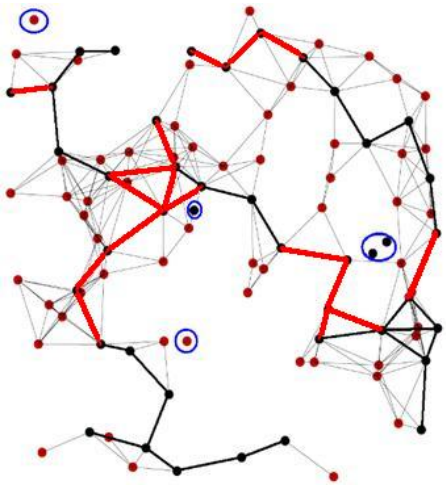

FIGURE 2.18 – Conséquences de la mort de nœuds sur la topologie CDS-IDS

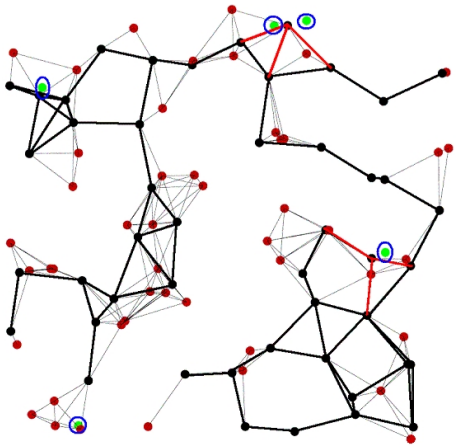

FIGURE 2.19 – Conséquences de la mort de nœuds sur la topologie CDS-*règle k*

la topologie logique quand plusieurs nœuds meurent. La figure 2.18 correspond à une topologie logique organisée avec CDS-IDS. Le nœud leader, qui amorce la construction de la topologie, est représenté en vert, les nœuds entourés de bleu sont les nœuds morts et les arêtes rouges représentent les changements topologiques induits par cette mort. Nous pouvons noter que les perturbations peuvent survenir loin des nœuds perdus. En effet, les changements de topologie peuvent se propager jusqu'à la fin d'une branche de l'arbre. À contrario, les topologies créées par le CDS-*règle k* (voir figure 2.19) réagissent généralement par le simple remplacement du nœud dominant mort par un voisin à 1 saut. Les perturbations sont localisées.

Nous observons également le comportement des protocoles d'auto-organisation quand de nouveaux nœuds sont déployés alors que la structure logique est déjà construite. Dans ce scénario, le CDS-*règle k* est extrêmement inefficace car sa phase initiale, le *marking process*, sur-sélectionne les nœuds dans l'ensemble dominant. Pendant la seconde phase de l'algorithme, la règle d'élagage k les dé-selectionne presque immédiatement (voir figure 2.16) mais cette variation d'un état dominant à un état dominé, d'un nombre aussi important de nœuds, même si elle n'a que peu d'effet néfaste sur la latence, peut coûter cher en énergie.

Le CDS-IDS réagit mieux mais 15% des nœuds du réseau vont subir ce changement. Le MPR et le MPR-DS ne vont souffrir de presque aucun changement de topologie et vont se contenter d'absorber les nouveaux nœuds dans leur topologie. Le degré moyen du réseau ne va pas changer radicalement ces comportements : seul l'identifiant des nœuds ajoutés peut avoir une influence pour le cas du protocole MPR-DS dont la topologie logique va être perturbée par l'apparition d'un nouveau minimum local. En effet, dans le cas de ce protocole, l'élection est en partie basée sur le numéro d'identifiant du capteur.

2.4 Évolution des propriétés structurelles des différentes structures d'auto-organisation

Pour les résultats qui suivent, chaque protocole a été implémenté dans le simulateur WSNet. 100 capteurs sont déployés suivant une loi aléatoire et uniforme sur une surface de 100x100m. Cela signifie que pour chaque point de cette surface, la probabilité que soit présent un capteur est la même. Chacun capteur est considéré comme fixe. La consommation énergétique des capteurs est modélisée de façon linéaire. Le coût d'une unité de temps de transmission sera égale à une unité de temps de réception. La consommation d'un noeud endormi est 10^4 fois moins importante qu'à l'état de veille. De plus, la consommation radio constitue 95% de la consommation totale d'un capteur. Nous avons donc choisi de négliger la consommation énergétique en dehors de la consommation liée aux communications radio. La puissance d'émission d'un capteur est fixée mais, en raison d'une modélisation fine du canal radio, la portée de communication de chaque capteur peut varier au cours du temps et ne forme généralement pas un disque unitaire. Malgré leur diversité, chaque protocole a été développé de façon à n'utiliser que des paquets `hello` périodiques et des paquets de données. Les paquets de données sont sensiblement plus importants que les paquets `hello` (1Ko pour un paquet de données contre 100 octets pour un paquet `hello`). La couche MAC (Medium Access Control) utilisée est une couche de type CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance).Les paquets de données sont générés par les capteurs du réseau et envoyés de façon périodique au puits selon un routage multi-saut sur la dorsale virtuelle dans le cas d'une topologie orientée dominant, suivant un routage par gradient dans le cas d'une topologie orientée élagage de liens. Ce scénario correspond à la fois à une spécification du projet ARESA et à une application-type du partenaire industriel Coronis. Chaque capteur possède une réserve d'énergie fixée. Lorsque le capteur transmet ou reçoit un signal radio (lui étant destiné ou non), il consomme de l'énergie.

Dans les simulations nous avons exploré deux cas de figure concernant les protocoles orientés dominant : avec mécanisme d'endormissement ou sans. Le mécanisme d'endormissement est mis en place de la façon suivante : les nœuds dominés se mettent en veille sauf pour envoyer leurs données, mettre à jour leur table de voisinage et participer ainsi à la dynamique de la topologie.

Nous présenterons ici les principaux résultats obtenus sur une topologie orientée dominant CDS-*règle k* et une topologie orientée élagage de liens : RNG.

2.4.1 L'effet donut

Dans cette section, nous observons comment évolue un réseau de capteurs dans le cas d'un scénario classique de remontée périodique de données vers un puits central.

Pour cela, nous étudions l'évolution du diamètre sur l'ensemble des topologies. Le diamètre d'un graphe est le plus long des plus courts chemins entre deux sommets de ce graphe.

Il est important de noter que l'organisation orientée dominant a une influence sur le diamètre de la topologie initiale. En effet, un chemin entre deux capteurs ou entre un capteur et le puits emprunte obligatoirement la dorsale virtuelle ce qui l'augmente potentiellement. On remarque, dans le cas d'une topologie CDS-IDS, un étirement de la topologie initiale de l'ordre de 75%.

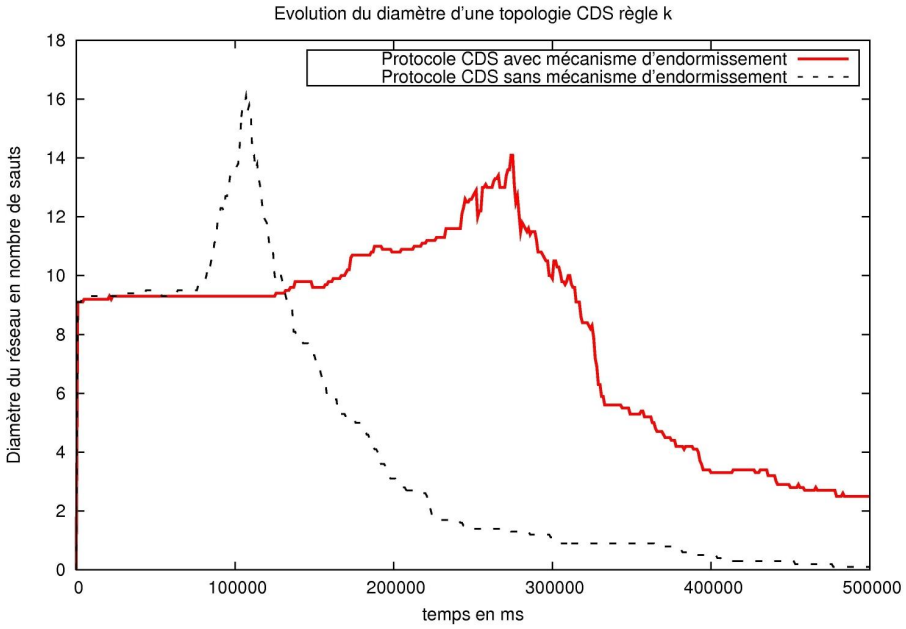

FIGURE 2.20 – Topologie CDS-*règle k* : allongement de la topologie au cours du temps

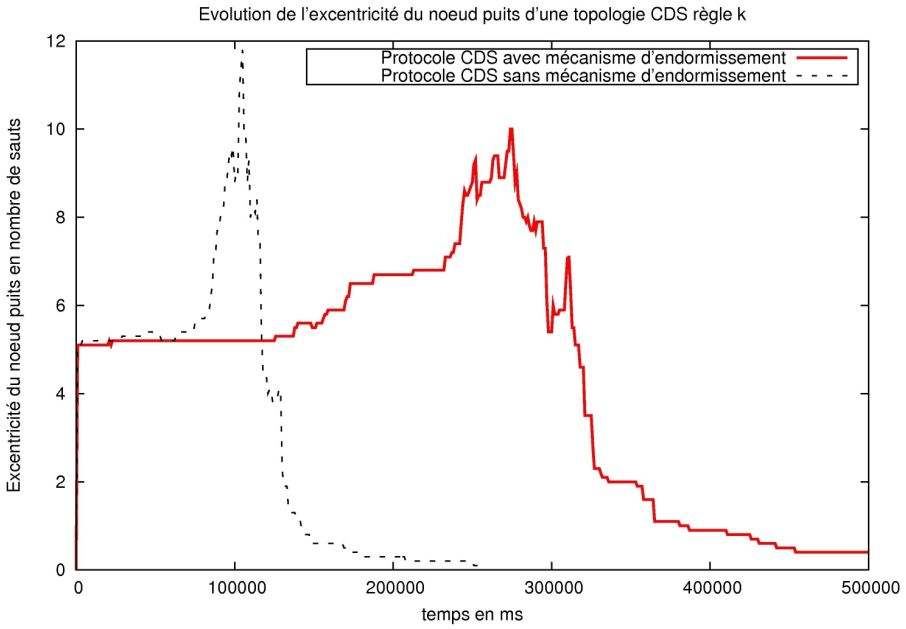

FIGURE 2.21 – Topologie CDS-*règle k* : excentricité du puits au cours du temps

La construction localisée dans le cas du CDS-*règle k* et du MPR-DS et la grande cardinalité de l'ensemble dominant dans le cas du MPR entraînent un étirement très limité.

La figure 2.20 représente l'évolution du diamètre d'une topologie CDS-*règle k*. Dans le scénario avec endormissement, elle montre l'allongement progressif de la topologie puis la contraction du réseau. En l'absence de mécanisme de veille, le réseau subit à la fois plus brutalement et

avec plus d'ampleur ce même phénomène. Ces deux courbes sont à mettre en relation avec l'évolution de l'excentricité du puits visible sur la figure 2.21.

L'excentricité du puits va mesurer le nombre maximal de sauts à effectuer par n'importe quel capteur encore connecté pour atteindre ce puits. Ces deux figures mettent en évidence un phénomène : sans mobilité physique des capteurs, il y a tout de même une expansion du réseau. Nous pouvons également remarquer une plus grande expansion du réseau en l'absence de mécanisme d'endormissement. Ce phénomène s'explique par la disparition plus rapide et donc de manière moins uniforme des capteurs sur l'ensemble du réseau. Alors qu'en présence de mécanismes d'endormissement les capteurs en bordure du réseau sont également touchés par la perte d'énergie, dans le cas d'une absence d'endormissement, ces capteurs peu sollicités, ont tendance à faire augmenter l'excentricité et le diamètre du réseau.

Si l'on répartit les capteurs dans 4 classes selon le chemin le plus court du capteur vers le puits (gradient), nous pouvons observer que le nombre de capteurs appartenant à la quatrième classe (correspondant aux gradients les plus élevés) augmente de façon importante (voir figure 2.22). Le même phénomène se produit dans le cas d'un scénario sans mécanisme d'endormissement (voir figure 2.23). Cela signifie que les capteurs, initialement à quelques sauts du puits, s'en retrouvent très éloignés suite à la perte de capteurs intermédiaires.

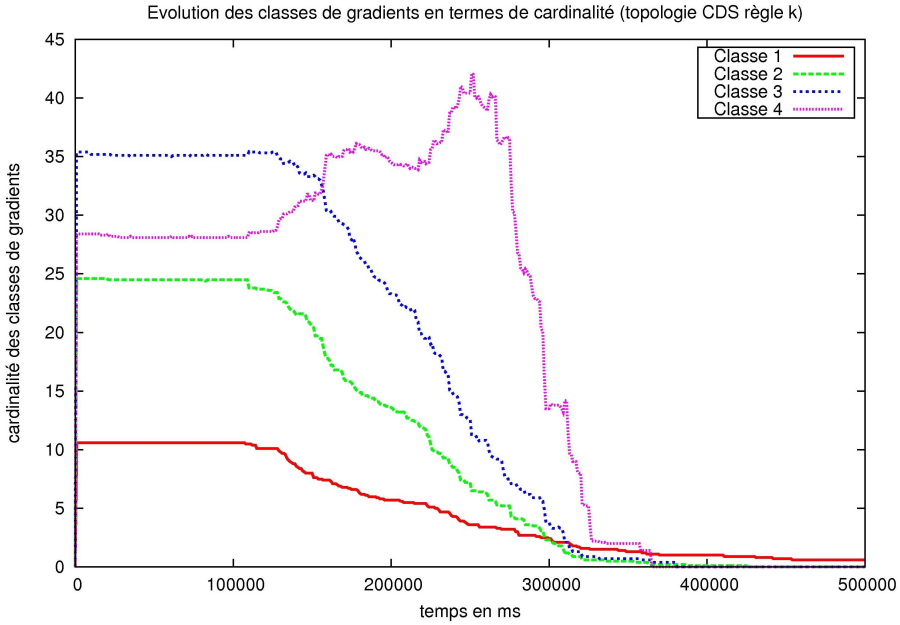

FIGURE 2.22 – Topologie CDS-*règle k* : évolution des classes de gradient au cours du temps (avec mécanisme d'endormissement)

À quoi est due cette expansion ? La mort des nœuds, en raison d'un épuisement d'énergie, n'est pas répartie uniformément sur l'ensemble du réseau. En effet, la consommation d'énergie d'un nœud résulte principalement de la réception et de l'envoi de paquets de données. Les nœuds sollicités pour la retransmission vont donc être particulièrement exposés. Dans le cas d'une topologie orientée dominant, l'énergie des nœuds dominants décroîtra de manière beaucoup plus importante que celle des nœuds dominés (voir figure 2.24). En outre, on remarque une

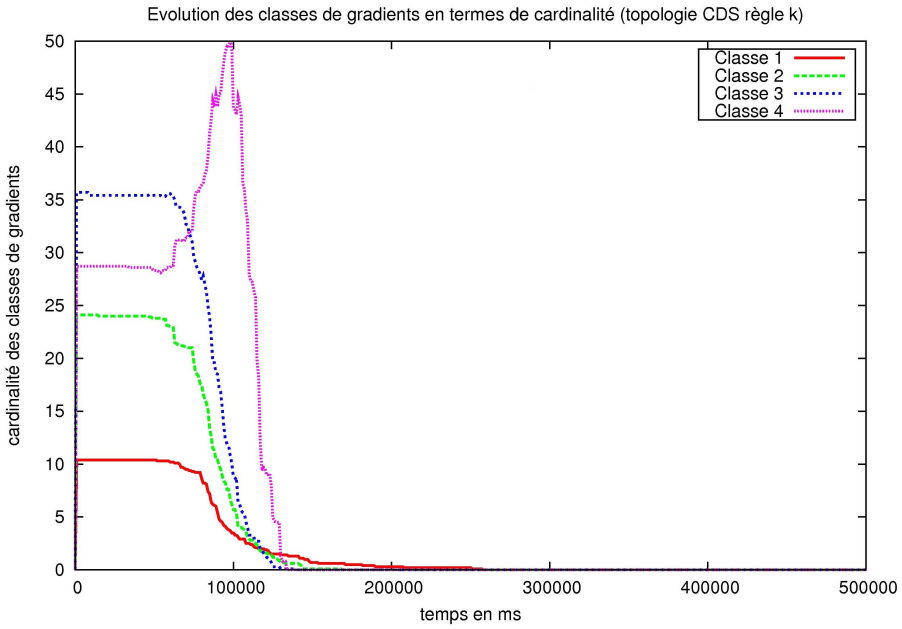

FIGURE 2.23 – Topologie CDS-*règle k* : évolution des classes de gradient au cours du temps (sans mécanisme d'endormissement)

forte corrélation entre niveau d'énergie et distance euclidienne au puits (voir figure 2.25). Cela correspond à l'**effet donut** [25] : les capteurs proches du puits vont épuiser leur énergie beaucoup plus rapidement que les autres nœuds du réseau. La désertification du centre du réseau va augmenter le diamètre du réseau et l'excentricité du puits (voir figure 2.29b)). Les capteurs morts vont créer peu à peu un trou autour du puits et finalement entraîner la déconnexion du réseau (voir figure 2.29c)). L'absence du mécanisme d'endormissement va simplement accélérer et amplifier ce phénomène.

Dans le cas des topologies à élagage de liens, le processus en oeuvre est le même (voir figures 2.26 et 2.27). Cependant, la particularité des protocoles choisis est d'étirer déjà initialement et de façon importante le réseau. La mortalité d'un nœud sera également très fortement corrélée avec sa distance euclidienne au puits (voir figure 2.28). Nous pouvons remarquer cependant que la consommation des capteurs est beaucoup plus importante et la vie du réseau bien plus courte en raison, à la fois de l'allongement des chemins, et de l'absence d'un mécanisme d'endormissement (complexe à mettre en place dans ce type de topologie sans hiérarchie).

Il est naturel que les capteurs proches du puits soient les premiers à disparaître car c'est dans cette région que se concentre tout le trafic de données. Cependant, les effets de ce phénomène sont presque exclusivement observés dans une problématique de contention du canal [6, 39]. Les solutions proposées consistent à modifier le protocole MAC des nœuds à 1 saut du puits [6] ou à détecter la contention pour mettre en place une réaction appropriée [39] (limitation de la fréquence d'envoi des paquets par exemple). Cependant, il est inévitable, si l'on exclut le déploiement de nouveaux capteurs, et dans le cas d'un réseau multi-saut de capteurs homogènes, que les nœuds près du puits soient, en moyenne, plus sollicités que les nœuds en bordure du réseau. Il est donc important, à défaut de pouvoir éviter ce phénomène, d'en comprendre les

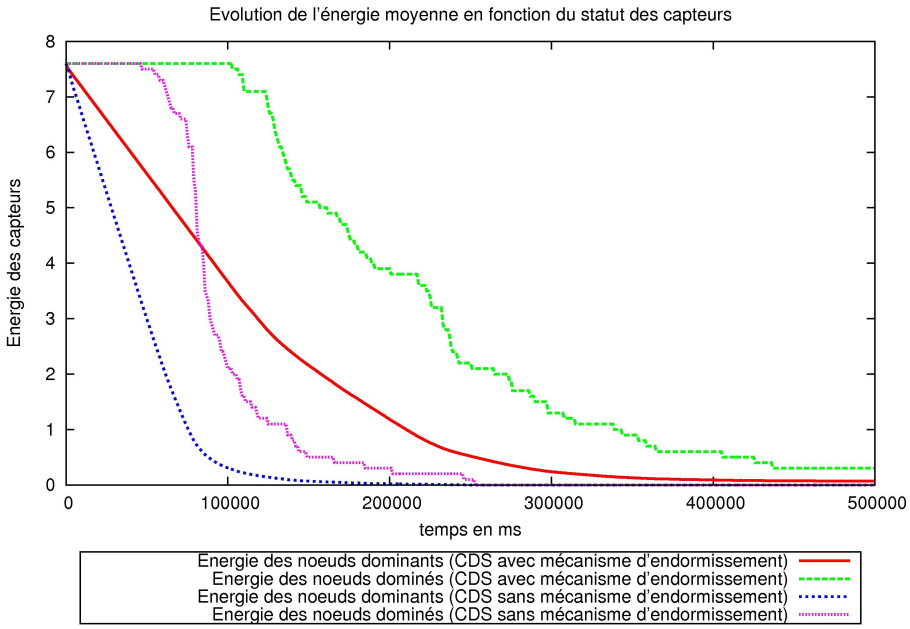

FIGURE 2.24 – Topologie CDS-*règle k* : évolution de l'énergie en fonction du statut des nœuds

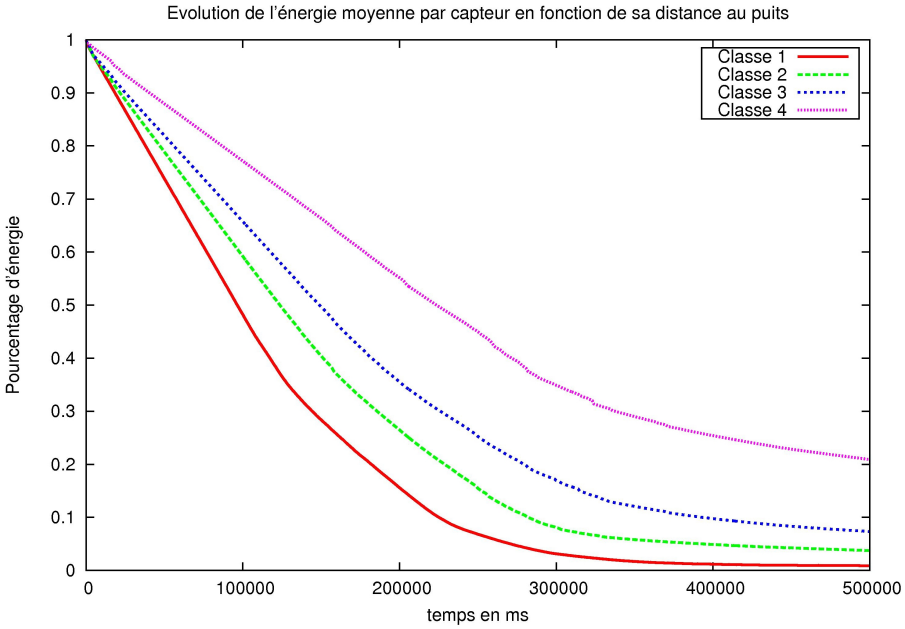

FIGURE 2.25 – Topologie CDS-*règle k* : évolution de l'énergie au cours du temps en fonction de la distance au puits (avec mécanisme d'endormissement)

mécanismes.

Il existe, à notre connaissance, deux études traitant de l'effet donut dans les réseaux de capteurs : [34] et [25]. Dans [34], les auteurs proposent d'équiper les capteurs de batteries dont la capacité serait inversement proportionnelle à la distance au puits. Dans [25], les auteurs proposent d'augmenter la densité des capteurs au voisinage du puits. Ces deux articles ne se

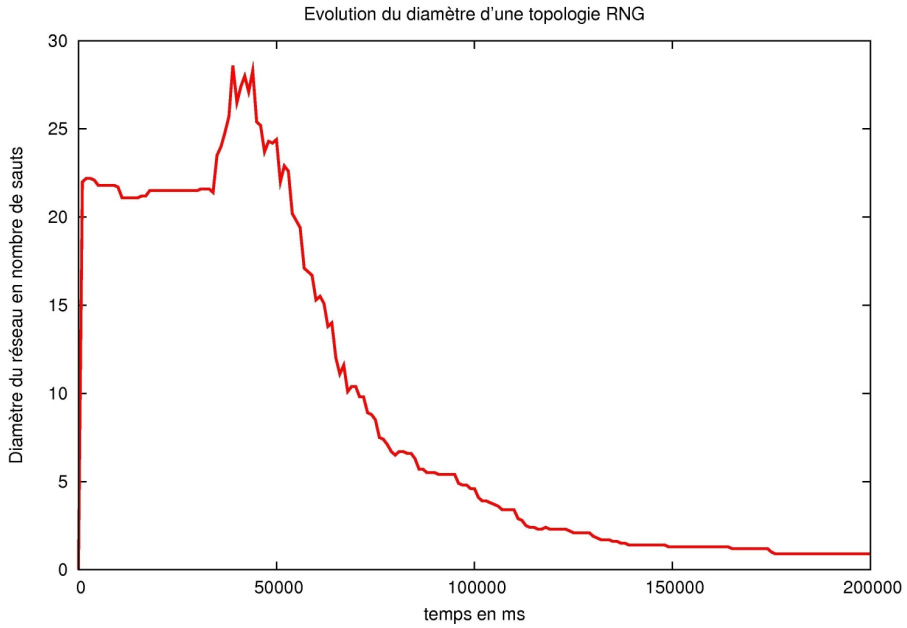

FIGURE 2.26 – Topologie RNG : allongement de la topologie au cours du temps

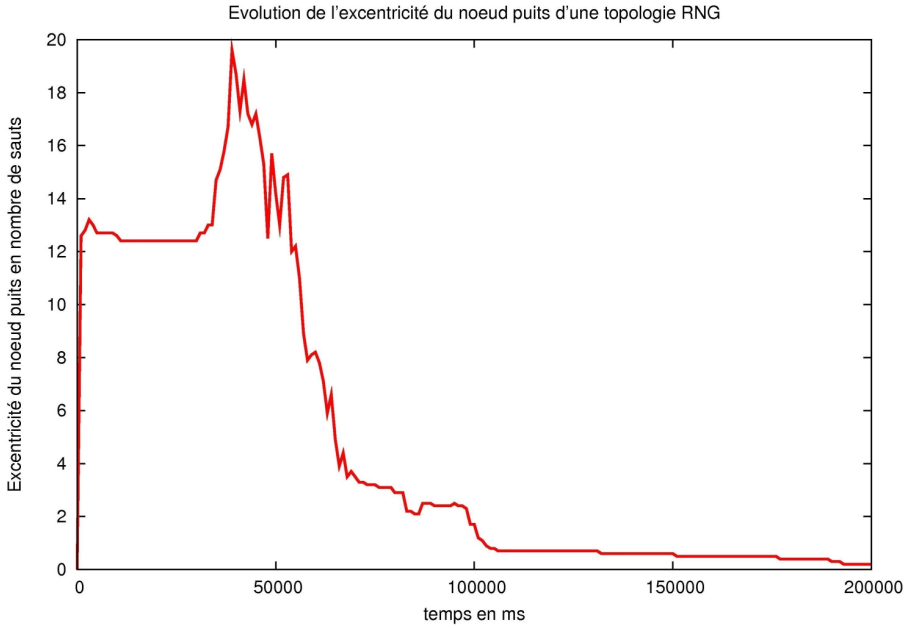

FIGURE 2.27 – Topologie RNG : excentricité du puits au cours du temps

placent cependant pas dans le cas de réseaux organisés et n'explorent pas les modifications topologiques que cette désertification non uniforme entraîne. De plus, ils supposent dans la première étude un réseau non homogène (présence de super-capteurs) et dans la seconde la possibilité de définir la densité du réseau.

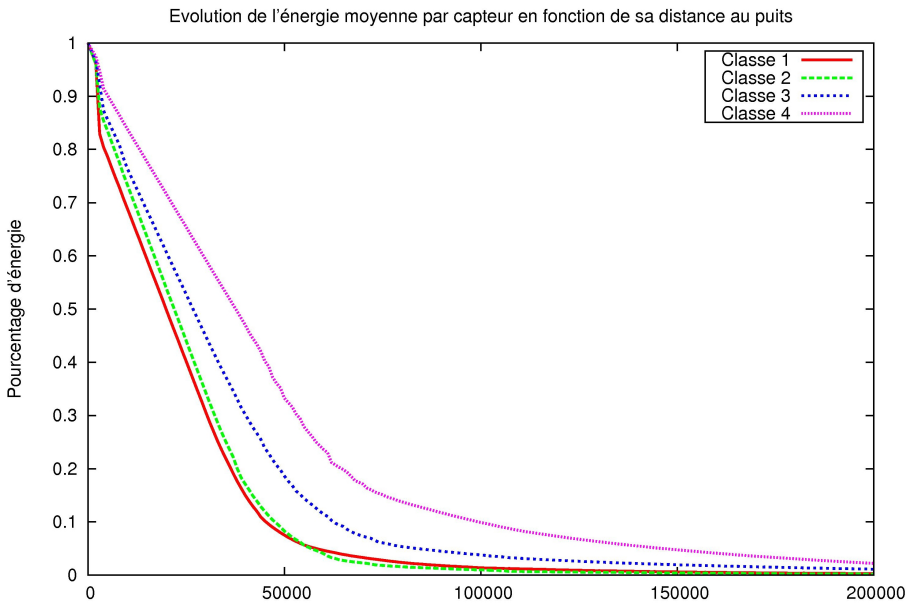

FIGURE 2.28 – Topologie RNG : évolution de l'énergie au cours du temps en fonction de la distance au puits

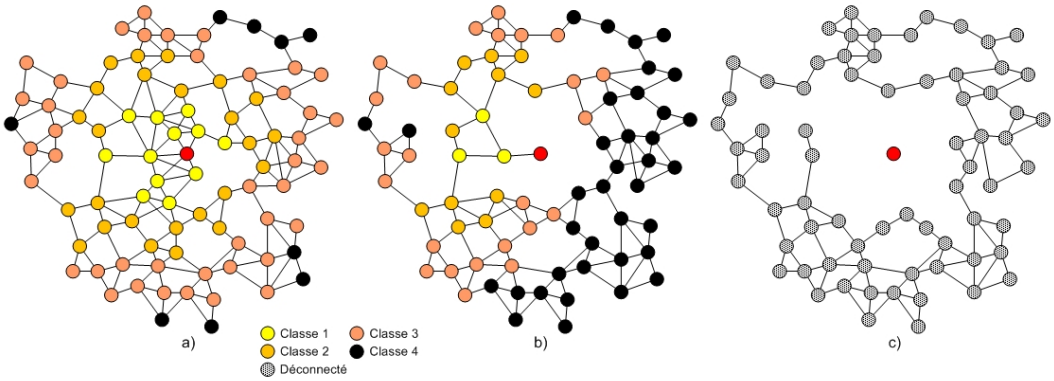

FIGURE 2.29 – Effet Donut

2.5 Conclusion

Dans ce chapitre, nous avons présenté une étude qualitative pour comprendre le comportement des protocoles d'auto-organisation, à la fois orientés dominant et orientés élagage de liens. Nous avons défini ces phases caractéristiques : la naissance, le fonctionnement normal et la mort. Nous avons étudié quatre principaux schémas d'auto-organisation orientés dominant (MPR, MPR-DS, CDS-*règle k* et CDS-IDS) et deux protocoles orientés élagage de liens (LMST et RNG) durant ces trois phases.

Notre étude s'est décomposée en deux parties :

- une étude sur les comportements au cours de la vie du réseau et insistant sur les notions de robustesse

- une étude sur l'évolution des propriétés structurelles des différentes structures d'auto-organisation

Nous avons ainsi observé comment ces protocoles réagissaient à l'arrivée de nouveaux nœuds ou à leur mort. Nous avons regardé l'évolution de la cardinalité et de la latence pour reconstruire une structure logique stable. Et nous avons observé les implications de ce que nous avons appelé « l'effet donut ». En définitive, il ressort de cette étude :

- Une grande robustesse des deux protocoles de sélection de liens RNG et LMST : malgré la construction de quasi-arbre couvrant, leur conception localisée (connaissance à deux sauts) leur permet de résister à la mort ou à l'ajout de nœuds dans le réseau.
- La construction non localisée de l'ensemble dominant, si elle permet une meilleure cardinalité dans le cas du CDS-IDS, est une cause certaine de fragilité.
- La conception localisée d'un protocole est souvent nécessaire mais pas suffisante pour garantir une forte robustesse comme le montre le comportement du protocole CDS-*règle k*. Dans ce cas, le déploiement de nouveaux nœuds entraîne de nombreux changements de topologie.
- D'un point de vue énergétique, les protocoles orientés dominant munis d'un mécanisme d'endormissement ne sont pas égaux : le CDS-*règle k* et le CDS-IDS permettent au réseau de garder la connexité la plus longue.
- Dans un scénario de remontée de données d'un ensemble de capteurs vers un puits, on définit l'effet donut par une mortalité inversement proportionnelle à la distance au puits.
- L'effet donut va entraîner un allongement des chemins vers le puits et une consommation supplémentaire sur la structure virtuelle.

L'ensemble de cette étude et l'ensemble des conclusions que nous venons de tirer nous ont permis d'élaborer un protocole d'auto-organisation original, dédié à la localisation du voisinage. Le prochain chapitre montre la fragilité de l'indication de la puissance du signal reçu (RSSI pour Received Signal Strength Indication) comme métrique de proximité et met en évidence la nécessité de ce protocole de localisation qualitative tel que proposé au chapitre 4.

Bibliographie

[1] C. Adjih, P. Jacquet, and L. Viennot. Computing cds with multipoint relays. Technical Report RR-4597, INRIA, October 2002.

[2] Rimon Barr, Zygmunt J. Haas, and Robbert van Renesse. *Scalable Wireless Ad hoc Network Simulation*, chapter 19, pages 297–311. CRC Press, August 2005.

[3] Prosenjit Bose, Luc Devroye, William Evans, and David Kirkpatrick. On the spanning ratio of gabriel graphs and beta-skeletons. *SIAM Journal on Discrete Mathematics*, 20(2) :412–427, February 2006.

[4] Prosenjit Bose, Pat Morin, Ivan Stojmenovic, and Jorge Urrutia. Routing with guaranteed delivery in ad hoc wireless networks. *Wireless Networks*, 7(6) :609–616, November 2001.

[5] Julien Cartigny, Francois Ingelrest, David Simplot-Ryl, and Ivan Stojmenovic. Localized lmst and rng based minimum-energy broadcast protocols in ad hoc networks. *Ad Hoc Networks*, 3(1) :1–16, November 2005.

[6] P. Casari, F. Zorzi, and M. Zorzi. Efficient packet converge-casting : Relieving the sink congestion in wireless sensor networks. In *18th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, pages 1–5, Athens, Greece, September 2007.

[7] T. Clausen, P. Jacquet, C. Adjih, A. Laouiti, P. Minet, P. Muhlethaler, A. Qayyum, and L. Viennot. Optimized link state routing protocol (olsr). RFC 3626 (Experimental), October 2003.

[8] Fei Dai and Jie Wu. An extended localized algorithm for connected dominating set formation in ad hoc wireless networks. *IEEE Transactions on Parallel and Distributed Systems*, 15(10) :908–920, October 2004.

[9] S Fortune. A sweepline algorithm for voronoi diagrams. In *2nd annual symposium on Computational geometry (SCG)*, pages 313–322, New York, NY, USA, June 1986. ACM.

[10] Ruben K. Gabriel and Robert R. Sokal. A new statistical approach to geographic variation analysis. *Systematic Zoology*, 18(3) :259–278, September 1969.

[11] P. Galiotos. Security-aware topology control for wireless ad-hoc networks. In *IEEE Global Telecommunications Conference (Globecom)*, volume 1, pages 1–6, New Orleans, USA, December 2008.

[12] François Ingelrest, David Simplot-Ryl, and Ivan Stojmenovic. A dominating sets and target radius based localized activity scheduling and minimum energy broadcast protocol for ad hoc and sensor networks. In *3rd Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net)*., Bodrum, Turkey., June 2004.

[13] Philippe Jacquet. On the robustness and stability of Connected Dominating Sets in mobile ad hoc networks Analysis of an hybrid scheme. Research Report RR-5684, INRIA, 2005.

[14] Lefteris M. Kirousis, Evangelos Kranakis, Danny Krizanc, and Andrzej Pelc. Power consumption in packet radio networks. *Theoretical Computer Science*, 243(1-2) :289–305, November 1997.

[15] F. Kuhn, T. Moscibroda, and R. Wattenhofer. Initializing newly deployed ad hoc and sensor networks. In *10th Annual International Conference on Mobile Computing and Networking (Mobicom)*, Philadelphia, USA, September 2004.

[16] Olaf Landsiedel, Olaf L, Katharina Anna Lehmann, and Klaus Wehrle. T-dht : Topology-based distributed hash tables. In *5th IEEE International Conference on Peer-to-Peer Computing (P2P)*, pages 143–144, Konstanz, Germany, September 2005.

[17] Ning Li, Hou J.C., and Sha L. Design and analysis of an mst-based topology control algorithm. *IEEE Transactions on Wireless Communications*, 4(3) :1195–1206, May 2005.

[18] Xiang-Yang Li, G. Calinescu, Peng-Jun Wan, and Yu Wang. Localized delaunay triangulation with application in ad hoc wireless networks. *IEEE Transactions on Parallel and Distributed Systems*, 14(10) :1035–1047, October 2003.

[19] JiaLiang Lu. *Impacts of self-organized Mechanism in Wireless Sensor Networks*. PhD thesis, INSA de Lyon, May 2008.

[20] G. Malkin. Rip version 2. RFC 2453, November 1998.

[21] J.P. Monks, V. Bharghavan, and W.-M.W. Hwu. Transmission power control for multiple access wireless packet networks. In *25th Conference on Local Computer Networks (LCN)*, pages 12–21, Tampa, USA, November 2000.

[22] T. Moscibroda, P. von Rickenbach, and R. Wattenhofer. Analyzing the energy-latency trade-off during the deployment of sensor networks. In *25th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, Barcelona, Spain, April 2006.

[23] J. Moy. Ospf version 2. RFC 2328, April 1998.

[24] R. Ogier, F. Templin, and M. Lewis. Topology Dissemination Based on Reverse-Path Forwarding (TBRPF). RFC 3684 (Experimental), February 2004.

[25] K. Padmanabh and R. Roy. Doughnut effect in wireless sensor network and its solution. In *3rd Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, volume 3, pages 957–963, Reston, USA, September 2006.

