



Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Ministère de l'Enseignement Supérieur et de la recherche Scientifique

Université L'arbi ben M'hidi Oum El Bouaghi

Département Informatique

Ecole Doctorale de l'Est

Algorithmes de routage pour les réseaux de capteurs

*Mémoire présenté en vue de l'obtention du Diplôme de Magistère en
Informatique
Option : Génie logiciel*

présenté par :
Tébessi Kamel

Sous la direction de :
Pr. M. Benmohammed

Composition du Jury :

Président: Dr. S. Chikhi (Université de Constantine)
Rapporteur: Pr. M. Benmohammed (Université de Constantine)
Examineurs: Dr. A. Chaoui (Université de Constantine)
Dr. A. Bilami (Université de Batna)

Année universitaire 2008 - 2009



PDF
Complete

Your complimentary
use period has ended.
Thank you for using
PDF Complete.

[Click Here to upgrade to
Unlimited Pages and Expanded Features](#)

À ma mère

À mon père

À mes frères et mes sœurs

À toute ma famille

À tous mes amis

À tous ceux qui me sont chères

Je dédie ce travail



Remerciement

Je tiens en premier lieu à remercier les membres de mon jury pour simplement avoir accepté d'œy figurer : **Dr. A. Chaoui** et **Dr. A. Bilami** en tant que examinateurs, et **Dr. S. Chikhi** en tant que président. C'œest un grand honneur qu'œils me font.

Je remercie bien évidemment le **Professeur Mohamed Benmohammed** d'avoir encadré ce mémoire. Cette année de travail en commun ma beaucoup appris scientifiquement. Je souhaite à tous les étudiants d'avoir un directeur de mémoire aussi généreux et aussi enclin à partager son savoir, son travail et son temps.

Enfin, « last but not least », je tiens à remercier: Moncef, et Mohamed El Arbi pour leurs aides.



Résumé

Beaucoup de résultats passionnants ont été obtenus récemment pour les réseaux de capteurs à grande échelle. Ces réseaux peuvent former la base pour beaucoup de types d'environnements futés (smart) tels que les hôpitaux, les champs de bataille, les systèmes de réponse aux séismes, et les environnements d'apprentissage. Tandis que ces applications potentielles demeurent diverses, elles partagent toutes le besoin d'un protocole de routage efficace et robuste.

Puisque les réseaux de capteurs agissent avec le monde réel, il est souvent nécessaire pour une communication de rencontrer des contraintes temps réel. Pour cela, un protocole de routage, appelé SPEED, a été développé pour supporter la communication temps-réel. Cependant, l'utilisation de ce protocole dans les réseaux de capteur dense à grande échelle fait augmenter le nombre total des paquets de contrôle générés ce qui crée: la surcharge du réseau, la diminution de la durée de vie du réseau, et des retards dans la livraison des données.

Ce mémoire présente un nouveau protocole de routage basé sur SPEED qui permettra d'éviter les problèmes cités auparavant. Les performances de notre protocole de routage par rapport à SPEED ont été validées par des simulations effectuées en utilisant le simulateur NS2.

Mots-clés : réseaux de capteurs, protocole SPEED, paquets de contrôle, NS2.



Abstract

Many exciting results have been obtained recently for large-scale sensor networks. These networks can form the basis for many types of smart environments, such as hospitals, battlefields, the system response to earthquakes, and learning environments. While these potential applications are diverse, they all share the need for an efficient and a robust routing protocol.

Since sensor networks operate with the real world, it is often necessary for communication to meet real-time constraints. For this, a routing protocol, called SPEED, was developed to support real-time communication. However, using this protocol in large-scale dense sensor networks increases the total number of control packets generated which creates: the network overload, the decrease in lifetime of the network, and delays in data delivery.

This paper presents a new routing protocol based on SPEED, which will avoid the problems mentioned above. The performance of our routing protocol compared to SPEED has been validated by simulations using the NS2 simulator.

Keywords: sensor networks, SPEED protocol, control packets, NS2.

Table des matières

Liste des figures	x
Liste des acronymes	xii
Introduction générale	14
Chapitre 1: Les réseaux sans fil	18
1.1 Introduction	18
1.2 Les différents standards	19
1.2.1 Les réseaux métropolitains sans fil (WMAN)	19
1.2.2 Les réseaux personnels sans fil (WPAN)	19
1.2.3 Les réseaux locaux sans fil (WLAN)	21
1.3 La mise en œuvre des réseaux sans fil	24
1.3.1 Le mode de fonctionnement centralisé	24
1.3.2 Le mode de fonctionnement ad hoc	25
1.4 Conclusion	26
Chapitre 2 : Les réseaux de capteurs sans fil -État de l'art	27
2.1 Introduction	27
2.2 Définition du réseau de capteurs	27
2.3 Composant d'un nœud capteur	28
2.4 Architecture des réseaux de capteurs	29
2.4.1 Les réseaux de capteurs sans fil plats	30
2.4.2 Les réseaux de capteurs hiérarchiques	30
2.5 Caractéristiques des réseaux de capteurs	30
2.5.1 Densité « importante » des nœuds	30
2.5.2 Topologie dynamique	30
2.5.3 Auto organisation	31
2.5.4 La tolérance de fautes	31
2.5.5 Scalabilité	31
2.6. Contraintes et facteurs conceptuelles des réseaux de capteurs	31
2.6.1 Pannes fréquentes	31
2.6.2 L'environnement	32
2.6.3 La topologie dynamique	32
2.6.4 La consommation d'énergie	32

années dans les réseaux de capteurs..	í í í .í ..	32
ent	í í í í í í í í í í í ..í í .í ..í í .	33
2.7.2 Le modèle commandé par requête	í í í í í í í í í í í í í íí í í ..	33
2.7.3 Le modèle continu	í í í í í í í í í í í í í í í í í í í ..í ..í í ...	34
2.8 Applications des réseaux de capteurs	í í í í í í í í í í í í í í .í í í í í .í í	34
2.8.1 Applications militaires	í í í í í í í í í í í í í í í í í í .í .í .í í .	34
2.8.2 Applications de santé	í í í í í í í í í í í í í í í í í í .í í í í í í ..	34
2.8.3 Applications environnementales	í í í í í í í í í í í í í í í í í í ..í í í ..	34
2.9 La zone de couverture d'un capteur	í í í í í í í í í í í í í í ..í í ..í .í .í í ..	35
2.10 Notion de cluster	í í í í í í í í í í í í í í í í í í ..í í í í íí í í ..	35
2.11 Exemples de capteurs	í í í í í í í í í í í í í í .í í í í í ..í .í í í .	36
2.11.1 Le capteur MICA	í í í í í í í í í í í í í í ..í í í í í ..í í í í ...	36
2.11.2 Le capteur MICA2í	í í í í í í í í í í í í í í í í ..í í ..í .í í í ..	37
2.11.3 Le capteur MICA2DOTí	í í í í í í í í í í í í í í í í í ..í í í .í ...	37
2.12 Comparaison entre les réseaux de capteurs et les réseaux ad hoc	í ..í ...í í í	38
2.13 Conclusion	í ..í í ..	39
Chapitre 3 : Routage dans les réseaux de capteurs sans fil		40
3.1 Introduction	í ..í .í í í ...	40
3.2 Conception d'architecture du système	í í í í í í í ..í í í ..í í ..í í í ...	41
3.2.1 Dynamique du réseau	í í í í í í í í í í í í í í í í í ..í í í ..í .í í í í ..	41
3.2.2 Le déploiement des nò uds	í í í í í í í í í í í í í í í í í ..í í ..í í í í	41
3.2.3 Considération d'énergie	í í í í í í í í í í í í í í .í í í í ..í .í í í í	41
3.2.4 Modèle de livraison des données	í í í í í í í í í í í .í í í ..í í í í í ..	41
3.2.5 Les capacités des nò uds	í í í í í í í í í í í í í í .í í í í í .í ...í í ..	41
3.2.6 Agrégation et fusion des données	í í í í í í í í í í í í í í í í í ..í í í ..	42
3.2.7 Hétérogénéité des nò uds	í í í í í í í í í í í í .í í í í ..í í í í ..	42
3.2.8 Tolérance aux fautes	í í í í í í í í í í í í í í .í í í í í ..í .í í í	42
3.2.9 Scalabilité	í ..í í ...	42
3.2.10 Support de transmission	í í í í í í í í í í í í .í í í í í í ..í í í	42
3.2.11 Connectivité	í ..í í í ..	43
3.2.12 Couverture	í ..í í í .	43
3.2.13 Qualité de service	í í í í í í í í í í í í í ..í í í í í ..í .í í ...	43
3.3 Les protocoles centrés-données (data-centric protocols)	í í ..í í í í ..í ..í í ..	43
3.3.1 Propagation et discussion (flooding and gossiping)	í í í í ..í í ..í .í í ...	43

Information par négociation (SPIN)	45
í í í í í .í í í í í í í í ..í í ...í í .	46
3.3.4 Routage avec considération de l'énergie (Energy-aware routing)	47
3.3.5 Routage par rumeur (Rumor routing)	48
3.3.6 Routage a base de gradient (GBR : Gradient-Based Routing)	48
3.3.7 CADR	49
3.3.8 COUGAR	49
3.3.9 Transmission active de requête dans les réseaux de capteurs (ACQUIRE)	50
3.4 Les protocoles hiérarchiques	50
3.4.1 Hiérarchie de regroupement adaptatif à faible énergie (LEACH)	51
3.4.2 Assemblage a puissance efficace dans les systèmes d'information de capteurs (PEGASIS)	51
3.4.3 TEEN et APTEEN	52
3.4.4 Routage avec considération de l'énergie à base de cluster	53
3.4.5 Protocole auto-organisateur	54
3.5 Les protocoles basés sur la localisation	55
3.5.1 MECN et SMECN	55
3.5.2 GAF	56
3.5.3 GEAR (geographic and energy-aware routing)	57
3.6 Protocoles avec considération du flux du réseau et de QoS	58
3.6.1 Routage a énergie de durée de vie maximale	58
3.6.2 Collecte de données de durée de vie maximale	58
3.6.3 Transmission à coût minimal	59
3.6.4 SAR	60
3.6.5 Protocole de routage QoS avec considération de l'énergie	60
3.6.6 SPEED	60
3.7. Conclusion	61
Chapitre 4 : Algorithme de routage EESPEED pour les réseaux de capteurs dense à grand échelle	62
4.1 Introduction	62
4.2 Le protocole SPEED	63
4.2.1 Paquet de localisation	64
4.2.2 Estimation de délai	64
4.2.3 SNGF (Stateless Non-deterministic Geographic Forwarding)	65



PDF Complete

Your complimentary use period has ended. Thank you for using PDF Complete.

[Click Here to upgrade to Unlimited Pages and Expanded Features](#)

.í í í í í .í í í í í í í í .í í í í í	95
	97
Perspectives	99
Bibliographie	100

te des figures

Figure 1.1 De l'âge de l'ordinateur personnel à l'âge de multi-appareille informatique	18
Figure 1.2 La portée et le débit des différents standards de communication sans fil.	20
Figure 1.3 La position du standard IEEE 802.11 dans le modèle OSI	22
Figure 1.4 Le problème des stations cachées avec le CSMA/CA	23
Figure 1.5 Un exemple de Scatternet composé de trois Piconet	25
Figure 2.1 Les composants d'un nœud capteur	28
Figure 2.2 Architecture d'un réseau de capteurs	29
Figure 2.3 La zone de perception (SR) et la zone de communication (CR)	35
Figure 2.4 La notion de cluster	36
Figure. 2.5 Le capteur MICA	37
Figure. 2.6 Le capteur MICA2	37
Figure. 2.7 Le capteur MICA2DOT	38
Figure 3.1 Le problème de la duplication des messages envoyés au même nœud.	44
Figure 3.2 Le problème de chevauchement des zones de couvertures	44
Figure 3.3 Le protocole SPIN	45
Figure 3.4 Phases du protocole de diffusion dirigée	46
Figure 3.5 Le groupement hiérarchique dans TEEN et APTEEN	52
Figure 3.6 Un cluster typique dans un réseau de capteur	54
Figure 3.7 Exemple sur la grille virtuelle dans GAF	56
Figure 3.8 Exemple sur RGF dans GEAR	58
Figure 4.1 Architecture fonctionnelle du protocole SPEED	63
Figure 4.2 Paquet de localisation	64
Figure 4.3 Calcul de la vitesse de livraison	65
Figure 4.4 Choix de nœud de prochain saut	66
Figure 4.5 Paquet « Delay Back pressure »	68
Figure 4.6 Procédure de re-routage pour délai «Delay back pressure rerouting »(cas 1).	69

Figure 4.9 Les paquets de contrôle générer périodiquement par tout les nò uds du réseau	71
Figure 4.10 Re-routage de paquet de données	73
Figure 4.11 Création de la grille virtuelle	74
Figure 4.12 Envoie de paquet contrôle d'énergie intra-grappe	75
Figure 4.13 Envoie de paquet de données aux chefs de grappes	77
Figure 4.13 Routage des données inter-grappe	78
Figure 5.1 Le déroulement d'une simulation sous ns2	79
Figure 5.2 L'outil de visualisation NAM	80
Figure 5.3 Le nombre total de paquet de contrôle	84
Figure 5.4 Le nombre total de paquets de contre pression	84
Figure 5.5 Le nombre total de paquets perdus	89
Figure 5.6 Le délai moyen bout en bout	91
Figure 5.7 L'énergie moyenne consommée	92
	93
	95



Your complimentary use period has ended.
Thank you for using PDF Complete.

[Click Here to upgrade to Unlimited Pages and Expanded Features](#)

des acronymes

ACQUIRE	ACtive QUery forwarding In sensoR nEtworks
APTEEN	Adaptatif Threshold sensitive Energy Efficient sensor Network protocol
BPP	Basic Printing Profile
CADR	Constrained anisotropic diffusion routing
CMLDA	Clustering Maximum Lifetime Data Aggregation
CR	Communication Rradius
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTP	Cordless Telephony Profile
CTS	Clear To Send
DCF	Distributed Coordination Function
EESPEED	Energy-awarE clustering SPEED
EWMA	Exponential Weighted Moving Average
FS	<i>Forwarding candidate Set of Node</i>
FTP	File Transfer Protocol
JSIM	Java Simulator
HIPERLAN	HIgh PErformance Radio Local Area Network
IDSQ	Information-driven sensor querying
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
GAF	Geographic adaptive fidelity
GEAR	geographic and energy-aware routing
GPRS	General Packet Radio Service
GSM	Global System for Mobile communication
LEACH	Low-Energy Adaptive Clustering Hierarchy
MAC	Media Access Control
MANET	Mobile Ad hoc NETwork
MECN	Minimum energy communication network
MLDA	Maximum Lifetime Data Aggregation



PDF Complete

Your complimentary use period has ended.
Thank you for using PDF Complete.

[Click Here to upgrade to Unlimited Pages and Expanded Features](#)

OPNET	Optimum Network Performance
OSI	Open Systems Interconnection
PDA	Personal Digital Assistant
PCF	Polling Coordination Function
PEGASIS	Power-Efficient GATHERing in Sensor Information Systems
QoS	Quality of Service
RCsF	Réseaux de Capteurs sans Fil
RGF	Recursive Geographic Forwarding
RTS	Ready To Send
SAR	Sequential Assignment Routing
SNGF	<i>Stateless Non-deterministic Geographic Forwarding</i>
SPEED	SPEED
SPIN	Sensor Protocols for Information via Negotiation
SPP	Serial Port Profile
SMECN	Small Minimum energy communication network
SR	Sensing Radius
TCP/IP	Transmission Control Protocol/Internet Protocol
TEEN	Threshold sensitive Energy Efficient sensor Network protocol
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
WIMAX	Worldwide Interoperability for Microwave Access
WMAN	Wireless Metropolitan Area Network
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
WWAN	Wireless Wide Area Network



Introduction générale

Depuis l'apparition des premiers calculateurs au début du siècle dernier, l'évolution des systèmes informatiques a été jalonnée de grandes étapes de miniaturisation. En effet, l'apparition du transistor, suivie de la puce micro-électronique, des ordinateurs personnels, des ordinateurs portables, puis de poche sont autant de révolutions qui ont marqué ce processus de progression. Désormais, les systèmes électroniques de taille réduite sont omniprésents dans notre environnement.

L'évolution de l'informatique a nécessité, pour sa part, un accroissement sans pareil des besoins, en termes de puissance de calcul et de stockage pour le traitement de l'information et la communication. Les systèmes centralisés sont arrivés logiquement à leur limite intrinsèque et l'apparition des réseaux communicants a permis d'atteindre une puissance de calcul comparable aux super-calculateurs pour un coût minime. Par la suite, la nécessité du partage d'informations à distance et l'évolution des mœurs de notre société vers une hyper-communication a permis la démocratisation de ces systèmes dit répartis. Ces systèmes permettent de distribuer les puissances de calcul et de stockage parmi un nombre grandissant d'entités participantes. De l'ordre de la dizaine au moment de la démocratisation du réseau Internet, à la fin des années 1980, ces systèmes répartis atteignent désormais communément la centaine de millions de participants avec la popularisation des systèmes pair-à-pair, tels que Napster , Skype , ou autres BitTorrent.

Le désir de miniaturisation, jumelé avec les technologies de ces systèmes communicants à calculs répartis, a fait récemment éclore un ensemble de nouveaux systèmes dit d'informatique diffuse ou embarquée. La réduction des entités électroniques se trouvant face à une limitation physique des composants, la distribution de la puissance au sein d'un système dit collaboratif a permis de pallier cette limitation.



PDF Complete
Your complimentary use period has ended.
Thank you for using PDF Complete.

[Click Here to upgrade to Unlimited Pages and Expanded Features](#)

communication sans-fil, les éléments de ces nouveaux systèmes peuvent donc être aisément déployés, sans nécessiter d'infrastructure matérielle coûteuse, encombrante et pénible à mettre en place et à entretenir. La restriction concernant la puissance et le déploiement s'accroissant, la réduction de taille des entités physiques s'est intensifiée permettant de voir apparaître des ordinateurs plus petits qu'une pièce d'un Dinar algérien. Ces nouveaux micro-ordinateurs, qui sont au cœur de notre étude, se situent actuellement à la frontière avec un nouveau domaine émergent : celui des nano-technologies.

En parallèle, les applications de surveillance, de protection et d'observation de notre environnement se sont accrues ces dernières années, aussi bien dans le milieu médical qu'écologique ou militaire. Malheureusement, l'intervention humaine n'est pas possible dans tous les lieux d'investigation. Les années 2000 ont alors vu la naissance de «poussières intelligentes», ensemble de plate-formes matérielles miniaturisées couplées avec un module d'acquisition de données permettant de capter et de collecter des stimuli ou événements issus de l'environnement local de ce capteur. Les faibles possibilités technologiques d'un capteur unique ne lui permettent pas d'avoir une utilité propre, mais la mise en réseau d'un grand nombre de ceux-ci ouvre des opportunités de progrès et de fonctionnement palpitantes.