[26] Joongseok Park and Sartaj Sahni. Power assignment for symmetric communication in wireless sensor networks. *International Journal of Distributed Sensor Networks*, 5(2) :185–200, April 2009.

[27] C. Prehofer and C. Bettstetter. Self-organization in communication networks : principles and design paradigms. *IEEE Communications Magazine*, 43(7) :78–85, July 2005.

[28] R. C. Prim. Shortest connection networks and some generalizations. *Bell Systems Technical Journal*, 1 :1389–1401, November 1957.

[29] A. Qayyum, L. Viennot, and A. Laouiti. Relaying for flooding broadcast messages in mobiles wireless networks. In *35th annual Hawaii international conference on system sciences (HICSS)*, Hawaii, USA, January 2002.

[30] Rajmohan Rajaraman. Topology control and routing in ad hoc networks : a survey. *ACM SIGACT News*, 33(2) :60–73, June 2002.

[31] Ram Ramanathan and Regina Rosales-hain. Topology control of multihop wireless networks using transmit power adjustment. In *19th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, volume 1, pages 404–413, Tel Aviv, March 2000.

[32] Tahiry Razafindralambo and David Simplot-Ryl. Mobile Sensor Deployment with Connectivity Guarantee. Research Report RR-6936, INRIA, 2009.

[33] H. Rivano, F. Theoleyre, and F. Valois. Influence de l'auto-organisation sur la capacité des réseaux ad hoc. In *7ème Rencontres Françaises sur les Aspects Algorithmiques des Télécommunications (AlgoTel)*, Prequ'île de Giens, France, May 2005.

[34] Sichitiu Mihail L.and Dutta Rudra. Benefits of multiple battery levels for the lifetime of large wireless sensor networks. *Networking*, 3 :1440–1444, May 2005.

[35] Jamil A. Shaikh, Julio Solano, Ivan Stojmenovic, and Jie Wu. New metrics for dominating set based energy efficient activity scheduling in ad hoc networks. In *28th Conference on Local Computer Networks (LCN)*, pages 726–134, Bonn, Germany, 2003.

[36] Ivan Stojmenovic, Mahtab Seddigh, and Jovisa Zunic. Dominating sets and neighbor elimination-based broadcasting algorithms in wireless networks. *IEEE Transactions on Parallel and Distributed Systems*, 13(1) :14–25, January 2002.

[37] Fabrice Theoleyre and Fabrice Valois. A self-organization structure for hybrid networks. *Ad Hoc Network*, 6(3) :393–407, may 2008.

[38] G. Toussaint. The relative neighbourhood graph of a finite planar set. *Pattern Recognition*, 12 :261–268, 1980.

[39] Chieh-Yih Wan, Shane B. Eisenman, and Andrew T. Campbell. Coda : congestion detection and avoidance in sensor networks. In *1st international conference on Embedded networked sensor systems (SenSys)*, pages 266–279, Los Angeles, USA, November 2003.

[40] P. Wan, K. Alzoubi, and O. Frieder. Distributed construction of connected dominating set in wireless ad hoc networks. In *21st Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, New York, USA, June 2002.

[41] J.E. Wieselthier, G.D. Nguyen, and A. Ephremides. On the construction of energy-efficient broadcast and multicast trees in wireless networks. In *19th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'00)*, volume 2, pages 585–594, Tel Aviv, March 2000.

[42] J. Wu and F. Dai. Distributed dominant pruning in ad hoc wireless networks. In *38th annual IEEE International Conference on Communications (ICC)*, Anchorage, USA, May 2003.

[43] Andrew C Yao. On constructing minimum spanning trees in k-dimensional spaces and related problems. Technical report, Stanford University, Stanford, CA, USA, 1977.

[44] Zeng Yuanyuan, Jia Xiaohua, and He Yanxiang. A distributed algorithm for constructing energy-balanced connected dominating set in wireless sensor networks. *International Journal of Sensor Networks*, 2(1-2) :68–76, April 2007.

Liste de publications liées à ce chapitre

Conférences & Workshops Internationaux

[1] **Karel Heurtefeux** and Fabrice Valois. Self-organization protocols : Behavior during the senso networks life. In *Personal, Indoor and Mobile Radio Communications, 2007. PIMRC 2007. IEEE 18th International Symposium on*, pages 1–5, Athen, Greece, September 2007.

[2] **Karel Heurtefeux** and Fabrice Valois. Topology control algorithms : a qualitative study during the sensor networks life. In *Mobile Adhoc and Sensor Systems, 2007. MASS 2007. IEEE Internatonal Conference on*, pages 1–7, Pisa, Italy, October 2007.

Conférences françaises

[3] **Karel Heurtefeux** and Fabrice Valois. Protocoles d'auto-organisation : une étude qualitative au cours de la vie des réseaux de capteurs. In *JDIR'08 : 9ème Journées Doctorales en Informatique et Réseaux*, Villeneuve d'Ascq, France, January 2008.

Séminaires

[4] **Karel Heurtefeux** and Fabrice Valois. Protocoles d'auto-organisation : comportement au cours de la vie d'un réseau de capteurs. In *Réunion ARESA*, Grenoble, France, May 2008.

[5] **Karel Heurtefeux** and Fabrice Valois. Protocoles d'auto-organisation : comportement au cours de la vie d'un réseau de capteurs. In *Journées ResCom*, Paris, France, March 2007.

Posters

[6] **Karel Heurtefeux** and Fabrice Valois. Protocoles d'auto-organisation : comportement au cours de la vie d'un réseau de capteurs In *Ecole d'été ResCom 2007 : Réseau autonomes et Internet du futur*, Calcatoggio, Corse, June 2007.

3

De l'instabilité du RSSI comme métrique

3.1 Motivations

De nombreuses études se basent sur la puissance du signal reçu comme métrique pour estimer la distance entre deux capteurs. L'indicateur de puissance du signal reçu (ou RSSI) est une estimation par le composant radio du niveau de la puissance du signal reçu. À chaque paquet reçu, le capteur notifie le RSSI. Mais peut-on réellement se baser sur une mesure de la puissance du signal radio comme métrique de proximité ? C'est à cette question que répond ce chapitre préalable à la présentation du protocole de localisation qualitative (QLoP) dans le chapitre 4.

Nous montrons, en nous basant à la fois sur des études précédentes et des expérimentations dans des conditions réelles, que le RSSI est à la fois instable à court terme, imprécis et entièrement dépendant des conditions de l'environnement de déploiement du réseau de capteurs. L'originalité de cette étude est de montrer que, sauf dans des conditions particulièrement favorables, il est erroné d'affirmer qu'un fort RSSI est synonyme d'une forte proximité, de même qu'un faible RSSI signifierai une faible proximité. En définitive, nous montrons que le RSSI n'est pas une bonne métrique pour estimer la distance.

3.2 État de l'art

La mesure du RSS peut être effectuée par chaque capteur durant la réception de paquets de données sans impacter la bande passante ou l'énergie. Non seulement les capteurs actuels

(Imote2, WSN430, etc.) permettent les mesures de signal reçu mais elles sont également supportées par les standards 802.11 [11] et ZigBee [10]. De plus, cette mesure paraît intuitive : plus le signal reçu est fort, plus le voisin est proche, moins ce signal est puissant plus le voisin est éloigné. Nous verrons dans ce chapitre qu'il n'en est rien.

Et effectivement, l'indicateur de puissance du signal reçu (RSSI) est pris par de nombreux articles comme mesure pour estimer la position ([1, 5, 12, 7]).

[1] et [5] se basent sur une carte de la puissance du signal reçu sur la zone de déploiement. Cette carte doit être obtenue préalablement par des mesures ou par un ensemble de capteurs dédiés (*sniffers*) dont l'emplacement est connu. Par exemple, la figure 3.1 montre une carte de mesures de RSSI obtenue par un *sniffer*. Chaque entité, à la fois non ancre et non *sniffer*, va mesurer la puissance du signal reçu de chaque ancre et fournir un vecteur qui va correspondre à une sorte d'« empreinte » RSSI. Un point central va comparer cette empreinte avec la carte des RSSI de la zone et ainsi déterminer, par exploration, la position de l'entité. Cependant, ces hypothèses ne correspondent pas aux contraintes de déploiement des réseaux de capteurs (point central, architecture fixe, super-nœuds, etc.).

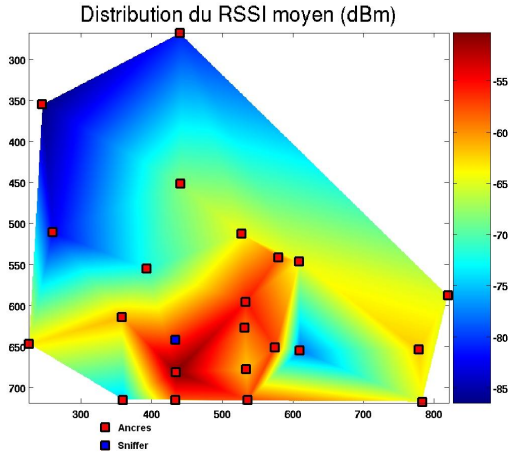

FIGURE 3.1 – Exemple de carte RSSI obtenue par un nœud *sniffer* [1]

À l'aide de simulations et d'une expérimentation, [12] propose de localiser un nœud *cible* grâce à plusieurs nœuds fixes connaissant leur position. En calculant l'erreur quadratique moyenne minimale (MMSE) des mesures effectuées, un nœud central est capable d'estimer la position du nœud *cible*. L'expérimentation donne cependant des erreurs de positionnement significatives au regard de la taille de la zone de déploiement.

[7] utilise la notion de proximité (i.e. la capacité d'un nœud à envoyer un message correctement à un nœud voisin) pour améliorer la précision de la localisation. Cependant, il est nécessaire d'avoir une correspondance entre le RSS et la portée. De plus, l'expérimentation reste limitée à de très courtes distances (0.25m), sans interférence extérieure.

L'ensemble de ces études va buter sur la difficulté d'établir un rapport entre la distance et la puissance du signal reçu. [3] montre que la puissance du signal reçu va être affectée par trois phénomènes, l'affaiblissement de propagation (ou *path-loss*), l'évanouissement (ou *fading*) et les

1. Figure issue de travaux d'Elyès Ben Hamida non publiés à la rédaction de ce document.

« zones d'ombre » (ou *shadowing*) :

- L'affaiblissement se caractérise par la dispersion de la puissance d'une onde électromagnétique lorsqu'elle parcourt une distance. Cet affaiblissement est généralement considéré comme proportionnel à d^n avec d la distance entre le récepteur et le transmetteur et n compris entre 1 et 6 selon les modèles. Par exemple, dans le cas d'un environnement sans obstacle, n sera égal à 2. C'est cette propriété que les auteurs utilisant le RSS comme mesure de la distance veulent exploiter.
- Le *fading* se caractérise par la déviation ou l'atténuation de l'amplitude et de l'énergie du signal à travers le médium qu'il traverse. Ce phénomène va varier en fonction du temps, de la position géographique et de la fréquence radio utilisée. La présence de réflecteurs dans l'environnement entre le récepteur et le transmetteur crée la possibilité de trajets multiples que le signal peut emprunter. Cela a pour conséquence la superposition de plusieurs copies du même signal émis, chacun ayant emprunté un trajet différent. La somme de ces signaux reçus peut atténuer, amplifier, ou bruiter le signal original. Dans le cas d'une mesure de RSS, comme le *fading* est dépendant de la fréquence, [7] propose de mesurer le RSS sur plusieurs fréquences espacées et d'établir une moyenne en fréquence.
- le *shadowing* est la perte de signal due à des obstacles (murs, vitres, immeubles, arbres, voitures, personnes, etc.) entre le transmetteur et le receveur. Alors que le *shadowing* induit par les murs ou les bâtiments ne va pas évoluer temporellement, [13], en étudiant le niveau d'un signal d'une fréquence de $2,4GHz$, montre que les mouvements de personnes vont créer du *shadowing* important (jusqu'à $-21dB$ d'écart avec la moyenne) et de façon imprédictible. Une solution possible sera alors de moyenner assez longtemps pour « lisser » ces variations.

Le retour d'expérience de Coronis dans le déploiement de réseaux de capteurs permet également de savoir que les conditions météorologiques telles que la pluie ou le brouillard peuvent dégrader considérablement la puissance du signal reçu.

Pour [8] cependant, la variation du RSSI n'est pas due au multitrajet mais principalement aux interférences extérieures (radio, objets mobiles, etc.). Il constate que, malgré un environnement particulièrement favorable (pas d'interférences en radiofréquences externes), des « caprices » matériels ou la mobilité d'objets à l'intérieur du réseau fera varier le RSSI de manière imprédictible.

Pour palier à ces difficultés, [6] propose non pas d'établir une correspondance directe entre distance et RSSI mais un classement parmi le 1-voisinage direct de chaque nœud en fonction du RSSI. Il se sert ensuite de ce classement pour améliorer des techniques de localisation par ancre comme MDS [9]. Ces techniques considèrent le saut comme unité de mesure, le classement des voisins en s classes va permettre de diviser un saut en s subdivisions et améliorer la précision (voir figure 3.2). Même si cette division en classe des voisins permettrait d'éviter les petites fluctuations du RSSI, cette proposition est encore dépendante du RSSI très instable sur une courte période de temps. De plus, l'étude ne se démarque pas de l'hypothèse d'une distance strictement proportionnelle au RSSI. Nous verrons plus tard que cette hypothèse est discutable.

Il n'existe donc pas, à notre connaissance, d'expérimentations dans un environnement réel qui ait montré une stabilité du RSSI. Au mieux, [8] arrive à obtenir une fluctuation dans une

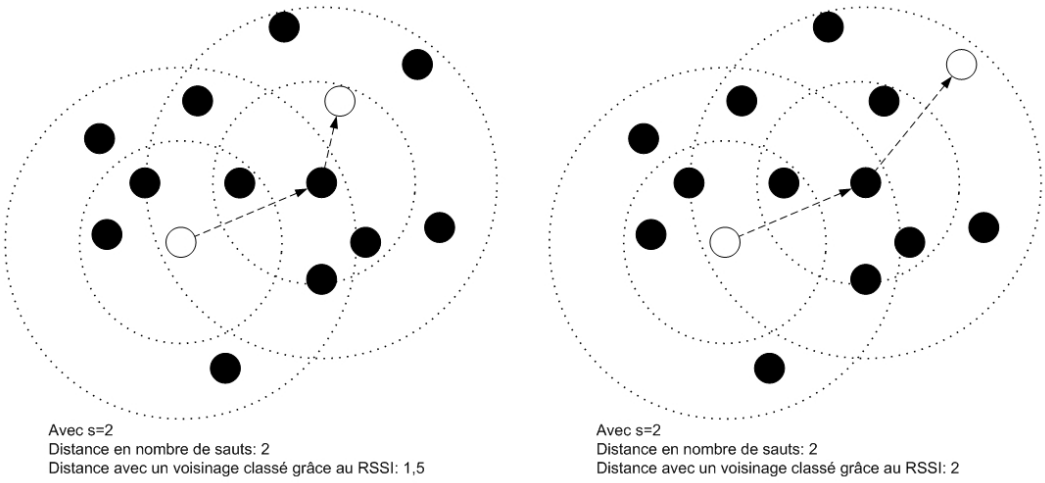

FIGURE 3.2 – Division en classes du voisinage à 1 saut afin d'améliorer la précision de localisation

bande « acceptable » de 4-5 dB en faisant abstraction des nœuds défectueux, dans un réseau sans bruit, aucun mouvement physique dans l'environnement et une météorologie favorable. [14] montre que sur la majorité des liens du réseau de capteurs déployés, le RSSI est compris dans une bande stable mais seulement à **long terme**. Néanmoins, une proportion non négligeable des liens n'exhibent pas les mêmes propriétés : la dispersion du RSS en fonction du temps, mesurée par l'écart-type, peut aller jusqu'à $7dB$ en raison d'une mobilité à proximité de certains capteurs.

Un exemple assez parlant pour illustrer l'instabilité du RSSI est l'utilisation de cette variation pour détecter les intrusions [4]. Dans cet article, les auteurs étudient avec succès la possibilité de détecter la présence de mobilité entre plusieurs capteurs en mesurant la puissance du signal reçu.

On peut noter de plus que la puissance du signal n'est pas nécessairement identique d'un capteur à l'autre même dans le cas d'un réseau homogène. Il dépend à la fois de la calibration du récepteur et du transmetteur, mais également du niveau d'énergie restant dans la batterie.

Si l'on résume, pour obtenir une métrique de RSS stable et utilisable, il est nécessaire de :

- mesurer le RSS sur plusieurs fréquences distinctes.
- mesurer le RSS sur un temps assez long pour lisser les fluctuations.
- calibrer les capteurs du réseau afin d'obtenir une puissance et une sensibilité d'émission comparable.
- être dans un milieu sans trop d'interférences extérieures (objets mobiles traversant la zone de déploiement, pluie, portes, etc.)

Cet ensemble de contraintes est, selon nous, incompatible avec une grande majorité des réseaux de capteurs pour les raisons suivantes :

- le saut de fréquences n'est pas disponible sur l'ensemble des capteurs du marché,
- le temps nécessaire à lisser les fluctuations va dépendre de la dynamique de l'environnement et entraînera nécessairement une latence dans la localisation et un surcoût énergétique,

- comme le montrent les scénarios mis en avant dans le chapitre 1, l'environnement d'un réseau de capteurs est souvent dynamique (bâtiments intelligents, surveillance de l'environnement, etc.).

Pour l'ensemble des raisons énoncées ci-dessus, il nous paraît indispensable d'établir une métrique stable, fiable et peu coûteuse en énergie. C'est dans cette optique que nous présentons dans le chapitre 4 le protocole de localisation qualitative, QLoP. En outre, nous présentons dans la suite de ce chapitre, un ensemble de 4 expérimentations afin de prouver que dans des conditions normales d'utilisation et de déploiement d'un réseau de capteurs, le RSSI ne constitue pas une métrique fiable.

3.3 Expérimentations

Dans cette section nous présentons l'ensemble du matériel et les scénarios utilisés dans ces expérimentations ainsi que les conditions dans lesquelles elles ont été effectuées. Elles ont été réalisées grâce à des capteurs WSN430 dans trois environnements différents : un appartement, le laboratoire CITI plus vaste, et un terrain de foot, zone ouverte sans obstacle. L'objectif de ces expérimentations est d'étudier à la fois le rapport entre distance et RSSI et la stabilité à court terme et à moyen terme.

3.3.1 Matériel

L'ensemble des expérimentations a été réalisé en utilisant des capteurs WSN430 développés au laboratoire CITI. Les caractéristiques de ces capteurs sont données dans le tableau 3.3. Nous utilisons la bande de fréquences ISM (industriel, scientifique, médical) : 868MHz. Cette fréquence, peu utilisée par le grand public, permet d'éviter au maximum les interférences dues aux signaux WIFI ou GSM. Le signal est modulé suivant la modulation par déplacement de fréquences (FSK). Le FSK est un mode de modulation dans lequel le signal modulé varie entre des fréquences prédéterminées. Un mécanisme de contrôle de redondance cyclique (CRC) permettant de détecter les erreurs de transmission par ajout de redondance est également présent. Durant ces expérimentations, nous n'utilisons qu'une seule sorte de paquet. Ce paquet est composé de 15 octets. À cela s'ajoutent 4 octets de début de trame afin que le récepteur puisse se synchroniser sur la porteuse pour le début des données. La fréquence d'envoi est de 1 paquet par seconde. La politique d'accès au canal est Aloha (i.e. pas d'écoute du canal avant l'envoi d'un paquet, pas d'accusé de réception ni de retransmission, pas d'allocation du canal ni de synchronisation). L'antenne utilisée est intégrée au circuit imprimé (antenne PCB) et possède, en théorie, un rayonnement isotrope (i.e. les propriétés physiques du rayonnement de l'antenne sont identiques quelque soit la direction). La durée d'expérimentation varie suivant les scénarios.

Pour le capteur WSN430, le RSSI est stocké sur 8 bits dans un registre de la radio. La valeur du RSSI est toujours moyennée sur 8 périodes de temps ($128\mu s$).

Le code en langage C est programmé et compilé puis injecté dans le capteur par l'intermédiaire de l'interface JTAG. Les données envoyées en sortie du capteur sont récupérées via le

Capteur	WSN430
Processeur	TI MSP430
Vitesse du processeur	8Mhz
RAM	10Ko
Espace programme	48Ko
Flash	1Mo
Communication série	DS2411, SPI
Batterie	PoLiFlex
Voltage	2.2 V
Radio	TI CC1100
Fréquence	315/433/868/915 Mhz
Débit de données	500 Kb/s
Dimension	65x40x8mm

FIGURE 3.3 – Caractéristiques du WSN430

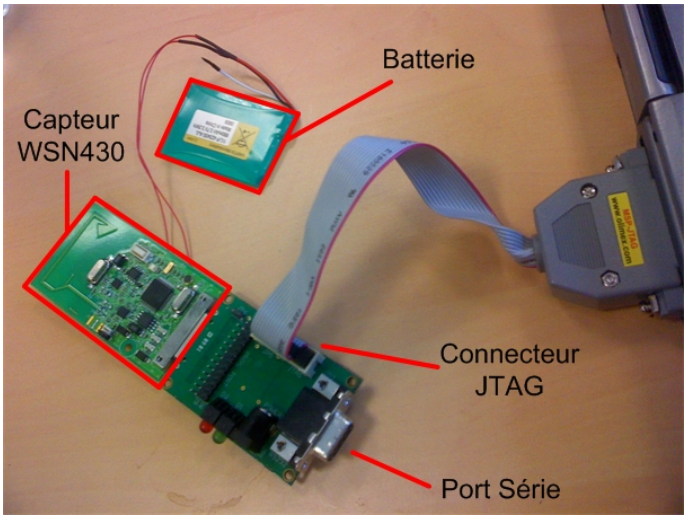

FIGURE 3.4 – Dispositif de mesures avec le capteur WSN430

port série ce qui va permettre de les stocker et de les traiter. La figure 3.4 illustre l'ensemble du dispositif de mesure.

3.3.2 Environnements et scénarios

Les expérimentations sont réalisées dans 3 environnements différents : un appartement exigu, un bâtiment de bureaux (le laboratoire), plus vaste, et un terrain de football, plat et dégagé (voir figure 3.5). L'objectif est de montrer que l'environnement joue une part essentielle dans les mesures de RSS. Dans le cas de l'appartement et du bâtiment de bureaux, la dynamique propre à ces environnements est conservée : des personnes se déplacent, des portes ou des fenêtres s'ouvrent et se ferment, etc. Ces conditions réalistes correspondent aux applications définies dans le chapitre 1. Pour l'expérimentation sur le terrain de football, il n'y a en revanche presque aucune dynamique.

Le scénario « RSSI-distance » sera réalisé sur une série de trois expérimentations dans trois environnements différents de la façon suivante. Nous prenons deux capteurs « récepteurs », qui

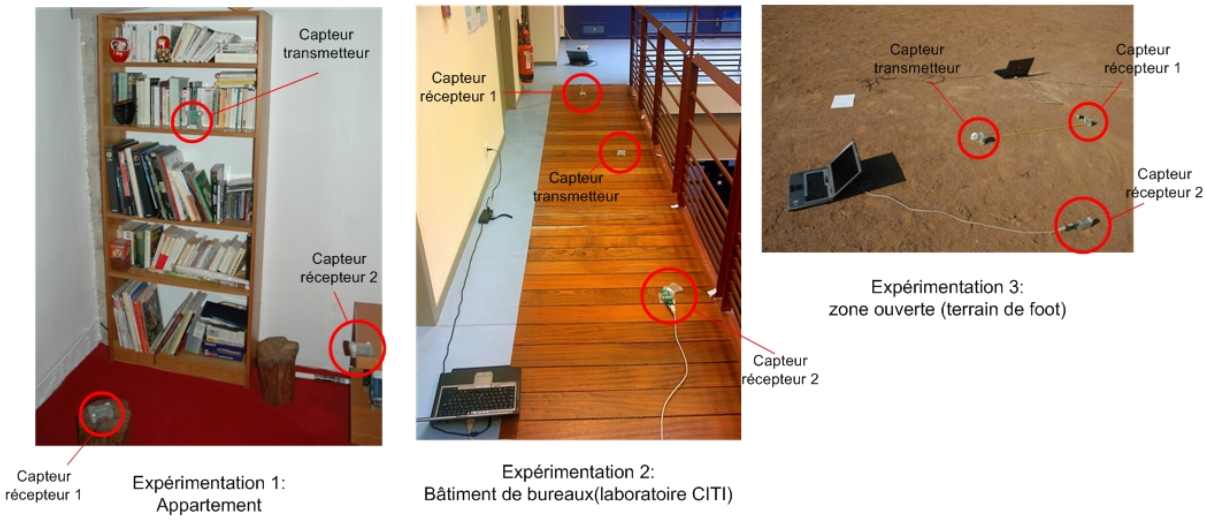

FIGURE 3.5 – Les 3 milieux différents des expérimentations

vont uniquement recevoir les paquets envoyés par un capteur « transmetteur ». Les 2 capteurs récepteurs sont placés de telle façon à se trouver à une même distance mais dans des directions différentes du capteur transmetteur. La figure 3.6 décrit ce scénario.

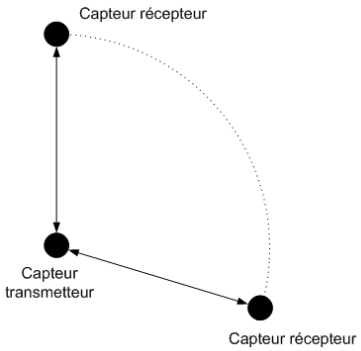

FIGURE 3.6 – Scénario « RSSI - distance »

Après un temps de capture qui peut varier de 10 à 15 minutes, nous déplaçons les deux capteurs récepteurs. La distance entre les deux capteurs récepteurs et le capteur transmetteur varie de $5cm$ jusqu'à une distance de $200cm$ dans l'appartement et de $650cm$ dans le laboratoire et jusqu'à $1000cm$ sur la zone dégagée. La puissance d'émission du capteur transmetteur est de 0dBm. Les distances maximales correspondent à la limite au-delà de laquelle le signal est trop faible ou détérioré pour être décodé convenablement. Les 3 expérimentations ont été réalisées en utilisant les mêmes capteurs.

L'objectif de ces 3 expérimentations est de montrer que la puissance reçue par un capteur est à la fois instable à court terme, imprécise car très dépendante de l'environnement de déploiement et différente selon la direction du capteur récepteur par rapport au capteur transmetteur.

La quatrième et dernière expérimentation est réalisée dans un appartement. Elle se déroule

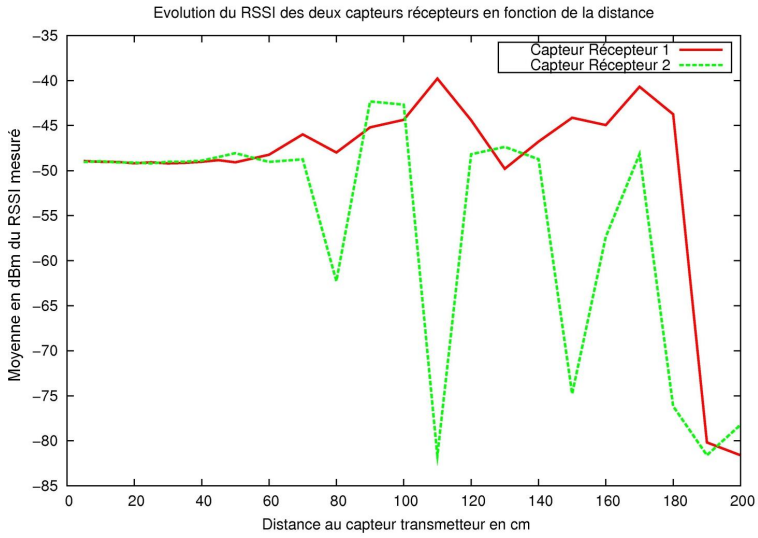

FIGURE 3.7 – Rapport entre RSSI et distance dans le cas du scénario « appartement »

sur 40 heures. 5 capteurs transmetteurs fixes sont placés à des distances comprises entre 2 et 4 mètres d'un sixième capteur récepteur (voir figure 3.14). La puissance de transmission est cette fois de $10dBm$. Les autres paramètres (fréquence, modulation, etc.) restent identiques.

L'objectif de cette dernière expérimentation est d'observer la variation des mesures de RSS à long terme et d'étudier la taille des échantillons nécessaires pour approximer la valeur moyenne du RSSI.

3.4 Résultats

3.4.1 Scénario « RSSI et distance »

Durant toute la durée des expérimentations, les capteurs restent en vue directe (i.e. aucun obstacle n'est présent entre eux).

Appartement

La figure 3.7 donne les valeurs moyennes de RSSI obtenues pour l'environnement « appartement ». La distance maximale retenue pour le capteur transmettant est de $200cm$. Au-delà de cette distance, sur au moins un des deux capteurs récepteurs, le taux de livraison devient extrêmement faible (de l'ordre de 0,3%) et le RSSI relevé particulièrement instable. Le RSSI moyen pour chacune des distances est obtenu avec un minimum de 100 paquets.

Les mesures de RSS obtenues par le capteur 1 et 2 ne sont semblables que sur les très courtes distances (de 5 à $65cm$). Alors que la puissance du signal reçu par le capteur 1 reste comprise entre $-50dBm$ et $-40dBm$ jusqu'à $190cm$, la puissance reçue par le capteur 2 est beaucoup plus fluctuante. Ces « trous » de puissance peuvent s'expliquer par les effets destructeurs du multi-trajet [2].

La figure 3.8 illustre plus en détail ce phénomène. Le signal reçu par le capteur récepteur est constitué de deux composantes : le signal propagé en ligne droite (S_1 sur la figure) et le signal réfléchi sur le sol (S_2 sur la figure). La différence de temps d'arrivée des deux signaux peut créer ces zones où le signal va être plus faible. C'est clairement le phénomène en jeu dans le cas du capteur 2. Un appartement de taille modeste possède de nombreuses surfaces (sol, murs, appareils ménagers, etc.) qui vont réfléchir le signal. D'une position du capteur à une autre, le phénomène de multi-trajet engendre des signaux qui peuvent être destructifs et affaiblir la puissance reçue lors de la réception d'un paquet ou, à l'inverse, des signaux constructifs qui augmentent la puissance reçue. De plus, la faiblesse de puissance du signal reçue même à courte distance trouve son explication à la fois dans l'atténuation du canal de transmission et le multi-trajet mais également dans la faible qualité des antennes PCB (gain négatif de $-10dB$).

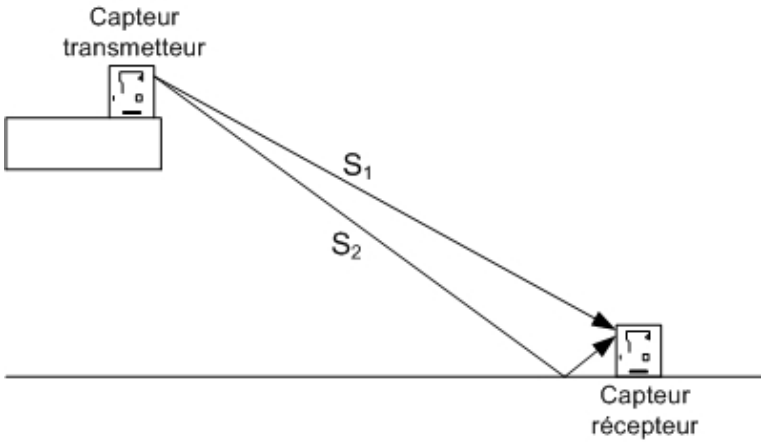

FIGURE 3.8 – Phénomène de multi-trajet

Lors de cette expérimentation, plus la distance entre les capteurs récepteurs et le capteur transmetteur est grande et plus on observe une grande volatilité des mesures de RSS. Nous mesurons cette volatilité grâce à l'écart-type entre les mesures de RSS. La figure 3.9 illustre ce phénomène : l'écart-type est jusqu'à 10 fois supérieur lorsqu'on s'approche de la limite de la portée. Cela signifie que les mesures sont plus dispersées et vont varier bien au-delà d'une bande « acceptable » de $4dBm$. Plus le signal est faible, plus il est sensible aux signaux réfléchis. Il est donc naturel d'avoir une plus forte variation pour des distances plus importantes.

Cela signifie qu'au-delà d'une certaine distance, réduite dans le cas d'un déploiement dans un appartement, le RSSI devient imprédictible. Il n'est alors plus possible de s'en servir comme métrique alors même que les capteurs parviennent encore à s'échanger des messages.

En définitive, les mesures de RSS effectuées dans un appartement apportent la confirmation de l'imprédictibilité du RSSI. Pour deux capteurs situés à distance identique d'une source, le RSS mesuré va être radicalement différent d'un capteur à l'autre.

Bâtiment de bureaux

Pour cette expérimentation, nous nous sommes placés dans le cadre du laboratoire CITI, en journée. Les capteurs sont posés sur le sol dans une pièce de grande taille ($10m$ x $5m$ x $3m$). La

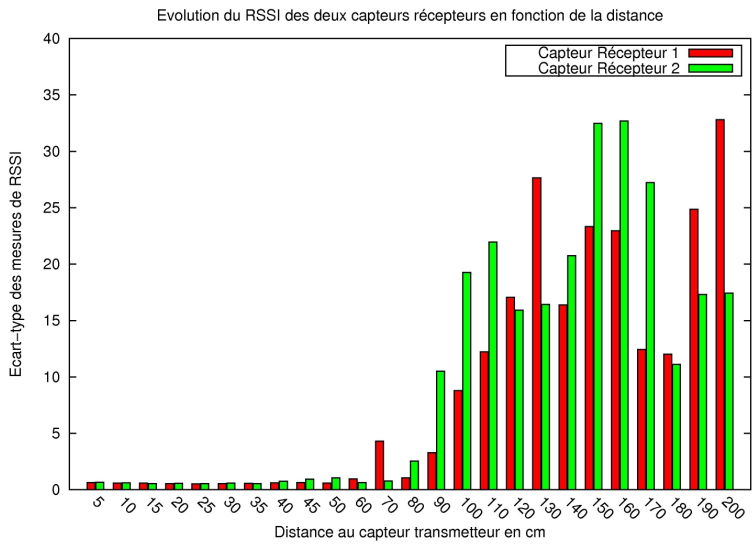

FIGURE 3.9 – Rapport entre écart-type des mesures RSS et distance pour les deux capteurs récepteurs (appartement)

portée maximale est établie à 650cm. La figure 3.10 présente les mesures de RSS par rapport à la distance.

Le phénomène de multi-trajet est beaucoup moins important du fait des dimensions de la zone de déploiement et du nombre moins important de surfaces pouvant réfléchir le signal.

Cependant, on constate à nouveau que les mesures des deux capteurs ne sont pas équivalentes. En effet, l'affaiblissement du signal est beaucoup plus rapide pour le capteur 2 que pour le capteur 1 (à 100cm pour le capteur 2 et à 200cm pour le capteur 1). Cette différence de comportement s'explique par un rayonnement non parfaitement isotrope de l'antenne PCB. Une antenne isotrope est un modèle théorique irréalisable dans la pratique : dans la réalité, l'énergie rayonnée est inégalement répartie dans l'espace. En effet, malgré une conception de l'antenne prévue pour respecter au maximum cette contrainte, des différences de puissance apparaissent en fonction de la direction de l'antenne. Cette propriété se manifeste également à la réception de façon similaire.

De plus, nous observons le même phénomène que dans l'environnement « appartement » en termes de dispersion des mesures (voir figure 3.11). Dans cet environnement cependant, la dispersion du RSSI n'est significative pour le capteur 1 qu'à une distance de 200cm contre 100cm pour l'environnement « appartement ». Il existe un autre facteur que le multi-trajet pour expliquer les différences de mesure du RSSI quand la distance augmente. Plus la distance entre les capteurs augmente et plus la probabilité qu'une interaction avec des personnes présentes dans le bâtiment augmente (passage entre les capteurs, ouverture/fermeture de portes, etc.). Nous avons détaillé dans le chapitre 1 l'ensemble des champs d'application les plus courants des réseaux de capteurs. Dans chacun des scénarios envisagés (surveillance environnementale, bâtiment intelligent, domotique ou BAN), il est probable qu'il existe, de façon non marginale, une dynamique à l'intérieur du réseau. Si le RSSI doit être utilisé comme métrique dans ce type de réseau, il nous paraît important de la prendre en compte. C'est pour cette raison que nous

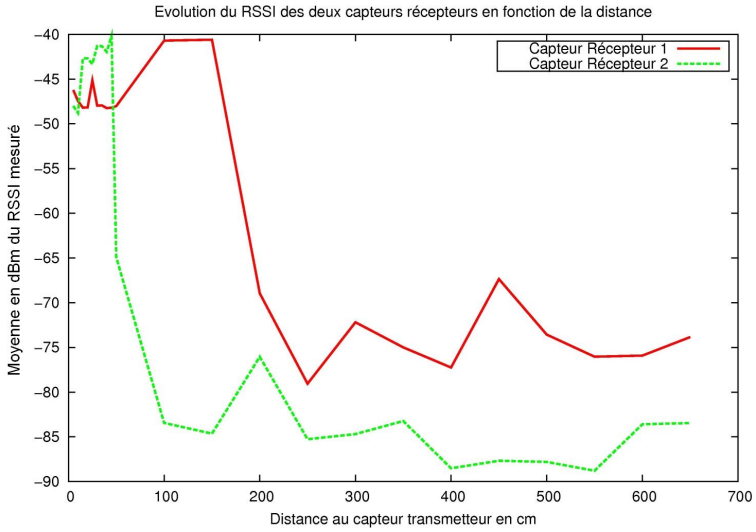

FIGURE 3.10 – Rapport entre RSSI et distance dans le cas du scénario « bâtiment de bureaux »

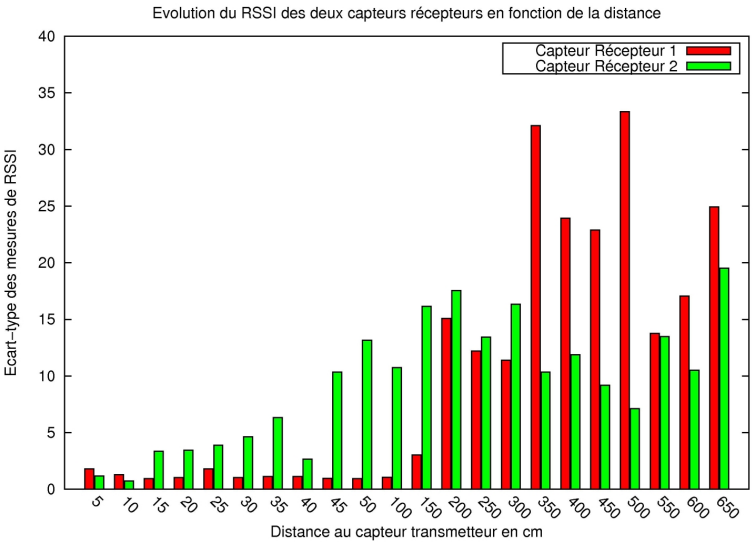

FIGURE 3.11 – Rapport entre écart-type des mesures RSS et distance pour les deux capteurs récepteurs (laboratoire)

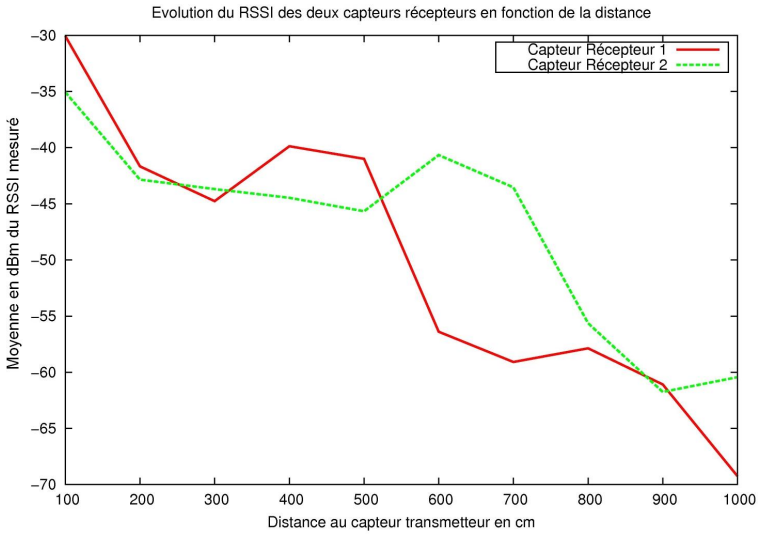

FIGURE 3.12 – Rapport entre RSSI et distance dans le cas du scénario « terrain de football »

n'avons pas interdit le passage entre les capteurs, sans toutefois le favoriser. Ce passage est donc très limité. Les caractéristiques de l'environnement « bâtiment de bureaux » entraînent une meilleure propagation du signal avec de moins fortes conséquences du multi-trajet. En revanche, la présence de mobilité à l'intérieur du réseau et le rayonnement non uniforme de l'antenne vont créer à la fois des incohérences dans le rapport RSSI-distance, une dispersion des valeurs de RSS relevées et la non-symétrie de ces valeurs selon les capteurs.

Terrain dégagé

Pour cette expérimentation, nous avons placé les capteurs au centre d'un terrain de football. Cet environnement est particulièrement favorable : espace ouvert et pas de mobilité à l'intérieur du réseau. Nous retrouvons dans cette configuration, un comportement différent des mesures précédemment effectuées : la décroissance du RSSI mesuré est moins brutale et les puissances de réceptions relevées sont plus importantes (voir figure 3.12). On peut remarquer également que la puissance du signal reçu dans les premiers mètres est bien plus importante que dans les 2 expérimentations précédentes : de l'ordre de $-30dBm$ contre $-40dBm$ et $-50dBm$. Cependant, de la même manière que dans les expérimentations précédentes, les deux capteurs relèvent des puissances comparables entre 1 et $3m$ puis les mesures divergent : le signal reçu par le capteur 1 tombe à $-55dBm$ à partir de $6m$ alors que le capteur 2 obtient une telle puissance de signal à partir de $8m$. Là encore, cela s'explique par le rayonnement non isotrope de l'antenne.

Malgré l'absence de dynamique dans le réseau et des conditions particulièrement favorables, le RSSI va varier d'un message à l'autre. Cette variation reste limitée dans les 7 premiers mètres pour le capteur 1 et 2 mais l'écart-type augmente de façon importante passé cette distance (voir figure 3.13).

Cependant, il est à noter que des différences peuvent apparaître d'un capteur à l'autre alors même que les caractéristiques matérielles et logicielles sont les mêmes. Ce fait renforce l'instabilité du RSSI comme métrique. La solution la plus courante est alors de calibrer les

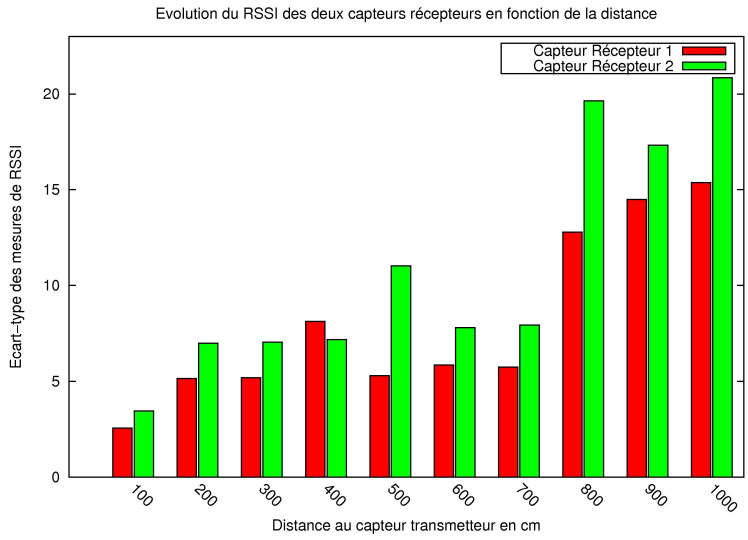

FIGURE 3.13 – Rapport entre écart-type des mesures RSS et distance pour les deux capteurs récepteurs (terrain de football)

capteurs. Dans l'éventualité d'un déploiement d'un réseau de centaines voire de milliers de capteurs, il est difficile d'envisager un tel calibrage de tous les capteurs individuellement.

3.4.2 Scénario « RSSI et stabilité à long terme »

Pour cette dernière expérimentation, nous avons placé dans un appartement 5 capteurs transmetteurs et 1 capteur récepteur. La figure 3.14 donne la disposition de l'ensemble des capteurs. Seuls les capteurs 2 et 3 sont en vue directe avec le capteur récepteur. La puissance de transmission de chaque capteur est de 10dBm. La durée de capture est de 40 heures. Cette expérience permet d'étudier le comportement du RSSI sur une longue durée.

Tous les capteurs n'ont pas le même comportement. Alors que le RSSI relevé des capteurs 2, 3 et 5 reste relativement stable (i.e. compris la plupart du temps entre -15dBm et -30dBm) à l'image du capteur 3 (voir figure 3.15), les mesures de puissance reçue des paquets en provenance du capteur 1 sont beaucoup plus fluctuantes (voir figure 3.16). Dans ce cas précis, la présence d'une structure métallique entre le capteur 1 et le capteur récepteur semble expliquer ce phénomène.

Pour le capteur 4, la volatilité des mesures est liée à l'environnement. En effet, cette dispersion des valeurs relevées n'est pas répartie sur l'ensemble de la durée de l'expérience mais uniquement à partir de 23 heures d'expérience (voir figure 3.17). Il s'agit ici d'un phénomène lié à la présence de plusieurs personnes dans l'appartement tandis qu'au début de l'expérience il était vide. Le passage entre le capteur transmetteur et le capteur récepteur au moment de l'émission ou la création de nouvelles réflexions du signal, etc. explique l'augmentation sensible des perturbations du signal. D'autres expériences effectuées au laboratoire ont montré ce phénomène avec des phases jour/nuit et semaine travaillée/weekend. La présence de sujets mobiles dans la zone de déploiement va créer de fortes interférences comme le montre [4].

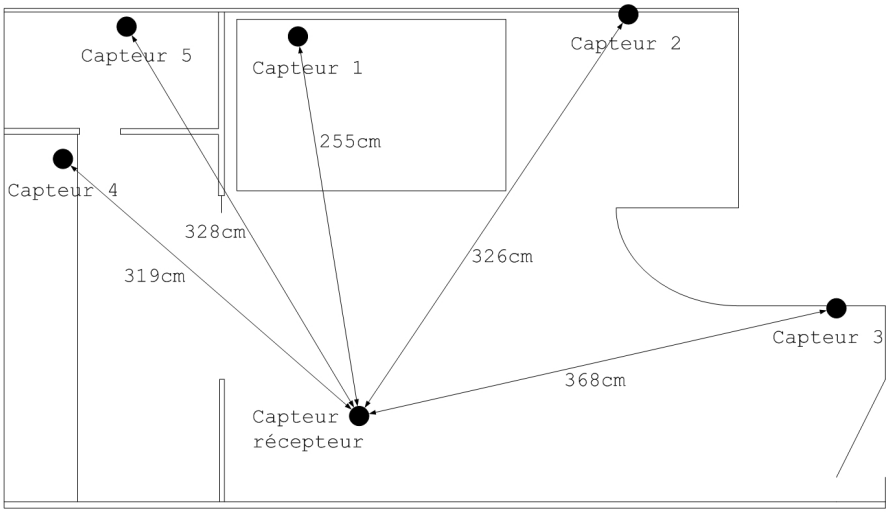

FIGURE 3.14 – Emplacement des 6 capteurs dans le scénario « stabilité à long terme du RSSI »

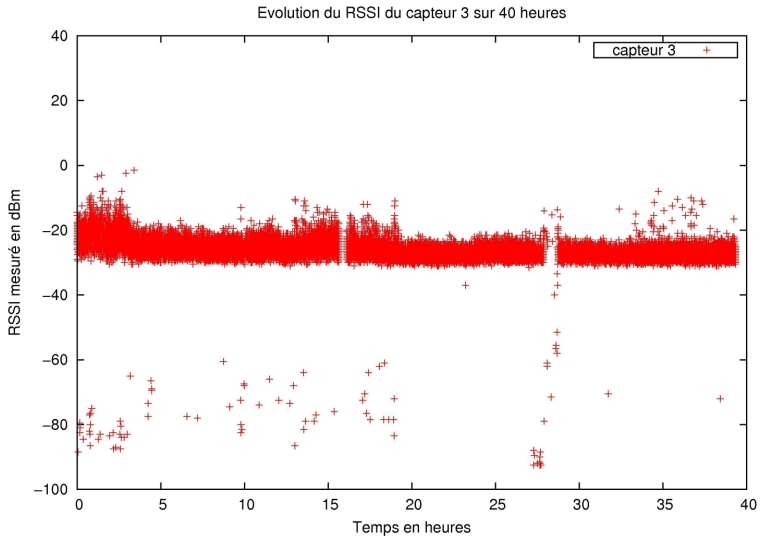

FIGURE 3.15 – Évolution du RSSI mesuré par le capteur 3 sur 40 heures

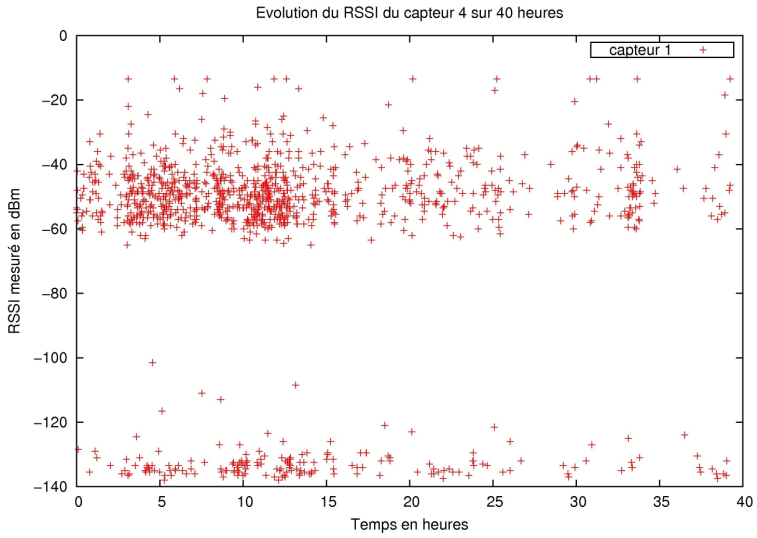

FIGURE 3.16 – Évolution du RSSI mesuré par le capteur 1 sur 40 heures

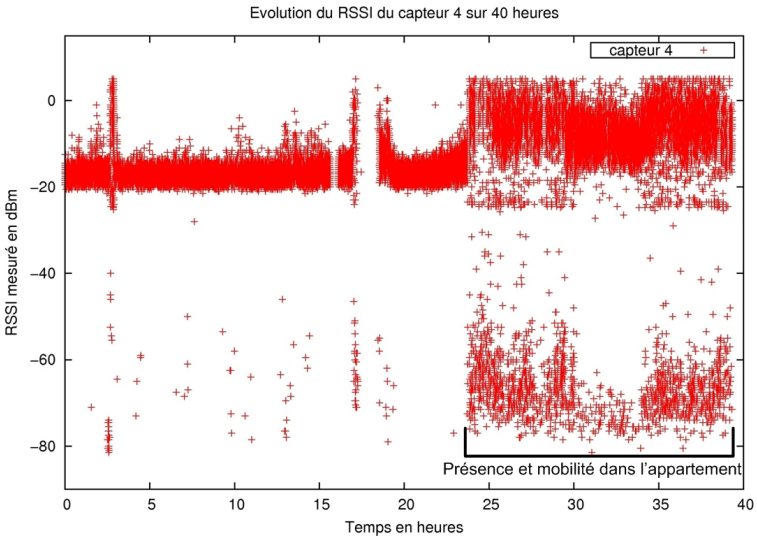

FIGURE 3.17 – Évolution du RSSI mesuré par le capteur 1 sur 40 heures

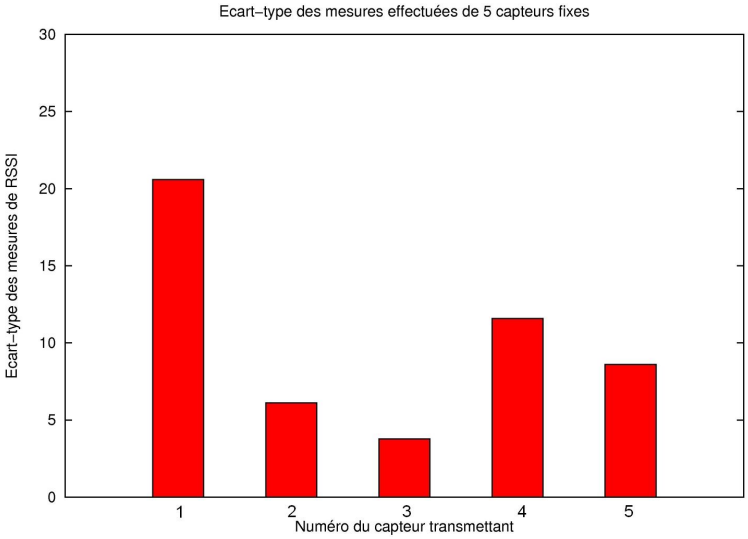

FIGURE 3.18 – Différences de stabilité du RSSI selon la disposition des capteurs

Comme attendu, l'écart type des mesures effectuées par les deux capteurs en vue directe est moins important que pour les autres capteurs. En revanche, contrairement aux scénarios précédents, une distance supérieure n'est pas synonyme d'une plus grande volatilité des puissances reçues. Le capteur 1 se situe à $255cm$ du capteur récepteur tandis que le capteur 2 en est séparé de $326cm$, or l'écart-type des mesures du RSSI provenant de 1 est supérieur à celui provenant de 2. Ici, le fait qu'un des deux capteurs ne soit pas en vue directe (le capteur 1) va avoir plus d'influence que la distance qui les sépare du capteur récepteur.

Par la suite, nous voulons étudier la possibilité d'approximer la moyenne du RSSI mesuré sur 40 heures avec seulement quelques paquets. La question à laquelle nous voulons répondre est la suivante : malgré la variation importante du RSSI à court terme, est-il possible, en faisant la moyenne obtenue après la réception de quelques paquets de s'approcher de la moyenne obtenue après 40 heures ? Pour cela nous prenons l'ensemble des échantillons de 2 paquets puis 3 etc. jusqu'à une taille de 50 paquets successifs par échantillon de l'expérience. Nous effectuons la moyenne de chaque échantillon et nous regardons l'écart obtenu avec la moyenne globale (obtenue après 40 heures).

Les résultats diffèrent selon les capteurs (voir figure 3.19). Pour le capteur 1, on remarque qu'il faut un échantillon d'une dizaine de paquets pour réduire l'écart à la moyenne de façon importante. Cependant, prendre des échantillons plus importants ne va réduire que de façon marginale cet écart qui va rester supérieur à $5dBm$. Pour les capteurs 4 et 5, le phénomène est le même mais dans une moindre mesure : un échantillon de deux messages va déjà permettre d'approximer la moyenne avec une erreur de $10dBm$, une dizaine de trames va permettre de réduire cette erreur à $5dBm$ environ. Pour l'ensemble des capteurs, la prise en compte dans le calcul d'une approximation de la moyenne d'un échantillon entre 10 et 50 messages ne va pas avoir d'impact sur sa précision. Cela signifie que moyenner les valeurs mesurées de RSSI va permettre de réduire dans une certaine mesure la volatilité du canal. Cependant, cette réduction va être limitée et va dépendre des caractéristiques du lien entre le capteur émetteur et le capteur

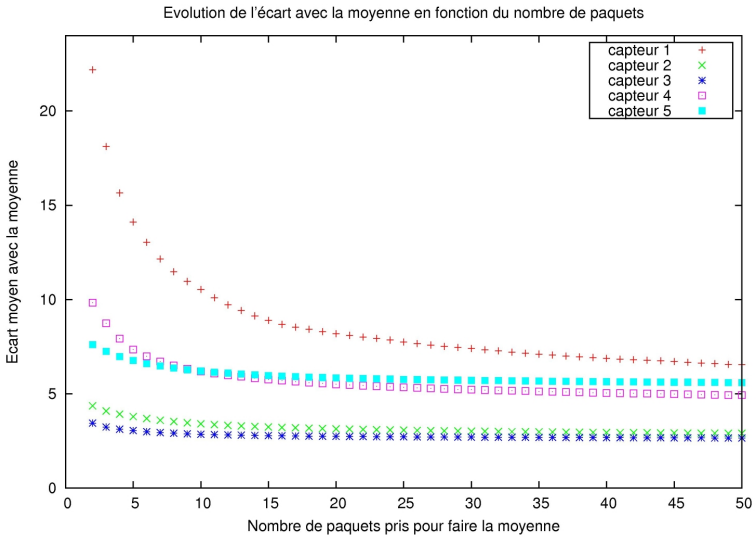

FIGURE 3.19 – Évolution du nombre de paquets nécessaire pour approximer la moyenne

récepteur.

3.5 Conclusion

Les réseaux de capteurs sont déployés dans des milieux dynamiques, c'est-à-dire des environnements dont les propriétés physiques ou structurelles sont susceptibles d'être modifiées à tout moment (changements météorologiques, mobilité d'objets ou de personnes à l'intérieur du réseau, diminution de l'énergie, etc.). Dans ce chapitre nous avons démontré que les propriétés de l'environnement dans lequel étaient déployés les capteurs influent de façon très importante la perception du RSSI : en termes de rapport entre RSSI et distance et en termes de volatilité des mesures. De plus, indépendamment de l'environnement nous retrouvons des constantes dans chacune des expérimentations effectuées : puissances reçues différentes selon la direction du capteur récepteur et sur-représentation des messages avec un fort RSSI pour les distances importantes. La faible qualité des antennes PCB et le rapport entre force du signal et le taux d'erreur (BER) expliquent ces phénomènes.

En conclusion, le RSSI, utilisé comme métrique de proximité, n'est pas fiable en raison de son imprédictibilité et de son instabilité. Cette imprédictibilité est due à plusieurs facteurs. En premier lieu, l'environnement :

- Si l'environnement est dynamique, les interférences vont perturber le RSSI. Les effets de *shadowing* vont entraîner une faible stabilité à court et à long terme.
- Si l'environnement est réduit, les effets de multi-trajet vont introduire des incohérences dans le rapport entre le RSSI et la distance.

En second lieu, le matériel :

- La qualité relative des composants intégrés au capteur (antenne principalement) va entraîner des propriétés de transmission et de réception du signal différente selon la direction.
- Les différences de calibrage entre les capteurs vont conduire à des différences de mesures.

Et en troisième lieu, la distance :

- Pour les distances à la limite de la réception, les messages qui seront décodés auront un RSSI plus élevé que la majorité des messages envoyés. Cette sur-représentation va conduire à fausser le rapport RSSI-distance.
- Plus la distance est grande, plus la stabilité du RSSI va être faible. Cela s'explique par une plus grande sensibilité du signal aux interférences, aux multi-trajets et une plus grande probabilité de *shadowing*.

En montrant les faiblesses de la mesure de la puissance du signal reçu dans le cadre des réseaux de capteurs sans fil, nous avons soulevé la nécessité d'une métrique de proximité fiable. Cette métrique ne peut se baser sur des propriétés physiques du signal, trop fluctuantes. Le prochain chapitre introduit le protocole de localisation qualitative, QLoP, et l'indice de proximité.

Bibliographie

[1] P. Bahl and V.N. Padmanabhan. Radar : an in-building rf-based user location and tracking system. In *The 19th Conference of the IEEE Computer and Communications Societies (Infocom'00)*, volume 2, pages 775–784, Tel Aviv, 2000.

[2] Andrea Goldsmith. *Wireless Communications*. Cambridge University Press, August 2005.

[3] H. Hashemi. The indoor radio propagation channel. *Proceedings of the IEEE*, 81(7) :943–968, July 1993.

[4] Sajid Hussain, Richard Peters, and Daniel L. Silver. Using received signal strength variation for surveillance in residential areas. In *Data mining, intrusion detection, information assurance, and data networks security (SPIE)*, pages 1–6, Orlando, Florida, USA, March 2008.

[5] P. Krishnan, A. S. Krishnakumar, Wen hua Ju, Colin Mallows, and Sachin Ganu. A system for lease : Location estimation assisted by stationery emitters for indoor rf wireless networks. In *23rd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, pages 1001–1011, Hong-Kong, China, March 2004.

[6] Xiaoli Li, Hongchi Shi, and Yi Shang. A sorted rssi quantization based algorithm for sensor network localization. In *11th International Conference on Parallel and Distributed Systems (ICPADS)*, pages 557–563, Fuduoka, Japan, July 2005. IEEE Computer Society.

[7] Neal Patwari and Alfred O. Hero, III. Using proximity and quantized rss for sensor localization in wireless networks. In *2nd ACM international conference on Wireless sensor networks and applications (WSNA)*, pages 20–29, San Diego, CA, USA, September 2003. ACM.

[8] B. Raman, K. Chebrolu, D. Gokhale, and S. Sen. On the feasibility of the link abstraction in wireless mesh networks. *Transactions on Networking*, 17(2) :528–541, April 2009.

[9] Yi Shang, Wheeler Ruml, Ying Zhang, and Markus P. J. Fromherz. Localization from mere connectivity. In *4th ACM international symposium on Mobile ad hoc networking and computing (MobiHoc)*, pages 201–212, Annapolis, MD, USA, june 2003. ACM.

[10] IEEE Computer Society. 802.15.4 part 15.4 : Wireless medium access control (mac) and physical layer (phy) specifications for low-rate wireless personal area networks (wpans). http://standards.ieee.org/getieee802/download/802.15.4-2006.pdf, september 2006.

[11] IEEE Computer Society. 802.11 part 11 : Wireless lan medium access control (mac) and physical layer (phy) specifications. http://standards.ieee.org/getieee802/download/802.11-2007.pdf, June 2007.

[12] M. Sugano, T. Kawazoe, Y. Ohta, and M. Murata. Indoor localization system using rssi measurement of wireless sensor network based on zigbee standard. In *Conference on Optical Communication Systems and Networks*, Banff, Canada, July 2006.

[13] E. Walker, H.-J. Zepernick, and T. Wysocki. Fading measurements at 2.4 ghz for the indoor radio propagation channel. In *International Zurich Seminar on Broadband Communications*, pages 171–176, Zurich, Switzerland, February 1998.

[14] Thomas Watteyne. *Energy-Efficient Self-Organization for Wireless Sensor Networks*. PhD thesis, INSA de Lyon, November 2008. number 2008-ISAL-0082.

4

QLoP ou l'auto-organisation appliquée à la localisation

4.1 Motivations

De nombreuses applications pour les réseaux de capteurs comme la surveillance des incendies de forêt, la télé-relève, etc. ont besoin d'avoir une information géographique pour fonctionner efficacement. Les protocoles de routage géographique ou orientés position vont pouvoir fonctionner sans avoir recours à un coûteux mécanisme de découverte de routes et ainsi économiser de l'énergie tout en améliorant le taux d'acheminement. Dans les protocoles de contrôle de topologie où chaque capteur doit ajuster sa puissance de transmission pour minimiser sa consommation énergétique, les algorithmes ont le plus souvent besoin d'informations sur la position de leurs voisins.

Le GPS [11] résout le problème de la localisation dans les environnements extérieurs. Cependant, pour les larges réseaux de capteurs où les nœuds doivent être de très petite taille, peu consommateurs et peu onéreux, équiper chaque unité avec une puce GPS est trop coûteux. En outre, la précision des puces GPS pour capteurs reste encore assez faible [8].

Dans ce chapitre, nous proposons un algorithme qui va permettre à chaque nœud de déterminer *qualitativement* la distance de ses voisins en utilisant uniquement des informations locales. Nous entendons par *qualitativement*, la possibilité de déterminer non pas une mesure plus ou moins précise en rapport avec la distance mais un **indice de proximité**. Cet indice de proximité sera une mesure locale, propre au capteur, qui lui permettra de classer ses voisins à un saut du plus proche au moins proche. Cette classification a un sens car elle permet de

contrôler la topologie, sélectionner les nœuds les plus robustes au bruit, etc. Notre objectif est de montrer qu'il existe une possibilité d'obtenir des informations assez précises sur la proximité des nœuds dans un réseau de capteurs sans s'appuyer ni sur un sous ensemble de nœuds connaissant leur position (ancres), ni sur des équipements spéciaux et sur la mesure de la puissance du signal reçu. L'algorithme déployé sur un nœud utilise uniquement des informations obtenues par l'échange de tables de voisinage à l'aide de paquets `hello` classiques pour calculer un indice de proximité pour chaque voisin à un saut.

Dans un premier temps, nous nous attacherons à exposer les études majeures existantes dans le domaine de la localisation et du positionnement. Nous n'insisterons pas sur les études traitant de la mesure de la puissance du signal reçu (RSS) traitées dans le chapitre 3. Le protocole de localisation qualitative avec les détails de l'algorithme et le calcul de l'indice de proximité est exposé dans un deuxième temps. Nous présentons ensuite les fondements théoriques de QLoP(Qualitative LOcalization Protocol). Nous montrons que, malgré une légère imprécision due à des incohérences de voisinage, l'algorithme reste fiable sur les topologies aléatoires et particulièrement performant sur les topologies régulières (grille). La figure 4.1 illustre le résultat de l'algorithme : les voisins à un saut du nœud étudié sont classés en 3 catégories : le *1-voisinage logique*, le *2-voisinage logique* et le *3-voisinage logique*. Nous concluons ce chapitre en comparant notre solution avec une solution aléatoire, la *pseudo distance* [6] et la mesure de RSSI.

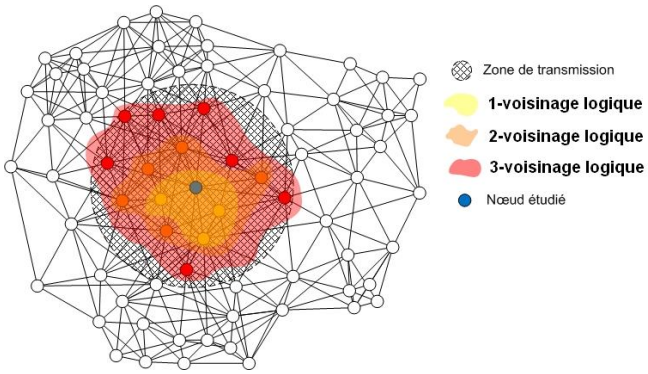

FIGURE 4.1 – Exemple d'une application de l'algorithme pour un nœud

4.2 État de l'art

De nombreuses techniques sont proposées pour permettre aux nœuds d'estimer leur position. Nous pouvons distinguer deux types de stratégie de localisation : les **localisations fines** et les **localisations approximatives**. Les localisations fines déterminent de manière précise la distance entre deux nœuds ou les coordonnées du nœud dans le réseau tandis que les localisations approximatives spécifient une surface, des coordonnées virtuelles, etc.

4.2.1 Localisations fines

L'utilisation du GPS permet de résoudre le problème de la localisation en extérieur sous certaines conditions et hypothèses. En effet, son coût, à la fois économique et énergétique, pose soucis. Dans les réseaux de capteurs denses, sa précision (de l'ordre d'une dizaine de mètres) peut également poser problème. Quelques articles contournent le problème et proposent l'utilisation d'ancres : seulement certains nœuds connaissent leur position précise et permettent autres nœuds du réseau, par triangulation ou multi-latération de connaître la leur. Pour cela, plusieurs solutions sont proposées :

- ToA (Time of Arrival) [5]. Sachant la vitesse de la propagation du signal dans l'air et l'instant où il a été envoyé, il est possible de déterminer avec précision la distance entre un récepteur et un transmetteur. En utilisant plusieurs nœuds de références, le nœud est capable de déterminer sa position relative par triangulation. Ce mécanisme, utilisé dans la localisation GPS, présente cependant une faille : pour être précis, il nécessite une synchronisation forte et une horloge interne stable (un décalage de 1 μs entraîne une erreur de $300m$ dans le cas d'un signal radio). Des solutions existent pour améliorer la précision en réduisant les imprécisions d'horloges mais elles nécessitent plus de nœuds de référence, des calculs importants ou des spécificités matérielles [20].
- TDoA (Time difference of Arrival) [22, 15]. Pour pallier l'obstacle de la synchronisation, le TDoA utilise deux signaux de différentes natures (ultrasons et radio par exemple), pour estimer la distance entre 2 nœuds. Connaissant le temps de propagation de chacun des signaux, la différence de temps d'arrivée va permettre de calculer la distance sans que la synchronisation ne soit nécessaire. Cependant, chaque nœud doit être équipé d'une antenne pour chaque signal et d'une horloge précise ce qui n'est pas le cas pour les capteurs actuellement sur le marché. De plus, cette solution entraîne un surcoût énergétique causé par la réception et l'envoi des deux signaux et la gestion de deux modules radio.
- AoA (Angle of Arrival) [16, 1, 18]. Chaque capteur est équipé d'un ensemble d'antennes. Ils sont donc capables de connaître l'angle d'arrivée d'un signal reçu. Cette information, obtenue de plusieurs nœuds voisins, va permettre d'appliquer une triangulation et le nœud sera capable d'obtenir une distance relative. Là encore, la consommation des capteurs est augmentée et les spécifications des capteurs présents sur le marché ne correspondent pas aux hypothèses initiales : ils ne possèdent qu'une seule antenne omnidirectionnelle.
- Combinaison de TDoA et de AoA [14]. Afin d'améliorer la précision et d'étendre la localisation à des environnements 3D. Les auteurs conçoivent une solution hybride en utilisant l'AoA pour améliorer la technique utilisée en 2D [5].

L'ensemble de ces protocoles ne prend pas en compte la consommation énergétique et le coût des nœuds avec comme hypothèses des capteurs suréquipés. En outre, le système des ancres n'évite pas le problème de la localisation mais ne fait que le réduire à un sous-ensemble des nœuds du réseau. En outre, il fait apparaître d'autres problèmes comme le placement optimal de ces ancres dans le réseau, pour permettre une meilleure localisation des nœuds [2, 9, 19]. Enfin, de nombreuses hypothèses existent concernant la synchronisation et le besoin de connaître le temps exact d'émission qui sont difficilement conciliables avec un réseau de capteurs dense où la contention et les interférences peuvent être importantes.

4.2.2 Localisations approximatives

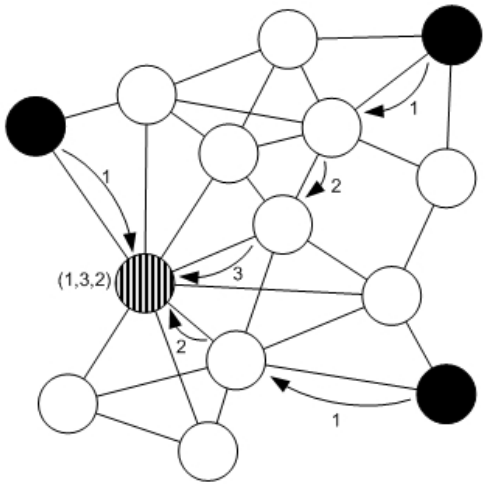

FIGURE 4.2 – Exemple d'une localisation approximative : coordonnées virtuelles

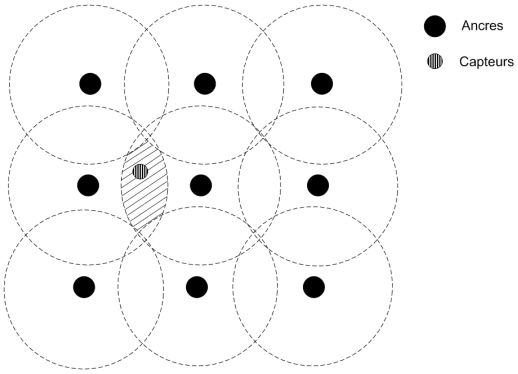

FIGURE 4.3 – Exemple d'une localisation approximative : intersection de signaux

D'autres stratégies consistent à trouver des coordonnées approximatives en déterminant imparfaitement la distance entre deux capteurs. Selon l'application, une localisation approximative des capteurs peut être un bon compromis et dans ce cas plusieurs approches sont possibles :

- Le système des badges actifs [12]. Dans ce système chaque nœud transmet un paquet `hello` périodique toutes les 10 secondes. Le signal est reçu par des ancres fixes placées à des endroits précis à l'intérieur d'un bâtiment. Ce sont ces ancres qui vont relayer l'information jusqu'au puits. La position d'un capteur est associée à la position de l'ancre la plus proche.
- L'intersection des signaux [3]. On considère également un réseau non homogène avec la présence régulière d'ancres. Chaque capteur compte le nombre d'ancres dont il reçoit le signal. En prenant comme hypothèse la connaissance de la portée radio des ancres et leur position, le capteur est en mesure de déterminer une zone de localisation (voir figure 4.3). Cette zone va correspondre à l'intersection théorique des disques de portée radio des ancres. Il est donc nécessaire ici d'avoir un nombre suffisant d'ancres connaissant leur position afin que tous les capteurs soient à portée directe d'au moins une ancre et de plusieurs pour avoir une meilleure précision.
- L'algorithme de localisation Monte-Carlo (MCL) [13]. Les auteurs se servent de la mobilité des nœuds dans le réseau pour affiner leur localisation. Ils utilisent la méthode séquentielle de Monte-Carlo pour calculer des probabilités de distribution des positions possibles des nœuds. En fonction de la position précédente des nœuds et des observations provenant d'ancres déployées dans le réseau, l'algorithme est capable de filtrer les positions impossibles.
- Le système de coordonnées virtuelles [4, 17]. Chaque nœud détermine sa distance aux ancres en nombre de sauts et détermine ainsi ses propres coordonnées dans un système

dont la dimension dépend du nombre d'ancres. Le routage devient possible en suivant le système de coordonnées ainsi établi (voir figure 4.2).

Ces protocoles sont peu adaptés aux réseaux de capteurs car ils nécessitent soit une architecture fixe préalable, ce qui interdit le déploiement des capteurs dans des zones inaccessibles ou dangereuses soit des calculs centralisés qui requièrent des communications régulières avec le puits de la part de l'ensemble de la topologie. Ce dernier mode de fonctionnement va être potentiellement très consommateur en énergie et peu résistant à un passage à l'échelle.

4.3 Algorithme de localisation qualitative : QLoP

L'objectif de QLoP est double. Il doit être capable de localiser qualitativement le voisinage direct d'un capteur : c'est à dire être capable de classer le voisinage physique d'un nœud en trois classes de voisinage logique. Il doit également être robuste à la dynamique du lien radio. Ces deux propriétés permettent de sélectionner des liens plus robustes entre des nœuds proches ou effectuer un contrôle de topologie sans information géographique, sans synchronisation ou hypothèses sur la portée radio des capteurs.

4.3.1 Détails de l'algorithme

Il faut garder à l'esprit que le but de notre algorithme est de permettre à chaque nœud de déterminer approximativement la proximité de ses voisins en utilisant uniquement des informations locales. Ces informations locales proviennent de paquets `hello` échangés périodiquement entre les voisins à 1 saut et contenant leurs propres voisins : ainsi une connaissance du 1-voisinage ouvert est réalisée. Un voisin peut appartenir à une de ces classes de proximité : le *1-voisinage logique*, le *2-voisinage logique* ou le *3-voisinage logique*. Ainsi, cette indication de proximité peut être utilisée pour construire un protocole de routage unicast efficace dans un environnement sans fil avec un haut niveau d'interférences : choisir les voisins considérés comme très proches (i.e. appartenant au 1-voisinage logique) permet de choisir les nœuds avec un rapport signal sur bruit important. Des applications au contrôle de topologie et aux coordonnées virtuelles pour le routage sont également possibles.