L'intérêt des communautés issues de la recherche et de l'industrie pour ces réseaux de capteurs sans fil (RCsF) s'est accru par la potentielle fiabilité, précision, flexibilité, faible coût ainsi que la facilité de déploiement de ces systèmes. Les caractéristiques des RCsF permettent d'envisager un grand nombre d'applications d'observation répartie dans l'espace. La spontanéité, l'adaptabilité du réseau et la dynamique de sa topologie dans le déploiement des RCsF soulèvent de nombreuses questions encore ouvertes. L'une des limitations contraignantes de ces réseaux est la faible ressource énergétique des capteurs due essentiellement à leur taille minimaliste et leur indépendance filaire. Cette contrainte doit être considérée comme la préoccupation de premier ordre dans la conception et le déploiement d'un RCsF.

Les réseaux de capteur se caractérisent par une absence d'infrastructure et de gestion centralisée. Dans ce type de réseaux, chaque élément peut bien évidemment émettre et recevoir des messages, mais assure également un rôle de relais de l'information afin que

de proche en proche. Chaque nœud du réseau doit donc posséder des capacités de routage. Grâce à ce routage, la portée radio d'un nœud peut être virtuellement étendue en utilisant ses voisins comme relais de l'information.

La problématique du routage de l'information dans ce type de réseau est complexe.

En effet, les réseaux de capteur sont souvent peu stables :

- Les nœuds peuvent être mobiles.
- les nœuds peuvent entrer et sortir du réseau à tout moment, soit parce qu'ils s'éteignent, soit parce qu'ils sortent de la portée radio de nœuds du réseau.
- les ressources des nœuds sont souvent limitées (capacité de calcul, énergie...).
- le médium radio est peu fiable en termes de perte.

Il existe différentes méthodes pour résoudre cette problématique qui correspondent à autant de protocoles de routage différents.

Parmi ces protocoles on trouve SPEED, qui est un protocole de routage basé sur la QoS temps réel. Sa caractéristique fondamentale est la garantie d'un délai de livraison de bout en bout optimale. Cependant, l'utilisation de ce protocole dans les réseaux de capteur dense à grande échelle fait augmenter le nombre total des paquets de contrôle générer ce qui crée plusieurs problèmes : 1) surcharge du réseau, 2) diminution de durée de vie du réseau, et 3) retards dans la livraison des données.

Notre travail consiste à :

1. Implémenter le protocole SPEED dans le simulateur ns-2.
2. Apporter des améliorations au protocole SPEED afin de lui éviter les problèmes cités auparavant.
3. Comparer le protocole ainsi obtenu au protocole SPEED par simulation dans ns-2.

En premier lieu, nous introduisons ce mémoire par un chapitre présentant de manière générique les différents standards utilisés dans les réseaux sans fil. Ensuite, le deuxième chapitre fait l'objet d'une description synthétique des réseaux de capteurs, leurs architectures, leurs caractéristiques et contraintes ainsi que leurs domaines d'applications variés. Le troisième chapitre synthétise tous les protocoles de routage



PDF
Complete

*Your complimentary
use period has ended.
Thank you for using
PDF Complete.*

[Click Here to upgrade to
Unlimited Pages and Expanded Features](#)

quatrième chapitre se consacre pour l'étude du protocole de routage SPEED ainsi que ces problèmes lorsqu'il est déployé dans les réseaux de capteur dense à grand échelle. Nous avons essayé de résoudre ces problèmes en proposant notre nouveau protocole EESPEED (Energy-aware clustering SPEED). Dans le dernier chapitre, nous exposons les résultats de nos simulations relatives aux deux protocoles de routage mentionnés et nous comparons les performances de chacun en termes de cinq métriques. Ces métriques sont en fonction de deux variables : la densité et la mobilité des nœuds dans le réseau. En finie ce mémoire par des conclusions et perspectives.

Chapitre 1

Les réseaux sans fil

1.1 Introduction

Au cours des dernières années, la prolifération des ordinateurs mobiles (par exemple, les ordinateurs portables, les appareils numériques de poche, et les assistants numériques personnels [PDA]) a entraîné un changement révolutionnaire dans le monde informatique. Comme l'illustre la figure 1.1, nous sommes passés de l'âge de l'ordinateur personnel (PC) (c'est-à-dire, un appareil informatique par personne) à l'âge de multi-appareil informatique dans lequel les utilisateurs utilisent au même temps, plusieurs plates-formes électroniques grâce à laquelle ils peuvent accéder à toute l'information requise quand ils veulent et où ils peuvent être [1]. La nature des ces appareils rend les réseaux sans fil la solution la plus facile pour leur interconnexion.

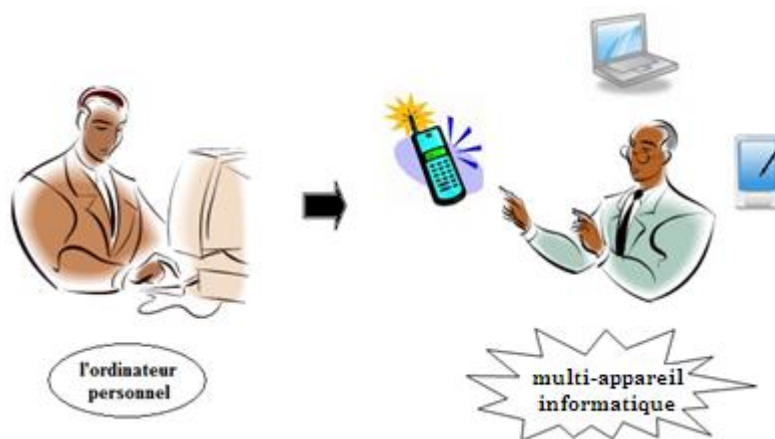


Figure 1.1 - De l'âge de l'ordinateur personnel à la l'âge de multi-appareil informatique

utiliser dans les réseaux sans fil, nous allons maintenant les présenter.

1.2 Les différents standards

Les différentes techniques utilisées dans les réseaux sans fil sont classées suivant leur débit et leur portée. Les technologies de communication cellulaires, également dénommées Wireless Wide Area Network (WWAN), comme le GSM (Global System for Mobile communication), le GPRS (General Packet Radio Service) ou l'UMTS (Universal Mobile Telecommunications System), présentent des débits moindres et des portées supérieures aux technologies utilisées pour les réseaux sans fil tout comme les communications satellites (voir la Figure 1.2). Cette capacité d'avoir un débit élevé permet d'utiliser ces nouvelles technologies radio pour un usage informatique, c'est-à-dire la création de réseaux performants. Ces techniques peuvent être segmentées en trois catégories :

- les réseaux personnels sans fil (WPAN pour Wireless Personal Area Network) qui sont constitués des standards 802.15 de l'IEEE.
- les réseaux locaux sans fil (WLAN pour Wireless Local Area Network) qui sont principalement constitués des normes IEEE 802.11x.
- les réseaux métropolitains sans fil (WMAN pour Wireless Metropolitan Area Network) qui regroupent les standards IEEE 802.16 et 802.20.

1.2.1 Les réseaux métropolitains sans fil (WMAN)

Les WMAN sont, comme leur nom l'indique, des réseaux de grandes dimensions (plusieurs kilomètres). Dans cette catégorie, se trouvent la norme IEEE 802.16 ou WIMAX (Worldwide Interoperability for Microwave Access) et les boucles locales radios.

1.2.2 Les réseaux personnels sans fil (WPAN)

Les WPAN concernent en général les réseaux de faibles portées, de quelques mètres à quelques dizaines de mètres. L'objectif premier de ces réseaux est de connecter des périphériques (imprimante, GPS...) à un ordinateur. De par leur utilisation, ces

les car elles sont destinées à des périphériques ne demandant pas un gros volume d'échange (≤ 1 Mo).

De plus, elles consomment peu d'énergie. Dans le cas d'appareils portables équipés de batterie (PDA, oreillette de téléphone...), l'autonomie est une variable très importante.

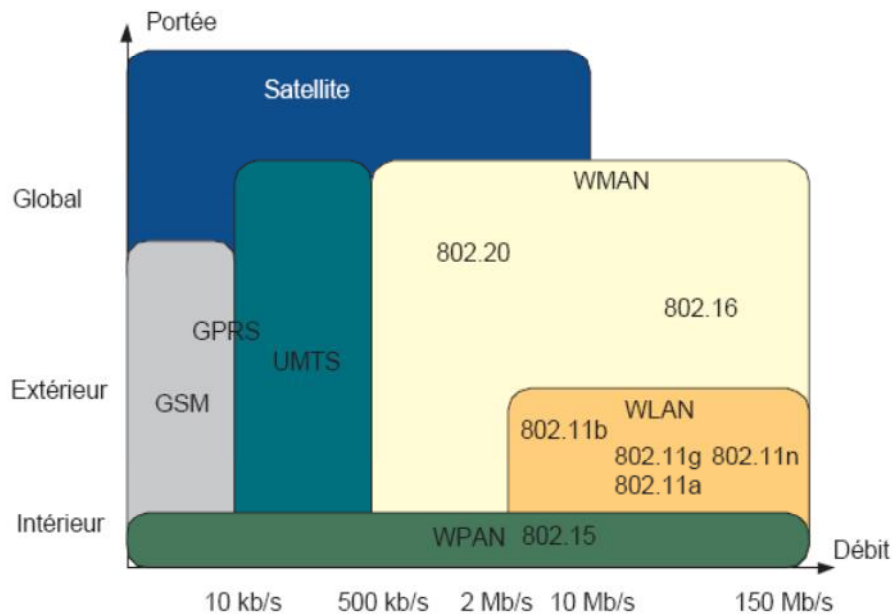


Figure 1.2 - La portée et le débit des différents standards de communication sans fil [2]

Les deux principales technologies de WPAN sont le Bluetooth et le ZigBee.

Le mode de représentation classique de l'implémentation des protocoles de communications est le modèle OSI [3]. Cette formalisation est définie selon une pile de sept couches : application, présentation, session, transport, réseau liaison et physique. Les données transitent depuis la couche application jusqu'à la couche physique à l'envoi et inversement à la réception. A chaque niveau de la pile, les données sont encapsulées. Le standard Bluetooth s'appuie sur une pile de protocoles propre plus complète que celle des réseaux filaires traditionnels car, en plus de l'IP, elle peut supporter de nombreuses applications via différents profils. Le débit offert est de l'ordre de 1 Mb/s. Cette technologie est principalement dédiée à la connexion de périphériques de manière sécurisée. Pour cela, la norme définit de nombreux profils d'application pour gérer les



par exemple le Basic Printing Profile (BPP), le Cordless Telephony Profile (CTP), le Serial Port Profile (SPP).

Le Bluetooth est peu adapté à la création de réseaux distribués de stations ayant des droits équivalents : il y a toujours dans cette technologie une relation de maître-esclave pour la gestion des connexions.

L'autre technologie de WPAN qui se développe de plus en plus est le ZigBee ou IEEE 802.15.413 [4]. Par rapport au standard Bluetooth, celui-ci présente un débit moindre (250 kb/s vs 1 Mb/s) mais consomme nettement moins d'énergie et est donc tout destiné aux réseaux de capteurs. Le standard ne définit que les couches MAC (Media Access Control) et physique du modèle OSI. Le principal avantage de ZigBee est de pouvoir supporter les réseaux distribués ad hoc.

1.2.3 Les réseaux locaux sans fil (WLAN)

Les WLAN sont un domaine des télécommunications en pleine expansion. Ils font le pont entre la téléphonie et l'informatique et possèdent de nombreux avantages :

- ils permettent de rendre mobile les équipements informatiques ;
- ils autorisent des débits compatibles avec les applications informatiques actuelles ;
- ils utilisent des bandes de fréquences libres de droit d'utilisation ;
- ils ne nécessitent que peu ou pas d'infrastructure ;

Il faut malgré tout pondérer tous ces avantages par le fait que les communications radio sont moins fiables que les filaires à cause des interférences radio, des problèmes de multi-trajets des ondes, les irrégularités électromagnétiques... De plus, les WLAN sont moins sûrs que les réseaux filaires : le médium pour faire transiter l'information étant l'air, celui-ci est ouvert à d'éventuels intrus.

A l'heure actuelle, la famille de standards IEEE 802.11 [5] domine le domaine des WLAN. Il existait d'autres normes comme l'HIPERLAN (HIGH PERFORMANCE Radio Local Area Network) [6], mais, grâce au poids économique de l'industrie américaine [7], elles ont été supplantées par les normes IEEE qui ont d'ailleurs repris bon nombre de propositions des standards européens HIPERLAN (le IEEE 802.11a est très proche de l'HIPERLAN 2).

norme pour les WLAN, connue aussi sous la dénomination Wi-Fi (Wireless Fidelity).

Par rapport au modèle OSI, le IEEE 802.11 ne concerne qu'une partie de la couche de liaison de données 2 et la couche physique 1 et reste donc entièrement compatible avec les couches supérieures (voir la Figure 1.3). Le standard est vu de manière transparente par les applications et les différents protocoles des couches supérieures (http, FTP, TCP/IP...).

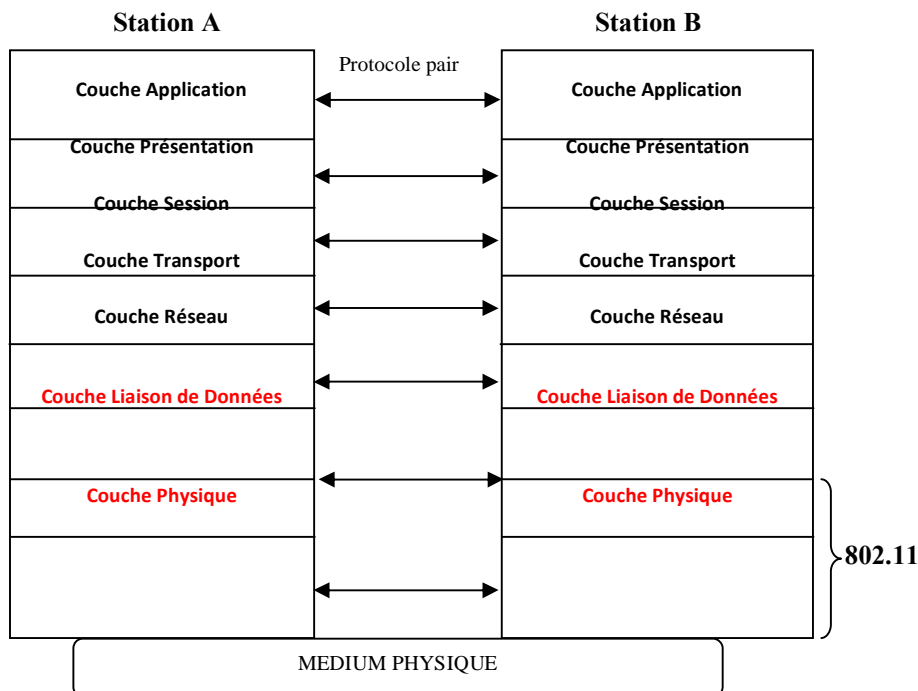


Figure 1.3 - La position du standard IEEE 802.11 dans le modèle OSI [3]

Au niveau de la couche de liaison de données, le IEEE 802.11 supporte deux mécanismes d'accès au médium : le PCF (Polling Coordination Function) et le DCF (Distributed Coordination Function).

Le PCF est un mode centralisé qui garantit à chaque station un accès minimum au médium, cette garantie est assurée par un point d'accès qui distribue les temps de parole à chaque station. Ce mode de fonctionnement est optionnel et est donc peu ou pas implémenté dans les équipements IEEE 802.11 [8].

ure, le mécanisme d'accès au médium utilisé est le DCF [Dhoutaut 03]. Cet algorithme est basé sur le CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). Ce mode consiste à écouter le médium avant d'émettre afin d'éviter les collisions. Lorsque le médium est libre, l'émission est possible mais, afin d'éviter que toutes les stations qui écoutaient se mettent à émettre au même moment, un compteur de valeur aléatoire est décrémente par la station une fois que le médium est libre et elle attend la fin du décompte pour envoyer ses trames. Ce mécanisme a pour objectif de désynchroniser les émissions des différentes stations et de limiter le risque de collision.

Mais ce mécanisme n'est pas suffisant dans le cas de stations cachées. En effet, comme le montre la Figure 1.4, la station B peut atteindre A et C qui ne se voient pas. Donc, si A envoie des trames vers B, C ne peut pas les entendre et peut émettre vers B, les trames émises par C rentrant alors en collision avec celles de A. Afin d'éviter ce problème, des trames particulières, RTS (Ready To Send) et CTS (Clear To Send) sont utilisées. Avant d'émettre les trames de données, une station émet une trame RTS, par exemple A vers B; B répond alors par une trame CTS indiquant qu'elle accepte l'échange de données.

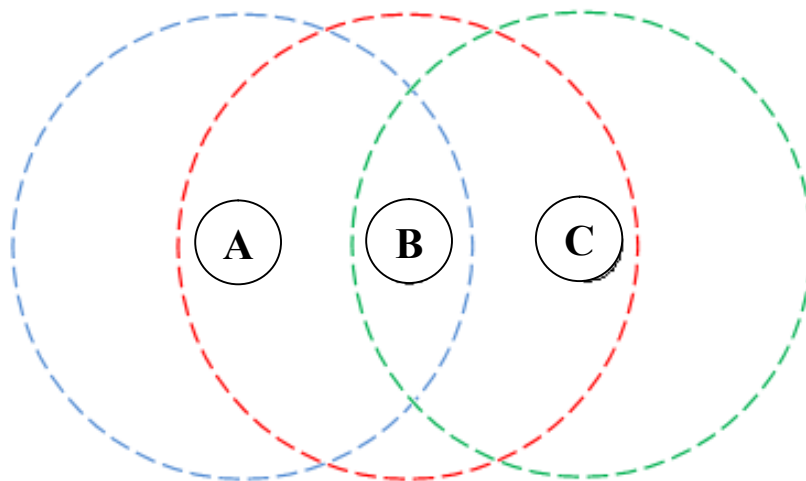


Figure 1.4 - Le problème des stations cachées avec le CSMA/CA

Dans ces 2 trames, la durée de l'échange est indiquée, donc toute station entendant une trame RTS ou CTS dont elle n'est pas destinataire (comme C), doit se taire pendant

qui permet de limiter les risques de collision en plus de l'algorithme de base CSMA/CA.

Les WLAN ont des portées d'émission de quelques centaines de mètres à quelques kilomètres en fonction des antennes utilisées et des obstacles présents. Ces portées permettent d'utiliser les WLAN en extérieur.

1.3 La mise en œuvre des réseaux sans fil

Les WPAN et les WLAN disposent de deux modes de fonctionnement : le mode centralisé et le mode distribué ou ad hoc.

1.3.1 Le mode de fonctionnement centralisé

Le mode de fonctionnement centralisé est basé sur la présence d'un nœud maître au sein du réseau qui administre les communications.