Le nœud y calcule l'indice de proximité PI_y d'un voisin x de la façon suivante :

$$PI_y(x) = (|V(y) \cap V(x)|) - \frac{max(|V(y)|, |V(x)|)}{2}$$

avec $V(y)$ et $V(x)$ le voisinage de y et x respectivement.
La construction de cet indice est justifiée en détail dans la section 4.3.2. L'idée générale est d'attribuer un indice fort aux voisins ayant à la fois un voisinage commun important et un voisinage distinct faible. L'indice de proximité va évaluer la similarité des voisinages. Ainsi, nous prenons en compte dans l'algorithme le rapport entre le nombre de voisins communs et le nombre de voisins disjoints. Il semble en effet logique que des voisins proches géographiquement aient un voisinage fortement semblable alors que deux voisins éloignés vont avoir un voisinage assez dissemblable. Ainsi, l'indice de proximité va représenter la distance **qualitative** d'un voisin. Nous allons voir que cette proximité qualitative va de pair avec la proximité géographique dans le cas

des réseaux de capteurs denses. Ce mécanisme permet d'établir trois classes distinctes parmi les voisins : le *1-voisinage logique* (ou 1), le *2-voisinage logique* (ou 2) et le *3-voisinage logique* (ou 3). Pour un nœud particulier, nous déterminons les classes de ces nœuds voisins de la façon suivante :

Soient $PI_y(x)$ l'indice de proximité du voisin x d'un nœud y, $PI_y(x_i)$ la liste des indices de proximité de tous les voisins x_i de y et $classe_y(x)$ la classe de x pour y :

$$\Delta = \frac{|max(PI_y(x_i)) - min(PI_y(x_i))|}{3}$$

$$classe_y(x) \quad = \begin{cases} 1 \ si \ PI_y(x) \geq max(PI_y(x_i)) - \Delta \\ 2 \ si \ max(PI_y(x_i)) - \Delta > PI_y(x) \geq max(PI_y(x_i)) - 2\Delta \\ 3 \ si \ PI_y(x) < max(PI_y(x_i)) - 2\Delta \end{cases}$$

Chaque nœud du réseau calcule l'indice de proximité de chacun de ses voisins en fonction des informations reçues de son voisinage à 1 saut. Chaque nœud maintient une table de voisinage à 1 et 2 sauts et diffuse celle à 1 saut avec des paquets `hello` périodiques. La figure 4.4 et le tableau 4.5 montrent une application de l'algorithme sur un nœud particulier. Le nœud 27 ordonne ses voisins en 3 classes de proximité. Nous pouvons voir en détail les valeurs trouvées par l'algorithme dans le tableau 4.5. Celui-ci permet également de mettre en parallèle ces valeurs avec les classes réelles déterminées par la distance euclidienne (l'indice de proximité est remplacé par la distance réelle et les classes 1 2 et 3 seront nommées respectivement classe très proche, proche et loin). Notons que sur cet exemple le réseau est relativement peu dense.

Le protocole est peu consommateur en énergie car il utilise seulement des informations nécessaires à beaucoup d'autres protocoles déployés dans les réseaux de capteurs : auto-organisation et contrôle de topologie (CDS-*rule k* [23], CDS-IDS [21], etc.) et protocoles de routages proactifs (OLSR [7], etc.). De plus, si le réseau est peu dynamique (faible mobilité, peu de naissance ou de mort de nœuds dans le réseau [10]) cet échange de paquets peut être réduit, voire limité simplement à la phase de déploiement du réseau.

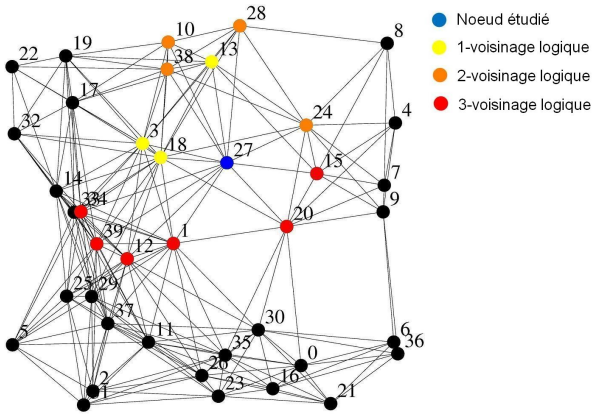

FIGURE 4.4 – Exemple de localisation qualitative calculée par le nœud 27.

Voisins	indice de proximité	distance euclidienne	classe de proximité	classe réelle
18	2.0	50.067	1-voisinage logique	très proche
3	1.0	65, 18	1-voisinage logique	très proche
13	0.5	77, 01	1-voisinage logique	proche
38	−0.5	83, 66	2-voisinage logique	loin
28	−0.5	103, 76	2-voisinage logique	loin
24	−0.5	66, 20	2-voisinage logique	très proche
10	−1.5	101, 18	2-voisinage logique	loin
1	−2.0	73, 09	3-voisinage logique	proche
20	−2.5	65, 96	3-voisinage logique	très proche
39	−3.0	115, 62	3-voisinage logique	loin
34	−3.0	115, 98	3-voisinage logique	loin
15	−3.5	68, 28	3-voisinage logique	très proche
12	−4.0	104, 40	3-voisinage logique	loin

FIGURE 4.5 – Comparaison de la localisation pour les voisins du nœud 27 obtenue avec l'algorithme de localisation qualitative et en utilisant la position réelle.

4.3.2 Analyse dans le cas d'une couche physique idéale

Dans cette section, nous considérons une couche physique idéale : c'est-à-dire un modèle à seuil. D'un point de vue théorique QLoP va utiliser les propriétés mathématiques suivantes. L'aire d'intersection de deux disques augmente inversement à la distance qui les sépare :

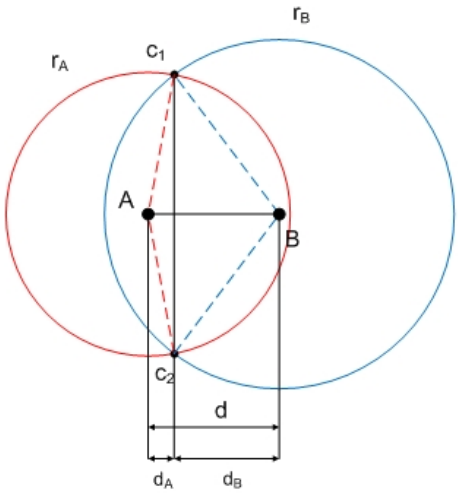

FIGURE 4.6 – Illustration de l'intersection des deux disques $\mathfrak{D}(A, r_A)$ et $\mathfrak{D}(B, r_B)$

Soit deux disques $\mathfrak{D}(A, r_A)$ et $\mathfrak{D}(B, r_B)$ de centre A et B et de rayon r_A et r_B respectivement. Soit d la distance entre leur centre respectif A et B. Si $d \geq r_A + r_B$ alors l'ensemble $(A, r_A) \cap (B, r_B)$ est vide ou réduit à 1 seul point et son aire est nulle. Si $d \leq r_A + r_B$ les deux cercles $S_1(A, r_A)$ et $S_2(B, r_B)$ se rencontrent en deux points c_1 et c_2. L'ensemble $\mathfrak{D}(A, r_A) \cap \mathfrak{D}(B, r_B)$ sera la réunion de deux portions de disques délimitées par la droite $(c_1 c_2)$ (voir figure 4.6).

Dans le cas où $r_A = r_B$ ces deux portions sont de même aire car elles sont isométriques. L'aire de $\mathfrak{D}(A, r_A) \cap \mathfrak{D}(B, r_B)$ sera alors le double de l'une de ces parties. Considérons la partie

du disque $\mathfrak{D}(A, r_A)$ comme la différence ensembliste entre le secteur $[A\widetilde{c_1c_2}]$ et le triangle $[Ac_1c_2]$ (voir figure 4.7) : $A_A = A_{secteur} - A_{triangle}$

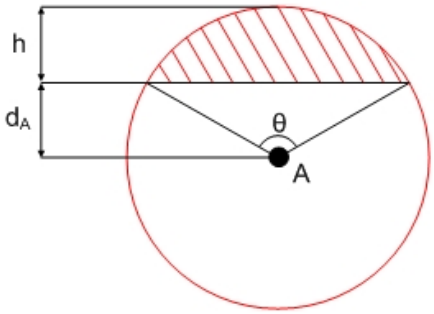

FIGURE 4.7 – Portion du disque

Soit $\mathfrak{D}(A, r_A)$ centré en $(0, 0)$ et $\mathfrak{D}(B, r_B)$ en $(d, 0)$ alors l'équation des 2 cercles est :

$$\begin{cases} x^2 + y^2 = r_A^2 \\ (x-d)^2 + y^2 = r_B^2 \end{cases}$$

On soustrait le premier terme du système au deuxième ce qui donne :

$$x = \frac{d^2 + r_A^2 - r_B^2}{2d} \tag{4.1}$$

$$d_A = x = \frac{d^2 + r_A^2 - r_B^2}{2d} \tag{4.2}$$

$$A_{sector} = \theta r_A^2 = r_A^2 arccos(\frac{d_A}{r_A}) \tag{4.3}$$

$$A_{triangle} = d_A \sqrt{r_A^2 - d_A^2} \tag{4.4}$$

L'aire de la portion de disque est donc égale :

$$A_A = \theta r^2 = r_A^2 arccos(\frac{d_A}{r_A}) - d_A \sqrt{r_A^2 - d_A^2} \tag{4.5}$$

On effectue le même raisonnement pour la portion du disque $\mathfrak{D}(B, r_B)$ avec

$$d_B = d - x = \frac{d^2 + r_B^2 - r_A^2}{2d} \tag{4.6}$$

ce qui nous donne :

$$A_B = r_B^2 arccos(\frac{d_B}{r_B}) - d_B \sqrt{r_B^2 - d_B^2} \tag{4.7}$$

Finalement, l'aire totale de l'intersection des deux disques $\mathfrak{D}(A, r_A)$ et $\mathfrak{D}(B, r_B)$ est égale à $A = A_A + A_B$ soit :

$$A = r_A^2 cos^{-1}\left(\frac{d^2 + r_A^2 - r_B^2}{2dr_A}\right) + r_B^2 cos^{-1}\left(\frac{d^2 + r_B^2 - r_A^2}{2dr_B}\right) - \frac{a}{2}$$

avec

$$a = \sqrt{(-d + r_A + r_B)(d - r_A + r_B)(d + r_A - r_B)(d + r_A + r_B)}$$

Il est clair que quand si $r_B > r_A$ et $d + r_A < r_B$, ce qui signifie que $\mathfrak{D}(A, r_A)$ est inclus dans $\mathfrak{D}(B, r_B)$, alors l'aire d'intersection des deux disques sera égale à l'aire du disque le plus petit (ici l'aire de $\mathfrak{D}(A, r_A)$).

L'indice de proximité de QLoP se base en partie sur l'intersection des voisinages. Si nous considérons que deux nœuds A et B sont voisins si la distance qui les sépare est inférieure à r_A et r_B leur rayon de transmission respectif, cela signifie que la métrique de QLoP se base sur la probabilité de présence d'un nœud dans la surface d'intersection des deux disques quand $d < r_A$ et $d < r_B$.

Puisque nous considérons le déploiement aléatoire et uniforme des capteurs sur la zone de déploiement, la probabilité de présence d'un nœud sur une surface est directement proportionnelle avec l'aire de cette surface.

Nous pouvons donc dire que le terme $|V(y) \cap V(x)|$ se rapprochera de la valeur de l'aire de l'intersection des deux disques quand la densité du réseau augmentera.

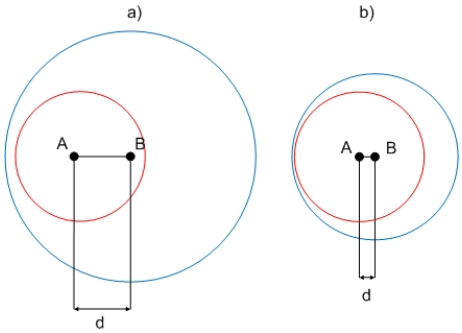

FIGURE 4.8 – Dans les cas a) et b), l'aire d'intersection est la même et pourtant la distance est différente

Cependant, la figure 4.8 met en évidence un exemple simple où cette métrique est mise en défaut. En effet, si $d + r_A < r_B$ alors $\mathfrak{D}(A, r_A) \cap \mathfrak{D}(B, r_B) = \mathfrak{D}(A, r_A)$. De plus, si $r_B << r_A$, alors la différence $r_B - r_A$ sera importante. L'aire de l'intersection du voisinage ne sera plus proportionnelle à la distance.

QLoP prend en compte ce phénomène. Il minore le premier terme $|V(y) \cap V(x)|$ par $\frac{max(|V(y)|,|V(x)|)}{2}$. D'un point de vue mathématique, cela revient à soustraire la moitié de l'aire du disque le plus grand. Le raisonnement est le suivant. La probabilité d'englober tout le voisinage d'un nœud est significative en termes de distance seulement si les deux disques sont de taille équivalente.

Considérons 2 cas de figure :

Soit deux nœuds u et v. u possède 4 voisins et v en possède 10. u et v ont 3 voisins en commun.

Soit deux nœuds u et w. u possède 4 voisins et w en possède 4. u et w ont 3 voisins en

commun.

Dans le premier cas v partage moins de 1/3 de son voisinage alors que dans le second il partage la presque totalité avec u. On voit alors que malgré un voisinage en commun identique en taille, il est plus probable que les deux nœuds u et v soient plus proches que les nœuds u et w. L'objectif de la métrique de QLoP est de classer les voisins par ordre de proximité. Dans ces deux cas, il va donc classer le voisin w devant le voisin v (d'après QLoP, $PI_u(v) = -2$ et $PI_u(w) = 1$). Montrons ce raisonnement sur un exemple. Soit 4 nœuds s,u,v et w avec s, v et w voisins de u. Soit $r_s = 16$, $r_u = 15$, $r_v = 10$ et $r_w = 20$ les rayons respectifs de s,u,v et w (voir figure 4.9).

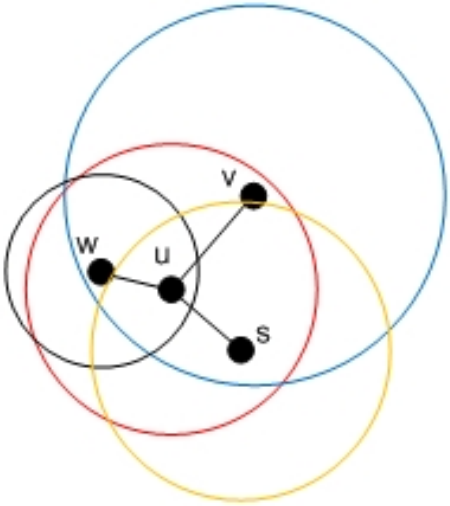

FIGURE 4.9 – Exemple d'estimation de la distance sur un voisinage de 4 nœuds par le nœud u.

Si on estime les distances us, uv et uw par la simple surface d'intersection des disques, nous obtenons 3 valeurs très dissemblables pour une même distance selon les voisins (voir figure 4.10). La probabilité de classer de façon exacte les nœuds sera d'autant plus faible. En estimant ces distances avec la métrique de QLoP, nous obtenons des valeurs plus rapprochées entre elles (voir figure 4.11). On le voit, QLoP va « pénaliser » les nœuds possédant un voisinage important relativement aux autres nœuds. C'est ainsi que l'on retrouve une valeur de QLoP pour la distance entre u et v inférieure à la valeur de QLoP pour la distance entre u et s.

Le calcul de l'écart-type permet d'obtenir la dissémination de la métrique et montrer ainsi sa stabilité. Nous insistons sur le fait que l'objectif de QLoP est de classer le voisinage direct d'un capteur, par conséquent, une bonne métrique sera une métrique qui aura une valeur identique pour une distance donnée quelque soit le voisin. La figure 4.12 nous montre clairement que QLoP est la métrique la plus stable. On peut également noter que cette dissémination de la métrique diminue encore avec la distance.

4.4 Étude des performances de QLoP

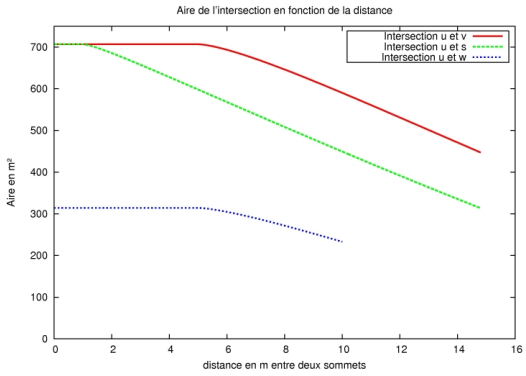

FIGURE 4.10 – Aire d'intersection des disques par rapport aux distances us, uv et uw

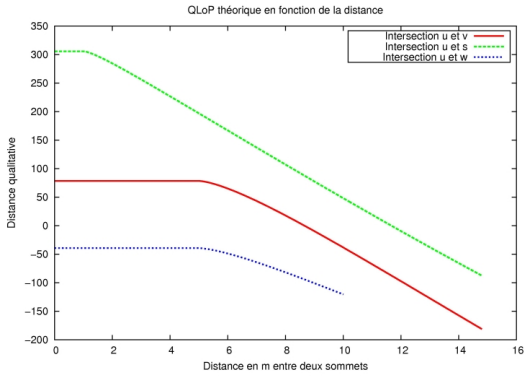

FIGURE 4.11 – Métrique QLoP par rapport aux distances us, uv et uw

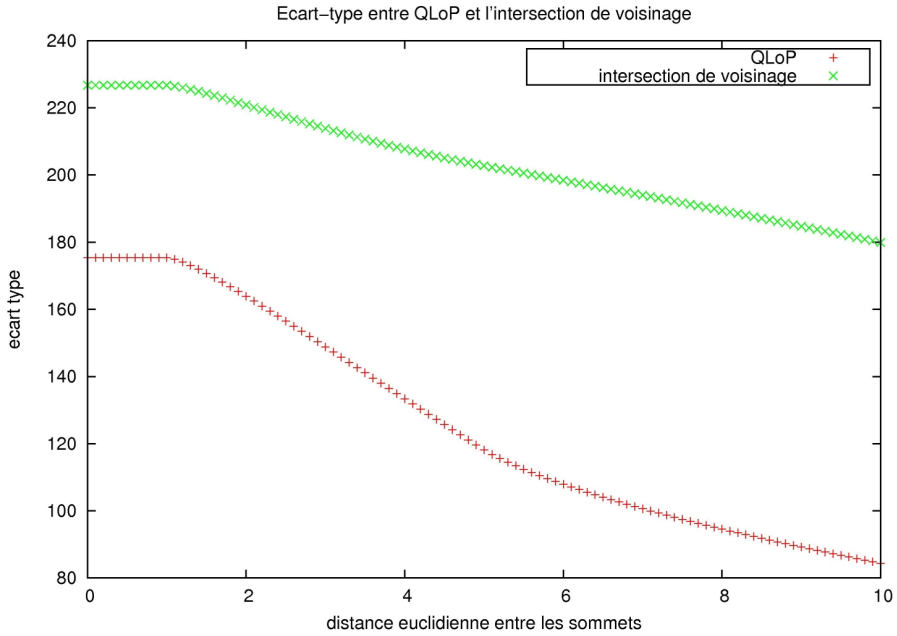

FIGURE 4.12 – Écart-type entre la métrique QLoP et l'aire d'intersection par rapport à la distance entre us, uv et uw

4.4.1 Comportement du protocole de localisation qualitative sur une topologie régulière

Nous simulons un réseau de 100 capteurs déployés de façon uniforme et régulière sur une grille de 10x10 nœuds (voir figure 4.13). Ensuite, nous augmentons la puissance de transmission de chacun des capteurs pour augmenter leur voisinage et nous observons comment réagit le protocole de localisation qualitative. Parfois, le voisinage n'est pas représentatif de la régularité de l'ensemble du réseau. Dans ce cas (voir scénario b) de la figure 4.13) ou quand les nœuds se trouvent sur les bords, l'algorithme ne parvient pas à ordonner correctement les voisins des deux premières classes de proximité à cause des incohérences dans le voisinage. Pour les

autres topologies, les différentes classes sont déterminées sans erreur et l'indice de proximité est identique pour des voisins éloignés de la même distance géographique. Nous pouvons conclure que lorsque la topologie et le voisinage sont uniformes et réguliers, la localisation qualitative est très efficace.

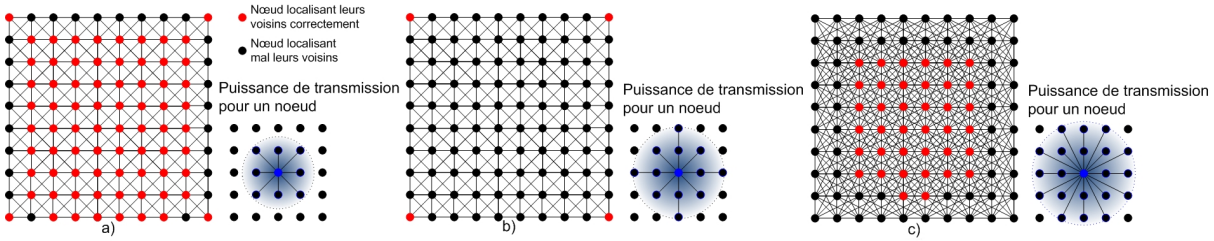

FIGURE 4.13 – Algorithme déployé sur une grille

4.4.2 Comportement du protocole de localisation qualitative sur des topologies aléatoires

Distance quadratique

Cependant, les réseaux de capteurs sont, la plupart du temps, déployés de façon aléatoire. Afin de mesurer la précision de l'algorithme dans un environnement plus réaliste, nous déployons, selon une distribution aléatoire et uniforme, 100 nœuds dont nous faisons varier la puissance de transmission pour augmenter le degré. Nous calculons ensuite la distance quadratique entre la liste des voisins de chacun des nœuds classée selon la position réelle des nœuds (GPS) et celle classée par l'algorithme.

Soit deux listes v et w dans R^n tel que : $v = (v_1, v_2, ..., v_n)$, $w = (w_1, w_2, ..., w_n)$. La distance quadratique dq est :

$$dq = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(v_i - w_i)^2}$$

Cette distance permet de mesurer le niveau de dissemblance entre deux classements. Dans ce chapitre nous étudions la distance quadratique de l'algorithme pour le *1-voisinage logique*, le *2-voisinage logique* et le *3-voisinage logique*. Nous observons (voir figure 4.14) que la distance quadratique augmente mais de façon plus lente que le degré moyen. Quand le degré moyen augmente, le nombre de voisins à classer pour chaque nœud augmente. Si la distance quadratique reste basse, cela signifie que la précision augmente. Ce phénomène s'explique par le grand nombre d'informations reçues quand le voisinage est important et donc une plus grande fiabilité dans l'indice de proximité. Les différentes classes varient de la même façon. En outre, nous pouvons noter une plus faible augmentation pour les deux premières classes : le 2-voisinage logique et le 1-voisinage logique.

Dans le cas d'une topologie dense (700 nœuds, degré moyen : 40), la localisation est très efficace. Nous pouvons voir le classement en trois classes par le nœud 27 de son voisinage sur la

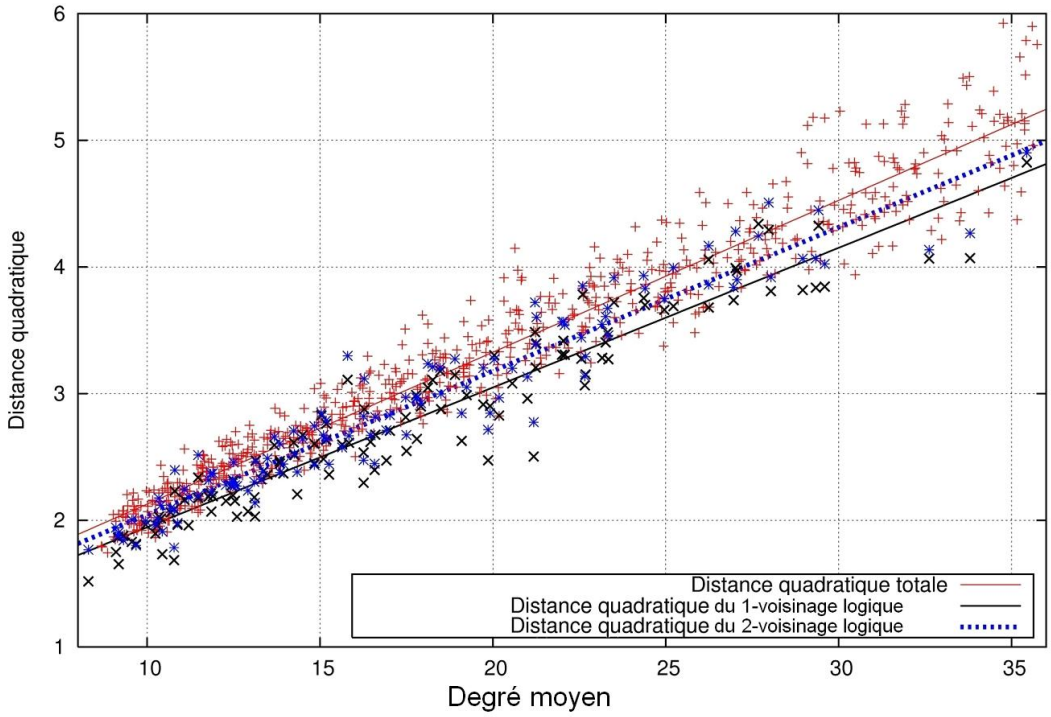

FIGURE 4.14 – Distance quadratique par classe

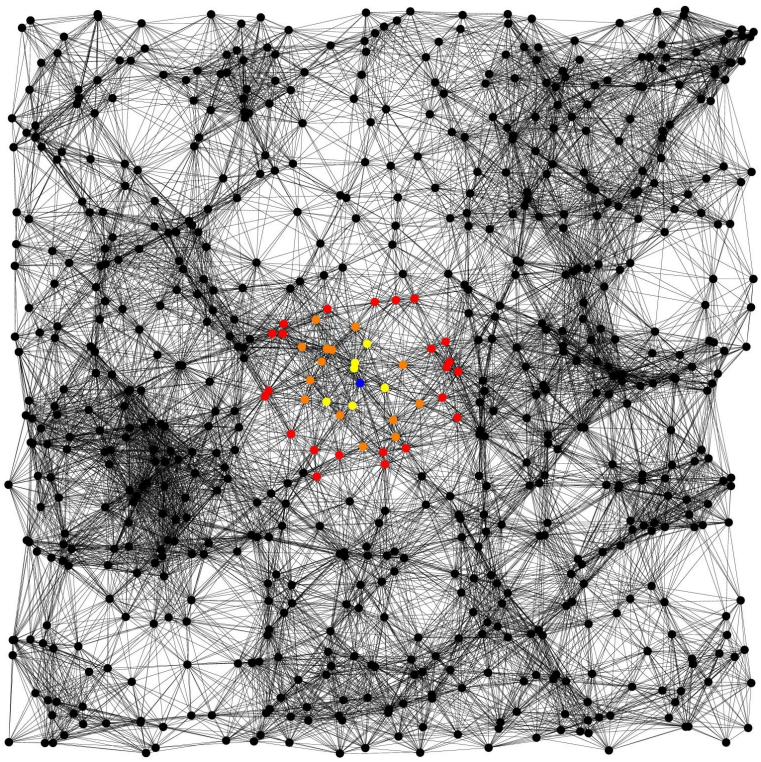

FIGURE 4.15 – Les 3 classes de voisinage logique de l'algorithme

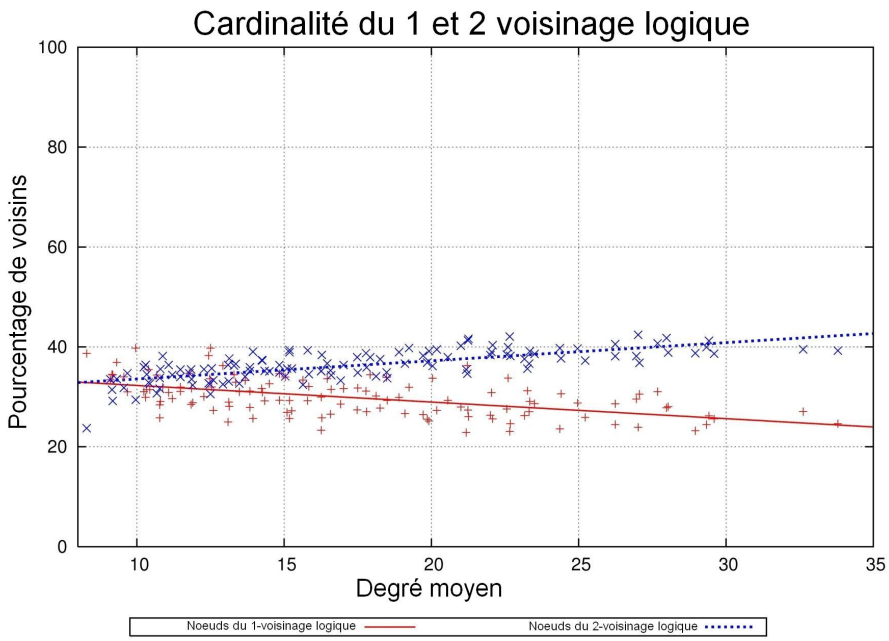

FIGURE 4.16 – Évolution de la cardinalité des voisinages logiques de proximité en fonction du degré moyen

figure 4.15. Les nœuds jaunes appartiennent au *1-voisinage logique*, les oranges au *2-voisinage logique* et les rouges au *3-voisinage logique*. Plus la densité d'un réseau est forte et moins les incohérences de voisinage influent sur le classement des voisins.

Cardinalité

Chaque nœud alloue une classe à ses voisins en fonction de son indice de proximité. Comment évoluent ces classes quand le degré moyen augmente ? La classe des nœuds du *1-voisinage logique* va-t-elle croître proportionnellement au nombre de voisins ? Nous avons vu que la distance quadratique augmente légèrement quand le degré moyen augmentait. Cependant, cette métrique est très sensible à la taille des listes évaluées. Ainsi, nous étudions le pourcentage moyen de nœuds sélectionnés dans le *1-voisinage logique* et *2-voisinage logique* (voir figure 4.16). Nous pouvons souligner que le pourcentage des nœuds du *1-voisinage logique* diminue alors que, dans le même temps, celui des nœuds appartenant au *2-voisinage logique* augmente. La cardinalité du *3-voisinage logique* reste constante. Cela indique que plus la densité est importante et plus l'indice de proximité est capable de distinguer les nœuds réellement proches.

Efficacité/fiabilité

Quand l'algorithme détermine une classe de distance pour un voisin, il est primordial de savoir si ce nœud sélectionné comme appartenant au 1 ou 2-voisinage logique, est effectivement proche ou très proche dans le monde réel. Pour répondre à cette interrogation, nous avons déterminé le nombre de nœuds et appartenant au *2-voisinage logique* et au *1-voisinage logique*

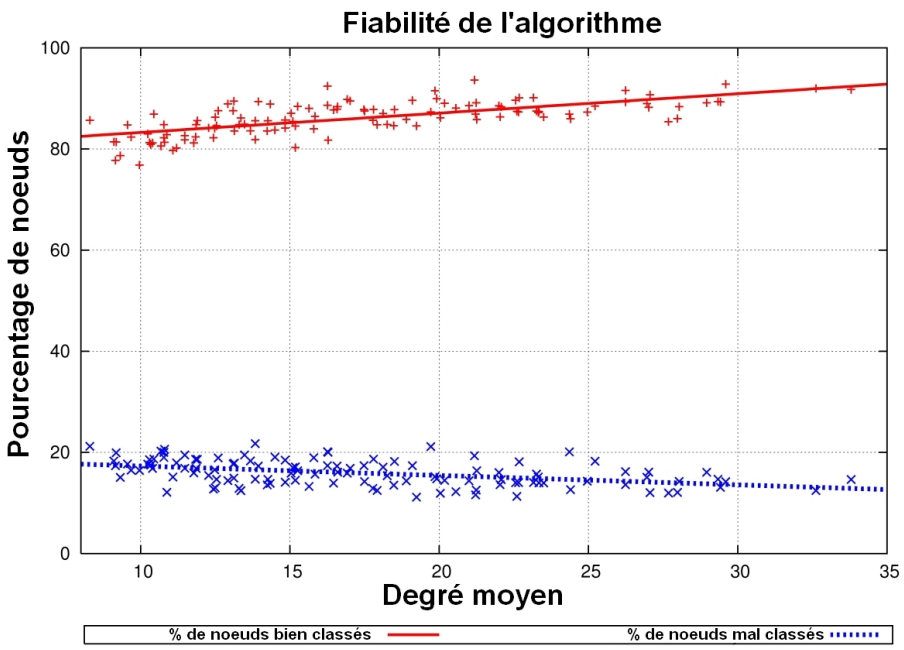

FIGURE 4.17 – Évolution de la fiabilité de l'algorithme en fonction du degré moyen

sélectionnés par l'algorithme appartenant effectivement à ces classes géographiquement. Ensuite nous regardons le nombre de nœuds réellement dans ces deux classes et non sélectionnés par l'algorithme. Nous avons ainsi la fiabilité de l'algorithme en répondant à ces deux questions : quelle probabilité qu'un voisin classé comme appartenant au *2-voisinage logique* ou au *1-voisinage logique* le soit effectivement et quelle probabilité qu'un nœud proche ou très proche soit manqué par l'algorithme ? Nous observons une fiabilité de plus de 80% même pour des topologies de faible degré (voir figure 4.17). Il est à noter que la prise en compte du voisinage au-delà de 2 sauts pour le calcul de l'indice de proximité dégrade la précision.

4.4.3 Comportement face aux phases de la vie du réseau

Nous avons décrit dans le chapitre 2 les différentes phases de vie d'un réseau de capteurs : la naissance, le fonctionnement normal et la mort. Nous avons montré que ces phases caractéristiques étaient inhérentes aux réseaux de capteurs. Il convient donc d'étudier le comportement de notre protocole durant ces phases de vie, comme nous l'avons réalisé avec les autres protocoles d'auto-organisation. Pour ce faire, nous avons étudié la variation de la distance quadratique moyenne de QLoP en utilisant le même scénario que dans le chapitre 2. Les nœuds sont déployés progressivement sur une surface de 100x100m de manière aléatoire et uniforme. Après $20s$, 15% de nœuds sont retirés de manière aléatoire. À nouveau après $20s$, on rajoute 15 nœuds aléatoirement. Nous pouvons voir les conséquences de la naissance et de la mort de nœuds sur la figure 4.18.QLoP base son fonctionnement sur la connaissance du voisinage à 1 et à 2 sauts. Un capteur va mettre à jour la valeur de la localisation de ses voisins uniquement si son voisinage proche est modifié. L'apparition d'un nouveau capteur ou la mort d'un nœud ne va donc affecter le réseau que de façon localisée. Cette figure met en évidence la robustesse de QLoP

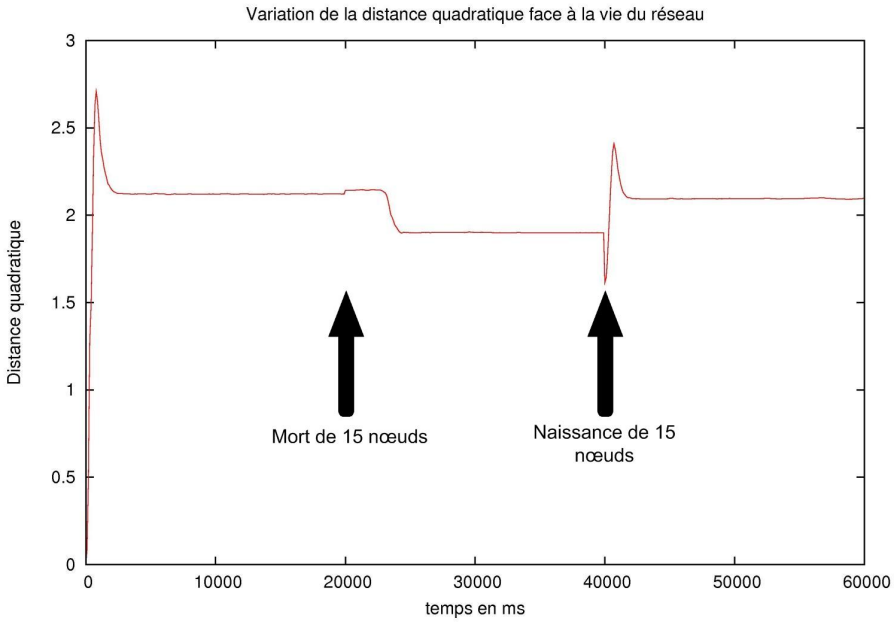

FIGURE 4.18 – Naissance, vie et mort : impacts sur QLoP

durant les phases de naissance et de mort.

Afin de pouvoir comparer les indices de proximité calculés par chacun des nœuds, il est nécessaire de les normaliser. En effet, chaque nœud calcule un indice de proximité strictement local dont il se sert pour classer ses voisins par ordre de proximité. Cet indice n'est donc pas, en l'état, comparable aux indices de proximité des autres nœuds. Pour cela, on effectue tout d'abord une translation des PI(x) afin d'avoir que des valeurs positives puis on les divise par l'intervalle PI_{max} afin de conserver l'ordre des indices mais compris dans un intervalle entre 0 et 1. La figure 4.19 montre qu'il existe un coefficient α tel que $d(u, v) = \alpha.PI_u(v)$ avec $PI_u(v)$ l'indice normalisé.

Pour trouver α il est nécessaire de connaître la distance maximale atteignable par le signal d'un capteur. Contrairement à l'ensemble des autres simulations faites précédemment, nous prenons cette hypothèse forte afin d'étudier les conséquences de l'ajout ou de la mort de nœuds sur la précision de QLoP en termes d'erreurs de localisation.