Dans le cas des WPAN (comme Bluetooth), c'est un nœud qui prend en charge ce rôle de chef d'orchestre du réseau. Les autres nœuds du réseau sont alors les esclaves du nœud maître : ce sont des "Piconet" (par exemple dans le cas du Bluetooth un maître peut avoir jusqu'à 7 esclaves en mode actifs et 255 esclaves en mode passif ou esclaves parked). Les esclaves ne peuvent pas communiquer entre eux. Des réseaux plus étendus peuvent être créés, dits "Scatternet", où un esclave peut avoir plusieurs maîtres, ce qui permet de relier entre eux des Piconet (voir la Figure 1.5).

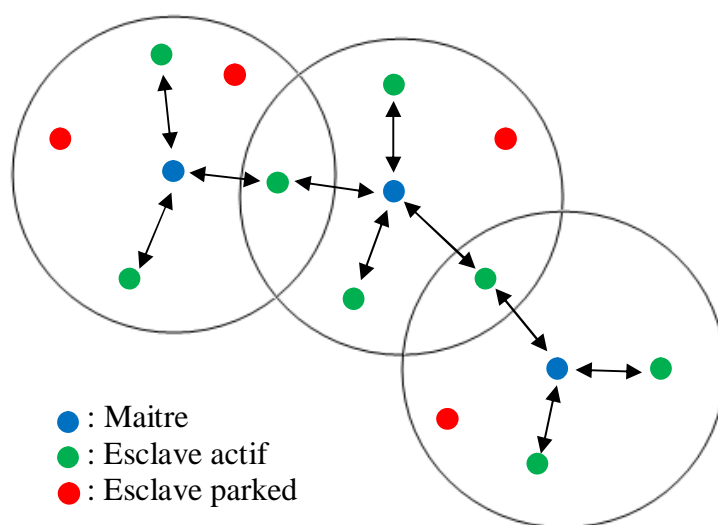


Figure 1.5 - Un exemple de Scatternet composé de trois Piconet [12]

peuvent spécifiquement se voir attribuer cette fonction, c'est le point d'accès. Ce mode de fonctionnement permet d'avoir un réseau relativement stable et de gérer la QoS. Le point d'accès permet de contrôler l'accès des stations au réseau et de leur attribuer des ressources. En revanche, tous les nœuds du réseau doivent être à portée radio du point d'accès. Si le réseau doit être plus grand que cette portée, il faut multiplier les points d'accès : c'est le type de fonctionnement utilisé dans les bureaux, les aéroports, les gares, les hôtels, etc., où des accès Internet sont fournis au public via les "Hotspot".

1.3.2 Le mode de fonctionnement ad hoc

Les réseaux sans fil ont également un mode de communication distribué dit ad-hoc. Ce mode correspond au cas où tous les nœuds du réseau ont le même rôle et dialoguent deux à deux sans relation maître-esclave ou sans point d'accès. Ce mode est intégré dans le fonctionnement de base des WLAN et dans certains WPAN comme le ZigBee. Mais ce mode, tel que défini dans les standards, est limité : en effet, pour dialoguer entre eux, les nœuds doivent être à portée radio, ce qui limite la couverture de tels réseaux.

Ce mode de fonctionnement de base peut être étendu par l'ajout au niveau des nœuds d'un protocole de routage qui permet aux nœuds de propager les informations dans le réseau même s'ils ne sont pas destinataires. Cela permet au nœud de se déplacer tout en gardant une connectivité avec les autres membres du réseau : ce sont des MANET (Mobile Ad hoc NETWORK) [9, 10]. Les travaux de recherche sur ces protocoles de routage sont fédérés au sein de l'IETF (Internet Engineering Task Force), organisation de normalisation d'Internet. Ce type de réseaux permet d'envisager de nombreuses applications comme la domotique, les réseaux de capteurs, les services d'urgence en cas de destruction des infrastructures, la coopération entre des machines de manière spontanée [11]. En outre, cette structure de réseau est souvent présentée comme l'avenir des communications sans fil de par son potentiel [12].



La technologie des réseaux sans fil est une véritable révolution dans le monde de l'informatique. Pouvoir être connecté à un réseau, connu ou non, sans avoir à se soucier du câblage est, en effet, un atout indéniable.

Dans ce chapitre on a vu Les différentes techniques utilisées dans les réseaux sans fil (WMAN, WPAN, WLAN), ainsi que leurs modes de fonctionnement centralisé et ad hoc.

Nous nous intéressons, dans la suite de ce mémoire, à présenter un État de l'art sur les réseaux de capteurs sans fil.



Chapitre 2

Les réseaux de capteurs sans fil :

État de l'art

2.1 Introduction

Grâce aux avancées technologiques de plusieurs secteurs des technologies de l'information, il devient aujourd'hui envisageable de produire en masse des systèmes d'une taille extrêmement réduite (de quelques centimètres) et embarquant des unités de calcul et de communication sans fil pour un coût réduit. Ayant ces caractéristiques, les nœuds capteurs sont capables de générer et d'échanger des données d'une manière autonome et complètement transparente pour les utilisateurs.

Les réseaux de capteurs représentent actuellement un nouveau domaine, en plein développement, émergeant des innovations des technologies de communication.

L'objectif de ce chapitre est de faire une description synthétique des réseaux de capteurs, leurs architectures, leurs caractéristiques et contraintes ainsi que leurs domaines d'applications variés.

2.2 Définition du réseau de capteurs

Les réseaux de capteurs sont souvent composés d'un nombre très important de nœuds, appelés capteurs. Ces nœuds sont des entités capables d'opérer en toute autonomie afin de collecter, traiter et envoyer les données relatives à leur environnement. Déployés de façon à couvrir un territoire donné, les capteurs communiquent par radio afin de concentrer l'information sur une station collectrice située au cœur ou en bordure du territoire, appelée nœud « Sink » [13]. Ces entités

qui est une source d'énergie non durable, ce qui présente la contrainte la plus gênante pour la survie d'un tel réseau.

Les réseaux de capteur ne définissent pas une architecture préexistante puisque les capteurs peuvent se trouver fixés à un endroit précis ou mobile, formant ainsi un réseau sans infrastructure prédéfinie. Tel réseau ne se limite pas à un domaine particulier mais il peut s'adresser à une diversité de secteurs [13,14,15,16] comme la biologie, la chimie, l'environnement, ainsi que la surveillance sismique et même la télésurveillance personnelle.

2.3 Composant d'un nœud capteur

Un nœud capteur est constitué des principales composantes suivantes :

- **Unité de captage (Sensing Unit)** : elle permet de capturer le phénomène observé et le convertir depuis un signal analogique en un numérique. Il sera, ensuite, fourni à l'unité de calcul.

- **Unité de traitement (Processing Unit)** : elle est chargée d'exécuter les protocoles de communication qui permettent aux nœuds capteurs de collaborer avec les autres nœuds pour accomplir la requête en question.

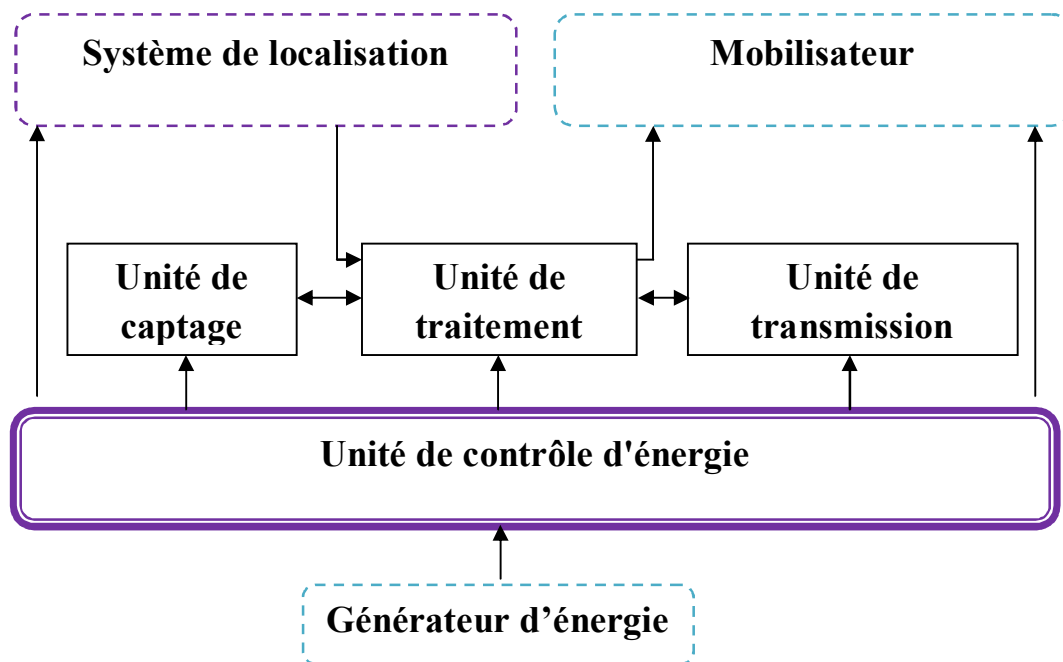


Figure 2.1 - Les composants d'un nœud capteur

Receiver Unit): elle est chargée d'effectuer toutes les émissions et les réceptions de données.

- **Unité de contrôle d'énergie (Power Unit)** : elle effectue des opérations de contrôle de l'énergie restante et de mesure de la durée de vie du nœud capteur.

- **Système de localisation (Location Finding System)** : il fournit des informations sur la localisation requise par les techniques de routage.

- **Mobilisateur (Mobilizer)** : il est appelé si le nœud capteur doit être déplacé pour accomplir la requête à traiter.

2.4 Architecture des réseaux de capteurs

Les nœuds de capteurs sont habituellement dispersés dans un champ de capteur « sensor field ». Ils forment ainsi un réseau sans fil à multi-saut comme (figure 2.2). Chaque nœud a pour mission la collecte des données et leurs routages vers la station de base « Sink ». A son tour, la station de base transmet les informations reçues à partir d'Internet ou par satellite à l'utilisateur final « task manager ».

Il existe deux types d'architectures pour les réseaux de capteurs : les réseaux de capteurs plats et les réseaux de capteurs hiérarchiques. [14,15]

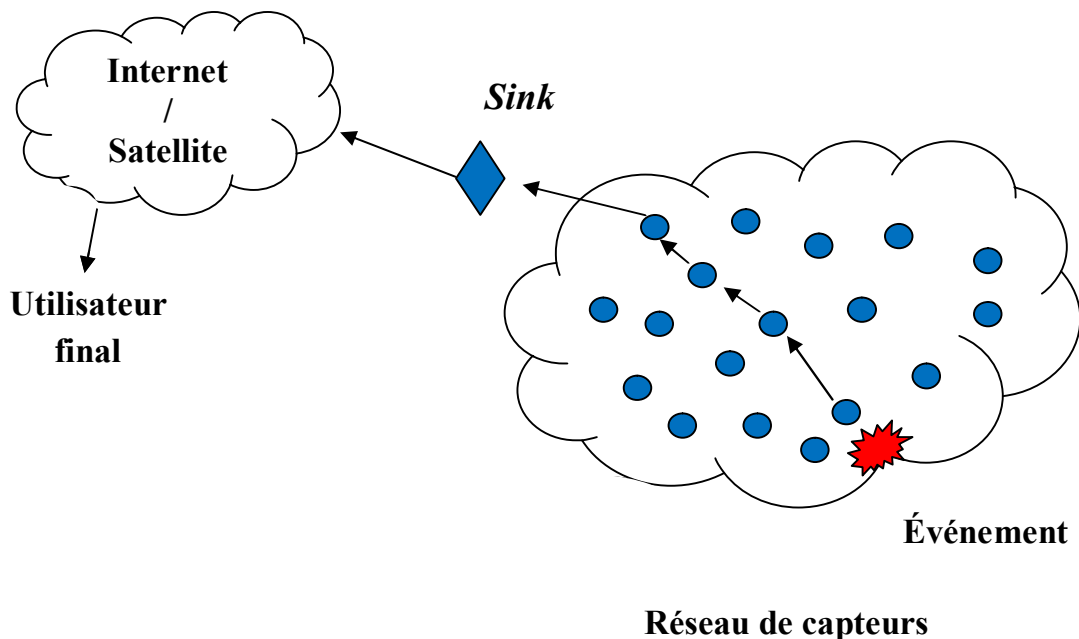


Figure 2.2 - Architecture d'un réseau de capteurs [14]



PDF Complete
Your complimentary use period has ended.
Thank you for using PDF Complete.
[Click Here to upgrade to Unlimited Pages and Expanded Features](#)

ans fils plats

Un réseau de capteurs sans fil plat est un réseau homogène, où tous les nœuds sont identiques en termes de batterie et des fonctions, excepté le « Sink » [15]. Ce dernier joue le rôle d'une passerelle et est responsable de la transmission de l'information collectée à l'utilisateur final.

2.4.2 Les réseaux de capteurs hiérarchiques

Une architecture hiérarchique a été proposée pour réduire le coût et la complexité de la plus part des nœuds capteurs. Elle consiste à introduire un ensemble de nœuds plus coûteux et plus puissants, en créant une infrastructure qui décharge la majorité des nœuds simples à faible coût de plusieurs fonctions du réseau. L'architecture hiérarchique est composée de plusieurs couches : une couche de capteur, une couche de transmission et une couche de point d'accès.

2.5 Caractéristiques des réseaux de capteurs

Les principales caractéristiques des réseaux de capteurs se résument dans ce qui suit :

2.5.1 Densité « importante » des nœuds

Les réseaux de capteurs se composent généralement d'un nombre très important des nœuds pour garantir une couverture totale de la zone surveillée. Ceci engendre un niveau de surveillance élevé et assure une transmission plus fiable des données sur l'état du champ de capteur.

2.5.2 Topologie dynamique

La topologie des réseaux de capteurs instable est le résultat des trois facteurs essentiels suivants:

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

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



PDF Complete
Your complimentary use period has ended.
Thank you for using PDF Complete.

[Click Here to upgrade to Unlimited Pages and Expanded Features](#)

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

2.5.3 Auto organisation

L'auto organisation s'avère très nécessaire pour ce type de réseau afin de garantir sa maintenance. Vu les différentes raisons résultant une topologie instable du réseau de capteur, ce dernier devra être capable de s'auto organiser pour continuer ses applications.

2.5.4 La tolérance de fautes

Le réseau doit être capable de maintenir ses fonctionnalités sans interruptions en cas de défaillance d'un ou plusieurs de ses capteurs. Cette défaillance peut être causée par une perte d'énergie, ou par dommage physique ou interférence de l'environnement. Le degré de tolérance dépend du degré de criticité de l'application et des données échangées [16].

2.5.5 Scalabilité

Les réseaux de capteurs peuvent contenir des centaines voire des milliers de nœuds capteurs [16]. Un nombre aussi important engendre beaucoup de transmissions inter nodales et nécessite que le nœud « Sink » soit équipé d'une mémoire importante pour stocker les formations reçues.

2.6 Contraintes et facteurs conceptuelles des réseaux de capteurs

L'architecture des réseaux de capteurs peut être influencée par certains facteurs pouvant agir sur son bon fonctionnement :

2.6.1 Pannes fréquentes

Pour que les paquets de données atteignent la destination finale « Sink », ils vont passer par un grand nombre de nœuds. A cause de sa topologie dynamique et la probabilité de rencontrer un nœud capteur en panne ou mort, le réseau de capteurs ne



son importants. De plus, la communication radio peut être bruitée, ce qui peut endommager l'information transmise

2.6.2 L'environnement

Les nœuds capteurs doivent être conçus d'une manière à résister aux différentes et sévères conditions de l'environnement : forte chaleur, pluie,...etc.

2.6.3 La topologie dynamique

La mobilité des nœuds, la possibilité d'étendre le réseau par ajout de nouveaux nœuds et la suppression de nœuds défectueux changent fréquemment la topologie des réseaux. Ceci nécessite une maintenance permanente pour assurer le bon fonctionnement des réseaux de capteurs.

2.6.4 La consommation d'énergie

Un capteur, de par sa taille, est limitée en énergie. Dans la plupart des cas, le remplacement de la batterie est impossible, ce qui veut dire que la durée de vie d'un capteur dépend grandement de la durée de vie de sa batterie. Les recherches actuelles se concentrent principalement sur les moyens d'optimiser la consommation d'énergie par les nœuds capteurs.

2.7 Les modèles de transmission des données dans les réseaux de capteurs

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

É Le modèle commandé par événement (event driven)

É Le modèle commandé par requête (query driven)

É Le modèle continu (continuous)



évènement

La génération et la transmission des paquets DATA est commandé par la réalisation d'un évènement. La plupart des applications commandées par évènement [17] sont des applications intolérantes aux délais (temps réel), critiques, interactives et de non bout en bout. En fait, au lieu d'avoir un nœud émetteur et un autre récepteur de l'information, on trouve un nœud récepteur (la station de base « sink ») et un groupe de nœuds capteurs, se trouvant proche de l'évènement, qui sont tous des émetteurs de la même information.

La réussite de ces applications, pour ce modèle, repose essentiellement sur la détection de l'évènement et la rapidité des prises des réactions nécessaires pour assurer l'aspect temps réel des applications.

L'inconvénient majeur de ce modèle est la redondance des données. En fait, les nœuds excités par le même évènement envoient la même information a la station de base « sink ». Pour cela, un protocole de routage basé sur la négociation des données est recommandé.

2.7.2 Le modèle commandé par requête

Le modèle commandé par requête est semblable au modèle commandé par évènement sauf que la collecte des informations sur l'état de l'environnement est initiée par des interrogations envoyées par la station de base « sink », alors que, pour le modèle précédant, elle est déclenchée suite à un évènement détecté. La plupart des applications commandées par requête sont des applications interactives, critiques, de non bout en bout et leur tolérance aux délais dépend de l'urgence de l'interrogation [17].

Notons que le modèle commandé par requête peut être utilisé pour contrôler et reconfigurer les nœuds. Par exemple, le « sink » peut envoyer des commandes au lieu des interrogations pour modifier le programme d'un nœud capteur, modifier son taux de trafic ou son rôle. Seul le nœud capteur jouant le rôle de « sink » est autorisé d'émettre des demandes d'interrogations ou des commandes et ce pour assurer l'ordre et la hiérarchie de réseau de capteur.



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

2.8 Applications des réseaux de capteurs

Les réseaux de capteurs promettent beaucoup de domaines de nouvelles applications à savoir :

2.8.1 Applications militaires

Les nœuds capteur devraient fournir les services suivants:

- É Surveillance du champ de bataille
- É Reconnaissance des forces d'opposition
- É Repérage des cibles
- É Évaluation des dommages de la bataille
- É Détection et reconnaissance d'attaque nucléaire, biologique et chimique.

2.8.2 Applications de santé

Certaines applications de santé des réseaux de capteurs sont:

- É Fourniture d'interfaces pour les handicapés;
- É Repérage et surveillance des médecins et des patients dans les hôpitaux, télésurveillance des données physiologiques humaines.