Nous avons regardé sur un ensemble de topologies identiques, l'évolution de cette erreur de localisation. La figure 4.20 illustre cette étude. Nous partons d'une topologie de 250 nœuds. Dans un premier cas, nous retirons 15 nœuds toutes les 20 secondes 10 fois de suite jusqu'à atteindre 100 nœuds. Dans un second cas, nous ajoutons 15 nœuds toutes les 20 secondes 10 fois jusqu'à atteindre 400 nœuds.

La mort de nœuds entraîne, comme attendu, l'augmentation de l'erreur de l'estimation, tandis que l'ajout de capteurs à la topologie initiale diminue cette erreur. Ces résultats sont cohérents avec ceux de la section 4.4.2 : une plus forte densité entraîne une augmentation d'information pour chacun des nœuds. Cela correspond également aux enseignements de la partie théorique.

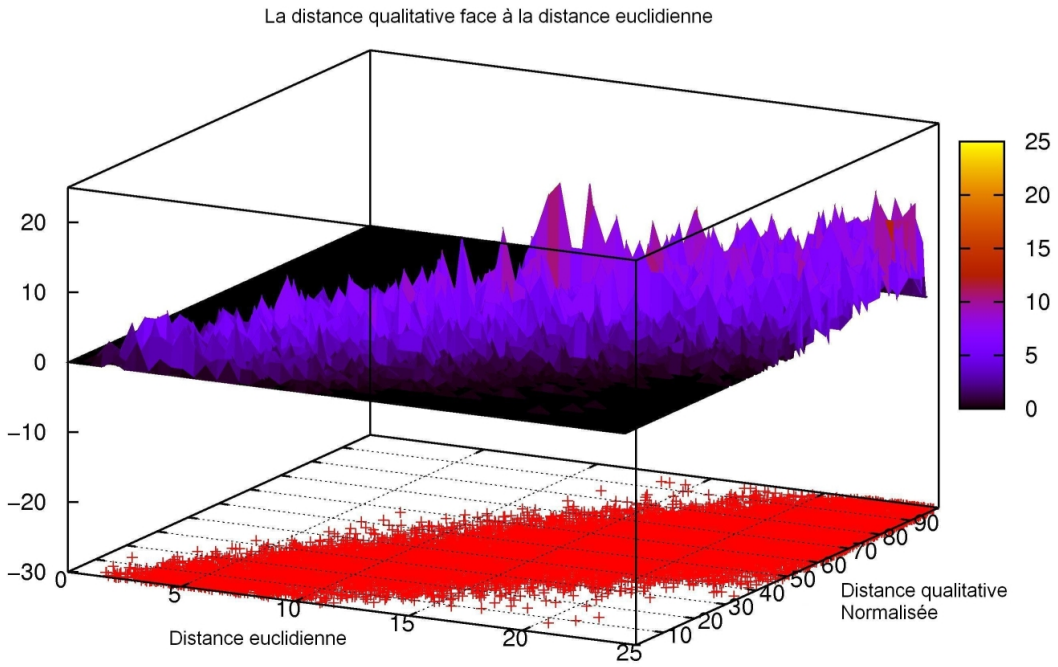

FIGURE 4.19 – Indice de proximité en fonction de la distance euclidienne sur l'ensemble des capteurs

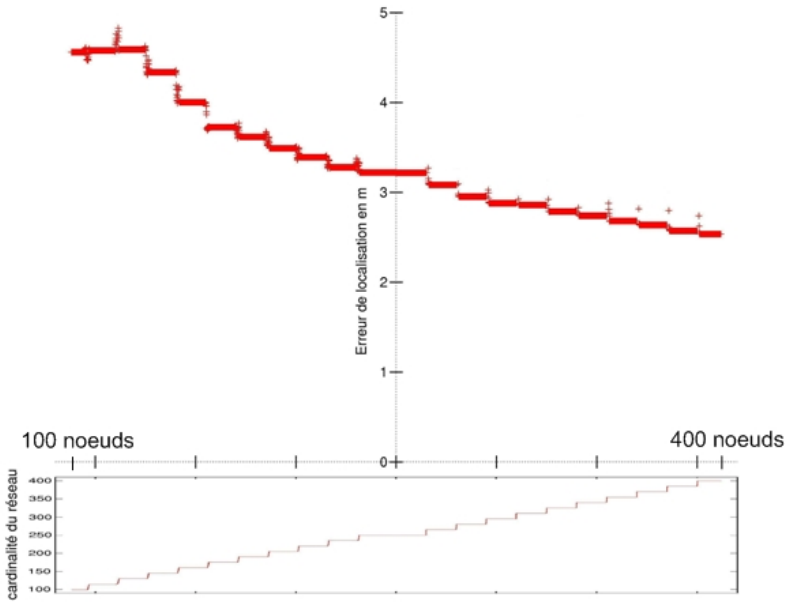

FIGURE 4.20 – Évolution de l'erreur de localisation de QLoP en face à l'ajout et à la mort de nœuds

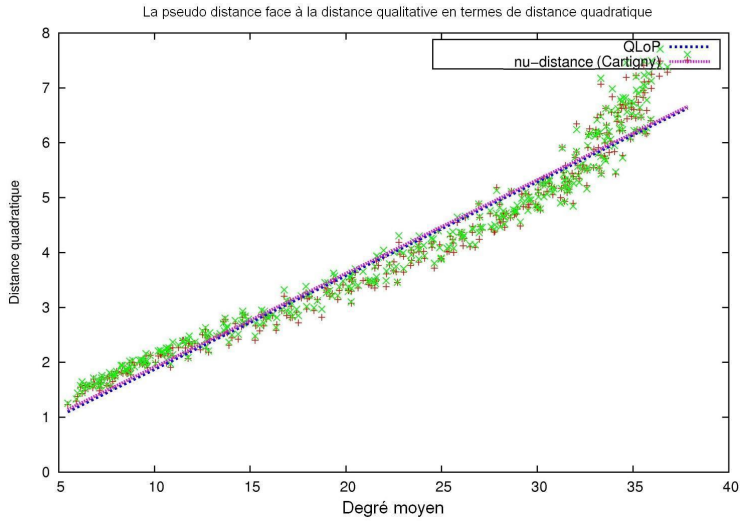

FIGURE 4.21 – Évolution de la distance quadratique pour QLoP et la pseudo-distance en fonction du degré moyen (topologie UDG)

4.4.4 QLoP face à la ν-distance

Nous avons vu que d'un point de vue théorique, dans le cas de l'intersection de disques de tailles différentes, l'indice de proximité de QLoP était plus efficace pour déterminer une métrique relative à la distance entre les centres de ces disques. Rappelons que la ν-distance de [6] est déterminé par :

$$\nu(u,v) = \frac{|N(u)N(v) \cup N(v)N(v)|}{|N(u) \cup N(v)|}$$

que l'on peut simplifier par :

$$\nu(u,v) = 1 - \frac{|N(u) \cap N(v)|}{|N(u) \cup N(v)|}$$

On le voit, cette métrique ne prend pas en compte les différences de densité des voisinages $N(u)$ et $N(v)$. Soit 4 nœuds u, v, w et s si dans un cas $N(u) >> N(v)$, et dans l'autre $N(w) = N(s)$ mais que $N(w) \cup N(s) = N(u) \cup N(v)$ la métrique restera proportionnel à l'intersection de $N(u)$ et $N(v)$ dans le premier cas et à $N(w)$ et $N(s)$ dans le second. Or, nous avons vu que cette métrique était moins performante que l'indice de proximité de QLoP.

Dans le cas d'une topologie UDG et avec une distribution aléatoire et uniforme, il n'existe qu'un faible avantage pour QLoP (voir figure 4.21). Cependant, cet avantage devient non négligeable lorsque le canal radio est réaliste et que les différences de cardinalité dans le voisinage des nœuds sont, de fait, plus importantes (voir figure 4.22).

4.4.5 QLoP face au RSSI

Nous avons vu précédemment que le RSSI (indicateur de la force du signal reçu) était souvent pris comme estimation fiable de la distance. Nous avons également mis en évidence,

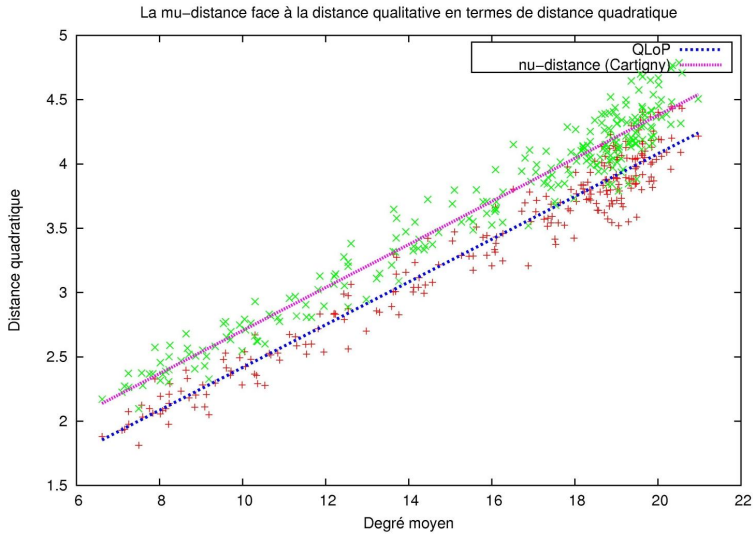

FIGURE 4.22 – Évolution de la distance quadratique pour QLoP et la pseudo-distance en fonction du degré moyen (topologie réaliste)

par l'examen des études théoriques, les simulations et les expérimentations réalisées sur ce sujet, que cette mesure n'était ni stable, ni précise. Nous détaillons dans ce chapitre pourquoi l'indice de proximité de QLoP est une mesure plus appropriée dans les réseaux de capteurs sans fil.

Le canal radio est instable et fluctuant. Que cela soit dû aux interférences, aux effets du multi-trajets, ou au *fading*, aucune expérimentation dans un environnement réaliste ne montre une stabilité de la puissance du signal reçu à court terme. Nous avons montré que, partant de cette constatation, des mécanismes de « lissage » devaient être mis en oeuvre, entraînant inévitablement de la latence et un surcoût énergétique (nécessité d'écouter le canal plus longtemps avant d'avoir une mesure stable).

QLoP, parcequ'il base son algorithme sur les informations topologiques obtenues, par exemple, par l'échange de paquets `hello`, ne prend en compte que des données binaires : la présence ou non d'un voisin dans la table de voisinage, indépendamment d'une mesure de la qualité du signal. À partir du moment où un réseau est dans la capacité de fonctionner, c'est-à-dire que chacun des capteurs est capable de communiquer avec ses voisins, QLoP est capable de fonctionner avec les performances exposées précédemment, quels que soient la dynamique dans le voisinage, le *fading*, ou les conditions météorologiques. QLoP n'est sensible qu'aux modifications topologiques et nous avons vu précédemment que cette sensibilité était purement locale.

Énergie. Si on considère que le RSSI n'est pas stable, la solution est de l'observer sur une longue période et de le moyenner ou de le traiter de façon plus efficace encore afin de le rendre précis. Non seulement cela s'avère inefficace si des changements non temporaires ou oscillatoires surviennent (changement d'une armoire de place dans un appartement, ouverture, fermeture d'une porte, déplacement de véhicules, etc.), mais cela engendre de la latence supplémentaire et une perte d'énergie. QLoP contourne cette difficulté en basant son indice de proximité sur des informations topologiques mises à jour.

En revanche, QLoP n'est pas opérationnel dans le cas d'un réseau radio limité à 1 saut ou

d'une densité faible. Cette configuration est rarement le cas pour les réseaux de capteurs.

4.5 Conclusion

Dans ce chapitre, nous avons étudié en détail les propriétés de notre algorithme d'auto-organisation appliqué à la localisation. Après avoir examiné les solutions existantes, nous avons donné les fondements théoriques de notre métrique et les performances sur une topologie régulière et sur des topologies aléatoires. Dans la continuité du chapitre 2, nous avons observé le comportement de QLoP sur les phases de naissance, vie et mort d'un réseau de capteurs. En se basant sur le voisinage à 1 et 2 sauts, QLoP est localisé et donc robuste aux changements de topologies. De plus, il est peu consommateur en énergie car son algorithme est peu complexe même dans le cas de fortes densités et ne nécessite pas de trafic de contrôle supplémentaire. Nous avons comparé notre métrique avec d'autres solutions proposées et ainsi mises en évidence les avantages de QLoP sur la ν-distance de [6] et sur la mesure de RSS.

Cependant, tout comme la hiérarchisation d'un réseau par un protocole orienté dominant n'est pas une fin en soi, arriver à déterminer avec une certaine fiabilité 3 classes de proximité n'a d'utilité que si cette propriété est en mesure d'améliorer les performances d'un réseau de capteurs. C'est pour cette raison que le prochain chapitre sera consacré à l'application de QLoP au contrôle de topologie et au routage en environnement bruité.

Bibliographie

[1] H. Akcan, V. Kriakov, H. Brönnimann, and A. Delis. Gps-free node localization in mobile wireless sensor networks. In *5th ACM International Workshop on Data Engineering for Wireless and Mobile Access (MobiDE)*, pages 35–42, Chicago, Illinois, USA, June 2006. ACM Press.

[2] F. Benbadis, K. Obraczka, J. Cortès, and A. Brandwajn. Exploring landmark placement strategies for self-localization in wireless sensor networks. In *18th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Athens, Greece, September 2007.

[3] N. Bulusu, J. Heidemann, and D. Estrin. Gps-less low-cost outdoor localization for very small devices. *IEEE Personal Communications Magazine*, 7(5) :28–34, October 2000.

[4] Q. Cao and T. Abdelzaher. Scalable logical coordinates framework for routing in wireless sensor networks. *ACM Transactions on Sensor Networks*, 2(4) :557–593, November 2006.

[5] S. Capkun, M. Hamdi, and J-P. Hubaux. Gps-free positioning in mobile ad-hoc networks. In *34th Annual Hawaii International Conference on System Sciences (HICSS)*, volume Volume 9, page 9008, Maui, Hawaii, January 2001. IEEE Computer Society.

[6] Julien Cartigny. *Contributions à la diffusion dans les réseaux ad hoc*. PhD thesis, Université des Sciences et Technologies de Lille, December 2003.

[7] T. Clausen, P. Jacquet, C. Adjih, A. Laouiti, P. Minet, P. Muhlethaler, A. Qayyum, and

L. Viennot. Optimized link state routing protocol (olsr). RFC 3626 (Experimental), October 2003.

[8] Crossbow Technology. *Environmental Sensor Board MTS 420/400*, 2009.

[9] J. Desai and U. Tureli. Evaluating performance of various localization algorithms in wireless and sensor networks. In *18th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Athens, Greece, September 2007.

[10] K. Heurtefeux and F. Valois. Topology control algorithms : a qualitative study during the sensor networks life. In *Internatonal Conference on Mobile Adhoc and Sensor Systems (MASS)*, pages 1–7, Pisa, Italy, October 2007.

[11] B. Hofmann-Wellenhof, H. Lichteneeger, and J. Collins. *Global Positioning System : Theory and Practice*. Springer, 2001.

[12] Andy Hopper, Andy Harter, and Tom Blackie. The active badge system (abstract). In *Conference on Human factors in computing systems (CHI)*, pages 533–534, Amsterdam, The Netherlands, April 1993. ACM Press.

[13] L. Hu and D. Evans. Localization for mobile sensor networks. In *10th annual international conference on Mobile computing and networking (MobiCom)*, pages 45–57, Philadelphia, Pennsylvania, USA, September 2004. ACM Press.

[14] A. Magnani and K. Leung. Self-organized, scalable gps-free localization of wireless sensors. In *IEEE Wireless Communications and Networking Conference (WCNC)*, pages 3798–3803, Hong Kong, China, March 2007.

[15] S. Nawaz and S. Jha. Collaborative localization for wireless sensor networks. In *18th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Athens, Greece, September 2007.

[16] D. Niculescu and B. Nath. Ad hoc positioning system (aps) using aoa. In *22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, San Francisco, USA, April 2003.

[17] D. Niculescu and B. Nath. Dv based positioning in ad hoc networks. *Telecommunication Systems*, 22(1-4) :267–280, January 2003.

[18] P Rong and M.L. Sichitiu. Angle of arrival localization for wireless sensor networks. In *3rd Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, volume 1, pages 374–382, Reston, USA, September 2006.

[19] C. Saad, A. Benslimane, and Jean-Claude König. Mur : A distributed preliminary method for location techniques in sensor networks. In *2nd IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pages 61–68, Montréal, Canada, June 2006.

[20] Andreas Savvides, Chih-Chieh Han, and Mani B. Strivastava. Dynamic fine-grained localization in ad-hoc networks of sensors. In *7th annual international conference on Mobile computing and networking (MobiCom)*, pages 166–179, Rome, Italy, June 2001. ACM.

[21] P. Wan, K. Alzoubi, and O. Frieder. Distributed construction of connected dominating set in wireless ad hoc networks. In *21st Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, New York, NY, USA, June 2002.

[22] A. Ward, A.Jones, and A. Hopper. A new location technique for the active office. *IEEE Personal Communications*, 4(5) :42–47, October 1997.

[23] J. Wu and H. Li. On calculating connected dominating set for efficient routing in ad hoc wireless networks. In *3rd International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications (DIAL-M)*, pages 7–14, New York, NY, USA, August 1999. ACM Press.

Liste de publications liées à ce chapitre

Conférences & Workshops Internationaux

[1] **Karel Heurtefeux** and Fabrice Valois. Distributed Qualitative Localization for Wireless Sensor Networks. In *AD-HOC Networks and Wireless, 2008. IEEE 7th International Conference on*, Sophia Antipolis, France, September 2008.

Conférences françaises

[2] **Karel Heurtefeux** and Fabrice Valois. Localisation collaborative pour réseaux de capteurs. In *Colloque francophone sur l'ingénierie des protocoles. CFIP*, Les Arcs, France, March 2008.

Séminaires

[3] **Karel Heurtefeux** and Fabrice Valois. Self-Organisation for Wireless Sensor Networks and Self-Organisation applied to localization : QLoP. Northwestern Polytechnical University, Xi'an, China, October 2008.
[4] **Karel Heurtefeux** and Fabrice Valois. QLoP : Localisation collaborative dans les réseaux de capteurs. In *Journées ResCom 2008*, Marne-la-Vallée, France, February 2008.
[5] **Karel Heurtefeux** and Fabrice Valois. QLoP : Localisation collaborative dans les réseaux de capteurs. In *Journées EmSoC 2007*, Aussois, France, Octobre 2007.

Posters

[6] **Karel Heurtefeux** and Fabrice Valois. QLoP : Protocole de distance qualitative pour réseaux de capteurs. Laboratoire CITI, Lyon, France, March 2009.

5

QLoP appliqué au contrôle de topologie et au routage

Dans le chapitre 2, nous avons exposé les propriétés et l'utilité d'utiliser le contrôle de topologie : économie d'énergie, réduction des retransmissions dans les processus d'inondation, augmentation du débit, stabilisation du degré moyen, etc.

Dans le chapitre 4, nous avons présenté QLoP, un protocole qui permet de localiser les voisins d'un nœud en estimant leur distance **qualitativement**. QLoP n'utilise ni GPS, ni équipements spéciaux, ni mesures de RSS et permet néanmoins d'estimer avec efficacité l'appartenance d'un voisin à 3 différentes classes de proximité : le 1-voisinage logique, le 2-voisinage logique et le 3-voisinage logique.

Dans ce chapitre nous montrons qu'il est possible d'appliquer les fonctionnalités de QLoP au contrôle de topologie et au routage en environnement bruité. QLoP sera utilisé pour construire un RNG. C'est sur cette structure logique que nous acheminons les paquets de données afin de maximiser le rapport signal-sur-bruit (SNR) entre deux nœuds. Cette propriété sera mise en évidence dans le cas de réseaux de capteurs en environnement bruité.

5.1 Contrôle de topologie

Classiquement, pour construire une topologie logique basée sur l'élagage de liens, les nœuds ont besoin d'avoir une connaissance géographique de leurs voisins afin de connaître la distance entre eux [9, 7, 3]. Dans cette section, nous montrons qu'il n'est pas nécessaire d'avoir cette connaissance géographique précise pour construire une topologie logique efficace. QLoP est

capable de fournir un mécanisme d'élagage de liens proche de la version classique.

Nous présentons ici la structure RNG-QLoP, un protocole d'auto-organisation orienté élagage de liens, basé sur l'indice de proximité de QLoP plutôt que la distance euclidienne. Nous examinerons les propriétés de cette structure et la comparerons à la topologie initiale.

5.1.1 RNG-QLoP

À notre connaissance et à l'exception de [2], l'ensemble des protocoles d'auto-organisation orientés élagage de liens se basent sur la connaissance des informations géographiques pour sélectionner les liens les plus courts. Les études prennent comme hypothèse la facilité d'obtenir une mesure de distance entre deux nœuds d'un réseau en s'appuyant sur l'hypothèse de capteurs suréquipés : GPS, ensemble d'antennes pour calculer l'angle d'un signal reçu, synchronisation précise entre les capteurs, horloge interne extrêmement précise et stable, etc. Nous avons vu précédemment que ces hypothèses ne correspondaient pas aux équipements disponibles dans le domaine des réseaux de capteurs.

L'idée développée par [2] et présentée en détail dans le chapitre précédent est appliquée pour la construction d'un RNG et pour l'inondation dans un réseau ad hoc. Cependant, l'auteur considère une densité strictement uniforme et le réseau est modélisé sous la forme d'UDG. En outre, aucune étude sur les caractéristiques de la structure formée n'est proposée. De plus, nous avons montré précédemment que la métrique de QLoP était plus précise même dans le cas d'une distribution uniforme.

Nous avons introduit dans le chapitre 2 les principaux protocoles de contrôle de topologie : pour rappel, le RNG [9] est défini de la façon suivante : un lien entre deux nœuds u et v existe si et seulement si il n'existe pas de sommets w plus proches à la fois de u et de v.

Dans RNG-QLoP, la distance euclidienne nécessaire au protocole RNG original est remplacée par la métrique de QLoP, l'indice de proximité. Grâce à la connaissance du voisinage à 1 et 2 sauts, un nœud élague les liens les plus longs de la façon suivante :

$$\forall u, v \in V : (u, v) \in E' ssi \nexists w \in V : max(PI_u(w), PI_v(w)) < PI_u(v)$$

où $PI_u(v)$ est l'**indice de proximité** entre les deux nœuds u et v.

Nous rappelons ici la définition de l'indice de proximité :

$$PI_v(u) = (|V(v) \cap V(u)|) - \frac{max(|V(v)|, |V(u)|)}{2}$$

Tout comme la distance euclidienne, l'indice de proximité est symétrique :

$$PI_v(u) = (|V(v) \cap V(u)|) - \frac{max(|V(v)|, |V(u)|)}{2}$$
$$PI_u(v) = (|V(u) \cap V(v)|) - \frac{max(|V(u)|, |V(v)|)}{2}$$
$$PI_v(u) = PI_u(v)$$

Cela signifie que si u supprime le lien uv, v supprimera également le lien vu :
si $\nexists w \in V : max\left(PI_u(w), PI_v(w)\right) < PI_u(v)$

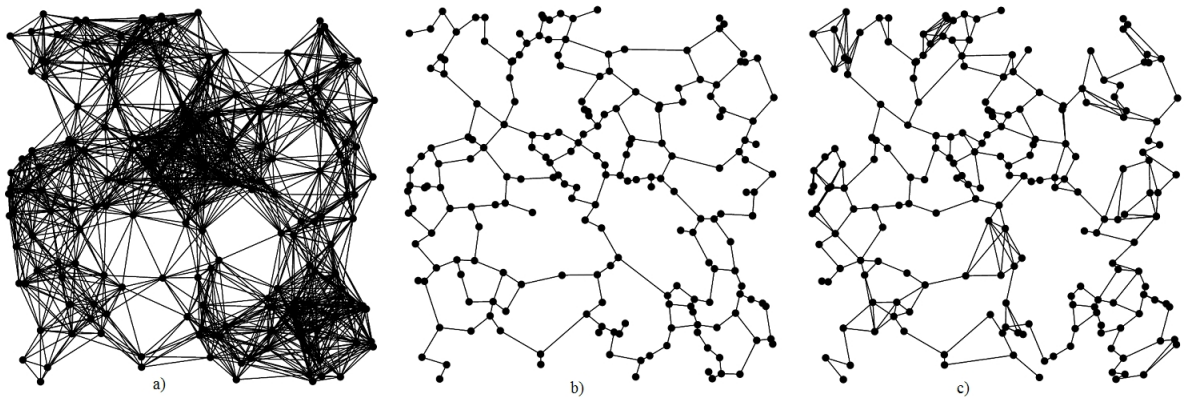

FIGURE 5.1 – a) Topologie physique, b) Topologie RNG avec informations géographiques (type GPS) c) Topologie RNG avec QLoP (RNG-QLoP)

alors $\nexists w \in V : max\,(PI_v(w), PI_u(w)) < PI_v(u)$

Le protocole RNG original garantit la connexité du réseau. Il en est de même pour une topologie RNG-QLoP : quelque soit la métrique d'estimation de la distance, l'élagage d'un lien entre deux nœuds u et v ne s'effectue que s'il existe un nœud w pour connecter u et v.

Le chapitre 2 et le chapitre 4 montrent qu'à la fois la topologie RNG et le protocole QLoP sont robustes et que les conséquences de la mort d'un ou plusieurs nœuds sont limitées et restent localisées.

La figure 5.1 montre le résultat sur une topologie particulière. Nous voyons que même s'il existe des imprécisions, la structure réussit néanmoins à élaguer la majorité des liens les plus longs.

Sur la figure 5.2, nous observons l'efficacité de l'élagage de liens effectué pour construire la structure logique en comptabilisant la longueur totale des liens sélectionnés : plus la sélection est fine et moins la longueur cumulée des liens sélectionnés est importante par rapport au graphe initial.

Afin d'étudier plus en détail les propriétés de notre nouvelle structure, nous mettons en perspective le degré moyen d'une structure RNG-QLoP face au degré moyen d'une structure RNG classique en fonction du degré physique de la topologie initiale. La figure 5.3 montre ce comparatif. Aux vues des études précédentes sur les performances de QLoP, il n'est pas étonnant de voir le degré moyen de la structure RNG-QLoP se rapprocher du degré d'une topologie RNG classique quand le degré moyen de la topologie initiale augmente. En effet, la précision de QLoP augmentant avec le degré physique, la structure RNG construite avec l'indice de proximité va comporter moins d'imprécision et va ainsi pouvoir élaguer plus de liens.

Cette analyse met en évidence deux points : les performances de l'algorithme RNG-QLoP sont très proches d'un RNG utilisant le positionnement GPS et plus la densité est importante et meilleures sont les performances de RNG-QLoP. Cela est dû aux propriétés de QLoP : davantage d'information de voisinage conduit à une amélioration de sa précision.

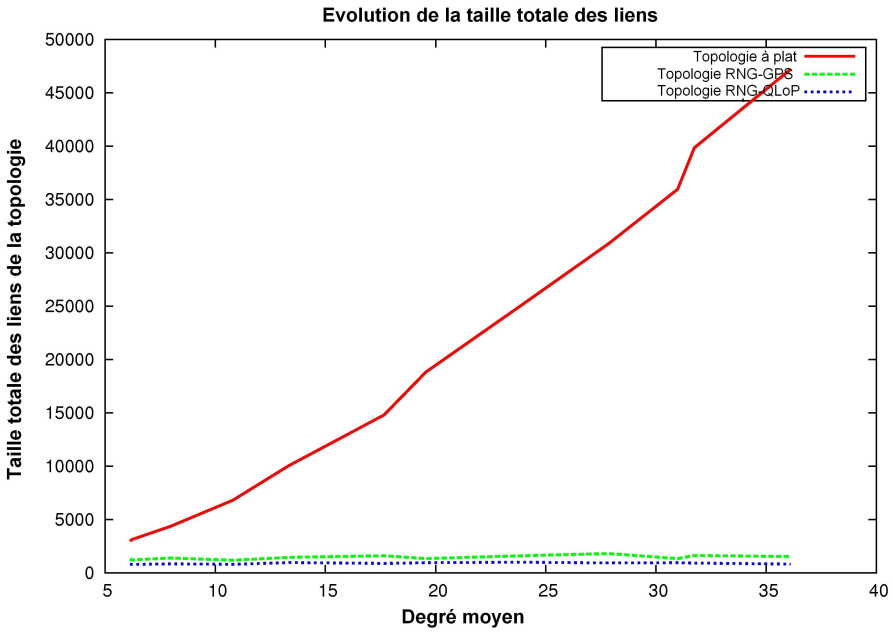

FIGURE 5.2 – Évolution de la longueur moyenne des liens de la topologie

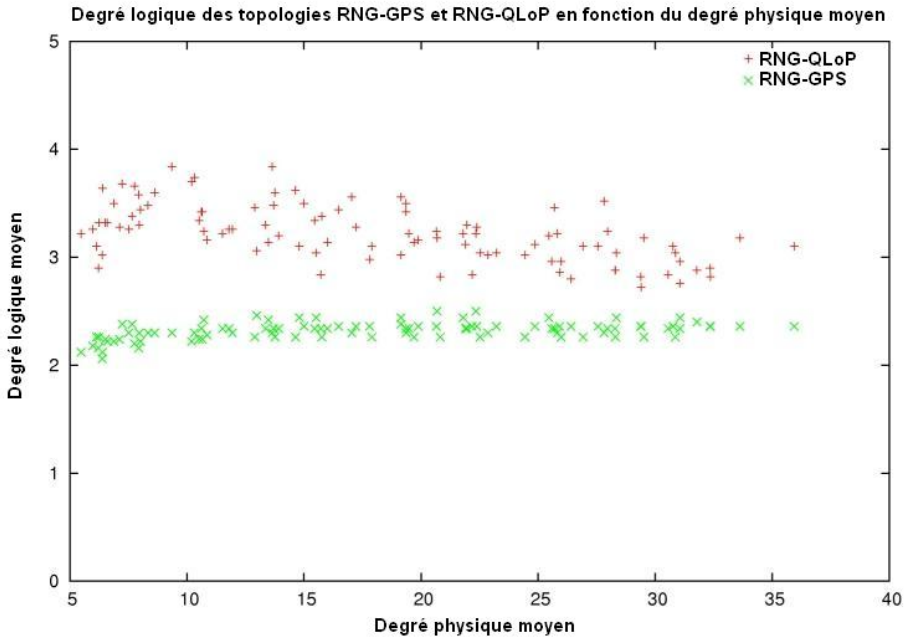

FIGURE 5.3 – Évolution du degré logique moyen des structures RNG-QLoP et RNG classique en fonction du degré physique

5.2 Routage en environnement bruité

5.2.1 Routage pseudo-DSR

Le Dynamic source routing (DSR) [6] est un protocole de routage pour réseaux mobiles et ad hoc standardisé par l'IETF [5] et qui peut être utilisé dans les réseaux de capteurs [10]. DSR est un protocole réactif, c'est-à-dire que le processus de découverte des routes d'un nœud source à une destination est mis en oeuvre uniquement au moment où la source en fait la demande. Il se distingue en cela des protocoles de routage pro-actif qui vont maintenir des informations de routage même en l'absence de trafic. Le protocole DSR est composé de deux mécanismes :

- le mécanisme de découverte de routes : un nœud source S va inonder le réseau avec un paquet de requête de route (RREQ). Chaque paquet contient un champ « route », initialement vide. À chaque retransmission, un nœud ajoute son identité dans le champ. Quand le nœud destination D reçoit ce paquet RREQ, il renvoie de la même manière un paquet de réponse (RREP) contenant le champ de la route parcourue par le paquet RREQ. Les nœuds intermédiaires, qui relaient ces messages RREQ et RREP, mettent à jour leur table de routage vers le nœud D ou S.
- le mécanisme de maintenance de routes : grâce à ce mécanisme un nœud source est capable de détecter si une route vers un nœud destination d n'est plus valide en raison de la cassure d'un lien. Quand ce mécanisme indique qu'une route n'est plus valide, le nœud source utilise une autre route vers d s'il en possède une autre ou il lance une découverte de route. Chaque nœud retransmettant utilisant une route doit se faire confirmer la réception du paquet de données par le nœud suivant. S'il ne reçoit pas de confirmation, il émet un message d'erreur de route (RERR) vers le nœud source.

Dans notre environnement de simulation, les routes possèdent une date d'expiration et doivent être rafraîchies de façon périodique. Pour étudier les impacts du routage sur structure virtuelle en environnement bruité, nous appliquons un routage pseudo-DSR sur une topologie RNG et sur une topologie RNG-QLoP (voir figure 5.4).

Pour l'ensemble des simulations nous utilisons uniquement 4 types de paquets : les paquets `hello` comprenant la table de voisinage du nœud source, les paquets RREQ et RREP et les paquets de données. Le format des paquets est donné en figure 5.5.

5.2.2 Modélisation du canal radio

Tous les résultats présentés proviennent de simulations. Nous avons utilisé le simulateur WSNet [1] dont l'originalité est de modéliser de façon très précise la couche physique. La portée d'une interface radio est basée sur la définition d'un seuil du rapport signal-sur-bruit (SNR) noté $\bar{\gamma}_{lim}$.

$$\begin{aligned} l_{ij} &: \Omega^2 \mapsto B = \{0,1\} \\ (x_i, x_j) &\mapsto l(x_i, x_j) = \begin{cases} 1 & \text{if } \bar{\gamma}_{ij} \geq \bar{\gamma}_{lim} \\ 0 & \text{else} \end{cases} \end{aligned} \tag{5.1}$$

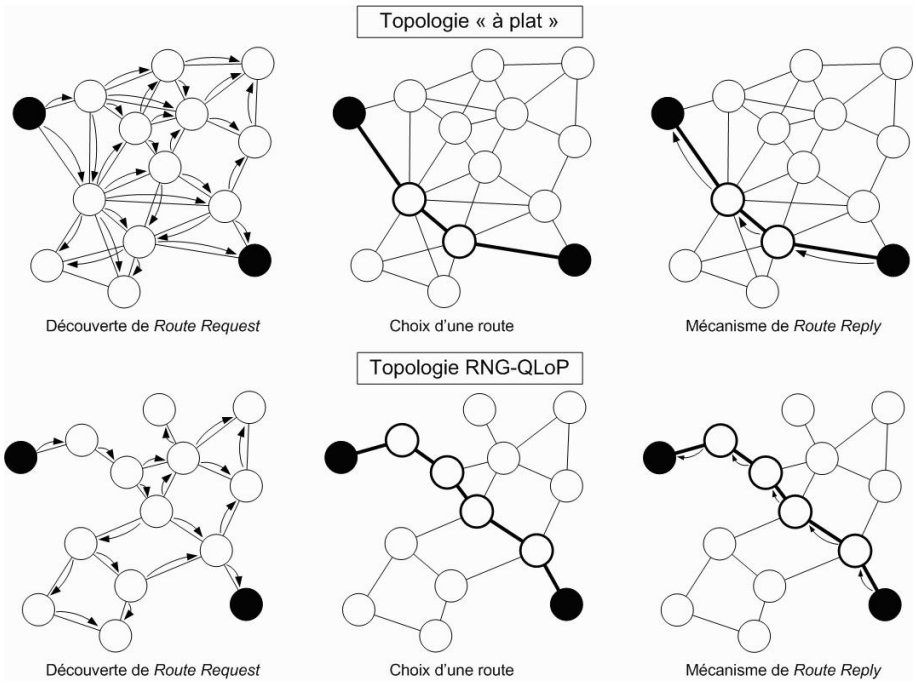

FIGURE 5.4 – Pseudo-DSR sur une topologie à plat et une topologie élaguée avec RNG-QLoP

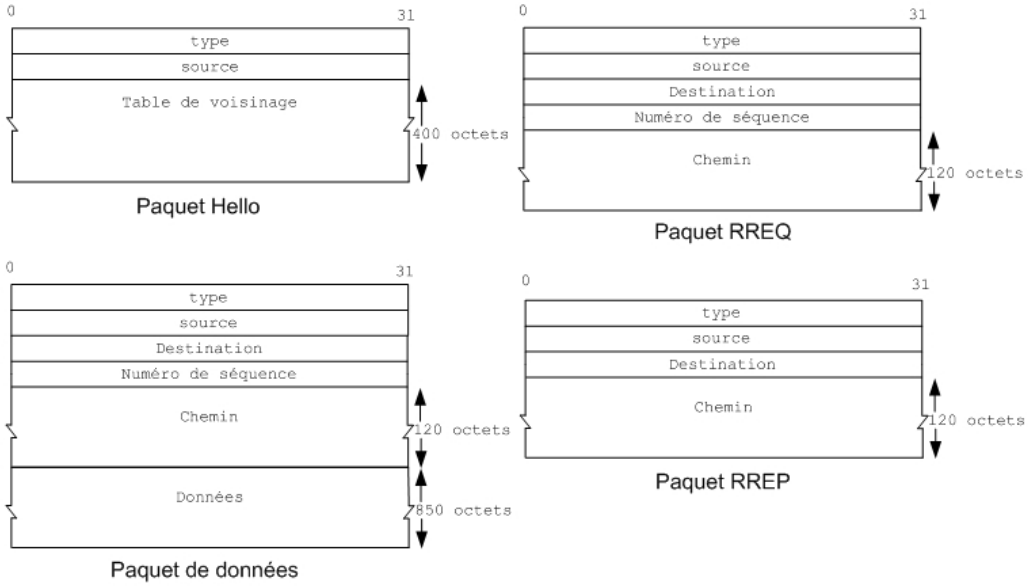

FIGURE 5.5 – Format des paquets utilisés

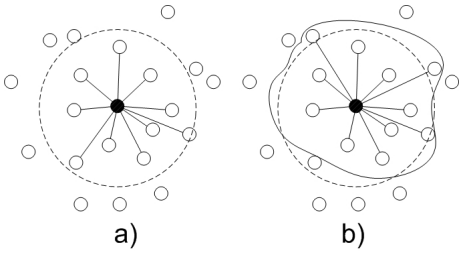

FIGURE 5.6 – Influence du modèle radio sur le voisinage : a) graphe de disques unitaires, b) liens avec path-loss et shadowing

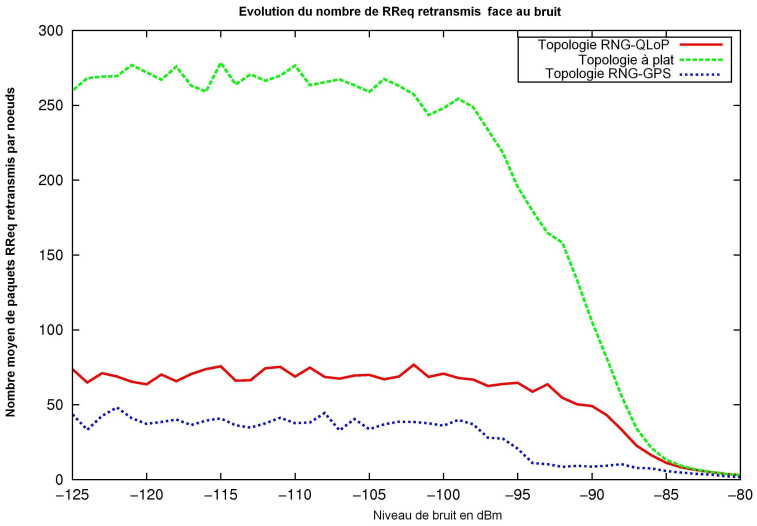

FIGURE 5.7 – Évolution du nombre de paquets RREQ retransmis par nœuds

Afin de modéliser les interférences, WSNet remplace le SNR par le SINR, le rapport signal sur bruit plus interférences SINR, qui peut être calculé de la façon suivante :

$$\bar{\gamma}_{ij} = h_{ij} \cdot \frac{P_i}{N_j + \sum_{k \neq i,j} h_{kj} \cdot P_k} \tag{5.2}$$

où h_{ij} est l'affaiblissement (ou path-loss) et P_i et N_j sont respectivement la puissance de transmission et le niveau de bruit. Il est important de noter que ce modèle réaliste conduit à une instabilité du voisinage et des zones de couvertures déformées comme illustrées figure 5.6. Nous déployons, de manière aléatoire et uniforme, 100 nœuds et nous faisons varier la puissance de transmission pour augmenter le degré moyen. La couche MAC utilisée est la couche IEEE 802.11 en mode DCF. Chaque nœud est considéré comme immobile.