2.8.3 Applications environnementales [16]

Ces applications incluent :

- É Le repérage des mouvements des oiseaux, des petits animaux et des insectes;
- É La surveillance des conditions environnementales qui affectent les récoltes et le bétail;
- É L'exploration planétaire;

die, séismeí)

É La détection d'inondation;

É L'étude de pollution.

2.9 La zone de couverture d'un capteur

Les capteurs fonctionnent avec un modèle à seuil.

Un capteur possède deux zones : une zone de perception (SR) et une zone de communication (CR). Ces deux zones sont représentées dans la figure 2.3 par deux cercles qui ont pour centre le capteur:

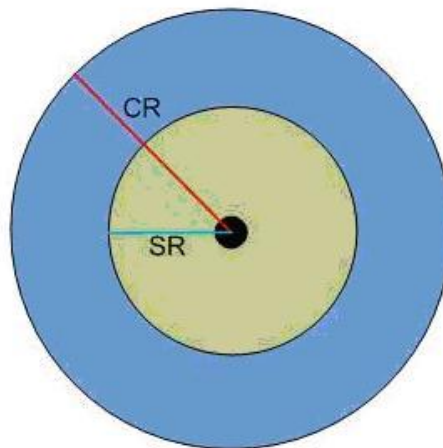


Figure 2.3 - La zone de perception (SR) et la zone de communication (CR)

En influant sur le rapport entre le rayon du SR et le rayon du CR, on va modifier les contraintes. Ainsi, on va pouvoir minimiser le nombre de nòuds actifs et maximiser la durée de vie du réseau.

Comme les capteurs sont généralement disposés sur la zone à couvrir de façon aléatoire, il est nécessaire de disposer d'une densité importante de capteurs. Mais si la densité de capteurs est trop importante et que la zone que l'on veut surveiller est "trop" couverte, alors des capteurs vont fonctionner inutilement.

2.10 Notion de cluster

L'agrégation de nòuds en clusters permet de réduire la complexité des algorithmes de routage, d'optimiser la ressource médium en la faisant gérer localement par un chef

faciliter l'agrégation des données, de simplifier la gestion du réseau et en particulier l'affectation d'adresses, d'optimiser les dépenses d'énergie, et enfin de rendre le réseau plus scalable. L'utilisation de clusters permet aussi de stabiliser la topologie et la gestion du réseau si les tailles de clusters sont grandes par rapport aux vitesses de nœuds mais cela ne fonctionne que dans le cas d'une faible mobilité [18].

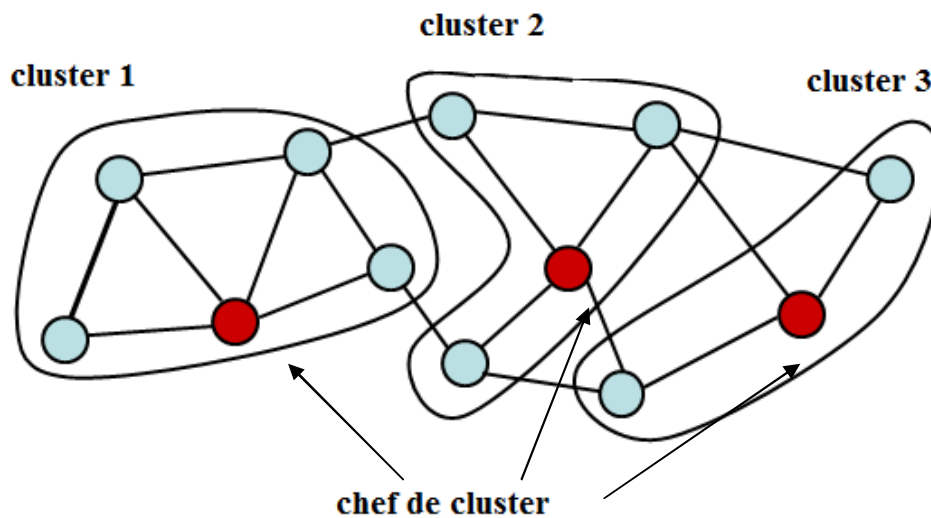


Figure 2.4 - La notion de cluster

2.11 Exemples de capteurs

Les capteurs se déclinent en une multitude de modèles en relation avec l'application à laquelle il est destiné. Parmi les modèles les plus courants, on trouve les MICA, les MICA2 et les MICA2DOT [18,19].

2.11.1 Le capteur MICA

Le capteur MICA (illustré par la Figure 2.5) est un capteur de 2ème génération utilisé pour la recherche et le développement des réseaux de capteur sans-fil et à faible consommation. Le capteur MICA a été développé par l'Université de Berkeley.

On retrouve ce type de nœuds dans les applications suivantes :

- Réseaux de capteurs sans-fil

- Surveillance et sécurité
- Réseaux de capteurs de grande capacité (+1000 nò uds)



Fig. 2.5 - Le capteur MICA

2.11.2 Le capteur MICA2

Le capteur MICA2 (illustré par la Figure 2.6) est un capteur de 3ème génération utilisé pour les réseaux de capteur sans-fil et à faible consommation.



Fig. 2.6 - Le capteur MICA2

2.11.3 Le capteur MICA2DOT

Le capteur MICA2DOT (illustré par la Figure 2.7) est un capteur de 3ème génération utilisé pour les réseaux de capteurs sans-fil et à faible consommation. Le capteur MICA2DOT est similaire au capteur MICA2 mis à part la taille de ce premier (25mm). Ce facteur très intéressant fait du MICA2DOT le plus répandu des capteurs.

On retrouve ce type de nò uds dans les applications suivantes :

- Réseaux de capteurs sans-fil
- Contrôles environnementaux
- Badges
- Ordinateurs portables

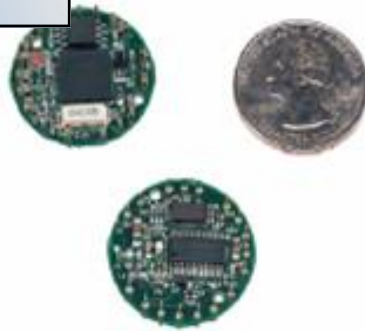


Fig. 2.7 - Le capteur MICA2DOT

2.12 Comparaison entre les réseaux de capteurs et les réseaux ad hoc

Les réseaux de capteurs sans fil sont apparentés aux réseaux ad hoc. En effet, ces deux types de réseaux ont de nombreux points communs [20] :

- Réseaux sans infrastructure
- Architecture décentralisée
- Autonomie
- Utilisation des ondes radio pour communiquer

Cependant, les besoins et les contraintes de ces réseaux diffèrent [13] :

	Capteurs	Ad hoc
Flot de communication	"many to one"	"any to any"
Contrainte clé	Energie	Débit
Communication	diffusion	Point à point
Relation entre les noeuds	Collaboration	Chaque nœud à son objectif

Tab. 2.1 - Différences entre les réseaux de capteurs et les réseaux Ad hoc



PDF Complete
Your complimentary use period has ended.
Thank you for using PDF Complete.

[Click Here to upgrade to Unlimited Pages and Expanded Features](#)

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

Cependant, la réalisation des réseaux de capteurs doit satisfaire quelques contraintes parmi lesquelles on peut citer : la consommation d'énergie, le changement de topologie, la densité importante des réseaux... Ces contraintes exigent que de nouveaux protocoles de routage soient mises au point.

Nous nous intéressons, dans la suite de ce mémoire, à la présentation des protocoles de routages déployés pour les réseaux de capteurs.



Chapitre 3

Routage dans les réseaux de capteurs sans fil

3.1 Introduction

Dans la couche réseau le but principal est de trouver une route et une transmission fiable des données mesurées des capteurs vers le sink qui optimise l'utilisation de l'énergie des capteurs. Ce routage diffère de celui des réseaux de transmission ad-hoc sans fils typiques par les caractéristiques suivantes [21] :

- Il n'est pas possible d'établir un système d'adressage global pour le grand nombre de nœuds.
- Les applications des réseaux de capteurs exigent l'écoulement de données mesurées de sources multiples à un sink particulier.
- Les multiples capteurs peuvent produire des mêmes données à proximité d'un phénomène (redondance).
- Les nœuds capteur exigent ainsi une gestion soignée des ressources.

En raison de ces différences, plusieurs nouveaux algorithmes ont été proposés pour le problème de routage dans les réseaux de capteurs. Ils sont répartis en quatre catégories : les protocoles centrés-données, les protocoles hiérarchiques, les protocoles basés sur la localisation et les protocoles avec considération du flux réseau et la qualité de service (QoS).

3.2 Conception d'architecture du système

La conception des protocoles de routage est influencée par plusieurs facteurs

3.2.1 Dynamique du réseau

La plupart des architectures de réseau suppose que les nœuds capteurs sont stationnaires et d'autre part supporte la mobilité du sink ou du chef de cluster. L'évènement à capturer peut aussi être dynamique ou statique. Pour une application à évènement statique le réseau travail en mode réactive. Par contre, une application à évènement dynamique nécessite des signalisations périodiques [21].

3.2.2 Le déploiement des nœuds

Le déploiement peut être soit déterministe ou auto-organisateur. Dans le premier cas, les capteurs sont placés manuellement et les chemins de routage sont prédéfinis. Dans l'autre cas, les nœuds capteurs sont éparpillés aléatoirement formant une infrastructure de manière ad hoc [21].

3.2.3 Considération d'énergie

Puisque la puissance d'une transmission radio sans fils est proportionnelle au carrée de la distance ou d'ordre plus grand en présence d'obstacle, le routage par saut multiple consommera moins d'énergie qu'une communication directe [21].

3.2.4 Modèle de livraison des données

Selon l'application, le modèle de livraison des données au sink peut être continu, commandé par évènement, commandé par requête ou hybride [21].

3.2.5 Les capacités des nœuds

Un nœud capteur peut être dédié à une fonction particulière telle que la retransmission, la capture et l'agrégation puisque l'affectation des trois fonctions à un même nœud peut épuiser rapidement son énergie [21].



3.2.6 Agrégation et fusion des données

Les nœuds capteurs peuvent générer des données redondantes, les paquets similaires provenant des différents nœuds peuvent être agrégés pour réduire le nombre de transmissions. Sachant qu'un calcul consomme moins d'énergie qu'une communication, des économies d'énergie considérables peuvent être obtenues par l'agrégation des données. On parle de fusion de données quand un nœud est capable de produire un signal plus précis en diminuant le bruit et en utilisant quelque technique pour combiner des signaux [21].

3.2.7 Hétérogénéité des nœuds

Selon l'application un nœud capteur peut avoir différents rôles. L'existence de l'ensemble hétérogène de capteurs soulève beaucoup de questions techniques liées au routage des données [22].

3.2.8 Tolérance aux pannes

La défaillance des nœuds ne devrait pas affecter la tâche globale du réseau. Si beaucoup de nœuds tombent en pannes, le protocole de routage doit s'adapter pour la formation de nouveaux liens [22].

3.2.9 Scalabilité

Le nombre de nœuds capteur déployés peut être dans l'ordre des centaines ou milliers, ou plus. N'importe quel protocole de routage doit pouvoir travailler avec ce nombre énorme de nœuds [22].

3.2.10 Support de transmission

Dans un réseau de capteur multi-saut, les nœuds communicants sont liés par un médium radio. Les problèmes classiques associés aux supports sans fils (taux d'erreur élevé) peuvent également affecter l'opération du réseau de capteur [22].



PDF Complete
Your complimentary use period has ended.
Thank you for using PDF Complete.

[Click Here to upgrade to Unlimited Pages and Expanded Features](#)

3.2.11 Connectivité

La densité élevée des nœuds dans les réseaux de capteur les empêchent d'être complètement isolés les uns des autres. Par conséquent, il est exigeant que les nœuds de capteur soient fortement connectés [22].

3.2.12 Couverture

Dans les réseaux de capteur, chaque nœud obtient une certaine vue de l'environnement. La couverture de l'espace est également un paramètre de conception important dans le routage [22].

3.2.13 Qualité de service

Dans certaines applications, les données devraient être fournies au cours d'une certaine période du moment où elles sont capturées, autrement les données seront inutiles [22].

3.3 Les protocoles centrés-données (data-centric protocols):

Dans le routage centré-données, le sink envoie des requêtes à certaines régions et attend les données des capteurs situés dans les régions choisies. SPIN [23] est le premier Protocole centrés-données, qui considère la négociation des données entre les nœuds en vue d'éliminer les données redondantes et d'économiser l'énergie. Après, le protocole diffusion dirigée [24] a été développé. Ensuite, de nombreux autres protocoles ont été proposés. Dans cette section, nous allons décrire ces différents protocoles.

3.3.1 Propagation et discussion (flooding and gossiping):

Dans le flooding, chaque capteur recevant un paquet de données le renvoie à tous ses voisins et ce processus continue jusqu'à ce que le paquet arrive à la destination ou le nombre maximum des sauts pour le paquet est atteint. D'autre part, le gossiping est une version légèrement améliorée du flooding où le nœud récepteur envoie le paquet à un voisin choisi aléatoirement. Qui va lui aussi envoyer le paquet à un autre voisin choisi aléatoirement et ainsi de suite [25].

Bien que le flooding est très facile à appliquer, il a plusieurs inconvénients, voir les figures 3.1 et 3.2. Ces inconvénients causés par la duplication des messages envoyés au même nœud, le chevauchement quand deux nœuds couvre la même région envoi des paquets similaires au même Voisin et la grande consommation d'énergie sans concédération de la Contrainte d'énergie [23]. Le gossiping évite le problème de duplication des messages par la sélection d'un nœud Aléatoire pour lui envoyer le paquet plutôt que d'utiliser la diffusion. Toutefois, cela cause des retards dans la propagation des données à travers les nœuds.

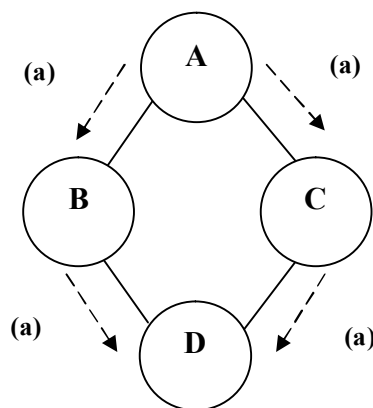


Figure 3.1 - Le problème de la duplication des messages envoyés au même nœud

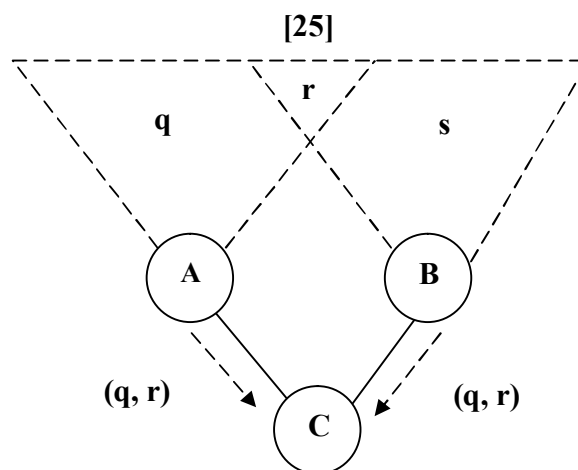


Figure 3.2 - Le problème de chevauchement des zones de couvertures [25]

3.3.2 Protocoles de capteur pour l'information par négociation (SPIN)

L'idée derrière le SPIN (Sensor Protocols for Information via Negotiation) est de nommer les données en utilisant des descripteurs de haut niveau ou des méta-données [23]. Avant transmission, les méta-données sont échangées entre les capteurs par un mécanisme de publicité de données. Chaque nœud recevant de nouvelles données, l'annonce à ses voisins et les voisins intéressés récupèrent les données en envoyant une requête. Il ya trois messages définis dans le protocole SPIN pour l'échange de données entre les nœuds. Ce sont:

- Le message ADV qui permet à un capteur de faire l'annonce d'une méta-donnée particulière.
- Le message REQ qui permet à un capteur de faire une requête (demande de donnée spécifique).
- Et le message DATA qui permet de transporter les données réelles.

La Figure 3.3, Résume les étapes du protocole SPIN.

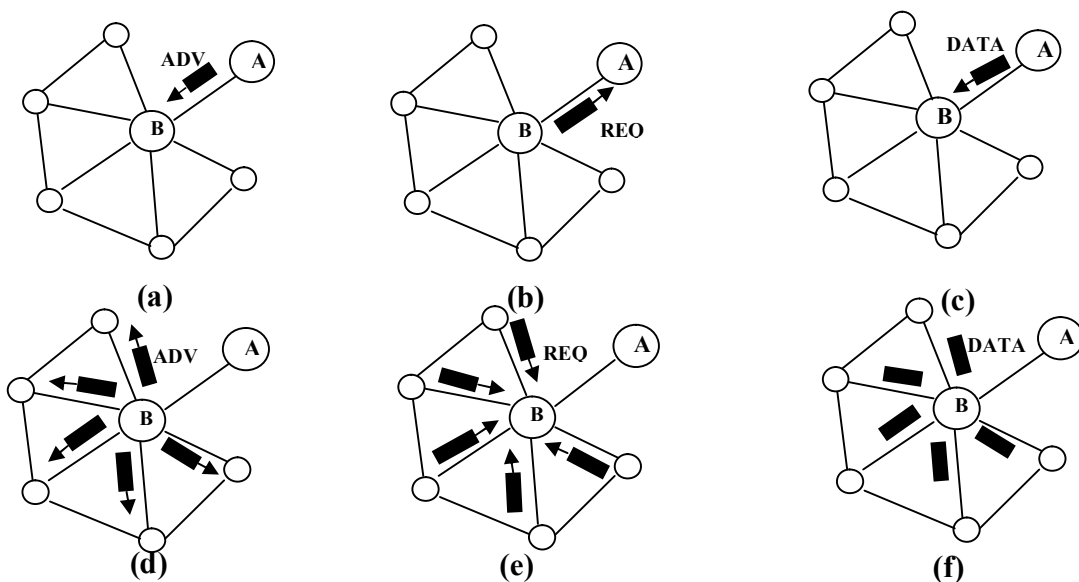


Figure 3.3 - le protocole SPIN [23]

(a) Le nœud A annonce ses données au nœud B, (b) B répond par une requête. (c) B reçoit les données requises, (d) B fait de la publicité à ses voisins qui répondent par des requêtes (e-f)

La négociation par les méta-données du protocole SPIN a résolu les problèmes classiques du flooding. Cependant, le mécanisme d'annonce des données du protocole SPIN ne peut pas garantir la livraison des données. Par Exemple, si les nœuds qui sont intéressés par les données sont très loin de la source et que les nœuds entre la source et la destination ne sont pas intéressés par ces données, ces données ne seront pas Livré à la destination. Par conséquent, SPIN n'est pas un bon choix pour des applications telles que la Détection d'intrusion, qui exigent une livraison fiable des paquets de données sur des intervalles réguliers [21].