5.2.3 Impacts sur le routage

Les résultats sont obtenus avec une puissance de transmission constante et une variation du bruit ambiant. Nous relevons une rupture de la connexité du réseau à partir d'un bruit de -90dBm. Nous comparons les performances des différentes topologies suivantes :

- Topologie physique (ou à plat) : les nœuds communiquent avec leurs voisins physiques

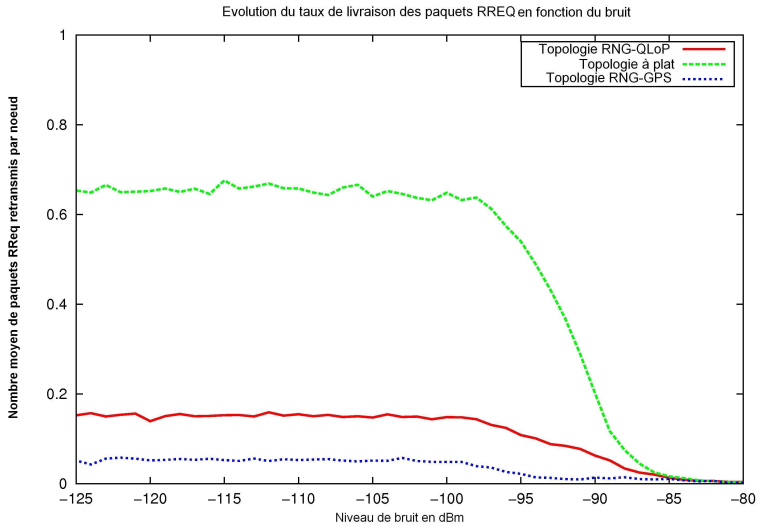

FIGURE 5.8 – Évolution du taux de livraison des paquets RREQ

- RNG-QLoP : chaque nœud construit localement une structure RNG en utilisant QLoP pour déterminer la localisation de ses voisins
- RNG-GPS : chaque nœud construit localement une structure RNG en utilisant la position réelle de ses voisins.

Il est important de souligner que RNG-QLoP et RNG-GPS ne modifient pas la propriété de connexité intrinsèque du réseau.

La figure 5.7 montre le nombre de retransmissions de paquets RREQ. Ces paquets sont essentiels pour la découverte de route d'une source à une destination. Dans un routage de type DSR, le réseau est inondé. Nous observons une grande disparité entre le flooding sur une topologie logique et celui sur une topologie à plat. Dans le cas d'une topologie à plat, et quand le bruit ambiant est faible, presque 3 fois plus de paquets sont relayés par chaque nœud à travers le réseau. Il en résulte une surcharge du réseau et donc une augmentation de la probabilité de collisions. La seconde conséquence est le gaspillage d'énergie.

Dans ce cas, les topologies RNG-QLoP et QLoP-GPS réduisent fortement le nombre de retransmissions de paquets RREQ.

Cependant, cette réduction de trafic a un impact sur la probabilité d'atteindre une destination (voir figure 5.8). Nous observons un taux de livraison des paquets RREQ plus bas pour le routage sur les topologies logiques RNG-QLoP et RNG-GPS. Quand un nœud destination reçoit un paquet RREQ, il retourne, en unicast, un paquet de réponse (RREP). Ce paquet est également sensible aux interférences et aux collisions. Cela signifie que seules quelques routes sont construites. Sur une topologie à plat, un nombre plus important de routes est construit mais elles sont moins robustes. Ces routes sont basées sur des liens opportunistes, non robustes dans le temps. Sur les topologies RNG-QLoP et RNG-GPS la construction des routes est basée sur des liens radio moins volatils.

Pour les résultats suivants, les nœuds envoient des données de façon périodique à un nœud destination choisi aléatoirement. Nous observons à la figure 5.9 le taux de livraison. Nous avons

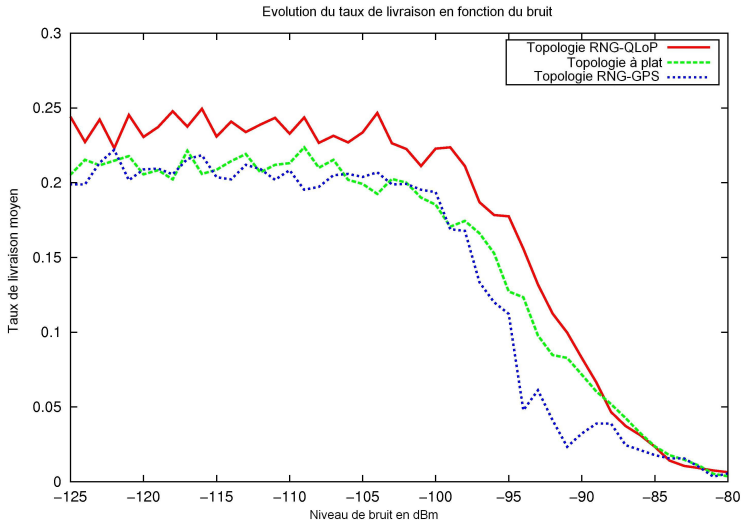

FIGURE 5.9 – Taux de livraison en fonction du niveau de bruit

vu précédemment que le processus de découverte de routes était différent selon la topologie : alors que de nombreuses routes sont construites sur une topologie à plat, le protocole de routage sur RNG-QLoP et RNG-GPS construit une route seulement si elle est stable. La topologie RNG-QLoP obtient le meilleur taux de livraison. Même dans le cas d'un fort bruit parasite, le routage sur cette topologie permet de transmettre des paquets à la destination. Ici, la taille (1ko) des paquets ne permet que très peu de transmissions opportunistes. Le routage sur la topologie à plat est donc peu efficace. Concernant la topologie RNG-GPS, l'élagage trop sévère des liens empêche les communications au lieu de les renforcer.

Nous pouvons remarquer que dans un réseau où les communications sont nombreuses et où le bruit est important, seulement un nombre limité de paquets de données arrive effectivement à destination. La distance euclidienne qui sépare la source de la destination influe beaucoup sur cette probabilité de succès : plus la distance est importante plus le taux de livraison est faible. Nous voyons sur la figure 5.10 quelle distance couvrent les paquets reçus et l'évolution de cette distance en fonction du bruit. L'impact du bruit et des interférences influe, de manière très importante, sur la diffusion des paquets de données. Il est très difficile pour un noeud d'envoyer ses données à une distance plus grande que 20m dans le cas d'une topologie RNG-QLoP (le diamètre du graphe est de 140m environ). Cela signifie que même quand le réseau est considéré connexe, les paquets ne parviennent pas à franchir, en moyenne, une certaine distance. Ici, la topologie logique, même si elle réduit la possibilité de longs sauts, augmente au final, la distance moyenne franchissable par un paquet. Cela confirme le fait que la probabilité de transmissions opportunistes utilisant des liens longs est négligeable.

Une des différences entre le routage sur topologie logique et sur topologie classique est la longueur des routes construites en termes de nombre de sauts entre la source et la destination. Les topologies RNG-QLoP diminuent le nombre de liens dans le réseau, pour s'appuyer majoritairement sur les liens les plus courts et donc, nous l'avons vu, sur les liens les moins sensibles au bruit. Dans le cas des liens les plus longs, la probabilité de succès d'une transmission est

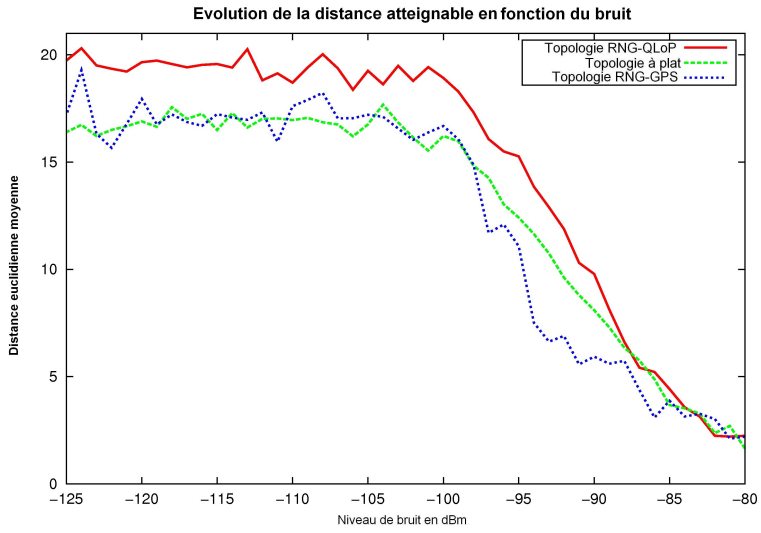

FIGURE 5.10 – La distance face au bruit

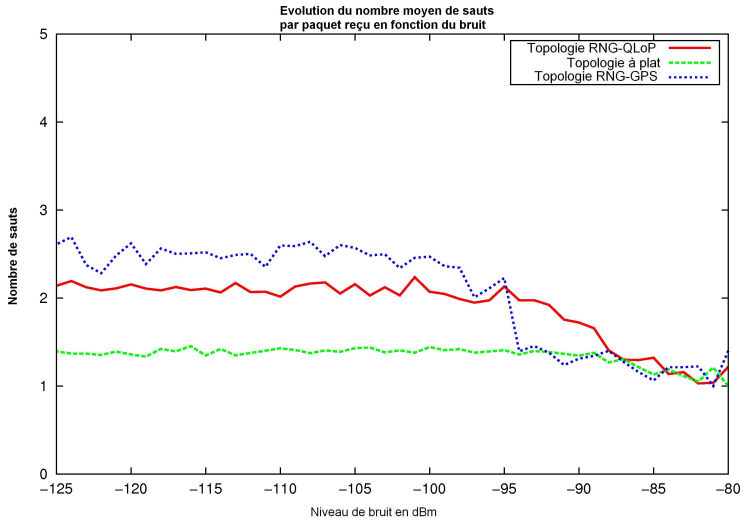

FIGURE 5.11 – Nombre de sauts parcourus par paquet reçu

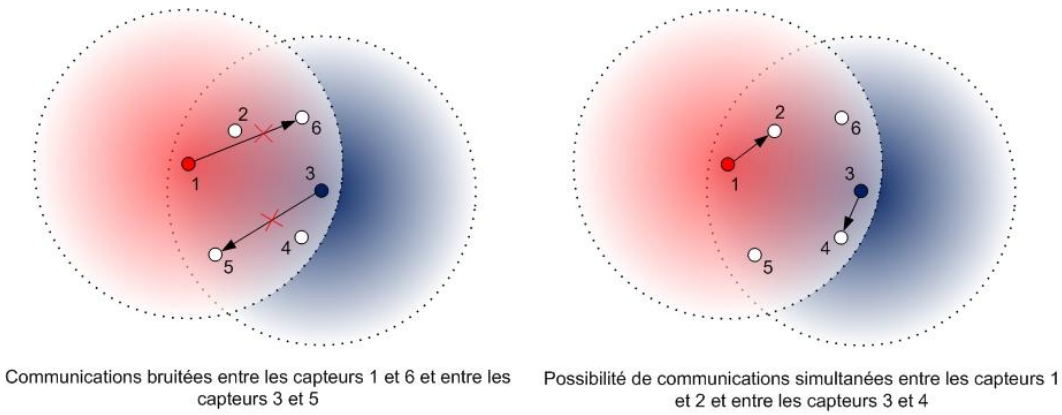

FIGURE 5.12 – Communications concurrentes

extrêmement faible et il est donc souhaitable de contourner un lien fragile par plusieurs liens plus courts et plus robustes. C'est ce que réalise RNG-QLoP (voir figure 5.11).

5.3 Consommation énergétique

QLoP n'utilise ni GPS, ni aucune spécificité matérielle particulière. La consommation d'un récepteur GPS n'est pas négligeable au regard de la consommation d'un capteur et si la recherche pour réduire la consommation des puces GPS existe, cela nécessite un équipement et des protocoles supplémentaires [8]. QLoP utilise uniquement des paquets `hello` ou « beacon » pour informer son voisinage de sa présence et pour transmettre son voisinage direct. En cela, QLoP est compatible avec les protocoles d'endormissement et d'auto-organisation qui sont également basés sur ce type de mécanisme. Il est donc important de souligner que dans la plupart des cas, QLoP utilise une information déjà disponible sans consommer d'énergie supplémentaire. Le calcul de $PI_A(B)$ (indice de proximité du noeud B calculé par le noeud A) est une simple intersection de 2 ensembles. La complexité de cet algorithme est donc en O(n+m) où n est la cardinalité du voisinage de A et m la cardinalité du voisinage de B. QLoP est donc extrêmement peu consommateur en énergie même lorsque la densité est très importante.

5.4 État de l'art

Le routage en environnement bruité est peu traité. À notre connaissance, il n'existe aucune étude qui traite de routage sur topologie logique, sans information géographique et dans un environnement physique réaliste.

[4] donne 18 raisons pour expliquer le compromis entre utiliser beaucoup de petits sauts et utiliser peu de grands sauts pour le routage. Cet article admet le besoin de routes stable dans le routage pro-actif mais ne traite que des liens opportunistes dans le cas d'un routage géographique. Il élude ainsi le problème de découverte de routes et le problème de l'inondation.

[11] explore également le compromis entre les stratégies de routage : grands sauts ou petits sauts en regardant l'aspect énergétique. Il détermine à quelle distance il est souhaitable de faire

un saut supplémentaire au regard de la consommation énergétique. Cet article ne se concentre cependant uniquement sur le lien physique et quand les noeuds sont capables d'ajuster leur puissance d'émission.

Dans ces deux articles, le cas de communications concurrentes n'est pas traité. Dans le cas de communications simultanées, quatre noeuds proches pourront échanger leurs données avec succès (voir figure 5.12).

5.5 Conclusion et discussion

Nous avons présenté dans ce chapitre une structure d'élagage de liens utilisant avec succès le protocole QLoP (RNG-QLoP). Elle est basée sur le protocole de localisation qualitative (QLoP) utilisant uniquement des informations localisées sans GPS. Les propriétés de cette structure sont proches de la structure RNG utilisant des informations géographiques. Nous utilisons cette topologie logique pour proposer un routage pseudo-DSR efficace pour les réseaux de capteurs en environnement bruité. Cette stratégie favorise les chemins utilisant de petits sauts et donc les noeuds relais ayant un rapport signal-sur-bruit plus important. La topologie RNG-QLoP réduit le coût de l'inondation pour la découverte de route, le nombre de communications sur le médium radio et construit de routes plus robustes. Nous croyons que RNG-QLoP est un bon compromis entre l'élagage de lien trop drastique de GPS basé sur des positions réelles (RNG-GPS) et une absence de contrôle de topologie.

La topologie RNG classique ou la topologie RNG-QLoP ne sélectionne le voisinage qu'au niveau 3 de la couche OSI. Le protocole de gestion d'accès au canal, lui, fonctionne toujours en fonction du voisinage physique. Dans le cas d'une couche MAC 802.11, le mécanisme d'écoute du canal avant l'envoi d'une trame (*carrier sense*), s'effectue sur le voisinage physique. Elle est utile pour diminuer les collisions. Mais, selon nous, la topologie RNG et l'élimination des voisins les moins robustes permettent justement de transmettre une trame en parallèle (voir figure 5.12).

C'est cette influence de la couche MAC dans les performances de notre topologie que nous étudierons dans le prochain chapitre.

Bibliographie

[1] Elyes BenHamida, Guillaume Chelius, and Jean-Marie Gorce. Scalable versus accurate physical layer modeling in wireless network simulations. In *22nd Workshop on Principles of Advanced and Distributed Simulation (PADS)*, pages 127–134, Washington, DC, USA, June 2008. IEEE Computer Society.

[2] Julien Cartigny. *Contributions à la diffusion dans les réseaux ad hoc*. PhD thesis, Université des Sciences et Technologies de Lille, December 2003.

[3] GK. Ruben Gabriel and Robert R. Sokal. A new statistical approach to geographic variation analysis. *Systematic Zoology*, 18 :259–278, 1969.

[4] M. Haenggi and D. Puccinelli. Routing in ad hoc networks : a case for long hops. *IEEE Communications Magazine*, 43(10) :93–101, October 2005.

[5] D. Johnson, Y. Hu, and D. Maltz. The dynamic source routing protocol (dsr) for mobile ad hoc networks for ipv4. RFC 4728 (Experimental), February 2007.

[6] D.B. Johnson. Routing in ad hoc networks of mobile hosts. In *Workshop on Mobile Computing Systems and Applications*, pages 158–163, Santa Cruz, California, USA, December 1994.

[7] Ning Li, Hou J.C., and Sha L. Design and analysis of an mst-based topology control algorithm. *IEEE Transactions on Wireless Communications*, 4 :1195–1206, May 2005.

[8] D. Raskovic and D. Giessel. Battery-aware embedded gps receiver node. *Mobile and Ubiquitous Systems : Networking & Services, 2007. MobiQuitous 2007. Fourth Annual International Conference on*, 1 :1–6, August 2007.

[9] G. Toussaint. The relative neighbourhood graph of a finite planar set. *Pattern Recognition*, 12 :261–268, 1980.

[10] Tao Yang, Makoto Ikeda, Giuseppe De Marco, Leonard Barolli, Arjan Durresi, and Fatos Xhafa. Routing efficiency of aodv and dsr protocols in ad-hoc sensor networks. In *28th International Conference on Distributed Computing Systems Workshops (ICDCSW)*, pages 66–71, Beijing, China, June 2008. IEEE Computer Society.

[11] Ruifeng Zhang and J.-M. Gorce. Optimal transmission range for minimum energy consumption in wireless sensor networks. *Wireless Communications and Networking Conference (WCNC'08)*, 1 :757–762, April 2008.

Liste de publications liées à ce chapitre

Conférences & Workshops Internationaux

[1] **Karel Heurtefeux** and Fabrice Valois. Distributed Localization Protocol for Routing in a Noisy Wireless Sensor Network In *5th International Workshop on Localized Communication and Topology Protocols for Ad hoc Networks (LOCAN)*, WuYiShan, China, December 2009.

Conférences françaises

[2] **Karel Heurtefeux** and Fabrice Valois. Localisation distribuée pour routage en environnement bruité dans les réseaux de capteurs. In *Colloque francophone sur l'ingénierie des protocoles. CFIP*, Strasbourg, France, October 2009.

6

Interactions entre l'auto-organisation et les protocoles MAC

6.1 Motivations

La couche gérant l'accès au canal (MAC), parce qu'elle définit la façon dont chaque nœud accède au médium radio, a un impact important sur les performances d'un réseau sans fil multi-saut. Le chapitre 5 présentait un moyen de limiter le routage aux liens les plus robustes au bruit. Cependant, cette sélection qualitative du voisinage par le biais du protocole QLoP et du protocole RNG ne s'applique qu'au niveau réseau de la pile protocolaire (i.e. au contrôle de topologie et au routage des paquets). Nous prenons comme hypothèses l'absence de contrôle de puissance (mise en place complexe, peu robuste aux modifications de topologie et aux interférences). Et en l'absence de contrôle de puissance, le partage du canal radio, par le biais d'un protocole MAC de type CSMA/CA, continue d'être effectué avec l'ensemble des voisins *physiques* du nœud. En d'autres termes, un capteur voulant accéder au médium rentre en concurrence avec l'ensemble des autres capteurs à portée radio qu'ils soient ou non dans son voisinage logique.

Les mécanismes d'évitement de collisions contenus dans les protocoles MAC vont empêcher deux capteurs proches de communiquer alors même que, selon les configurations, ils peuvent transmettre avec succès (voir figure 6.1). Il nous apparaît donc pertinent d'étudier la possibilité d'éliminer ces mécanismes d'esquive de collisions pour améliorer les performances telles que le délai et la durée de vie du réseau. Nous proposons une couche MAC adaptative basée sur l'indice de proximité de QLoP après une étude des performances de la couche MAC Aloha. Nous montrerons dans cette étude préalable l'importance de la topologie dans les performances.

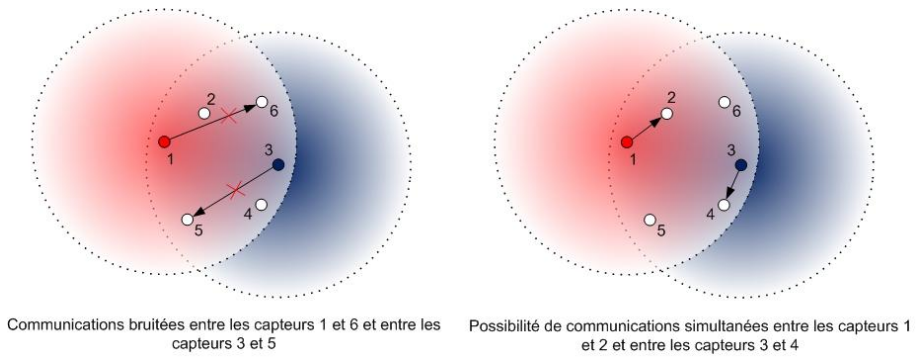

FIGURE 6.1 – Influence des mécanismes d'esquive de collisions en termes de performances

6.2 État de l'art

L'organisation internationale de la normalisation (ISO) a proposé le modèle de communication entre systèmes informatiques OSI (Open Systems Interconnection). La volonté de ne pas favoriser un industriel, la prise en compte de l'hétérogénéité des équipements, et la possibilité d'une évolution et d'une adaptation facile ont nécessité l'adoption de règles communes de communication et de coopération entre les équipements. Traditionnellement donc, la pile protocolaire utilisée dans le monde des réseaux est organisée suivant un modèle en couches superposées l'une sur l'autre. Chaque couche va assurer de manière indépendante une partie des fonctionnalités nécessaires à la communication entre les entités du réseau.

Dans ce contexte, la couche MAC a pour objectif de définir une politique d'accès au médium radio afin que les capteurs puissent transmettre leurs données en tentant de réduire les collisions avec d'autres données envoyées simultanément à proximité. Un ensemble de mécanismes a été conçu afin d'éviter que les nœuds à portée radio ne communiquent en même temps.

Dans ce chapitre, nous nous limitons à l'étude des couches MAC à accès probabiliste. Nous ne considérons pas le multiplexage temporel (Time Division Multiple Acces ou TDMA) ni le multiplexage en fréquence (Frequency Division Multiple Acces ou FDMA). Le multiplexage permet de partager une même ressource entre plusieurs utilisateurs : le multiplexage temporel répartit le temps d'utilisation du canal entre les différents utilisateurs, tandis que le multiplexage fréquentiel leur alloue des espaces de fréquences. Cependant, cette répartition du temps de parole ou des fréquences nécessite une entité centralisée et donc un processus préalable (création de clusters, élection, etc.).

Le « carrier sense » consiste, pour un capteur, à écouter le canal radio avant d'émettre. Il existe 3 types de *carrier sense* :

- **1-persistant**. Chaque capteur prêt à envoyer sa donnée écoute le canal radio. Si celui-ci est occupé, il continue l'écoute et envoie sa trame quand le médium se libère [6].
- **p-persistant**. Si le canal est occupé, le capteur continue l'écoute jusqu'à sa libération puis envoie sa trame avec une probabilité p. Si la trame n'est pas envoyée (probabilité $1 - p$), il attend un temps défini et recommence le même processus [6].
- **non persistant**. Dans le cas où le canal est occupé, le capteur reporte son émission un temps aléatoire et recommence l'écoute jusqu'à la libération du canal [6].

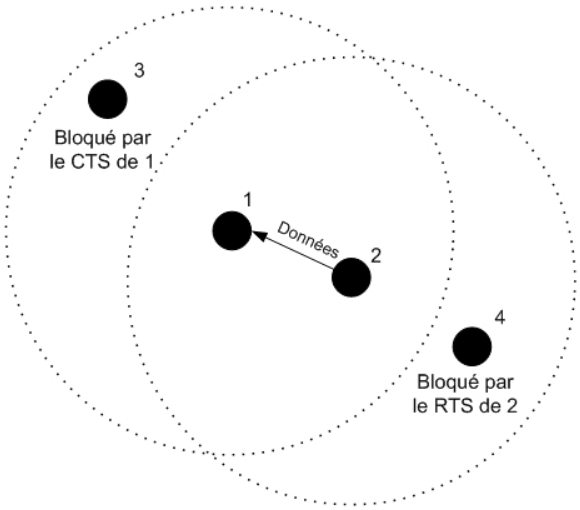

FIGURE 6.2 – Mécanisme RTS/CTS

Contrairement aux réseaux filaires, il est complexe de détecter une collision quand elle a lieu. Le mécanisme *RTS/CTS* consiste en une « poignée de main » avant la transmission : un capteur voulant transmettre une trame à un autre capteur commence par transmettre un paquet « *Request To Send* » (RTS). Le nœud destination répond avec un paquet « *Clear To Send* » (CTS). Tous les autres capteurs du voisinage recevant une de ces 2 trames ne doivent pas envoyer de paquets durant une période donnée. Cette période, le « *Network Allocation Vector* » (NAV), est incluse dans les trames RTS et CTS. Ce mécanisme permet de résoudre le problème des stations cachées (voir figure 6.2)

Enfin, l'envoi d'un paquet d'accusé de réception (ACK) permet de retransmettre une trame en cas de non-réception de cet accusé.

De nombreuses études montrent que le choix du protocole MAC va influer sur les performances de la couche réseau, en particulier sur les performances du routage [15, 12, 2].

[15] explique l'impact possible de la couche MAC sur les protocoles de routage prenant comme métrique la longueur du chemin en nombre de sauts. Dans cette étude, les auteurs montrent comment le mécanisme de contrôle de congestion de la couche MAC va empêcher la découverte de la route la plus courte par le protocole DSR ou comment ce même mécanisme peut générer des paquets *Route Error* intempestifs.

[12] étudie les effets du choix d'une couche MAC particulière sur un protocole de routage pour réseau ad hoc mobile. Cette étude se concentre sur 3 protocoles de routage (Wireless Routing Protocol [8], Fisheye State Routing Protocol [9] et AODV [10]) et 4 protocoles MAC (Carrier Sense Multiple Access (CSMA), Multiple Access Collision Avoidance (MACA) [5], Floor Acquisition Multiple Access (FAMA) [4] et 802.11 DCF [13]). CSMA va uniquement utiliser le mécanisme de *carrier sense*. MACA utilise le même mécanisme, mais définit des paquets de contrôle *Request-To-Send* (RTS) et *Clear-To-Send* (CTS). FAMA est une amélioration de MACA dans le sens où ce protocole va écouter le canal avant d'envoyer une trame RTS. Enfin, le protocole 802.11 DCF ajoute l'emploi de paquets d'acquittement et de retransmissions en

cas de collision. Nous le voyons, les versions de la couche MAC présentées correspondent à la progression d'un même protocole à différents stades de son évolution. Cependant, contrairement à l'intuition, les auteurs montrent que ces améliorations n'améliorent (ni ne dégradent) de façon significative les performances des deux premiers protocoles de routage dans le cas de réseaux mobiles multisaut. Seul le protocole AODV est légèrement plus sensible que les autres et subit une légère amélioration avec le protocole 802.11 DCF.

Dans [2], les auteurs comparent les performances (délai, taux de livraison, *overhead* et débit) de deux protocoles de routage DSR et AODV. Ils étudient leur comportement face à différents paramètres : mobilité, charge de trafic, taille du réseau mais également l'influence de la couche MAC 802.11 dans l'*overhead* (i.e. la fraction du trafic utilisé pour le trafic de contrôle). Ils constatent que AODV génère beaucoup plus de paquets de contrôle que DSR au niveau routage mais que ces paquets sont principalement de type RREQ, donc envoyés en mode *broadcast* (i.e. sans accusé de réception ni mécanisme de « poignée de main » du canal (RTS/CTS)). Le trafic de contrôle de DSR, quant à lui, est constitué principalement de paquets RREP ou RERR envoyés en mode *unicast* (i.e. avec accusé de réception et mécanisme de type RTS/CTS). La gestion différentiée des paquets *unicast* ou *broadcast* par la couche MAC entraîne donc une diminution significative du trafic utile pour le protocole DSR.

[16] isole pas moins de 12 mécanismes de gestion du canal (*carrier sense*, RTS/CTS, ACK, etc.) présents dans différents protocoles MAC (CSMA, FAMA, IEEE 802.11 DCF, etc.) et déterminent les effets de ces mécanismes sur les performances du réseau. L'objectif est de déterminer quelle combinaison fonctionne le mieux pour le *User Datagram Protocol* (UDP) et le *Transfer Control Protocol* (TCP), deux protocoles de niveau 4 dans le modèle en couches OSI. Les simulations apportent une série d'enseignements :

- le *carrier sense* seul est préférable pour le protocole UDP.
- le mécanisme RTS/CTS va améliorer l'équité en partageant plus équitablement le canal radio entre les différents nœuds.
- La combinaison de mécanismes CSMA/CA/RTS/CTS/ACK utilisée dans 802.11 est celle qui donne les meilleures performances d'équité, de débit sur les différentes topologies étudiées et avec TCP.

[11] montre cependant que le mécanisme de « poignée de main » *RTS/CTS* peut entraîner la congestion du réseau en raison de *faux blocages*. Un *faux blocage* définit le blocage d'un nœud du réseau après la réception d'un paquet RTS ou CTS alors même qu'aucun nœud ne transmet ou ne reçoit de trame à proximité. Les auteurs montrent que ce phénomène peut se propager à travers le réseau et conduire au faux blocage de nombreux capteurs. La figure 6.3 illustre ce phénomène. Avant l'envoi de données du nœud 2 au nœud 1, l'échange des messages RTS/CTS bloque les nœuds dans le voisinage de 1 et de 2 pendant la durée de la communication. L'objectif du mécanisme est rempli : les communications entre 1 et 2 ne sont pas perturbées. Si le nœud 4 envoie un paquet RTS à 3 à ce moment-là, celui-ci sera dans l'incapacité de répondre puisque bloqué par le RTS du nœud 2. Néanmoins, l'envoi d'un paquet RTS par le nœud 4 a pour conséquence de bloquer la communication des nœuds du voisinage de 4. Le nœud 5 est donc bloqué alors même qu'il est loin de la communication entre 1 et 2. Ce processus peut potentiellement s'étendre à travers tout le réseau.

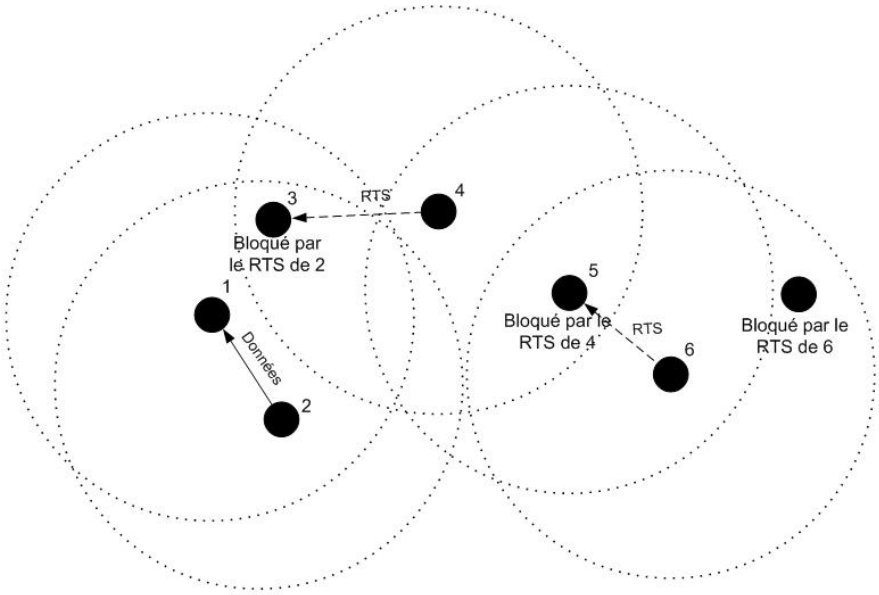

FIGURE 6.3 – Blocage en chaîne avec le mécanisme RTS/CTS

L'aspect contradictoire de la couche MAC dans un réseau de capteurs est qu'elle doit limiter le plus possible les communications simultanées dans la zone d'un signal et, dans le même temps, permettre le plus de communications simultanées dans d'autres régions du réseau.

6.3 Les protocoles MAC pour réseaux de capteurs

De nombreux articles proposent des protocoles MAC spécialement conçus pour réseaux de capteurs. Le principal souci de ces protocoles est de limiter la consommation énergétique de la couche MAC. En effet, il existe de nombreuses sources de gaspillage d'énergie. [3] en relève quatre principales, exception faite des collisions :

- La réception et le décodage de paquets destinés à un autre nœud.
- L'envoi et la réception de paquets de contrôle.
- L'écoute inutile du canal radio.
- La transmission d'un message alors que le capteur de destination est déjà occupé.

Les principaux défis à relever dans les réseaux de capteurs sont différents de ceux rencontrés dans les réseaux sans fil classiques. La sauvegarde de l'énergie est plus importante que l'équité ou la latence.

Ces problématiques ont inspiré plusieurs protocoles. [18] propose S-MAC, un protocole MAC inspiré de [14] et CSMA/CA qui va alterner périodes de sommeil et périodes d'écoute du canal. En début de chaque période d'écoute, les capteurs s'échangent des paquets SYNC dans lesquels se trouve leur temps de parole où planning qui leur permettra de transférer des données grâce à un mécanisme de RTS/CTS. Cependant, le passage à l'échelle de ce protocole va être problématique. En effet, si la taille du voisinage augmente, S-MAC va devoir maintenir les plannings de chacun de ses voisins ainsi que multiplier les tours de resynchronisation. Ce fonctionnement pose

également des difficultés dans le cas d'une couche radio réaliste où la probabilité de transmission peut être faible.

Le protocole TMAC [17] est une amélioration de S-MAC. Ce protocole réduit le temps de la fenêtre d'écoute. Si le canal est inoccupé après l'échange des paquets SYNC et le temps dédié aux paquets RTS-CTS, le capteur bascule en mode sommeil alors que le protocole S-MAC restait en mode éveil de telle façon à avoir une période d'éveil de taille constante. Dans le cas d'une charge de trafic faible, T-MAC permet de réduire considérablement les temps de réveil. Il possède en revanche les mêmes défauts que S-MAC concernant le passage à l'échelle.

Le protocole DMAC [7] va avoir la particularité de fonctionner dans le cas d'un trafic convergecast (i.e. la communication se fait des nœuds du réseau vers un unique nœud). Durant la période de réception de chaque nœud, les fils de ce nœud vont avoir une période de transmission. L'ordonnancement est effectué selon le niveau dans l'arbre d'agrégation. L'inconvénient de ce protocole est qu'il nécessite à la fois la construction d'un arbre d'agrégation préalable mais également une synchronisation entre les nœuds.

En définitive, les protocoles MAC dédiés aux réseaux de capteurs, se concentrent sur la réduction de l'écoute inutile du canal radio et sur l'intégration de périodes d'endormissement dans les mécanismes classiques d'accès au canal sans en proposer de nouveaux. La suite de ce chapitre étudie, en revanche, les méthodes d'esquive de collision. C'est pour cette raison que nous prendrons les protocoles d'accès au canal classiques.

Dans ce chapitre nous allons étudier l'influence de la couche MAC sur les performances de la couche réseau dans le cadre d'un réseau de capteurs multisaut. Nous nous intéressons tout particulièrement au protocole Aloha qui n'utilise aucun mécanisme d'évitement de collision, ni aucun paquet de contrôle. Nous étudierons ses propriétés théoriques et les mettrons en rapport avec les performances obtenues par simulation. Par la suite, nous mettons en perspectives ces propriétés par rapport à deux autres protocoles d'accès au canal : CSMA/CA et CSMA. Le premier utilisant les mécanismes *carrier sense*, *RTS/CTS* et *ACK*, le second uniquement le *carrier sense*.