3.3.3 Diffusion dirigée

L'idée de la Diffusion dirigée vise à diffusion les données a travers les nœuds capteurs En utilisant un schéma de nommage pour ces données [21]. La raison principale derrière l'utilisation d'un tel système est de se débarrasser des opérations inutiles de routage dans la couche réseau afin d'économiser l'énergie.

Une requête intérêt est définie par une liste de couples attribut-valeur comme le nom des objets, intervalle, la durée, la zone géographique, etc. L'intérêt est diffusé par le sink vers ses voisins. L'intérêt contient aussi plusieurs champs gradient. Un gradient est un lien de réponse de la part du voisin recevant l'intérêt. En utilisant les intérêts et les gradients, plusieurs chemins peuvent être établis entre le sink et la source. L'un de ces chemins est sélectionné par renforcement (figure 3.4).

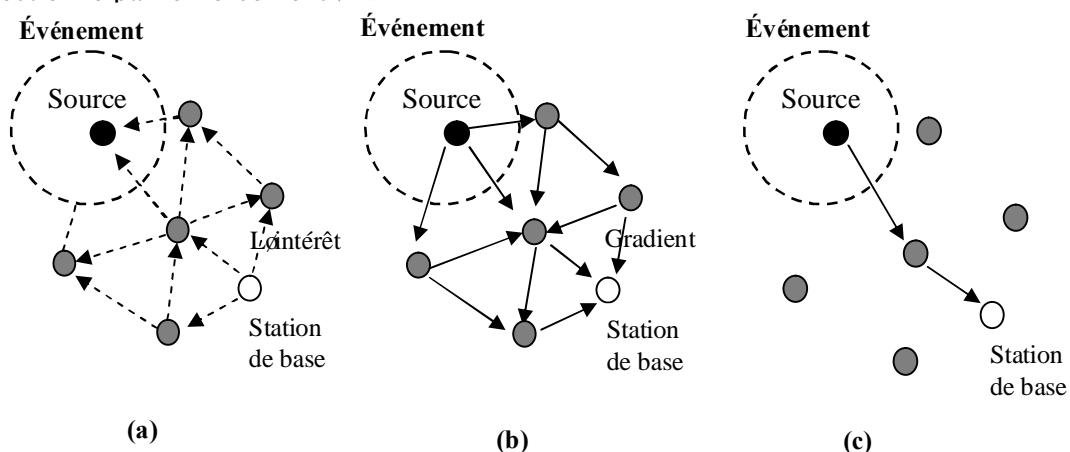


Figure 3.4 - Phases du protocole de diffusion dirigée. [21]

(a)propagation de l'intérêt. (b)construction des gradients initiaux (c)livraison de données par renforcement.



Your complimentary
use period has ended.
Thank you for using
PDF Complete.

[Click Here to upgrade to
Unlimited Pages and Expanded Features](#)

Le sink retransmit le message d'intérêt original a travers le chemin sélectionnez celui qui a le plus Petits intervalle donc renforce le nò ud source à envoyer les données sur ce chemin. Si ce chemin échoue un nouveau ou un alternatif doit être identifié.

Pour cela, la Diffusion dirigée réinitialise le renforcement et recherche un autre chemin, qui permet d'envoyer les données avec le taux le plus bas. Ganesan et al. [26] suggèrent d'employer plusieurs chemins à l'avance, en cas de panne d'un Chemin, l'un des chemins possibles est choisi sans aucun coût pour la recherche d'un autre.

La Diffusion dirigée présente plusieurs avantages. Comme il est centré-données, toutes les Communication sont de voisin à voisin, sans avoir besoin d'un mécanisme d'adressage des nò uds. En outre, la diffusion dirigée consomme peut d'énergie car il est a la demande et il n'y a aucun besoin du maintenir la topologie du réseau.

Toutefois, La Diffusion dirigée ne peut pas être appliquée à toutes les applications de réseaux de capteurs puisque elle est basée sur le modèle de livraison de données à la demande. Les applications qui nécessitent la livraison continue des données au sink ne vont pas fonctionner de façon efficace avec le modèle de livraison de données à la demande. Par conséquent, La diffusion dirigée n'est pas un bon choix comme un protocole de routage pour les applications telles que la surveillance de l'environnement.

3.3.4 Routage avec considération de l'énergie (Energy-aware routing)

Shah et al. [27] on proposé d'utiliser un ensemble de chemins sous-optimal de temps en temps pour augmenter la durée de vie du réseau. Ces chemins sont choisis par le biais d'une Fonction de probabilité, qui dépend de la consommation d'énergie de chaque chemin. Cette technique considère que l'utilisation du chemin d'énergie minimale tout le temps épuise l'énergie des nò uds dans ce chemin. Au lieu de cela, l'un des Multiples chemin est utilisée avec une certaine probabilité pour que la durée de vie du réseau augmente.

Dans ce protocole le fait de choisir un seul chemin limite la capacité de couvrir l'échec d'un nœud ou d'un chemin par opposition à la diffusion dirigée. En outre, l'approche nécessite la collection d'informations de localisation et la mise en place d'un mécanisme d'adressage. Pour les nœuds, ce qui compliquerait le routage par rapport à la diffusion dirigée.

3.3.5 Routage par rumeur (Rumor routing)

L'idée est de transmettre les requêtes aux nœuds qui ont observé un événement particulier. Quand un nœud détecte un événement, il l'ajoute à sa table locale et génère un agent. L'agent parcourt le réseau afin de propager des informations sur les événements locaux aux nœuds distants. Quand un nœud génère une requête pour un événement, les nœuds qui connaissent l'itinéraire, peuvent répondre en référant la table d'événement [28]. Le routage par rumeur maintient un seul chemin entre la source et la destination à l'opposition de la diffusion dirigée ou les données peuvent être envoyées à travers plusieurs chemins.

Les résultats de simulation ont montré que le routage par rumeur économise l'énergie et peut aussi traiter l'échec du nœud. Cependant, le routage par rumeur fonctionne bien lorsque le nombre d'événements est petit. Pour un grand nombre d'événements, le coût de maintenir les agents et les tables d'événement dans chaque nœud ne peut être supporté s'il n'y a pas assez d'intérêts sur ces événements par le sink.

3.3.6 Routage à base de gradient (GBR : Gradient-Based Routing) :

Schurgers et al. [29] ont proposé le routage à base de gradient. L'idée est de garder le nombre de sauts quand l'intérêt est diffusé dans le réseau. Ainsi, chaque nœud peut découvrir le nombre de sauts minimal vers le sink, ce qui est appelé l'altitude du nœud. La différence entre l'altitude d'un nœud et celle de son voisin est le gradient sur ce lien. Un paquet est envoyé sur un lien avec le plus grand gradient.

Grâce à la simulation le routage à base de gradient a montré plus de performance par rapport à la diffusion dirigée en termes de l'énergie totale de communication.



3.3.7 CADR

Cette approche est basée sur deux idées principales CADR (Constrained Anisotropic Diffusion Routing) et IDSQ (Information-Driven Sensor Querying).

CADR est réalisé en activant seulement les capteurs qui sont proches d'un événement particulier et en ajustant dynamiquement les chemins de données. Dans CADR, chaque nœud évalue un objectif information/coût et conduit les données suivant le gradient local et les besoins de l'utilisateur final.

Dans IDSQ, le nœud demandeur peut déterminer quel nœud peut fournir l'information la plus utile avec un avantage additionnel d'équilibrer le coût énergétique. IDSQ fournit une façon de choisir l'ordre optimal des capteurs pour un gain maximal d'information incrémentale, il ne définit spécifiquement pas la requête et la manière dont les informations sont acheminées entre les capteurs et sink. Par conséquent, IDSQ peut être considérée comme une procédure d'optimisation complémentaire.

CADR diffuse des requêtes à l'aide d'un ensemble de critères pour sélectionner les capteurs à recevoir les données, les résultats de simulation ont confirmé que CADR économise plus d'énergie que la Diffusion dirigée. Où les requêtes sont diffusées dans un mode isotrope, atteignant les voisins les plus proches en premier [30].

3.3.8 COUGAR

C'est un protocole qui voit le réseau comme un énorme système de base de données réparties. L'idée principale est d'employer des requêtes déclaratives afin d'abstraire le traitement des requêtes des fonctions de la couche réseau et d'utiliser l'agrégation de données pour économiser de l'énergie. L'abstraction est soutenue par une nouvelle couche de requête entre les couches réseau et application.

COUGAR propose une architecture pour le système de base de données des capteurs dans lequel les nœuds sélectionnent un nœud chef pour effectuer l'agrégation et transmettre les données au sink [31].



Your complimentary
use period has ended.
Thank you for using
PDF Complete.

[Click Here to upgrade to
Unlimited Pages and Expanded Features](#)

Bien que COUGAR fournit une solution indépendante de la couche réseau pour interroger les capteurs, Il a quelques inconvénients: tout d'abord, l'introduction d'une couche supplémentaire pour les requêtes dans chaque nœud capteur apporte des frais supplémentaires aux nœuds en termes de consommation d'énergie et de stockage. Deuxièmement, le calcul des données provenant de plusieurs nœuds exige la synchronisation, c'est-à-dire un nœud relié doit attendre tout les paquets entrant à partir de chaque source, avant de transmettre les données au nœud chef. Troisièmement, les nœuds chef doivent être maintenus dynamiquement pour les empêcher de lâcher.

3.3.9 Transmission active de requête dans les réseaux de capteurs (ACQUIRE)

Comme dans le protocole COUGAR le protocole ACQUIRE (ACTIVE QUery forwarding In sensoR nEtworks) considère le réseau comme une base de données réparties et bien adaptée pour les requêtes complexes. Une requête est expédiée par le sink et chaque nœud recevant la requête peut répondre partiellement en employant l'information dans son cache ou recueille l'information de ses voisins accessible par d sauts puis la transmet à un autre capteur. Une fois la requête complètement résolue, elle est renvoyée au sink.

Le mécanisme ACQUIRE permet de fournir des requêtes efficace par l'ajustement de la valeur du paramètre d . Notez que si d est égale à la taille du réseau, le comportement du protocole est similaire à inondation. D'autre part, la requête parcourt plusieurs nœuds si d est trop petit [32].

Dans ACQUIRE, la sélection du prochain nœud pour lui transmettre la requête est soit par hasard ou basé sur le potentiel maximal de satisfaction de la requête.

3.4 Les protocoles hiérarchiques:

Le but principal du routage hiérarchique est de maintenir efficacement la consommation d'énergie des nœuds capteurs en les impliquant dans une

communication multi-sauts dans un cluster particulier et en exécutant l'agrégation et la fusion des données afin de diminuer le nombre de messages transmis au sink.

3.4.1 Hierarchie de regroupement adaptatif à faible énergie (LEACH)

LEACH (Low-Energy Adaptive Clustering Hierarchy) est l'algorithme de routage le plus connue dans les réseaux de capteurs. L'idée de LEACH est de former des clusters de nœuds capteurs en se basant sur la force du signal reçue et d'employer le chef de grappe local comme routeur au sink. Tout traitement de données est local au cluster. Le rôle de cluster-head est échangé aléatoirement entre les nœuds afin d'équilibrer les charges [33].

LEACH est entièrement distribué et n'exige pas une connaissance globale du réseau. Cependant, LEACH utilise le routage à seul saut où chaque nœud peut transmettre les données directement au cluster-head et au sink. Par conséquent, il n'est pas applicable aux réseaux déployés dans les grandes régions. En outre, l'idée de la dynamique du cluster, Peut diminuer le gain en consommation d'énergie.

3.4.2 Assemblage a puissance efficace dans les systèmes d'information de capteurs (PEGASIS)

PEGASIS (Power-Efficient GATHERing in Sensor Information Systems) est une amélioration du protocole LEACH. Au lieu de former plusieurs grappes, PEGASIS forme des chaînes de nœuds de sorte que chaque nœud transmet et reçoit d'un voisin et seulement un nœud est choisi parmi cette chaîne pour transmettre au sink. Les données recueillies se déplacent d'un nœud à un autre, seront agrégées puis envoyées au sink par un nœud chef (leader).

La différence de PEGASIS par rapport à LEACH réside dans : (1) l'utilisation du routage multi-sauts en formant des chaînes et (2) la sélection d'un seul nœud pour transmettre les données à la station de base au lieu d'utiliser plusieurs nœuds. PEGASIS a montré qu'il est plus performant que LEACH en termes de la taille et la topologie du réseau. Ces gains en performance sont obtenus grâce à l'élimination de la surcharge causer par la dynamique du cluster dans LEACH et aussi par la diminution du nombre de transmissions et de réception

à l'aide de l'agrégation de données. Toutefois, PEGASIS introduit des retards excessifs pour les nœuds distants de la chaîne. En plus, un seul nœud chef peut devenir un goulot d'étranglement. [34]

Le PEGASIS hiérarchique est une extension du PEGASIS, dans le quel les nœuds construisent une chaîne qui forme un arbre hiérarchique, et chaque nœud chef choisi dans un niveau particulier transmet des données aux nœuds dans le niveau supérieur de la hiérarchie jusqu'à atteindre la station de base.

3.4.3 TEEN et APTEEN

TEEN (Threshold sensitive Energy Efficient sensor Network protocol) est un protocole hiérarchique conçu pour être sensible aux changements soudains des attributs captés tels que la température. L'architecture du réseau est basée sur un groupement hiérarchique où les nœuds les plus proches forment des clusters, ce processus est appliqué au deuxième niveau jusqu'à la station de base comme il est représenté dans la figure 3.5.

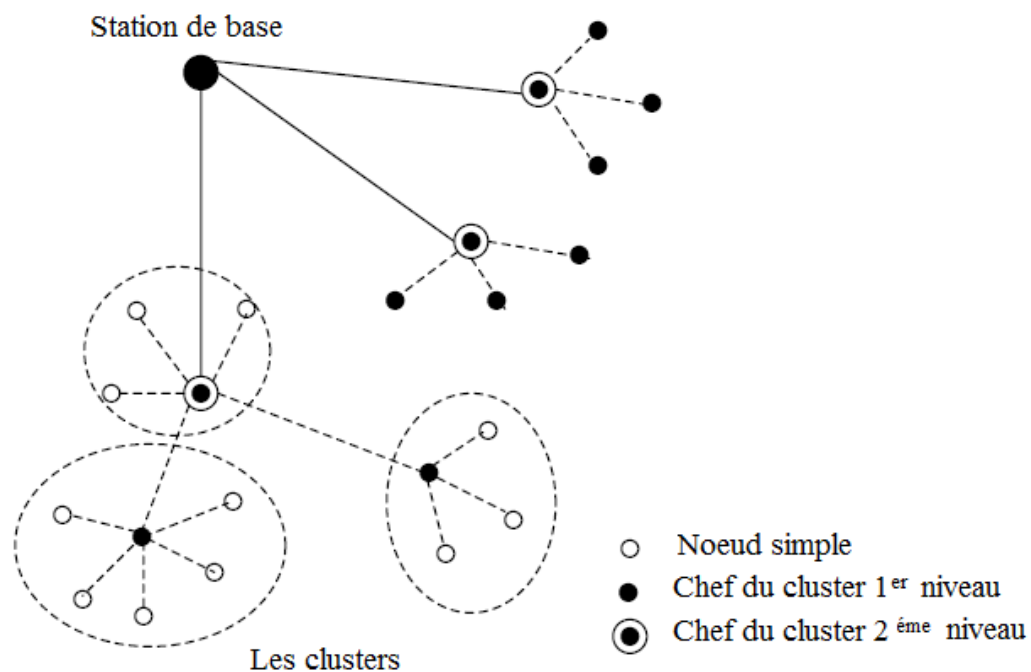


Figure 3.5 - Le groupement hiérarchique dans TEEN et APTEEN [35]

Après la construction des clusters, le chef du cluster diffuse deux seuils aux nœuds. Qui sont la valeur minimale d'un attribut pour pouvoir être transmis et le degré minimale du changement de cet attribut. Cependant, TEEN n'est pas bon pour les applications qui nécessitent des rapports périodiques, en plus l'utilisateur ne recevra rien si les seuils ne sont pas atteints [35].

Le TEEN adaptatif (APTEEN) est une extension du TEEN basée sur la capture périodique des données et la réaction aux événements temps-réel. Quand la station de base forme les clusters, les chefs des clusters diffusent les attributs, les seuils et le plan de transmission à tous les nœuds et effectuent également l'agrégation des données afin d'économiser de l'énergie.

L'inconvénient principal de ces deux approches est la complexité de former les clusters à plusieurs niveaux.

3.4.4 Routage avec considération de l'énergie à base de cluster

Basé sur une architecture trois-tiers. Les clusters sont formés avant l'opération du réseau. L'algorithme utilise les chefs des clusters (passerelles) qui sont moins contraints par l'énergie que les capteurs et qui sont supposés connaître l'endroit des nœuds capteurs [21]. Les passerelles maintiennent les états des capteurs et installent les routes multi-sauts pour la collecte des données et informent chaque nœud des slots dans lesquelles il devrait écouter d'autres transmissions et les slots, que le nœud peut employer pour sa propre transmission. Le sink communique seulement avec les passerelles.

Les nœuds capteurs dans un cluster peuvent être dans un des quatre états (figure 3.6) : capture seulement, transmission seulement, capture et transmission ou inactif.

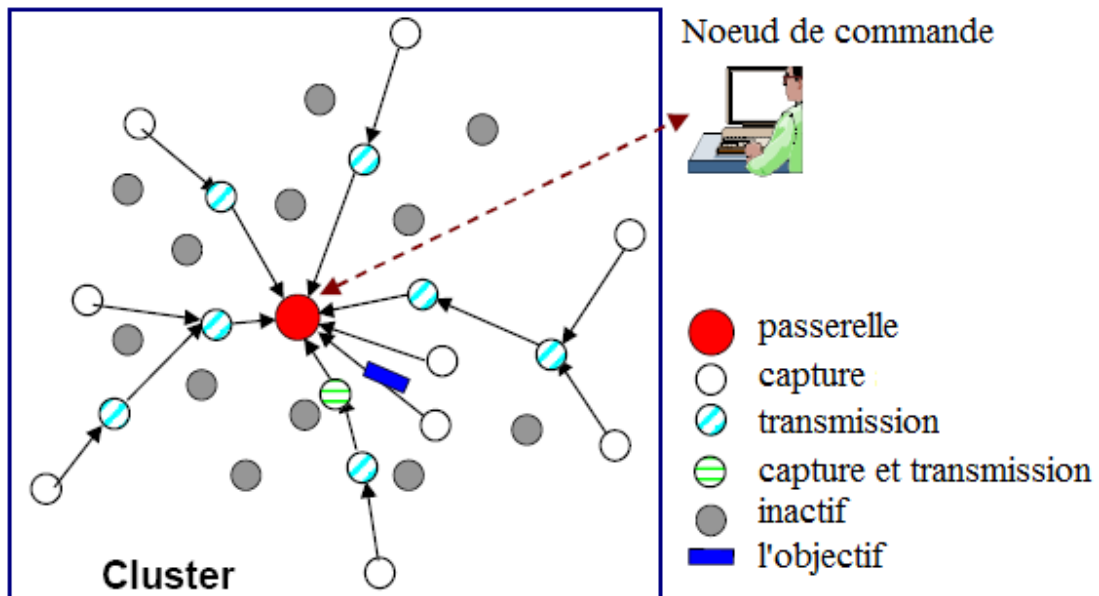


Figure 3.6 - Un cluster typique dans un réseau de capteur [21]

3.4.5 Protocole auto-organisateur

L'architecture de routage exige l'adressage de chaque nœud. Un nœud capteur est identifié par l'adresse du routeur auquel il est connecté. L'architecture de routage est hiérarchique où les groupes de nœuds sont formés et fusionnés si nécessaire.

L'algorithme d'auto-organisateur est composé de quatre phases [36]:

É *La phase de découverte*: Les nœuds dans le voisinage de chaque capteur sont découverts.

É *La phase d'organisation* : Les groupes sont formés et fusionnés en formant une hiérarchie. Une adresse est attribuée à chaque nœud. Les tables de routage sont créées pour chaque nœud. Les arbres de diffusion qui couvrent tous les nœuds sont construits.

É *La Phase de maintenance*: La mise à jour des tables de routage et des niveaux d'énergie des nœuds sont faites dans cette phase. Chaque nœud informe ses voisins sur sa table de routage et son niveau d'énergie.

É *La phase d'Auto-réorganisation*: En cas de partition ou l'échec d'un nœud, la réorganisation des groupes est exécutée.

L'avantage principal de l'utilisation de cet algorithme est le petit coût de maintenir les tables de routage. De plus, l'énergie consommée pour la diffusion d'un message est inférieure à celle consommée dans le protocole SPIN à cause de l'utilisation des arbres de diffusion dans l'algorithme.

L'inconvénient de l'algorithme est dans *la phase d'organisation*, qui n'est pas à la demande. Un autre problème est possible dans formation de l'hierarchie quand il ya beaucoup de coupures dans le réseau. Ce qui augmente la probabilité d'appliquer la *phase de réorganisation*, qui est coûteuse.

3.5 Les protocoles basés sur la localisation

Dans la plupart des protocoles de routage l'information sur la localisation des nœuds est nécessaire afin de calculer la distance entre deux nœuds particuliers de sorte que la consommation d'énergie puisse être estimée.

3.5.1 MECN et SMECN

MECN (Minimum Energy Communication Network) utilise le GPS à basse puissance. L'idée principale est de trouver un sous-réseau, qui aura moins de nœuds et exige moins de puissance pour la transmission entre deux nœuds particuliers quelconques. SMECN (Small MECN) est une extension de MECN. Le sous-réseau construit par SMECN est probablement plus petit (en termes de nombre d'arcs) que celui construit par MECN si les diffusions peuvent atteindre tous les nœuds dans une région circulaire autour du diffuseur.

Les résultats de simulation ont montré que SMECN utilise moins d'énergie que MECN et le coût de maintenance des liens est aussi moins. Cependant, trouver un sous-réseau avec un petit nombre d'arcs introduit un coût de plus dans l'algorithme [37].

3.5.2 GAF

GAF (Geographic Adaptive Fidelity) est un algorithme de routage qui prend en compte l'énergie basé sur la localisation conçu principalement pour les réseaux ad hoc mobiles, mais peut être appliqué au réseaux de capteurs. Il conserve l'énergie par la mise en veille des nœuds inutiles dans le réseau sans affecter le niveau de fidélité du routage. Il forme une grille virtuelle pour le domaine couvert. Chaque nœud emploie sa position indiquée par le GPS pour s'associer à un point dans la grille virtuelle. Des nœuds liés au même point sur la grille sont considérés équivalents en termes de coût de routage. Une telle équivalence est exploitée en maintenant quelques nœuds situés dans un secteur particulier de la grille dans l'état de sommeil afin d'économiser de l'énergie [38].

Un exemple sur GAF est illustré dans la figure 3.7. Le nœud 1 peut atteindre les nœuds 2, 3 et 4, ces derniers peuvent atteindre le nœud 5. Par conséquent, les nœuds 2, 3 et 4 sont équivalents et deux d'entre eux peuvent dormir.

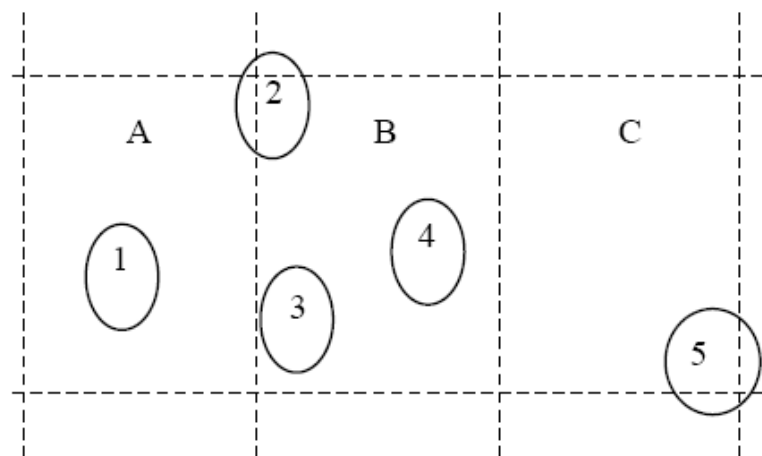


Figure 3.7 - Exemple sur la grille virtuelle dans GAF [38]

Les nœuds change d'états de dormir à actif par tour de sorte que la charge est équilibrée. Il ya trois états définis dans GAF. Ces états sont : *l'état de découverte*, pour la détermination des voisins dans la grille, *l'état actif* reflétant la participation dans le routage et *l'état de sommeil* quand la radio est éteinte.

Les résultats de simulation montrent que GAF se comporte au moins comme un protocole de routage ad hoc en termes de temps de latence et perte de paquets, il permet aussi d'augmenter la durée de vie du réseau par les économies d'énergie.

3.5.3 GEAR (geographic and energy-aware routing)

L'idée est de restreindre le nombre d'intérêts dans la diffusion dirigée en considérant seulement certaines régions plutôt que d'envoyer les intérêts au réseau entier.

En GEAR, chaque nœud conserve un coût estimé et un coût d'apprentissage pour atteindre la destination à travers ses voisins. Le coût estimé est la combinaison de l'énergie résiduelle et la distance vers destination. Le coût d'apprentissage est le raffinement du coût estimé qui est utilisé pour le routage autour des trous dans le réseau. Un trou se produit quand un nœud n'a pas de voisin plus proche de la région cible que lui-même. S'il n'y a pas de trous, le coût estimé est égal au coût d'apprentissage. Il y a deux phases dans l'algorithme [39]:

1) Transmission des paquets vers la région cible: Dès la réception d'un paquet, le nœud vérifie ses voisins pour voir s'il y en a un qui est plus proche de la région cible que lui-même. Si il y a plus qu'un, le voisin le plus proche de la région cible est sélectionnée comme prochain saut. S'ils sont tous plus loin que le nœud lui-même, cela signifie qu'il y a un trou. Dans ce cas, l'un des voisins est choisi pour lui envoyer le paquet, ce choix est basé sur la fonction du coût d'apprentissage. Ce choix peut être mis à jour en fonction de la convergence du coût d'apprentissage au cours de la livraison des paquets.

2) L'envoi des paquets dans la région: Si le paquet a atteint la région, il peut être diffusée dans cette région par RGF (Recursive Geographic Forwarding) ou par l'inondation limitée. L'inondation limitée est bonne lorsque la densité des capteurs est petite. Dans les réseaux à haute densité, RGF est plus efficace que l'inondation limitée. Dans ce cas, la région est divisée en quatre sous-régions et quatre exemplaires du paquet sont créés. Ce processus continue jusqu'à ce qu'il ne reste que des régions avec un seul nœud. Un exemple sur RGF est représenté dans la figure 3.8.

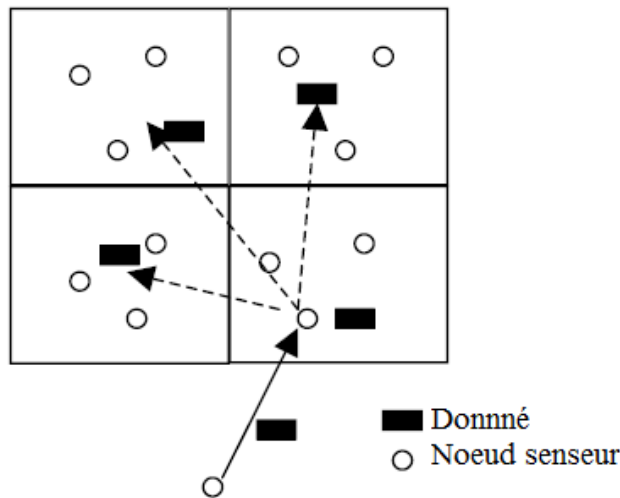


Figure 3.8 - Exemple sur RGF dans GEAR [39]

3.6 Protocoles avec considération du flux du réseau et de QoS

Les protocoles de routage décrits par la suite adoptent des approches d'établissement de chemins en considérant le flux de réseau et la qualité de service (QoS).

3.6.1 Routage à énergie de durée de vie maximale

C'est une approche basée sur le flux du réseau. Son objectif principal est de maximiser la durée de vie du réseau en définissant soigneusement le coût d'un lien en fonction de l'énergie résiduelle du nœud et de l'énergie de transmission requise en utilisant ce lien [40].

En suite par l'utilisation de l'algorithme du plus court chemin de Bellman-Ford pour les coûts des liens, les chemins de coût minimal à la destination sont trouvés.

3.6.2 Collecte de données de durée de vie maximale

Cette approche considère le routage dans les réseaux de capteurs comme un problème de maximisation de la durée de vie de la collecte des données et présente un algorithme de temps polynomial [41].

La durée de vie "T" du système est défini comme le nombre de tours ou de période de lecture des données à partir des capteurs jusqu'à la mort du premier capteur. Le scheduler d'agrégation des données spécifie pour chaque période comment collecter et router les données vers le sink.

Un algorithme appelé MLDA (Maximum Lifetime Data Aggregation) a été proposé. L'Algorithme considère l'agrégation de données avec la mise en place des routes de durée de vie maximale.

MLDA se comportent mieux que les autres protocoles en termes de la durée de vie du système. Cependant, les calcule dans l'algorithme deviens cher pour les grands réseaux de capteurs. Par conséquent, les auteurs on proposer une autre solution (CMLDA) basée sur les clusters pour résoudre le problème.

3.6.3 Transmission à coût minimal

Le protocole vise à trouver le chemin de coût minimal dans un grand réseau de capteur, qui sera également simple et scalable. La fonction de coût pour le protocole capture l'effet du retard, du débit et de la consommation d'énergie de tout nœud au sink [42].

Il y a deux phases dans le protocole. La première phase est la phase d'installation pour le calcule des coûts dans tous les nœuds. Elle commence par le sink et puis elle est diffusée à travers tout le réseau. Chaque nœud calcul la valeur de son coût, qui est égale à la somme du coût du nœud qu'il lui a envoyé le message et le coût de la liaison. Par conséquent, l'algorithme trouve le coût optimal de tous les nœuds vers le sink.

Dans la deuxième phase, la source diffuse les données vers ses voisins. Les nœuds recevant le message diffusé, ajoute leurs coûts de transmission (vers sink) au coût du paquet. Ensuite, le nœud vérifie le coût restant dans le paquet. Si le coût qui reste du paquet n'est pas suffisant pour atteindre le sink, le paquet est abandonné. Sinon, le nœud transmet le paquet à ses voisins.

3.6.4 SAR

SAR (Sequential Assignment Routing) est une approche multi-chemins géré par table qui s'efforce à réaliser l'efficacité énergétique et la tolérance aux fautes [21]. SAR crée des arbres en prenant en compte la métrique QoS, ressource énergétique sur chaque chemin et le niveau de priorité de chaque paquet. En utilisant ces arbres, des chemins multiples du sink aux capteurs sont formés. Un de ces chemins est choisi selon les ressources énergétiques et QoS du chemin. SAR maintient multiples chemins des nœuds au sink. Bien que cela assure la tolérance aux pannes et la récupération facile, le protocole souffre de la surcharge de maintenir les tables et les états de chaque nœud capteur en particulier lorsque le nombre des nœuds est grand.

3.6.5 Protocole de routage QoS avec considération de l'énergie [43]

Le coût de lien utilisé dans ce protocole est une fonction qui capture la réserve d'énergie du nœud, l'énergie de transmission, le taux d'erreur et toute autres paramètres de communication et trouve une liste des chemins de coût minimale en employant une version étendue de l'algorithme de Dijkstra et sélectionne un chemin de cette liste qui trouve le délai bout à bout requis.

3.6.6 SPEED

Le protocole exige à chaque nœud de maintenir des informations sur ses voisins et emploie une transmission géographique pour trouver les chemins [44]. En outre, SPEED s'efforce d'assurer une certaine vitesse pour chaque paquet dans le réseau de sorte que chaque application puisse estimer le délai bout à bout pour les paquets en divisant la distance au sink par la vitesse du paquet avant de prendre la décision d'admission. SPEED peut éviter la congestion quand le réseau est encombré.



3.7 Conclusion

La technologie des réseaux de capteurs reste très prometteuse, et leur défis majeurs est de trouver des protocoles de routage qui permettent, à la fois, de :

- É consommer le moins d'énergie possible,
- É assurer la connectivité du réseau et la couverture du champ surveillé,
- É assurer une livraison fiable et rapide,
- É tolérer les pannes,
- É s'adapter aux changements de topologie í

Nous avons présenté dans ce chapitre les différents algorithmes de routage déployés dans les réseaux de capteurs sans fil. Dans la suite, nous présentons un nouveau algorithme de routage nommé EESPEED.



Chapitre 4

Algorithme de routage EESPEED pour les réseaux de capteurs dense a grand échelle

4.1 Introduction

Les protocoles de routage avec qualité de service existants, comme ceux utilisés dans les réseaux Ad Hoc, se basent sur la découverte des chemins de bout en bout, la réservation des ressources et la récupération des chemins en cas de changement de la topologie de réseau. Ces caractéristiques rendent ces protocoles non adaptés à la nature des réseaux de capteurs et leurs applications : Tout d'abord, le temps mis pour la découverte de chemin augmente le délai de bout en bout, chose non tolérable surtout pour les trafics très urgents. Ensuite, la réservation des ressources pour des trafics imprévisibles, comme les trafics urgents, apparaît illogique. De ce fait, le développement de nouveaux protocoles de qualité de service pour les réseaux de capteurs s'avère indispensable.

Le protocole SPEED [44] est conçu pour fournir des garanties temps-réel de bout-en-bout pour les paquets dans les réseaux de capteurs sans avoir une connaissance globale sur la topologie du réseau. Cependant l'utilisation de ce protocole dans les réseaux de capteurs dense a grand échelle influe sur les performances du protocole ainsi que sur la durée de vie du réseau.

Dans ce chapitre, nous présentons le protocole de routage SPEED ainsi que ses limites, puis nous présentons un nouveau algorithme de routage basé sur le protocole SPEED dédié aux réseaux de capteurs dense à grand échelle.

Le protocole SPEED [44] est classé parmi les protocoles de routage géographique, basé sur la qualité de service. Sa caractéristique fondamentale est la garantie d'un délai de livraison de bout en bout optimale. Grâce à cette spécification, SPEED est le protocole le plus approprié pour des applications temps réel des réseaux de capteurs [44]. En effet, ce protocole essaye de garantir une vitesse de transmission des paquets constante dans tout le réseau.

Afin d'assurer le routage avec qualité de service temps réel, SPEED fait appel à l'interfonctionnement de plusieurs modules, comme l'illustre la figure 4.1.

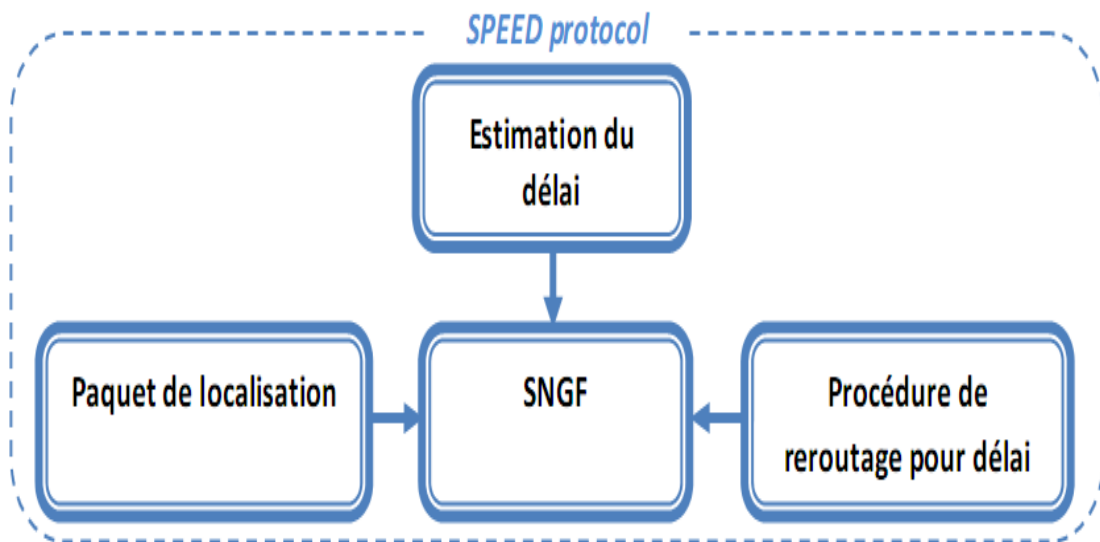


Figure 4.1 - Architecture fonctionnelle du protocole SPEED

Les modules mis en évidence par l'architecture fonctionnelle de SPEED opèrent de la façon suivante :

Le SNGF (*Stateless Non-deterministic Geographic Forwarding*) est le module de routage, responsable de la sélection du prochain saut offrant la vitesse de livraison des paquets souhaitée. La Procédure de re-routage pour délai (*Backpressure Rerouting*) est appelée si un cas de congestion du nœud de prochain saut est rencontré. Le module Estimation du délai (*Delay Estimation*) est le mécanisme permettant la prédiction du délai nécessaire pour la transmission des paquets vers le prochain saut. Module Paquet de localisation (*Beacon Exchange*) permet la localisation géographique des nœuds.