6.4 Le protocole Aloha

Le protocole Aloha a été développé à l'université de Hawaï en 1970 [1]. Le principe de ce protocole est simple : chaque nœud du réseau partage en même temps une même bande de fréquence pour communiquer. Il n'existe ni mécanisme de synchronisation entre les nœuds ni écoute préalable du canal. Cela implique qu'il n'y a pas d'allocation de ressources pour une ou plusieurs entités du réseau.

Les performances du protocole Aloha en termes de débit utile souvent mises en avant sont celles-ci :

Soit t la durée d'une trame. Pour qu'il n'y ait pas de possibilité de collision, il ne faut qu'aucune trame ne soit émise par un capteur à proximité pendant une durée égale à 2t (voir figure 6.4). En prenant G le nombre moyen de trames émises par durée de trames et si l'on suppose que le nombre des trames émises pendant la durée d'émission d'une trame obéit à la loi de Poisson, alors la probabilité que k trames soient émises pendant la durée d'une trame est

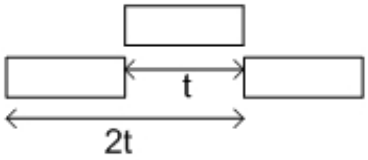

FIGURE 6.4 – Probabilité de collision de deux trames

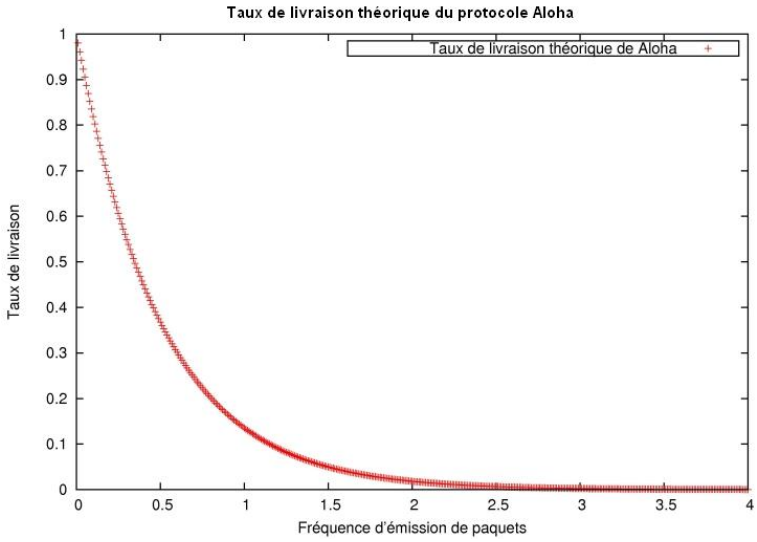

FIGURE 6.5 – Aloha : Taux de livraison théorique

égale à :

$$P(k) = \frac{G^k e^{-G}}{k!}$$

En supposant que le nombre de nœuds partageant le canal soit grand, la probabilité qu'il n'y ait aucun paquet émis pendant une durée t est égale à :

$$P(0) = e^{-G}$$

La probabilité qu'il n'y ait pas de paquets émis pendant 2t est donc :

$$P(0)^2 = e^{-2G}$$

En théorie donc, lorsque la fréquence d'envoi des trames est faible, le taux de livraison est proche de 1 (voir figure 6.5). Le canal n'est pas saturé et la probabilité de collision est donc faible. Quand la fréquence d'envoi augmente, la probabilité de collision augmente. Comme le montre la figure 6.6, le débit utile maximum est atteint lorsque la fréquence d'envoi des paquets est égale à 0.5, c'est-à-dire qu'en moyenne un paquet est envoyé tous les 2t (t étant le temps nécessaire à émettre une trame). À cette fréquence, seuls 36% des paquets sont émis sans collision. Pour une fréquence d'envoi importante, le nombre de paquets reçus sans collision est très faible car le nombre de collisions devient tellement important que le nombre de paquets

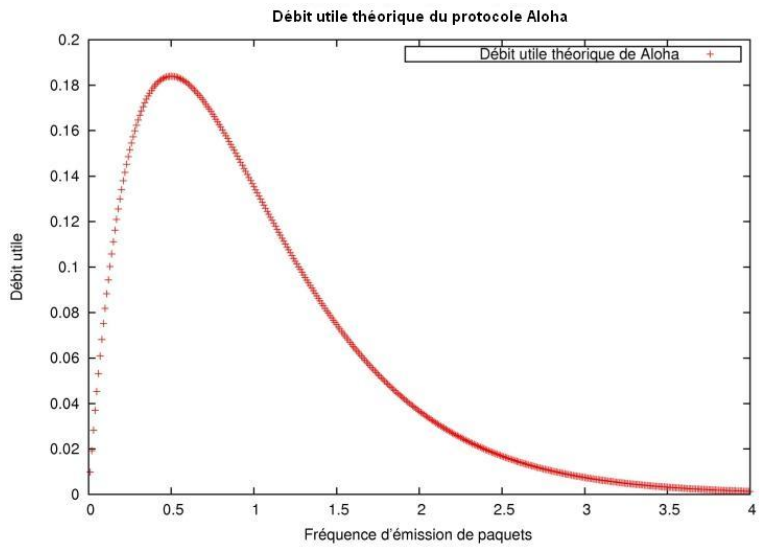

FIGURE 6.6 – Aloha : Débit utile théorique

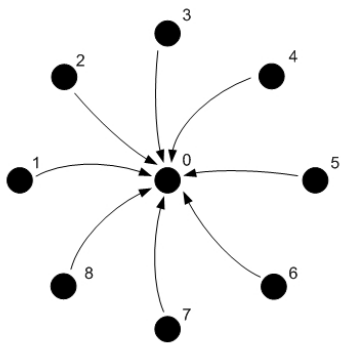

FIGURE 6.7 – Aloha : Accès concurrent de 8 nœuds équidistants du nœud destination

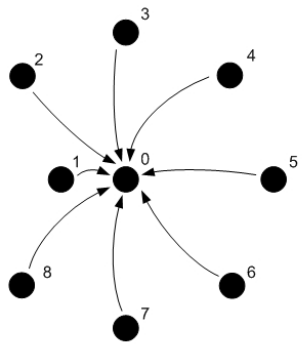

FIGURE 6.8 – Aloha : Accès concurrent de 7 nœuds équidistants du nœud destination et d'un nœud proche

reçus devient très faible.

Cependant, en prenant en compte les réalités de la couche physique, il n'y a pas nécessairement destruction des messages lorsqu'une collision à lieu. Même dans le cas de signaux destructifs, si deux messages se chevauchent sur une faible fraction du message, ils pourront être reconstitués grâce au code correcteur d'erreur compris dans le message (voir figure 6.9).

6.5 Hypothèses de simulation

Nous nous plaçons dans des conditions de simulation avec une couche physique réaliste. De la même façon que dans le chapitre précédent, nous avons utilisé le simulateur WSNet avec une modélisation réaliste du rapport signal sur bruit plus interférences, dont le détail du calcul est donné par l'équation 5.2. La topologie est telle que 8 capteurs accèdent de manière

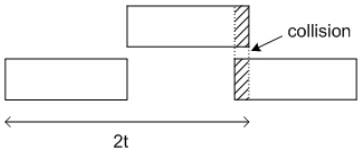

FIGURE 6.9 – Collision non nécessairement destructrice

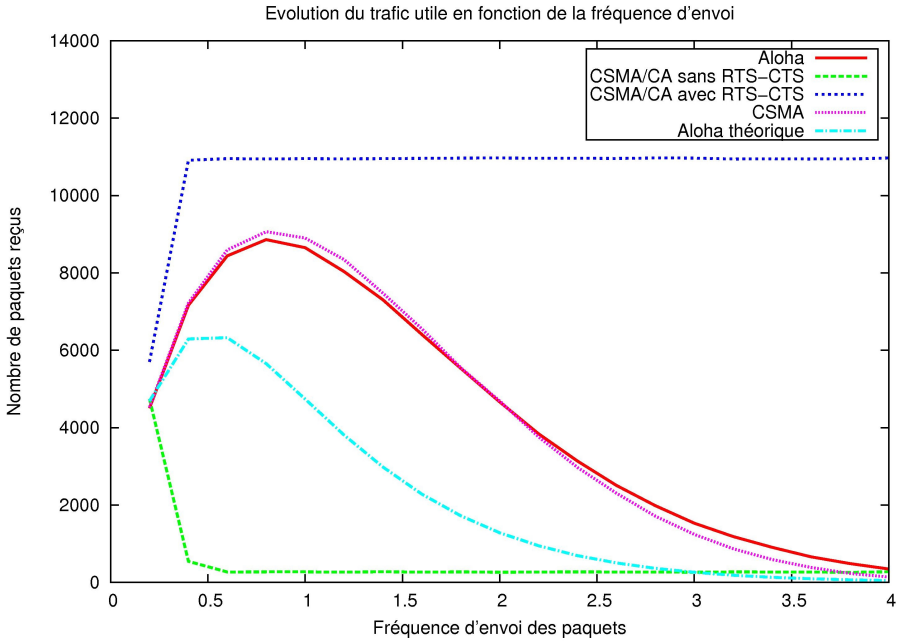

FIGURE 6.10 – Cas a) : débit utile du réseau en fonction des protocoles MAC

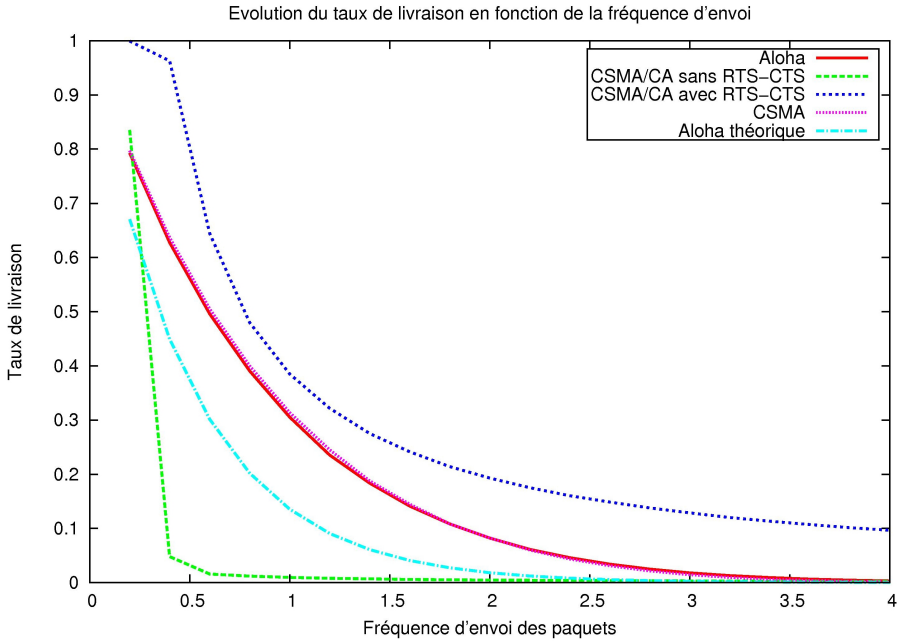

FIGURE 6.11 – Cas a) : taux de livraison du réseau en fonction des protocoles MAC

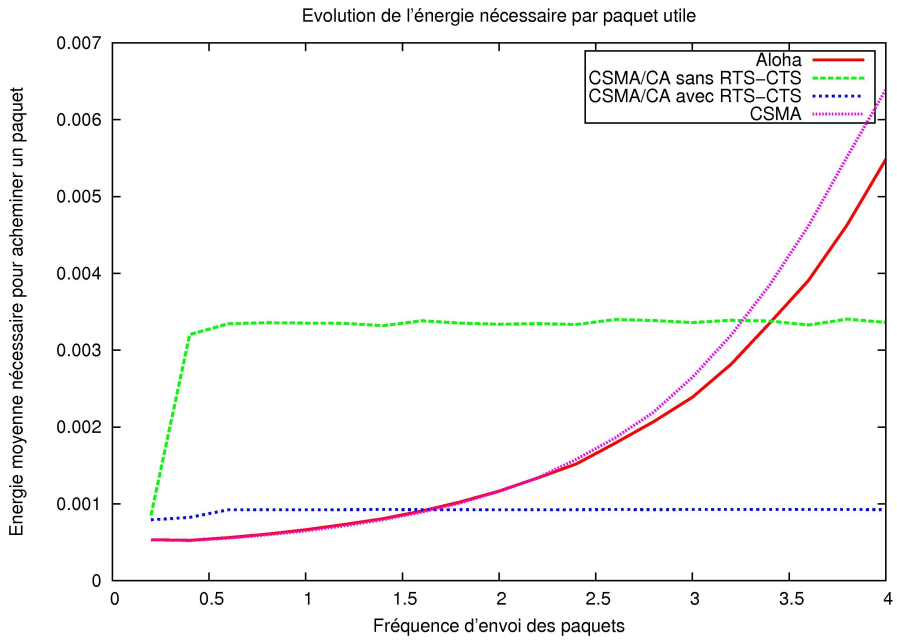

FIGURE 6.12 – Énergie moyenne nécessaire pour acheminer un paquet utile

concurrente à un même capteur. Les 8 capteurs sources sont placés à une même distance du capteur destination 0. La topologie est donnée par la figure 6.7. Dans le cadre de ce scénario, la figure 6.10 montre le débit utile des 4 couches MAC suivantes : Aloha, CSMA, CSMA/CA sans RTS/CTS et CSMA/CA avec RTS/CTS. La fréquence d'envoi des paquets est exprimée en nombre moyen de trames envoyées sur le réseau par durée de transmission d'une trame. La fréquence 1 signifie qu'un paquet, en moyenne, est envoyé sur le réseau toutes les 4 ms, temps de transmission d'une trame de données. Les paquets sont envoyés de manière indépendante selon un processus poissonnien. Ces résultats sont mis en parallèle avec le débit théorique d'Aloha.

6.6 Performances de Aloha

Quand plusieurs capteurs équidistants envoient des données à un même capteur, les performances en termes de débit sont très dépendantes du choix de la couche MAC. Le mécanisme RTS/CTS permet un partage du canal efficace en allouant celui-ci pour un capteur précis. Il permet d'écouler un trafic constant. Lorsque la fréquence d'envoi devient importante, les autres protocoles ne peuvent réduire les probabilités de collisions, le réseau est saturé. Dans le cas du protocole CSMA/CA, lorsqu'un paquet n'est pas acquitté (i.e. la trame de données ou d'accusé de réception n'a pas été reçu) le nœud retransmet le message. Ce mécanisme, en ajoutant aux collisions des retransmissions et des accusés de réception, accélère, de fait, la saturation du réseau. Ces comportements entraînent en conséquence une diminution importante du taux de livraison (voir figure 6.11). Les protocoles Aloha et CSMA possèdent les mêmes caractéristiques. Le protocole Aloha ne possède aucun mécanisme d'évitement des collisions. En revanche, le protocole CSMA possède un mécanisme de *carrier sense* mais utilisé seul il ne permet d'éviter

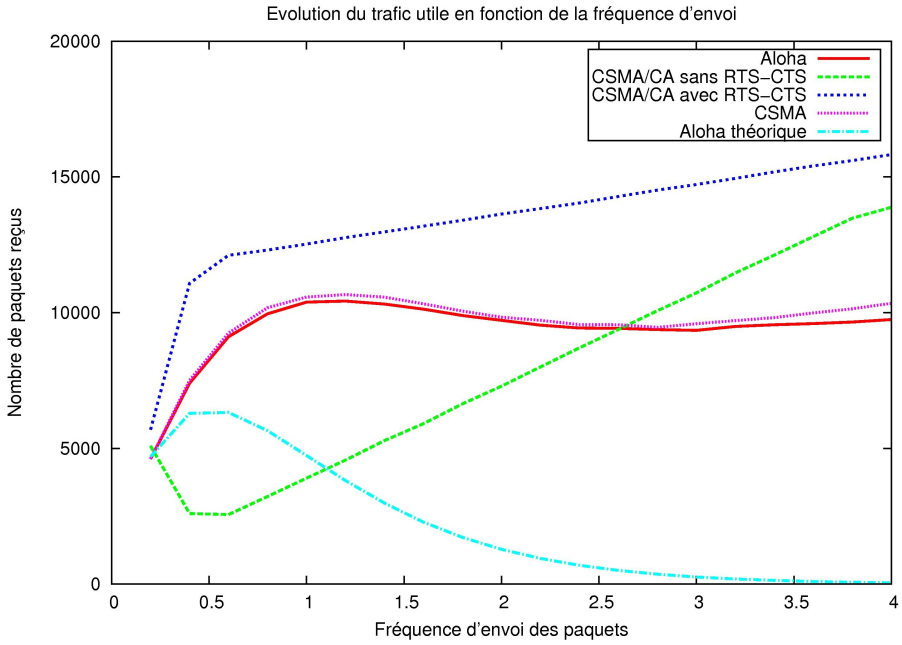

FIGURE 6.13 – Cas b) : débit utile du réseau en fonction des protocoles MAC

qu'une fraction infime des collisions. Cependant, la simplicité de ces protocoles permet de ne pas surcharger le réseau avec des paquets de contrôle. En dépit d'un nombre de collisions élevé, ils parviennent à écouler bien plus de trames à destination que le protocole CSMA/CA sans RTS/CTS. On peut noter également que le débit utile ou le taux de livraison du protocole Aloha se situe très au-delà du débit utile ou du taux de livraison théorique même s'il en garde l'allure générale.

Si nous observons l'énergie nécessaire pour transmettre un paquet à destination pour les quatre protocoles d'accès au canal dans cette même configuration (voir figure 6.12), nous remarquons que malgré une utilisation la plus importante de paquets de contrôle, le CSMA/CA avec mécanisme RTS/CTS est le plus efficace. En effet, en réduisant le nombre de collisions et de retransmissions, elle permet d'acheminer un message avec un coût fixe, certes plus important, mais qui devient relativement faible au regard du taux de livraison des paquets.

Le scénario suivant place un des 8 capteurs source à une distance plus proche que les autres (voir figure 6.8). Dans ce scénario, le nœud proche 1 va parvenir à transmettre ses paquets à destination malgré la transmission dans le même temps de paquets d'autres sources. La proximité des deux capteurs 0 et 1 permet au lien entre eux d'être robuste aux collisions. Avec Aloha ou CSMA comme couche MAC, alors que le débit utile chutait à partir d'un paquet par durée de trame, il reste ici pratiquement constant alors même que la fréquence d'envoi des paquets augmente (voir figure 6.13). Ici, cependant presque uniquement le capteur 1 va écouler ses données, il va être à l'origine de jusqu'à plus de 90% du trafic. La figure 6.15 met en évidence cette iniquité dans le partage du médium radio. Ces résultats illustrent parfaitement l'importance du SiNR dans la probabilité de succès lors de transmissions simultanées.

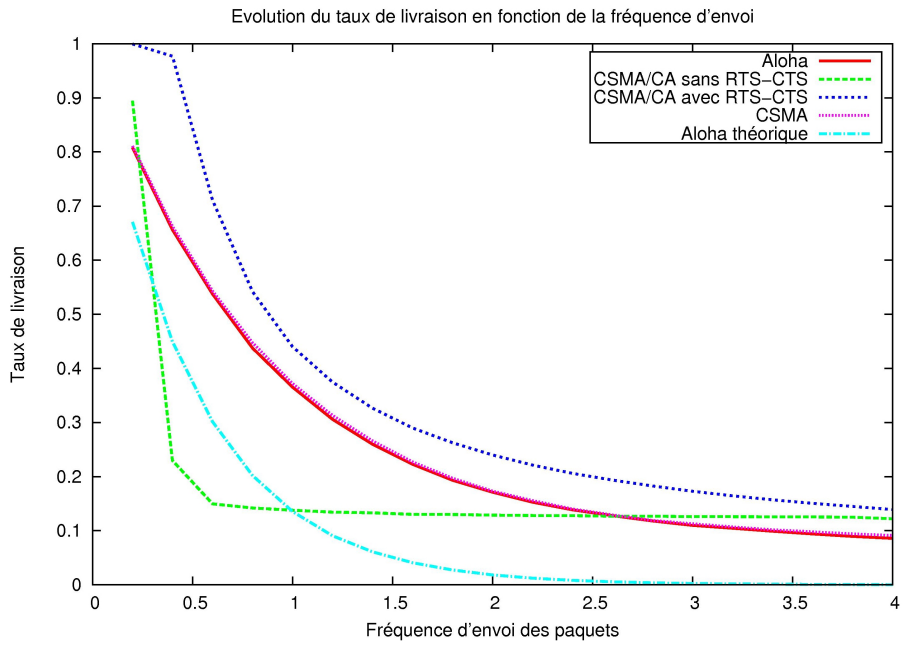

FIGURE 6.14 – Cas b) : taux de livraison du réseau en fonction des protocoles MAC

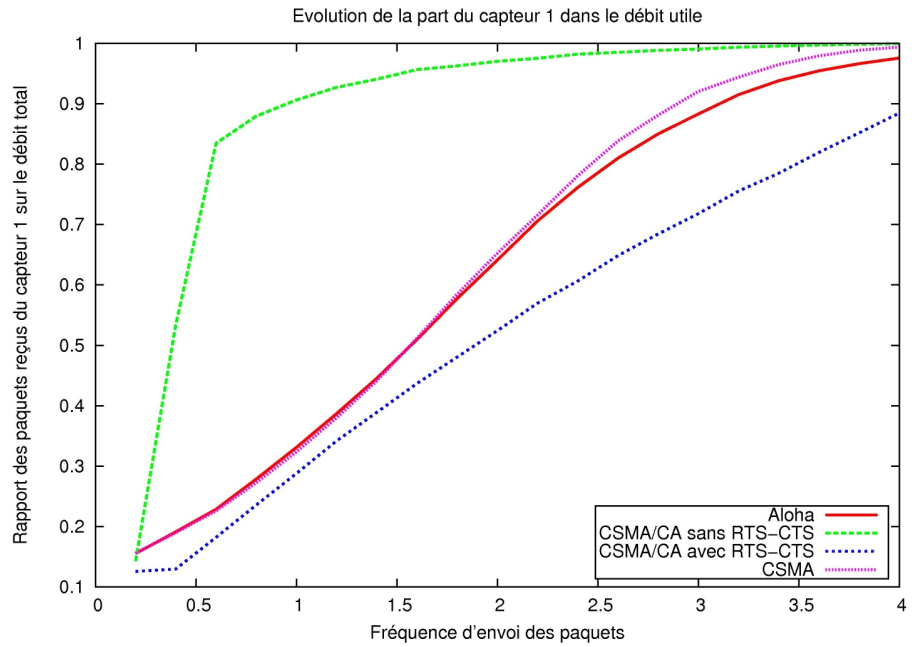

FIGURE 6.15 – Cas b) : seul le capteur 1 proche de la destination est capable de transmettre avec succès

6.7 L'influence de la topologie

L'hypothèse généralement prise est que si deux capteurs communiquent en même temps, une collision apparaît et les deux messages sont perdus. Cette hypothèse n'est pas nécessairement vraie pour deux raisons : les trames possédant des codes correcteurs d'erreurs, il est possible de décoder les messages si seulement une fraction des bits est erronée. La seconde raison est que, d'un point de vue physique, un message va être perdu si son rapport SiNR devient défavorable. Ce n'est pas toujours le cas si les deux signaux reçus n'ont pas la même puissance. En sélectionnant les liens les plus courts au niveau 3 de la couche OSI, nous avons montré que le routage était moins perturbé par le bruit. Cette propriété peut, selon nous, être étendue au niveau du protocole d'accès au canal pour améliorer le débit total du réseau.

Nous partons de l'hypothèse qu'il n'existe aucune synchronisation ni aucune division fréquentielle du canal : les capteurs communiquent sur un seul canal radio, sans calendrier commun. La synchronisation dans un réseau de capteurs pose de nombreuses difficultés :

- Passage à l'échelle : les chemins multisauts nécessitent une synchronisation sur l'ensemble des nœuds traversés par un paquet
- Capacité de calcul, mémoire et énergie limitées : l'échange de messages ou le calcul de la dérive d'horloge indispensable pour la synchronisation ne sont pas nécessairement compatibles avec les contraintes matérielles des réseaux de capteurs.

En définitive, nous ne considérons que les protocoles MAC à accès aléatoire.

Nous avons étudié les conséquences du choix de la couche MAC sur la couche réseau en termes de taux de livraison (i.e. rapport entre paquets arrivés à destination et paquets envoyés), débit utile (i.e. nombre de paquets de données arrivés à destination) et consommation énergique. Pour ce faire, nous avons déterminé un ensemble de scénarios. L'objectif est double : le premier but est de déterminer un compromis entre mécanismes d'évitement de collisions, potentiellement coûteux en énergie, et les performances réseau. En d'autres termes, dans quelles conditions le coût supplémentaire qu'imposent les mécanismes d'évitement de collision est-il nécessaire dans un réseau de capteurs ? Le deuxième but est de montrer que la topologie du réseau à une influence non négligeable sur les performances. Le choix d'un nœud proche (et donc d'un lien plus fiable) dans une route permet de protéger la communication des collisions destructrices. Sans modifier la puissance d'émission, nous montrerons qu'il est possible d'augmenter les performances réseau grâce à une topologie logique.

L'évolution de la couche MAC étudiée a été dans le sens de la réduction de la probabilité d'un envoi simultané de messages sur le même canal au prix d'une augmentation des paquets de contrôle (RTS, CTS, ACK) et donc, d'une perte d'énergie, ou de la latence (*carrier sense*, *backoff* aléatoire, etc.). Notre objectif n'est pas de diminuer encore cette probabilité, mais d'en réduire les conséquences. Nous pensons qu'en contrôlant la topologie, i.e. en favorisant l'utilisation de liens plus robustes aux interférences, nous réduirons le nombre de collisions entraînant la perte des paquets envoyés.

Nous avons vu, sur un scénario simple à un saut, que la topologie était d'une importance capitale dans les performances réseau. Nous établissons un ensemble de 6 scénarios décrits par les figures 6.17 et 6.18. La modélisation du canal radio est réaliste. On ne peut donc garantir, comme dans un déploiement réel, qu'un capteur ne va jamais interférer avec un autre.

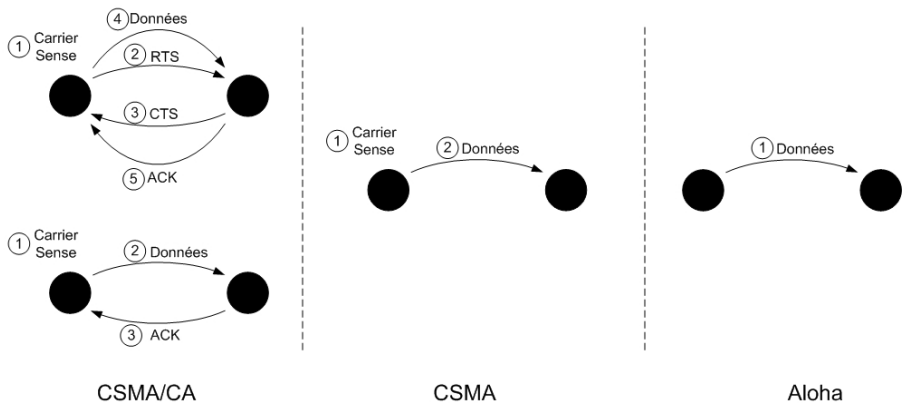

FIGURE 6.16 – Détails des 3 couches MAC utilisées : CSMA/CA, CSMA et Aloha.

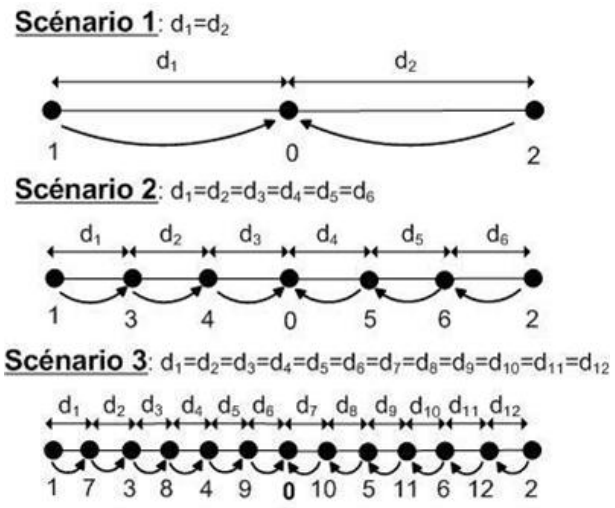

FIGURE 6.17 – Scénario 1, 2 et 3 : accès de deux nœuds sources vers un même nœud destination par l'intermédiaire de 0, 2 ou 5 nœuds intermédiaires

Cependant, la puissance d'émission est telle que les capteurs généralement en contention avec les capteurs source 1 et 2 sont respectivement les capteurs 7, 3, 8, 4, 9, 0 et 10 et les capteurs 12, 6, 11, 5, 10, 0 et 9. Nous étudions, grâce à ces scénarios, le compromis entre fiabilité du lien radio et couche MAC. En d'autres termes, est-il plus efficace d'utiliser des liens peu fiables avec une couche MAC fiable (par le biais de paquets d'acquittement et de retransmissions) ou, à l'inverse, favoriser les liens plus fiables avec une couche MAC simple (choix de liens courts et d'une couche MAC de type Aloha) ? C'est dans cette optique que nous étudions les interactions entre couche MAC et performances réseau dans les scénarios qui suivent.

Dans le scénario 1, les deux capteurs sources sont éloignés du capteur destination de telle façon qu'ils soient à la limite de leur puissance d'émission. Cela signifie :

- les deux capteurs sources ne sont pas à portée de communication
- la couche physique étant modélisée de façon réaliste, le lien entre les capteurs sources et le capteur destination est intermittent et donc peu fiable.

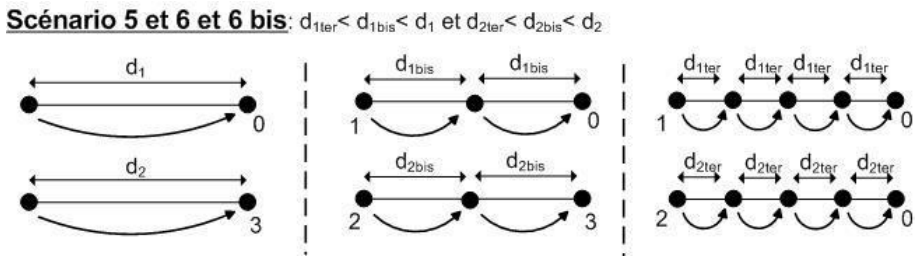

FIGURE 6.18 – Scénarios 4, 5 et 6 : transmissions de 2 nœuds sources vers 2 nœuds destinations

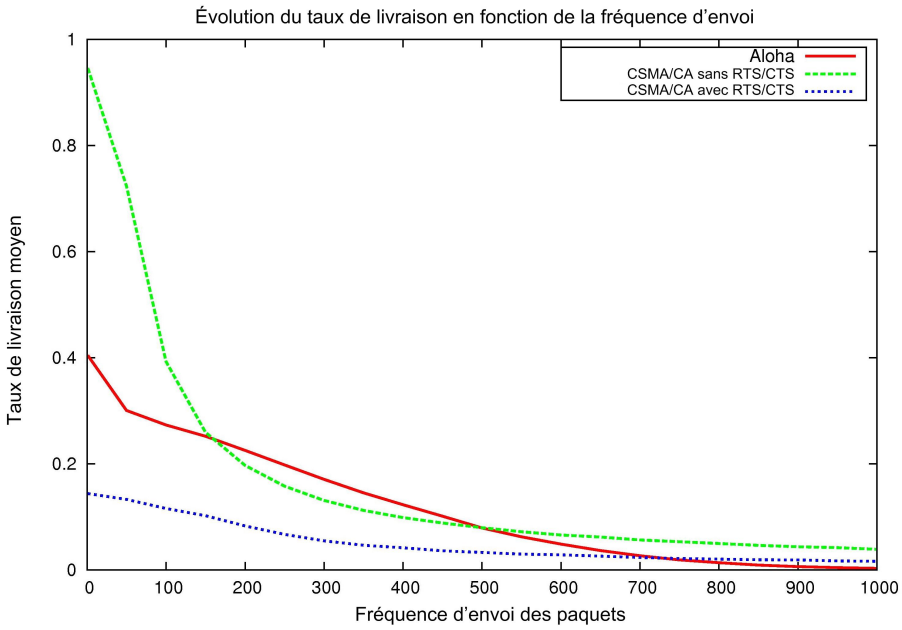

FIGURE 6.19 – Débit moyen pour le scénario 1

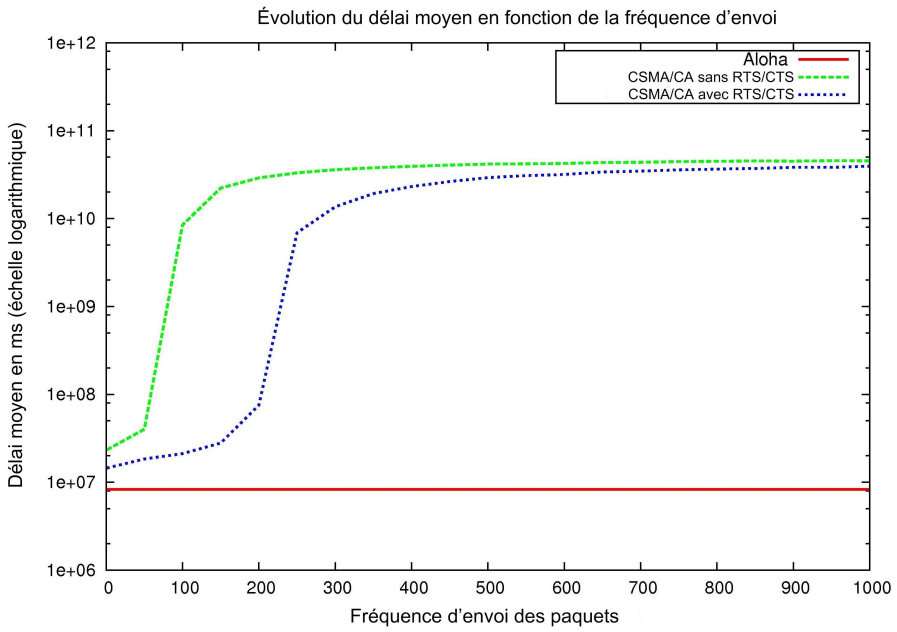

FIGURE 6.20 – Délai moyen pour le scénario 1

La figure 6.19 montre les différences de débit en fonction du nombre de paquets envoyés par seconde par chacun des capteurs sources pour 3 couches MAC (Aloha, CSMA avec et sans mécanisme RTS/CTS). Dans ce cas précis, nous pouvons observer que l'application d'une couche MAC fiable va avoir comme conséquence, une moins bonne utilisation du canal radio et donc un nombre moins important de paquets délivrés pour le nœud destination. Cela s'explique par deux raisons :

- le mécanisme de fiabilisation de CSMA/CA utilisé sur un lien non fiable va saturer le canal et est peu efficace pour éviter le problème des stations cachées. Par exemple, la perte d'un paquet RTS ou CTS entraîne une réinitialisation complète du processus d'envoi, créant ainsi de la congestion. De plus, la faible probabilité de réception d'une transmission empêche la réservation efficace du canal par le biais d'un paquet CTS.
- le temps d'attente nécessaire à la réservation du canal ou au contrôle de réception associé à une fréquence d'envoi élevée entraîne une perte de paquet au niveau de la file d'attente de la couche MAC. Alors qu'une couche Aloha, envoie un paquet sans contrôle, l'écoute du canal avant d'émettre, l'attente du paquet d'accusé de réception conduit à des supplémentaires (voir figure 6.20).

Dans le scénario 2 et 3, nous plaçons, entre les 2 capteurs sources et le capteur destination, respectivement 2 et 5 capteurs qui vont avoir pour unique rôle de relayer les paquets de données. Les simulations ont lieu sans changer la puissance d'émission des capteurs. Cela signifie que les liens utilisés dans ces deux scénarios sont plus fiables que précédemment. Les liens du scénario 3 étant également plus fiables que ceux du scénario 2. En revanche, le nombre de retransmissions est plus important. Ici, l'objectif est clair, il s'agit de trouver le compromis en termes de débit et de délai entre l'utilisation directement d'un lien non fiable ou l'utilisation de plusieurs liens fiables avec retransmissions. Nous regardons également l'influence du choix de la couche MAC.