Les nœuds, exécutant le protocole SPEED, diffusent périodiquement des paquets de localisation pour tenir à jour les changements de la topologie du réseau. Les nœuds récepteurs interprètent les informations reçues et les sauvegardent pour construire leurs tables de voisinage. Ces paquets ont le format suivant:

<i>ID Voisin</i>	<i>Position</i>	<i>Délai d'Envoie</i>	<i>Temps d'Expiration</i>
------------------	-----------------	-----------------------	---------------------------

Figure 4.2 - Paquet de localisation

- Le champ **ID Voisin** identifie le voisin émetteur de ce paquet de localisation.
- Le champ **Position** contient la position géographique du nœud émetteur du paquet.
- Le champ **Délai d'Envoie** est le délai estimé pour atteindre le nœud destination identifié par Global_ID.
- Le champ **Temps d'Expiration** est un *timer* désignant la validité de l'information transportée, c'est-à-dire, à son expiration, le nœud supprimera ces informations de sa table de voisinage.

Le nombre de paquets de localisation échangé devient de moins en moins important si les nœuds se déplacent lentement ou sont fixes.

4.2.2 Estimation de délai

Le module « *Delay estimation* », utilisé par le protocole SPEED, joue un rôle très déterminant dans la maintenance et la garantie de la livraison des paquets dans les délais exigés.

Les réseaux de capteurs disposent généralement d'une bande passante limitée [44], ce qui rend difficile l'utilisation des paquets de signalisation propre à l'estimation des délais de livraison.

Pour cela, l'exploitation des paquets DATA, passant par un nœud capteur, s'avère la meilleure solution pour ce genre de mesure.

L'estimation du délai se fait au niveau du nœud émetteur. Celui-ci enregistre instantanément le temps de départ du dernier bit du paquet DATA, noté $t_{ij}^{départ}$, et calcule le temps mis pour effectuer un seul saut quand il reçoit l'acquiescement de son paquet envoyé. A son arrivée au nœud j , ce dernier acquitte la réception du paquet DATA en indiquant le temps écoulé du traitement du paquet ACK, noté t_{ij}^{ACK} . Ainsi, le nœud émetteur enregistre le temps d'arrivée du paquet ACK, noté $t_{ij}^{arrivé}$, et mesure le temps mis pour effectuer un seul saut suivant la formule suivante :

$$t_{ij}^{saut} = t_{ij}^{arrivé} - t_{ij}^{ACK} - t_{ij}^{départ}$$

L'estimation du délai courant est donnée en combinant cette nouvelle valeur calculée avec les délais antérieurs suivant la méthode EWMA (*Exponential Weighted Moving Average*) [45].

4.2.3 SNGF (Stateless Non-deterministic Geographic Forwarding)

- Calcul de la vitesse de livraison

L'exemple suivant explique la méthode de calcul de la vitesse de livraison entre deux nœuds voisins :

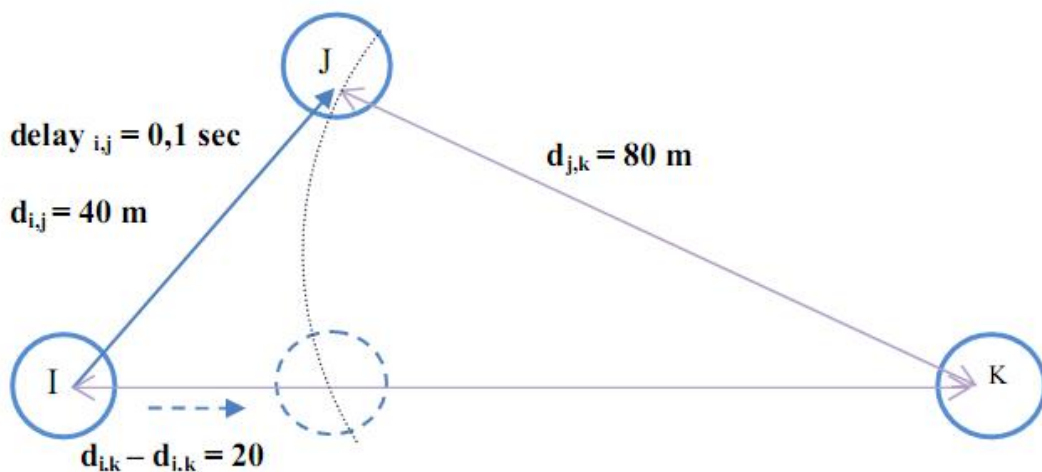


Figure 4.3 - Calcul de la vitesse de livraison

voisins i et j (figure 4.3). Les distances leurs séparant de la destination k sont respectivement $d_{ik} = 100\text{m}$ et $d_{jk} = 80\text{m}$. Si le nœud i transmet ses paquets vers le nœud j dans un délai $\text{delay}_{ij} = 0.1$ seconde, ce qui permet de s'approcher de la destination d'une distance d égale à $(d_{ik} - d_{jk}) = 20\text{m}$. Dans ce cas, la vitesse de transmission intermédiaire speed_{ij}^k se mesure comme le rapport $(d_{ik} - d_{jk}) / \text{delay}_{ij} = 200\text{m/s}$.

Il est clair que la vitesse de transmission intermédiaire change d'un saut à un autre puisqu'elle varie en fonction de la distance entre les nœuds voisins et le temps de transmission. Si chaque nœud du réseau envoie les paquets vers le voisin en maintenant une vitesse supérieure à une vitesse seuil setspeed , alors cette dernière est forcément garantie par tous les nœuds. Ainsi de n'importe quel nœud source vers le nœud destination « Sink », le délai de bout en bout est estimé comme suit [44]:

$$\text{Délai bout en bout} = D_{\text{source, Sink}} / \text{Setspeed}$$

avec $D_{\text{source, Sink}}$: distance entre le nœud source et la destination finale « Sink ».

• **Choix de nœud de prochains sauts :**

Le SNGF (*Stateless Non-deterministic Geographic Forwarding*) est le module responsable de la sélection du prochain saut offrant la vitesse de livraison des paquets souhaitée. Nous expliquons son principe en se basant sur l'exemple de la figure 4.4 :

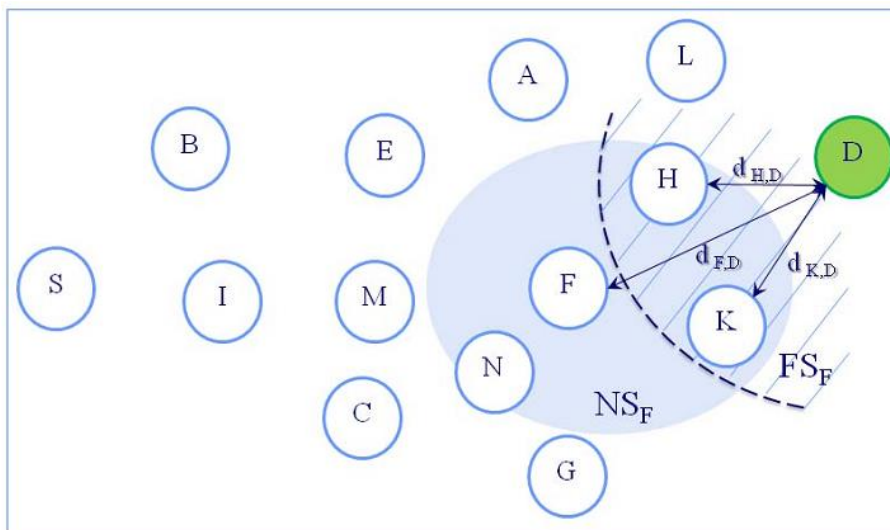


Figure 4.4 - Choix de nœud de prochain saut



mettre un paquet DATA vers la destination D. il doit alors choisir le nœud de saut suivant tout en respectant les règles suivantes :

1. Les paquets ne sont transmis que vers les nœuds se trouvant dans le champ FS_F (*Forwarding candidate Set of Node F*). Ce champ contient les nœuds qui sont à la portée du nœud F et qui sont susceptibles d'être sélectionnés pour continuer la transmission des données vers le nœud destination.

Le champ FS_F groupe les nœuds de prochain saut qui sont plus proche à la destination que le nœud F et qui offre une vitesse de livraison supérieure ou égale à la vitesse de seuil *Setspeed*. Ceci est exprimé par [44]:

$$FS_F = \{ \text{nœud } j \in NS_F / d_{F,D} - d_{j,D} > 0 \text{ et vitesse de livraison} \geq \text{Setspeed} \}$$

avec NS_F : (*Neighbors Set*) nœuds voisins du nœud F,

$d_{F,D}$: la distance séparant le nœud F du nœud destination

$d_{j,D}$: distance séparant le nœud j de prochain saut du nœud destination.

2. Le nœud du prochain saut devra être choisi parmi le premier groupe et disposant de la vitesse de transmission la plus importante.

3. Dans le cas où la zone FS_F est dépourvue des nœuds, autrement dit, si le nœud F échoue de trouver un prochain saut, il rejette alors le paquet en question et envoie des paquets *Backpressure* aux nœuds précédents pour leur interdire momentanément la transmission des paquets vers sa région.

4.2.4 Procédure de re-routage pour délai

a) Format du paquet « *Delay Back pressure* »

Le paquet « *Delay Back pressure* » comporte les champs suivants :



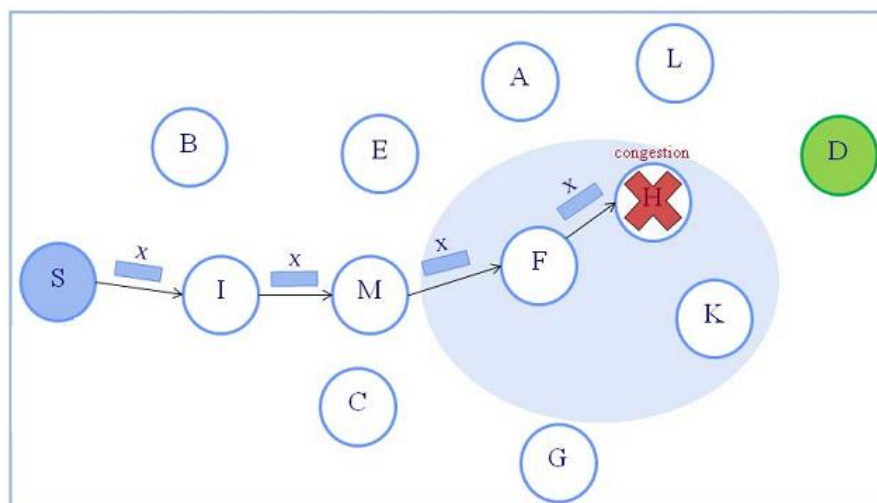
Figure 4.5 - Paquet « Delay Back pressure »

- le champ ID contient l'identité du nœud émettant le paquet «Delay Back pressure ».
- le champ Destination contient l'identité du nœud destination.
- le champ *Délai d'Envoie* contient la durée de livraison estimée entre les deux nœuds ID et Destination. Cette durée est le délai intermédiaire nécessaire ($delay_{ID, Destination}$) pour effectuer le saut entre ces deux derniers. Ce champ prend la valeur infinie $\hat{\infty}$, si le nœud ID ne trouve aucun nœud voisin pour lui envoyer le paquet DATA.

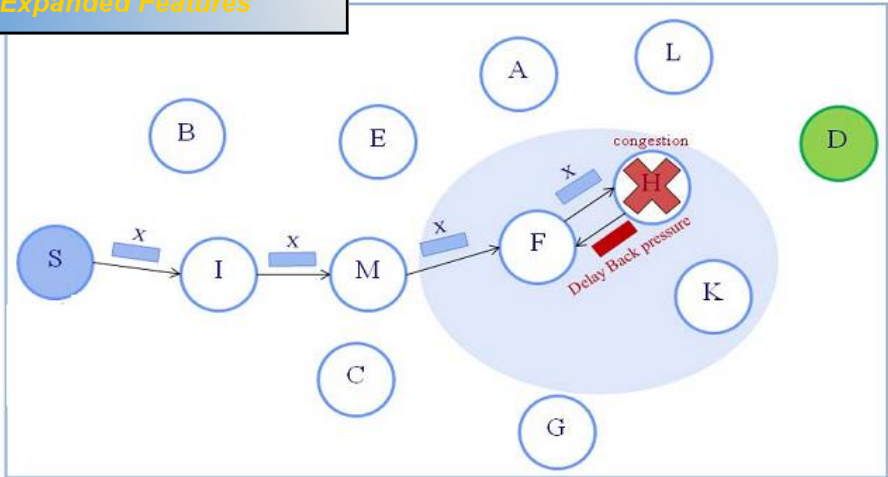
b) Procédure de re-routage en cas de congestion

Le protocole SPEED utilise une procédure de re-routage appelée « Backpressure rerouting », si au cours de route, on rencontre des nœuds congestionnés.

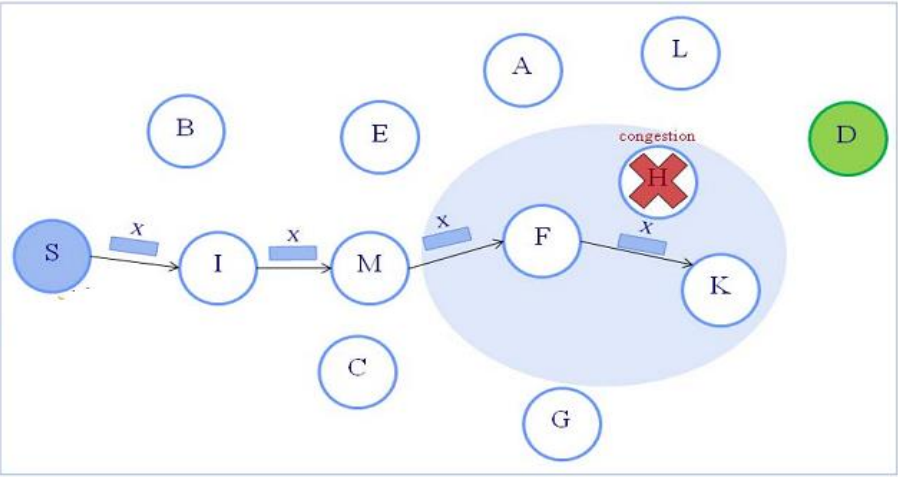
L'exemple illustré par les figures 4.6 (a, b, c, d), décrit clairement la procédure de re-routage :



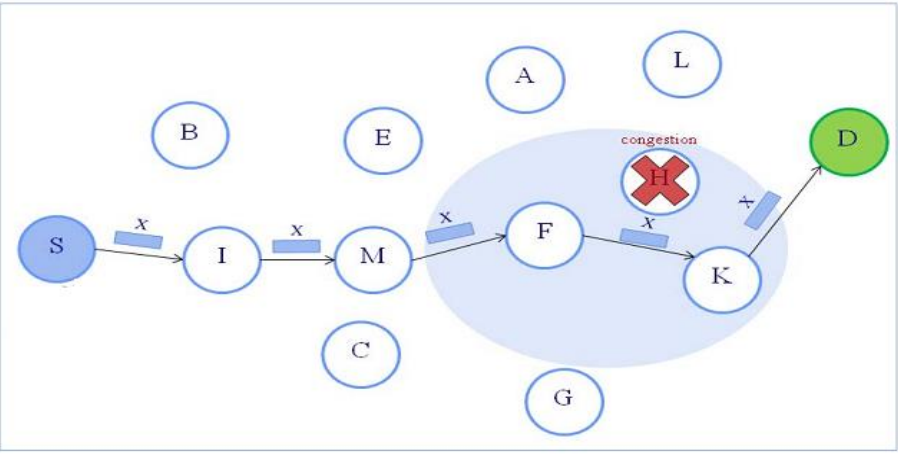
(a)



(b)



(c)

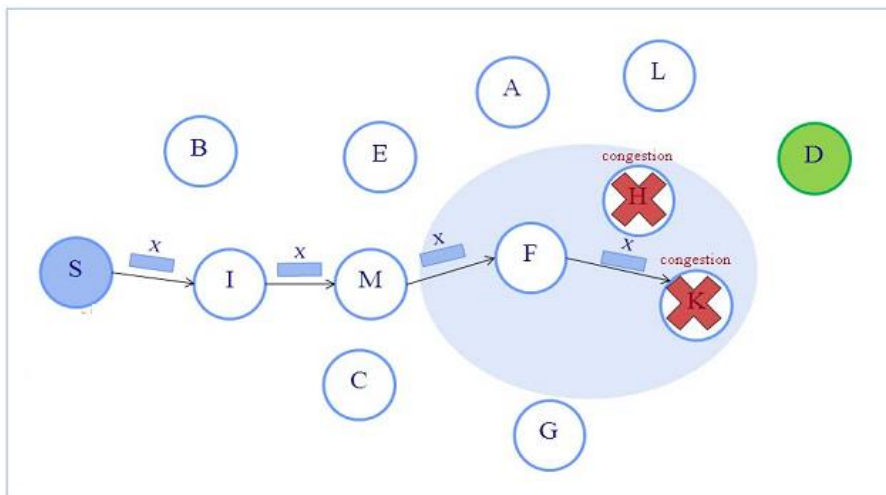


(d)

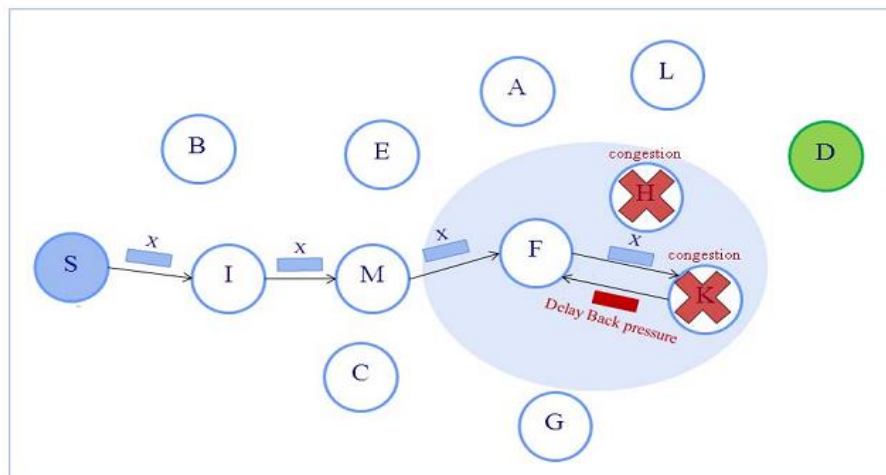
Figure 4.6 - Procédure de re-routage pour délai « Delay back pressure rerouting » (cas 1)

paquet DATA, noté X, jusqu'à la destination D. En arrivant au nœud F, celui-ci choisit comme prochain saut le nœud H (le choix du nœud est effectué par le module SNGF). Mais il se trouve que ce nœud est congestionné, alors il répond le nœud F par un paquet « *Delay back pressure* » pour lui informer qu'il ne peut pas délivrer le paquet X dans un délai favorable vu son état de congestion. Le nœud F active, alors, son module SNGF pour re-sélectionner un autre nœud appartenant à l'ensemble FS_F (*Forwarding Set* pour le nœud F), et il finit par re-router le paquet X au nœud K.