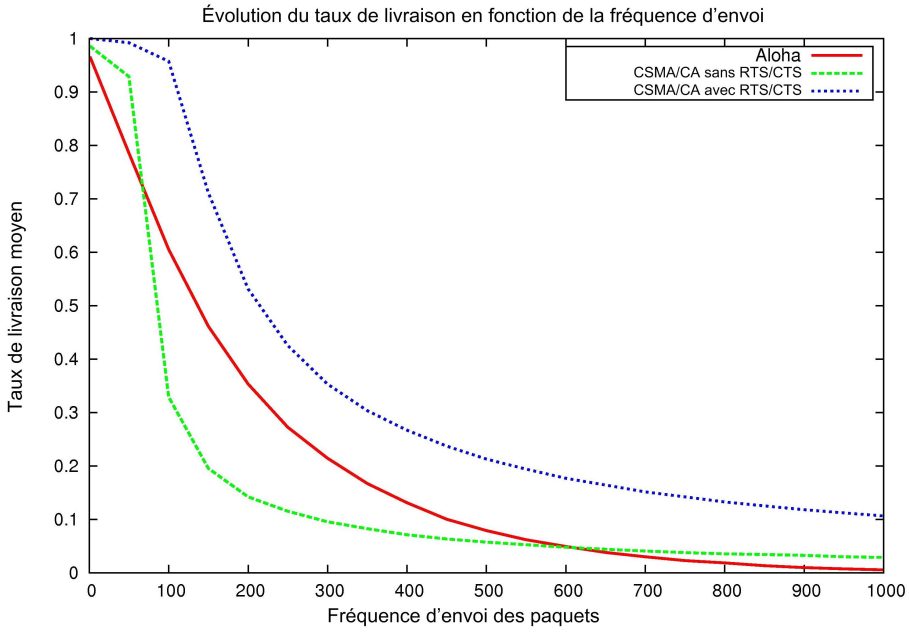

FIGURE 6.21 – Débit moyen pour le scénario 2

Les figures 6.21 et 6.22 donnent les résultats sur le scénario 2 en termes de débit. Les débits constatés sont très différents du scénario 1. Le gain apporté par l'utilisation de liens fiables surpasse de loin la nécessité de retransmissions par des nœuds intermédiaires. Cependant, ce gain est légèrement amoindri par l'ajout supplémentaire de capteurs retransmettants (voir figure 6.23). Dans ces deux scénarios, on peut remarquer que l'utilisation du mécanisme de réservation du canal RTS/CTS permet de minimiser les collisions induites par l'ajout de nœuds relais. En revanche, l'utilisation de l'écoute préalable du canal et de la retransmission de paquets non acquittés va entraîner de la congestion. Dans ces deux scénarios, le protocole Aloha en dépit d'une utilisation sans contrôle va permettre d'écouler plus de trafic que la couche CSMA/CA sans RTS/CTS. En transmettant les paquets sans contrôle, la couche MAC Aloha permet de ne pas saturer le réseau en utilisant de surcroît un minimum d'énergie. La proximité importante des capteurs relais permet de profiter d'un rapport SiNR favorable en cas de transmissions simultanées.

En revanche, le délai de transmission d'un paquet entre la source et la destination va naturellement augmenter avec l'ajout de capteurs relais (voir figure 6.23). On peut noter cependant que non seulement les paquets transmis grâce au protocole Aloha ne sont pas beaucoup impactés en termes de délai, mais que l'augmentation de la fréquence de transmission (et donc de la charge du réseau) n'influe pas sur le délai des paquets reçus.

Nous reprenons, dans les scénarios 4, 5 et 6, les mêmes conditions que pour les scénarios précédents (même puissance d'émission, même distance entre les capteurs sources et le capteur destination, même modélisation de la couche physique). Mais, alors que les scénarios 1, 2 et 3 prenaient l'hypothèse de capteurs sources hors de portée radio et d'un capteur destination commun, les scénarios 4, 5 et 6 prennent comme hypothèse des communications parallèles :

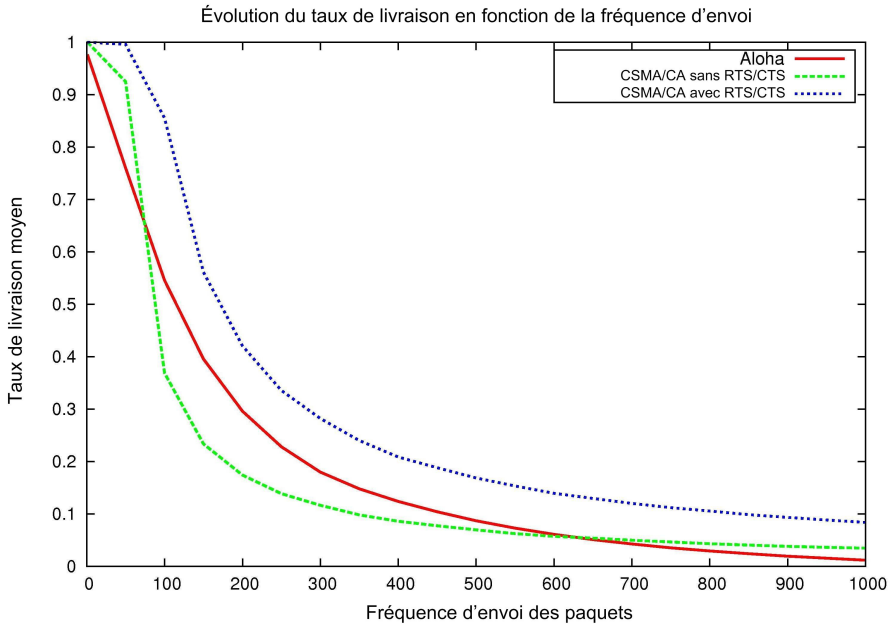

FIGURE 6.22 – Débit moyen pour le scénario 3

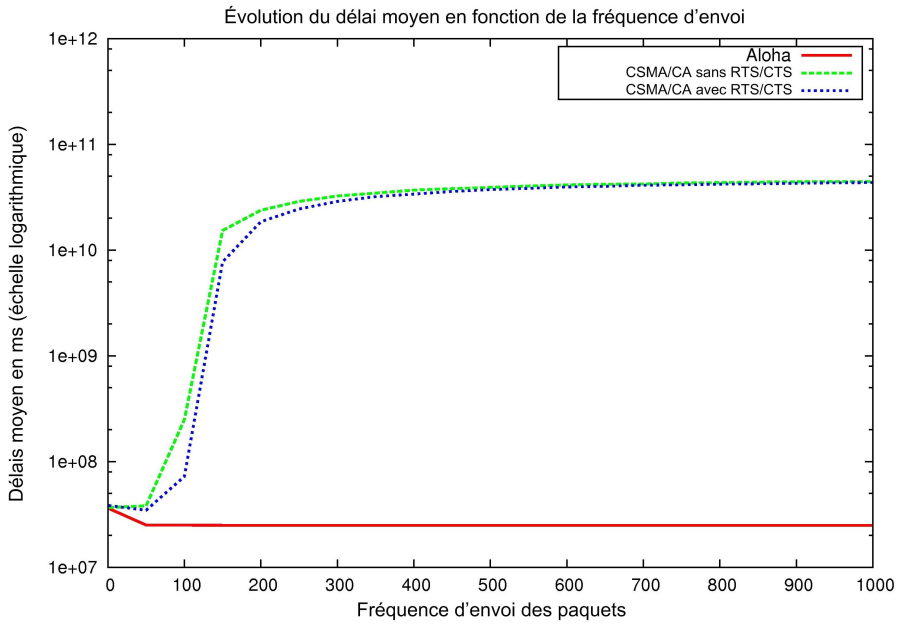

FIGURE 6.23 – Délai moyen pour le scénario 2

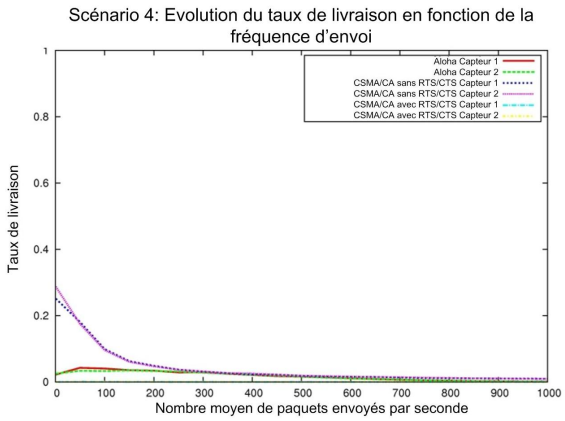

FIGURE 6.24 – Taux moyen de livraison pour le scénario 4

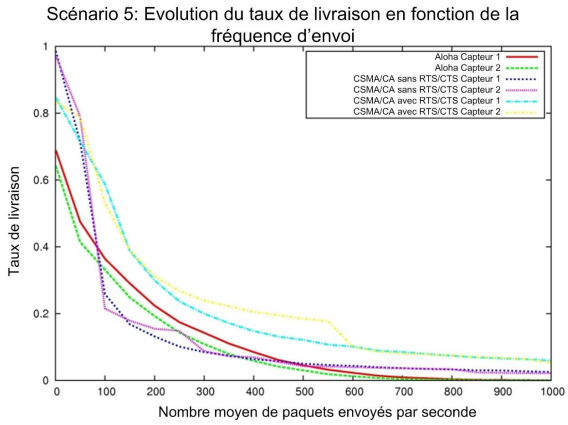

FIGURE 6.25 – Taux moyen de livraison pour le scénario 5

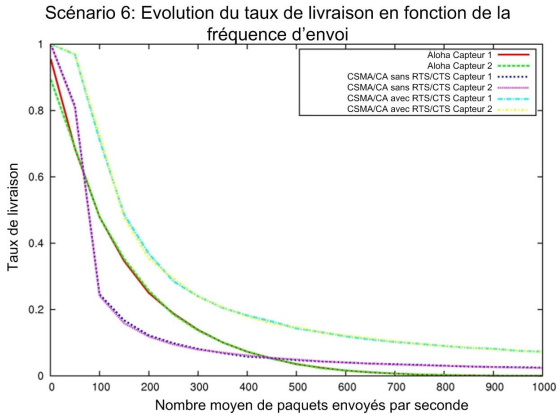

FIGURE 6.26 – Taux moyen de livraison pour le scénario 6

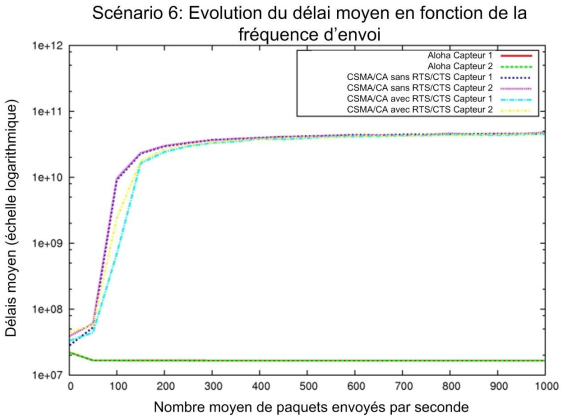

FIGURE 6.27 – Délai moyen pour le scénario 5

deux capteurs sources veulent transmettre leurs données à deux capteurs destinations distincts, l'ensemble des nœuds étant à portée de communication. Dans ces scénarios, l'utilisation de liens peu fiables est encore plus pénalisante. Pour cette configuration, nous voyons que les performances sont meilleures pour un nombre de relais égal à 5. Pour atteindre un taux de livraison optimal dans ces conditions de fonctionnement plus difficiles, il est nécessaire d'utiliser des liens avec un SiNR encore plus important.

Le choix de la couche MAC pour accéder au médium radio a également une importance dans cet ensemble de scénarios. Les caractéristiques restent cependant similaires aux trois premiers scénarios : l'absence de contrôle associée au choix de liens avec un SiNR favorable permet d'éviter beaucoup de collisions destructives. Cependant, dans le cas d'un lien relativement fiable, il est encore plus efficace de réserver le canal par l'intermédiaire d'un échange de paquets RTS et CTS (voir figures 6.24, 6.25, 6.26 et 6.27).

En définitive, ces simulations sur des topologies simples nous permettent de tirer un ensemble de conclusions utiles pour l'élaboration d'un protocole inter-couche :

- L'utilisation d'une couche MAC sans contrôle permet de réduire le délai et de le rendre

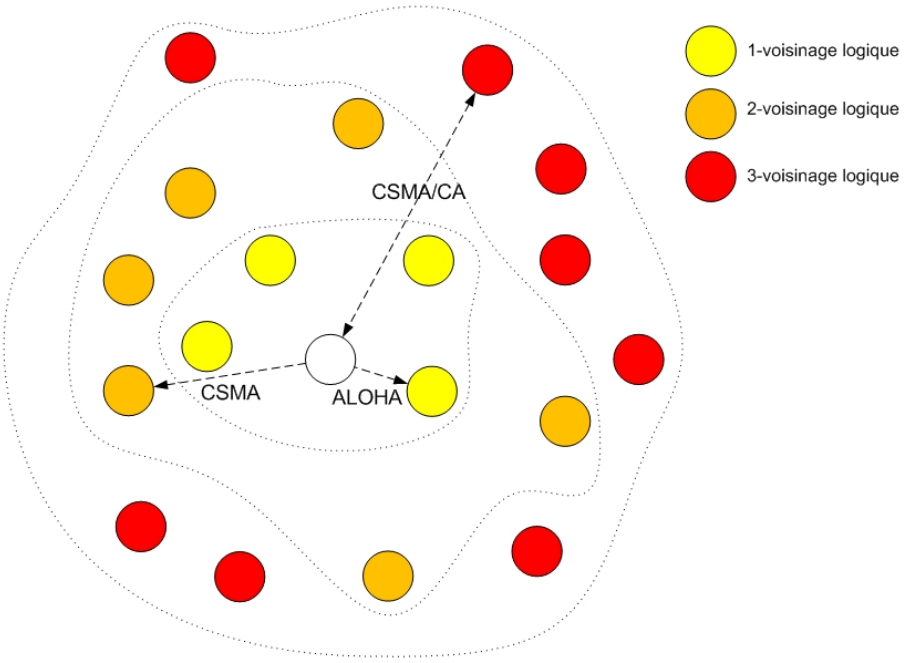

FIGURE 6.28 – Fonctionnement de la couche MAC adaptative

indépendant de la charge du réseau.

- Le routage sur des liens plus courts à puissance d'émission constante permet de bénéficier d'un SiNR favorable. Cette propriété permet de réduire le taux de collisions destructives dues aux interférences même dans le cas d'absence de mécanismes d'esquive de collisions.
- L'utilisation de retransmissions en cas de non-acquittement d'un paquet de données surcharge inutilement le réseau. Dans le cas de taux de transmission élevé, ce mécanisme pénalise fortement le taux de livraison.

6.8 Couche MAC adaptative

6.8.1 Principes

Pour les simulations suivantes, nous procédons à l'élaboration d'une couche MAC adaptative. Pour rappel, QLoP détermine 3 voisinages logiques qui vont correspondre à une division du voisinage physique d'un nœud en fonction de l'indice de proximité des voisins. Nous avons pu déterminer précédemment que l'utilisation d'un lien long (et donc peu fiable) nécessitait une couche MAC fiable avec réservation du canal et retransmissions. En revanche, les liens courts (et donc fiables) nécessitent une couche MAC moins fiable pour transmettre un paquet avec succès. En partant des conclusions tirées des simulations précédentes, nous avons élaboré une couche MAC qui s'adapte à la proximité de la destination. Pour déterminer à quel niveau de fiabilité elle va transmettre, la couche MAC utilise le classement en 3 classes du protocole QLoP. QLoP se basant sur des informations topologiques (une connaissance du voisinage à 1 et 2 sauts) pour fonctionner la couche MAC adaptative est véritablement inter-couche. Si le nœud est dans le

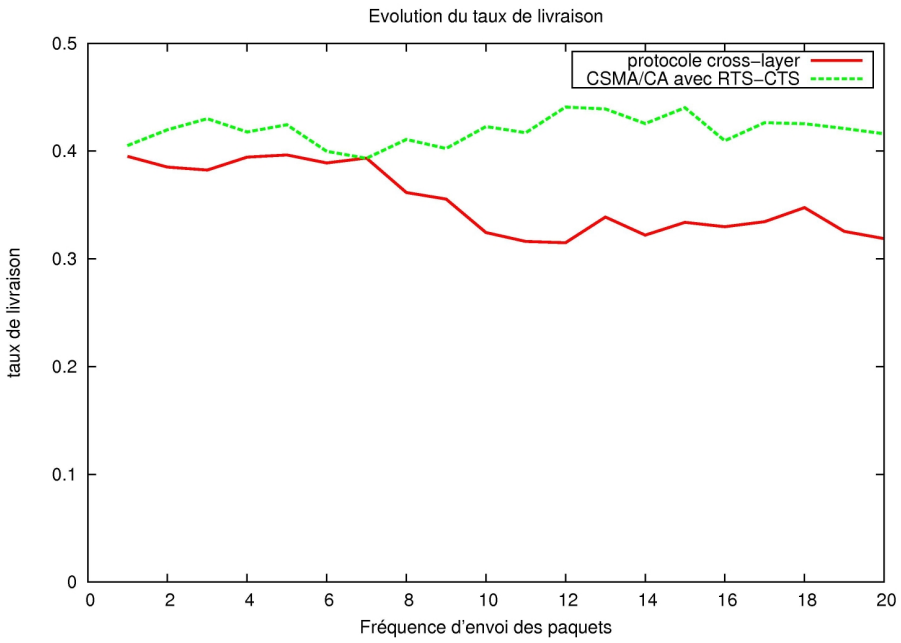

FIGURE 6.29 – Taux de livraison entre une couche MAC CSMA/CA avec RTS/CTS et une couche MAC adaptative

1-voisinage logique, la couche MAC utilisée est de type Aloha (i.e. sans contrôle). Pour un nœud dans le 2-voisinage logique, le capteur transmettant effectuera un « *carrier sense* » avant de transmettre un paquet de données. Enfin, pour un nœud du 3-voisinage logique la couche MAC sera de type CSMA/CA avec RTS/CTS. Le fonctionnement de cette couche MAC adaptative est illustré par la figure 6.28.

6.8.2 Évaluation de performances

Nous l'avons vu précédemment, l'utilisation de liens courts et fiables associée à une couche MAC Aloha ne permet de pas d'égaler le taux de livraison d'une couche MAC de type CSMA/CA avec RTS/CTS. Les simulations sur une topologie aléatoire donnent une confirmation de cet état (voir figure 6.29).

En revanche, les gains que l'on peut attendre d'une couche MAC adaptative sont en termes d'économie d'énergie. Nous pouvons constater une augmentation significative de la durée de vie du réseau grâce aux gains d'énergie réalisés. En effet, même si le nombre de paquets reçus est moins important que dans le cas d'une couche MAC CSMA/CA classique, l'énergie nécessaire pour transmettre un paquet à destination avec succès est nettement moins importante (voir figure 6.30). Cela conduit à une consommation énergétique totale du réseau significativement réduite avec l'utilisation d'une couche MAC adaptative (voir figure 6.31).

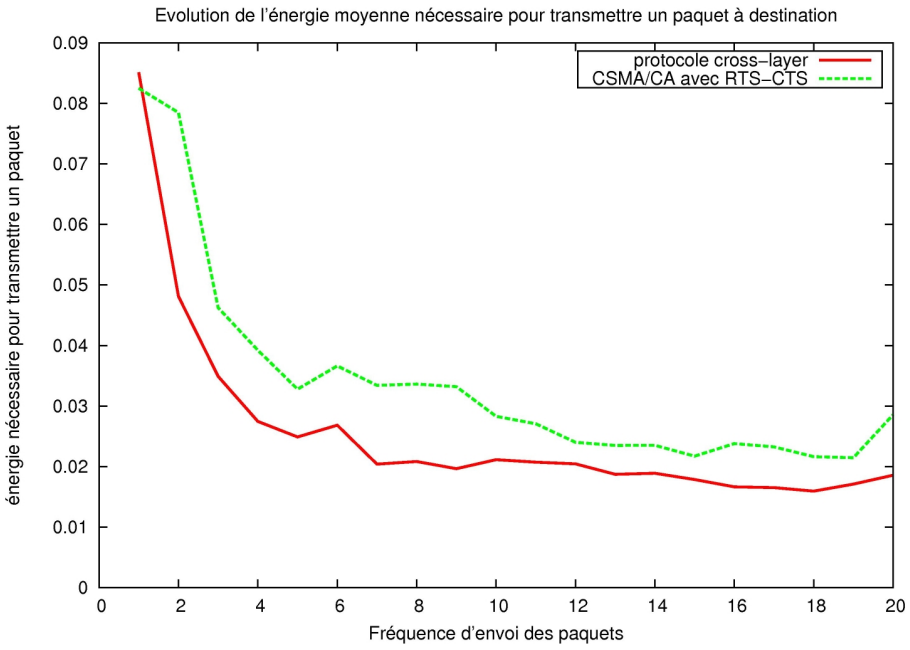

FIGURE 6.30 – Évolution de l'énergie moyenne par paquet reçu entre une couche MAC CSMA/CA avec RTS/CTS et une couche MAC adaptative

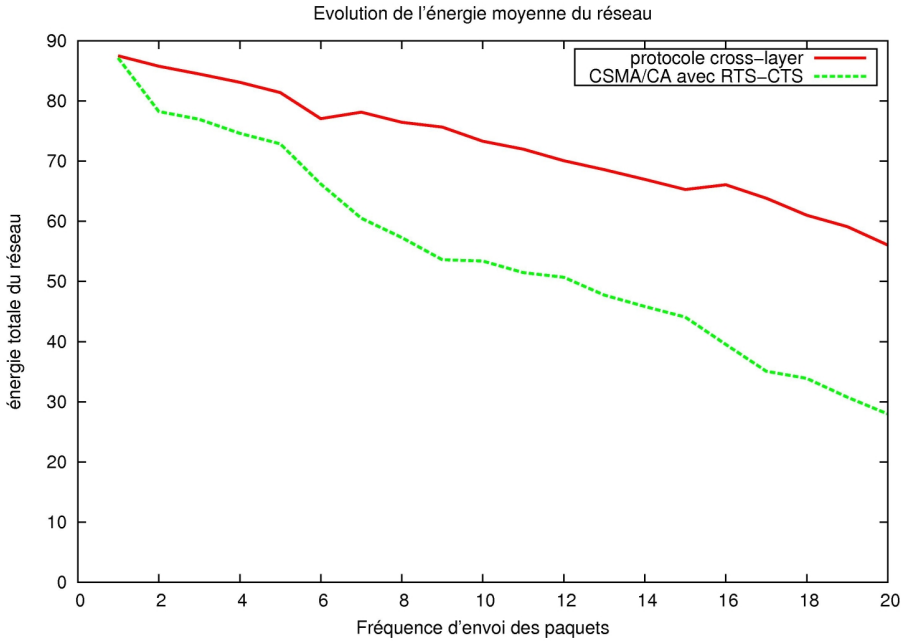

FIGURE 6.31 – Évolution de l'énergie moyenne du réseau entre une couche MAC CSMA/CA avec RTS/CTS et une couche MAC adaptative

6.9 Conclusion

De nombreuses études ont montré l'influence du choix de la couche MAC dans les performances en termes de débit ou de délai. Dans ce chapitre nous avons montré que le protocole sans contrôle Aloha avait des performances bien supérieures au modèle théorique généralement pris en hypothèse. De plus, en partant de scénarios simples, nous avons mis en évidence l'importance du couple topologie-couche MAC dans la probabilité de succès d'une communication : un capteur en contention avec d'autres capteurs mais se trouvant à proximité de la destination a une plus forte probabilité d'accéder au canal et de délivrer avec succès sa trame. Ces études préalables nous ont permis de concevoir un protocole d'accès au canal adaptatif. Basé sur l'indice de proximité du protocole QLoP, il adapte la fiabilité de la couche MAC à la qualité du lien, déterminée par la proximité de la destination. Ce mécanisme permet d'économiser l'énergie et d'améliorer la durée de vie du réseau.

Bibliographie

[1] Norman Abramson. The aloha system : Another alternative for computer communications. In *Fall Joint Computer Conference*, pages 281–285, Atlantic City, New Jersey, USA, April 1970. ACM.

[2] Samir R. Das, Charles E. Perkins, and Elizabeth E. Royer. Performance comparison of two on-demand routing protocols for ad hoc networks. In *19th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, pages 3–12, Tel-Aviv, March 2000.

[3] I. Demirkol, C. Ersoy, and F. Alagoz. Mac protocols for wireless sensor networks : a survey. *IEEE Communications Magazine*, 44(4) :115–121, April 2006.

[4] Chane L. Fullmer and J. J. Garcia-Luna-Aceves. Floor acquisition multiple access (fama) for packet-radio networks. In *Conference on Applications, technologies, architectures, and protocols for computer communication (SIGCOMM)*, pages 262–273, Cambridge, Massachusetts, USA, August 1995. ACM.

[5] Phil Karn. MACA – a new channel access method for packet radio. In *ARRL/CRRL : Amateur Radio 9th Computer Networking Conference*, pages 134–140, London, Ontario, Canada, September 1990.

[6] L. Kleinrock and F. Tobagi. Packet switching in radio channels : Part i–carrier sense multiple-access modes and their throughput-delay characteristics. *IEEE Transaction on Communications*, 23(12) :1400–1416, December 1975.

[7] G. Lu, B. Krishnamachari, and C.S. Raghavendra. An adaptive energy-efficient and low-latency mac for data gathering in wireless sensor networks. In *18th International Parallel and Distributed Processing Symposium (IPDPS)*, pages 224–232, Santa Fe, New Mexico, USA, April 2004.

[8] Shree Murthy and J. J. Garcia-Luna-Aceves. An efficient routing protocol for wireless networks. *Mobile Networks and Applications*, 1(2) :183–197, October 1996.

[9] Guangyu Pei, M. Gerla, and Tsu-Wei Chen. Fisheye state routing : a routing scheme for ad hoc wireless networks. In *International Conference on Communications (ICC)*, pages 70–74, New Orleans, Louisiana, USA, June 2000.

[10] C.E. Perkins and E.M. Royer. Ad-hoc on-demand distance vector routing. In *2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA)*, pages 90–100, New Orleans, Louisiana, USA, February 1999.

[11] S. Ray, J. B. Carruthers, and D. Starobinski. Rts/cts-induced congestion in ad hoc wireless lans. In *Wireless Communications and Networking Conference (WCNC)*, pages 1516–1521, New Orleans, Louisiana, USA, March 2003.

[12] E. M. Royer, Sung-Ju Lee, and C. E. Perkins. The effects of mac protocols on ad hoc network communication. In *Wireless Communications and Networking Conference (WCNC)*, pages 543–548, Chicago, Illinois, USA, March 2000.

[13] IEEE Computer Society. 802.11 part 11 : Wireless lan medium access control (mac) and physical layer (phy) specifications. http://standards.ieee.org/getieee802/download/802.11-2007.pdf, June 2007.

[14] Singh Suresh, Mike Woo, and C.S. Raghavendra. Power-aware routing in mobile ad hoc networks. In *4th annual ACM/IEEE international conference on Mobile computing and networking (MobiCom)*, pages 181–190, Dallas, Texas, USA, October 1998. ACM.

[15] Violet R. Syrotiuk and Amaresh Bikki. Modeling cross-layer interaction using inverse optimization. In *Mobile Ad Hoc Networking*, chapter 15, pages 411–425. Stefano Basagni, 2004.

[16] Ken Tang, Mario Correa, and Mario Gerla. Effects of ad hoc layer medium access mechanisms under tcp. *Mobile Networks and Applications*, 6(4) :317–329, August 2001.

[17] Alec Woo and David E. Culler. A transmission control scheme for media access in sensor networks. In *7th annual international conference on Mobile computing and networking (MobiCom)*, pages 221–235, Rome, Italy, June 2001. ACM.

[18] Wei Ye, John Heidemann, and Deborah Estrin. Medium access control with coordinated adaptive sleeping for wireless sensor networks. *IEEE/ACM Transaction on Networking*, 12(3) :493–506, June 2004.

7

Conclusions et perspectives

Mon objectif, au travers de cette thèse, a été de développer une solution d'utilisation des réseaux de capteurs en utilisant les principes de l'auto-organisation afin de faciliter et d'améliorer leur utilisation. L'intérêt des protocoles d'auto-organisation pour structurer les réseaux ad hoc a en grande partie été démontré [2], ainsi que son utilité dans les réseaux de capteurs [1]. Cependant, il manquait une étude sur les propriétés dynamiques des réseaux de capteurs, de leur installation à leur fin de vie. La localisation, le contrôle de topologie et le routage sont trois des problématiques les plus importantes dans les réseaux de capteurs. Nous avons voulu démontrer que ces problématiques pouvaient être adressées grâce à un protocole d'auto-organisation localisé sans recourir, ni à des équipements coûteux, ni à des mesures basées sur un canal radio instable. Les solutions proposées n'auraient pas été complètes sans une analyse cross-layer. Nous nous sommes placés dans le contexte des réseaux de capteurs sans fil. Statiques et homogènes, les capteurs n'en restent pas moins dynamiques (voisinage fluctuant causé par un canal radio réaliste et donc instable, mort de nœuds due à leur manque d'énergie, apparition de nouveaux capteurs lors de redéploiements) et divers (degré, niveau d'énergie ou proximité différents).

7.1 Contributions de la thèse

Pour définir une solution réaliste, il était important de prendre en compte la dynamique d'un réseau, ce qui n'avait jamais été réalisé entièrement, de son déploiement à sa fin de vie. Nous avons donc caractérisé 3 phases de la vie d'un réseau de capteurs :

- La phase de naissance correspond à l'arrivée progressive des nœuds, à la fois durant le déploiement initial du réseau de capteurs et durant le redéploiement de nouveaux nœuds

dans le réseau. Il en résulte une phase où les nœuds découvrent leur voisinage et où des incohérences dans ces tables de voisinage apparaissent. En effet, à cause du déploiement progressif, les capteurs ont généralement une vision partielle de leur voisinage durant l'envoi de leurs premiers messages. Cela conduit à des erreurs durant le processus d'élection des nœuds dominants ou le processus de sélection de liens.

- La phase de fonctionnement normal commence dès que la structure organisée est stabilisée. Cette phase correspond à ce que nous pouvons attendre de l'auto-organisation. La phase de fonctionnement normal se termine quand il y a trop de modifications dans le réseau pour que la structure soit maintenue.
- Alors commence la troisième et dernière phase : la mort. Lorsqu'un ou plusieurs nœuds disparaissent, la reconstruction de la structure logique, globale ou localisée va être nécessaire. Là encore, les capteurs n'ont pas immédiatement la perception de la disparition d'un voisin, cela a pour conséquence une certaine inertie. Cette dernière phase peut être assimilée à un processus de maintenance et d'auto-réparation.

Durant la phase de naissance, nous avons observé les incohérences de voisinage et leurs implications au niveau de l'organisation de 6 principaux protocoles d'auto-organisation (MPR, MPR-DS, CDS-IDS, CDS-règle k, LMST, RNG) avec, en particulier, la latence entre la *naissance physique* d'un réseau et sa *naissance logique*. Durant la phase de fonctionnement normal, nous avons mis en évidence la qualité d'une auto-organisation en analysant notamment la cardinalité de la structure dominante et, dans le cas de protocoles orientés dominant et le degré logique moyen du réseau dans le cas de protocoles à élagage de liens. Lors de la mort progressive de capteurs, nous avons analysé les conséquences de la perte d'un ou plusieurs nœuds sur la structure logique. Nous avons également défini et mis en évidence l'**effet donut** : la désertification du voisinage du puits. La construction d'une topologie logique distribuée sur l'ensemble du réseau est souvent avancée car elle donne les meilleures performances quand le réseau est fixe et que la couche physique est idéale. Cependant, notre travail a montré que cette structure logique basée sur un arbre et un nœud racine était préjudiciable pour la robustesse.

Partant de ces conclusions, nous avons montré qu'il était souhaitable et possible de réaliser un protocole d'auto-organisation original dédié à la localisation relative basé sur des informations topologiques de niveau 3 : QLoP. Alors que de nombreuses propositions prennent la puissance du signal reçu (RSSI) comme métrique de la proximité des voisins, nous avons montré que cette métrique n'était pas fiable et consommatrice en énergie. En nous basant à la fois sur des résultats théoriques, des simulations et des expérimentations sur des capteurs développés au laboratoire CITI nous avons prouvé que QLoP s'avère à la fois plus rapide à converger, plus précis et s'accommode parfaitement d'une forte densité.

Dans un réseau de capteur, le bruit peut provenir tant de sources extérieures que de capteurs à proximité dans le cas d'un réseau dense. La solution de localisation développée nous a permis de proposer un contrôle de topologie efficace tel que le RNG afin de fournir une topologie logique, cadre nécessaire pour les protocoles de niveau 3. Le routage sur la topologie RNG, en sélectionnant les voisins les plus proches et les liens les plus stables, permet de router de manière plus efficace en environnement bruité : les routes construites sont plus stables, moins sensibles

aux variations du signal et au bruit, et les paquets parcourent une distance plus importante que sur une topologie à plat.

Les performances de la structure virtuelle au niveau 3, ont mis en lumière le gain qu'il y a à router les données sur les liens les plus courts, en moyenne. Cependant, le mécanisme de "*carrier sense*" utilisé dans les normes IEEE 802.11 (WIFI) et 802.15.4 n'utilise pas cette structure. Nous avons proposé une approche résolument inter-couche en développant une couche MAC adaptative basée sur l'indice de proximité du protocole QLoP.

7.2 Perspectives

Les travaux effectués au cours de la thèse offrent plusieurs perspectives. Ils se situent dans l'extension des travaux réalisés. Nous les détaillons dans cette section.

7.2.1 Localisation globale

Le protocole QLoP permet une localisation du voisinage direct. Cependant, dans des applications comme la surveillance d'environnement ou la remontée d'alerte, une localisation globale est inévitable pour que ces applications soient utilisables : on ne peut concevoir, par exemple, la détection d'incendies sans informations du lieu précis du départ de feu. De plus, un routage géographique a l'avantage de s'affranchir de la découverte de route et s'adapte ainsi à la fois à la mobilité des capteurs qu'aux changement topologiques. Le véritable défi est donc de passer d'une information locale à une information globale.

Dans cet optique, une partie de la recherche actuelle se concentre encore sur l'exploitation du RSSI comme métrique pour estimer la distance entre deux capteurs. Le chapitre 3 nous conforte dans l'idée que cette métrique n'est pas utilisable en l'état. Il peut être envisageable de la traiter ou de lui appliquer des mécanismes de fiabilisation. Ces algorithmes restent à découvrir mais, selon nous, cela se fera inévitablement au dépend de l'énergie ou de la latence.

Une autre stratégie est possible en utilisant une des propriétés importantes de l'algorithme QLoP montrée dans le chapitre 4 de cette thèse : le rapport linéaire entre la distance qualitative normalisée et la distance euclidienne. Ce résultat important ouvre la voie à une localisation globale et à l'établissement de coordonnées virtuelles qui resteraient néanmoins en lien avec la distance euclidienne réelle. Il convient donc d'établir une stratégie qui permette de passer d'un référentiel local à un référentiel global sans inonder le réseau de paquets de contrôle. On pense à une stratégie de *overhearing*, c'est-à-dire qu'il n'y a pas de paquets dédiés mais que les capteurs découvrent la topologie grâce au trafic de données et affinent la localisation au cours de la vie du réseau.

7.2.2 Sécurité

Nous avons vu que les réseaux de capteurs peuvent être utilisés dans les domaines urbains, industriels et médicaux. Selon la nature de l'application, les réseaux de capteurs peuvent donc manipuler des données sensibles ou confidentielles. Le mode de communication (radio) et le déploiement des capteurs dans des environnements ouverts rendent nécessaires les solutions pour

garantir la sûreté et l'intégrité du réseau. Cependant, les limitations physiques des capteurs imposent, bien plus que dans la sécurité informatique traditionnelle, une vision asymétrique entre l'attaquant et le capteur attaqué : on ne peut s'appuyer ni sur des algorithmes de cryptographie traditionnels trop consommateurs en énergie, en puissance de calcul et en temps, ni sur des mécanismes complexes de sauts de fréquences (FHSS) (les capteurs de type MICA2 vont être capables d'utiliser 2 fréquences uniquement). Il faut donc définir une défense globale du réseau, ne garantissant pas une intégrité absolue d'un capteur, mais la résilience de l'ensemble du réseau. Pour nous, cette problématique devra s'appuyer sur des protocoles d'auto-organisation robustes face aux différentes phases de la vie d'un réseau de capteurs. Un pas a été fait dans ce sens : il existe déjà une solution de sécurité inspirée par QLoP [4]. Basée également sur l'intersection de voisinage, cette solution de détection de Worm Hole a été développée au CITI.

7.2.3 Corrélation spatiale

Dans les applications de surveillance d'environnement, le principal objectif d'un réseau de capteurs est de rapporter un évènement détecté. Dans certains cas, cet évènement (température, luminosité, etc.) est fortement corrélé spatialement, c'est-à-dire, que son intensité est liée à la distance. C'est ainsi possible de calculer la température du soleil, sans jamais y avoir posé une sonde : en connaissant la température dégagée à une distance donnée.

L'exploitation de ces corrélations spatiales est un puissant outil qui peut améliorer grandement les performances du réseau, en particulier sa durée de vie. On pense, bien entendu, à l'agrégation ou à la compression de données : en connaissant la distance d'un nœud et sa mesure, il devient inutile pour un voisin de retransmettre tous les paquets reçus mais seulement les variations pertinentes. On limite ainsi le nombre de paquets réémis. Récemment, [3] a proposé un protocole MAC réduisant le nombre de transmissions. L'idée est de se servir de la corrélation spatiale parmi un ensemble dense de nœuds pour limiter le nombre de nœuds relayant l'évènement. Cela limite ainsi le nombre de collisions, améliore le délai et économise de l'énergie.

La division en 3 classes de proximité de QLoP ouvre la voie à de nouvelles stratégies d'agrégation spatiale. On voit bien dans ces deux exemples comment pourrait être utilisé QLoP : en déterminant l'indice de proximité d'un voisin, et l'intensité de l'évènement détecté, nous sommes en mesure de déterminer si les paquets reçus s'écartent de la prévision et méritent d'être retransmis et réduire ainsi le nombre de retransmissions. Il est également possible de déterminer, en fonction du même indice de proximité, quels capteurs du voisinage sont nécessaires pour couvrir un évènement.

Bibliographie

[1] JiaLiang Lu. *Impacts of self-organized Mechanism in Wireless Sensor Networks*. PhD thesis, INSA de Lyon, May 2008.

[2] Fabrice Theoleyre and Fabrice Valois. A self-organization structure for hybrid networks. *Ad Hoc Network*, 6(3) :393–407, may 2008.

[3] Mehmet C. Vuran and Ian F. Akyildiz. Spatial correlation-based collaborative medium access control in wireless sensor networks. *IEEE/ACM Transanction on Networking*, 14(2) :316–329, April 2006.

[4] W. Znaidi, M. Minier, and J.-P. Babau. Detecting wormhole attacks in wireless networks using local neighborhood information. In *19th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Cannes, France, September 2008.