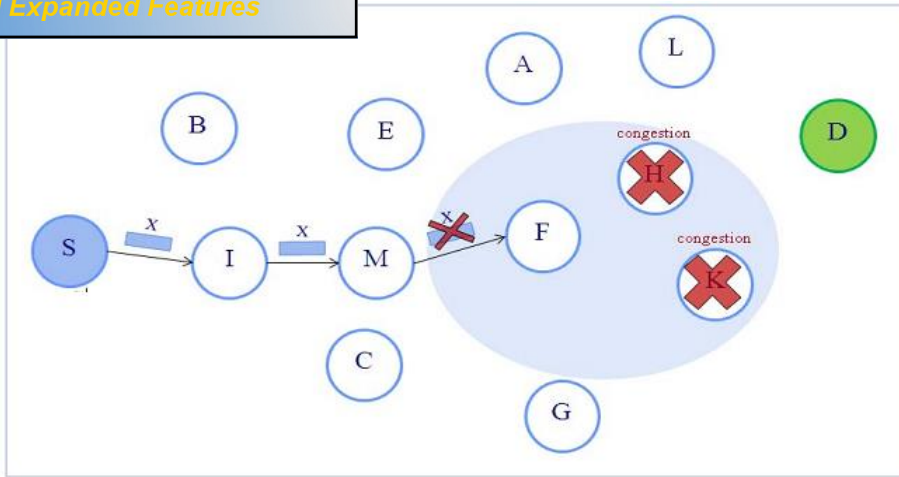
Un deuxième cas peut se présenter si tous les nœuds de l'ensemble FS_F est en état de congestion. Ce cas de figure est illustré par les figures 4.7. (e,f,g,h,i):



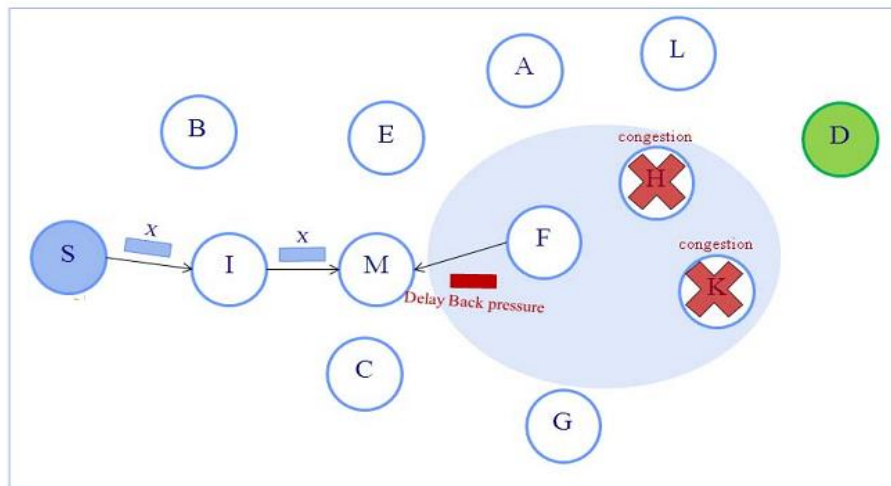
(e)



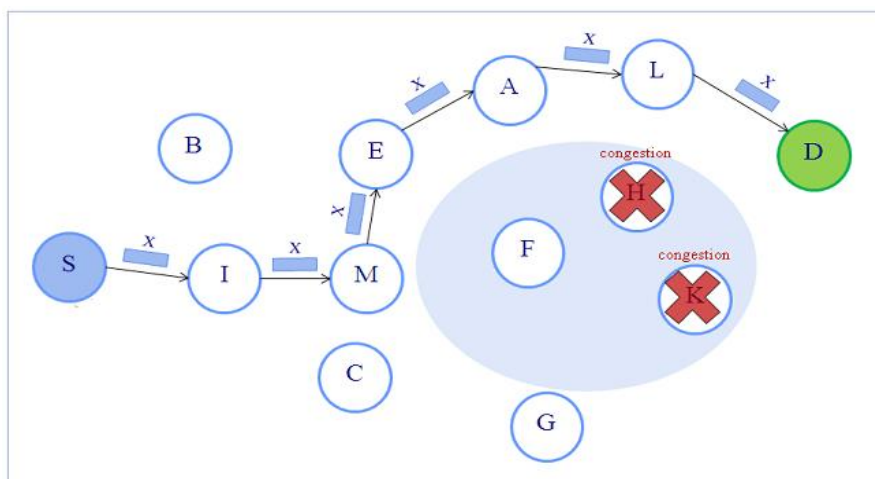
(f)



(g)



(h)



(i)

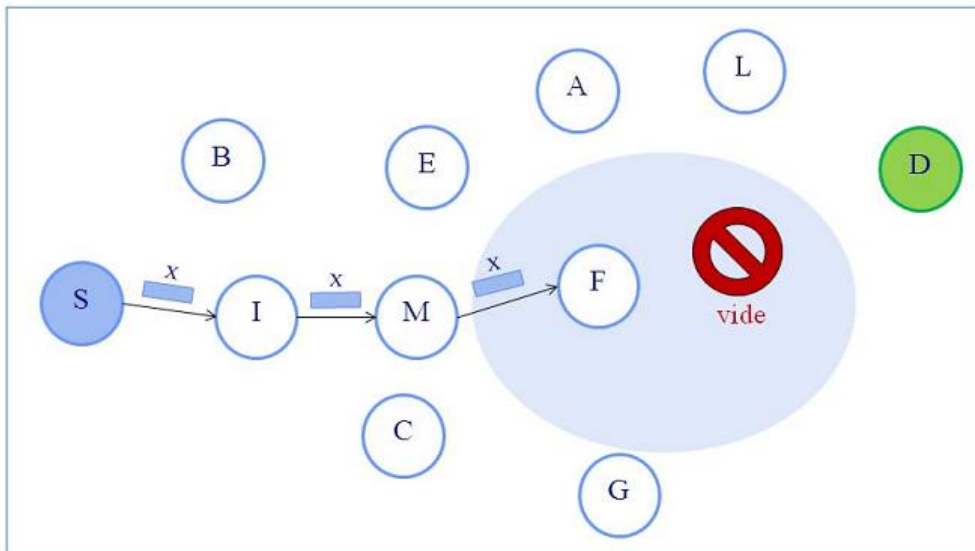
Figure 4.7 - Procédure de re-routage pour délai « Delay back pressure rerouting » (cas 2)

(a), (b), (c) et (d) de la figure 4.6. Supposant qu'à l'étape (d), le nœud F trouve, aussi, le nœud K en état de congestion. Ce dernier va lui envoyer, alors, le paquet « *Delay back pressure* ». Supposant maintenant que F ne trouve aucun autre nœud susceptible d'être celui du prochain saut. Ce nœud F supprime, alors, le paquet DATA et envoie au nœud M un paquet « *Delay back pressure* » lui indiquant qu'il a échoué de transmettre ce paquet X. Dans ce cas, le nœud M active son SNGF pour sélectionner un autre prochain saut (dans notre exemple, le nœud E est choisi. De même, si le nœud M trouve tous ses voisins, appartenant à son champ FS_M , congestionnés, il réagit de la même façon que le nœud F et le nœud I devra alors acheminer les paquets vers un autre nœud.

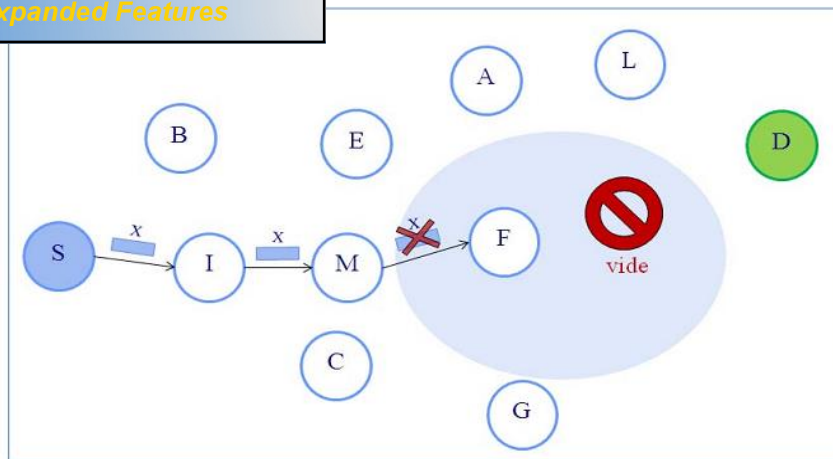
c) Void avoidance

Un troisième cas peut se présenter si l'ensemble des nœuds de prochains sauts FS_F est vide.

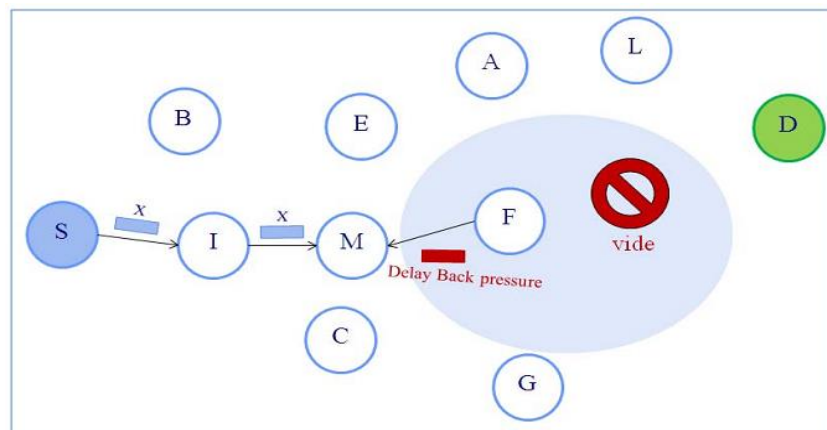
Le protocole SPEED sait résoudre ce genre de problème en se basant sur la notion de *Void Avoidance* illustré par les figures 4.8. (a,b,c) :



(a)



(b)



(c)

Figure 4.8 - Mécanisme de Void avoidance

D'après le scénario de ces figures, le nœud F ne trouve aucun nœud voisin qui mène vers la destination D, par conséquent, il supprime le paquet DATA et envoie le paquet « *Delay Back pressure* », contenant les champs suivants (ID, DESTINATION, \hat{O}), vers le nœud du saut précédent. À son tour, le nœud M affecte la valeur \hat{O} au champ *SendToDelay* pour dire que le choix du nœud F, comme un intermédiaire, nécessite un délai de transmission très important, donc il ne va plus être sélectionné comme un prochain saut vers la destination finale et le nœud M se trouve obligé de choisir un prochain saut différent.

4.2.5 Le protocole de la couche MAC

Le protocole SPEED utilise le protocole DCF (Distributed Coordination Function) pour le routage des paquets au niveau de la couche MAC [46].

Function) qui est une variante améliorée de la méthode d'accès CSMA/CA. Celle-ci permet d'éviter les collisions lors de la transmission par ralentissement aléatoire après chaque trame (backoff).

4.3 Limites du protocole SPEED

Le protocole SPEED permet de garantir un délai de livraison de bout en bout optimale. Cependant l'utilisation de ce protocole dans les réseaux de capteurs dense à grand échelle crée plusieurs problèmes. Dans la suite nous allons les voir :

Chaque nœud dans un réseau de capteurs qui utilise SPEED comme protocole de routage génère périodiquement deux types de paquets de contrôles : contrôle de localisation pour tenir à jour les changements de la topologie du réseau, et contrôle de délai pour garantir la livraison des paquets dans les délais exigés. Donc avec l'augmentation du nombre des nœuds dans le réseau le nombre total des paquets de contrôle générer périodiquement augment ce qui engendre les problèmes suivants :

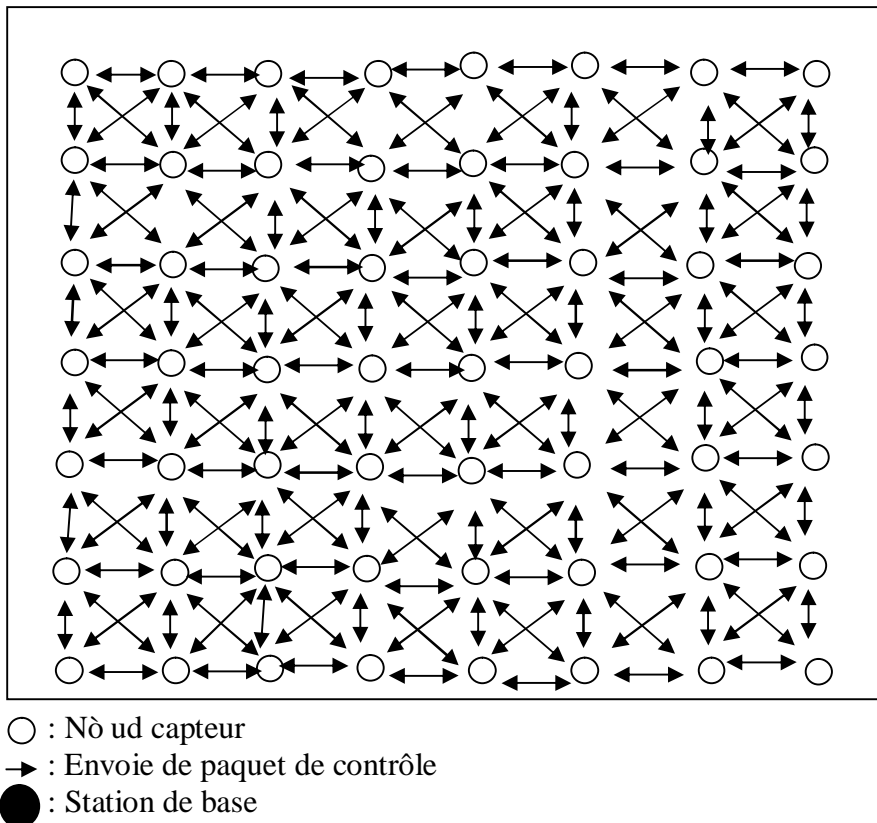
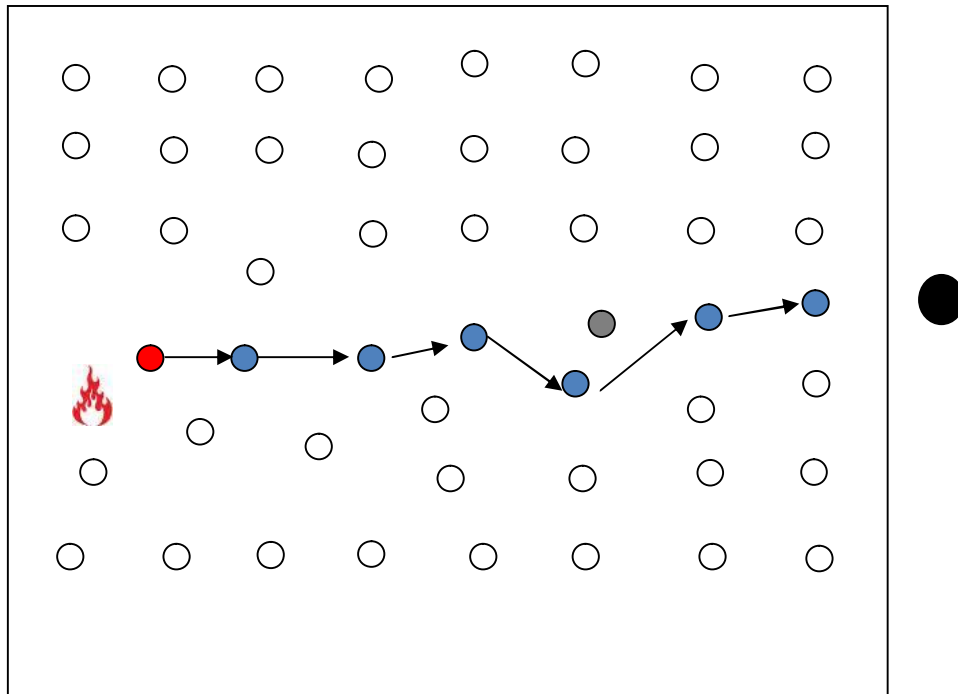


Figure 4.9 - Les paquets de contrôle générés périodiquement par tous les nœuds du réseau

au avec ces paquets de contrôle (regarder la figure 4.9).

- Diminution de la durée de vie du réseau à cause de l'augmentation de l'énergie consommée pour l'envoi et la réception de ces paquets de contrôle (regarder la figure 4.9).

- L'encombrement du réseau par ces paquets de contrôle fait augmenter le nombre des nœuds congestionnés ce qui produit des retards dans la livraison des données à cause de l'utilisation de la procédure de re-routage (regarder la figure 4.10).



- : Nœud capteur
- (red) : Nœud qui a capté le feu
- (blue) : Nœud routeur
- (grey) : Nœud congestionné
- : Envoi des données capter
- (black) : Station de base

Figure 4.10 - Re-routage de paquet de données



PDF Complete
Your complimentary use period has ended.
Thank you for using PDF Complete.

[Click Here to upgrade to Unlimited Pages and Expanded Features](#)

Un nouveau algorithme de routage dédié aux réseaux de capteurs dense à grande échelle, qui permet de prolonger la durée de vie du réseau par la minimisation du nombre total des paquets de contrôle générés périodiquement et qui garantit les performances de l'algorithme SPEED.

4.4 L'Algorithme de routage EESPEED pour les réseaux de capteurs denses a grands échelle

Avant de passer à la description de l'algorithme proposé, nous commençons tout d'abord par présenter le modèle du réseau utilisé.

4.4.1 Modèle du réseau

Nous avons considéré un réseau de capteurs dense à grand échelle déployé dans une région carrée :

Les hypothèses adoptées sont les suivantes :

- Les nœuds sont distribués de manière aléatoire dans le réseau.
- Ils sont mobiles.
- Tous les capteurs collectent les données et servent une unique station de base.
- Ils sont (sauf la station de base) identiques et à capacité égale (même énergie initiale, même capacité de stockage et de traitement de données).
- Chaque nœud a deux portées de transmission. La plus faible portée est utilisée par tous les nœuds pour le choix des chefs de grappes et aussi pour la collection des données. Ensuite, les données seront routées de chefs en chefs vers la station de base en utilisant la plus haute portée.
- Une fois déployés, les capteurs sont laissés sans surveillance. Il est donc impossible de les recharger en cas de déplétion d'énergie ou de panne.
- Les capteurs sont équipés d'un système de localisation (tel que GPS)

4.4.2 Présentation de l'algorithme de routage EESPEED

Par souci de résistance aux facteurs d'échelle et de densité nous avons choisi d'utiliser la technique d'agglomération (ou clustering). En effet, grâce à la création de grappes nous pouvons diminuer le nombre de paquets de contrôle générés périodiquement dans le réseau.

rouvés à la station de base a travers les chefs des grappes en utilisant le protocole de routage SPEED. Le résultat est appelé EESPEED pour Energy-awarE clustering SPEED.

- **Les phases de l’algorithme de routage EESPEED**

L’algorithme de routage EESPEED proposé est constitué de 4 phases :

Phase 1 : création de la grille virtuelle

Nous allons former une grille virtuelle sur le réseau de capteurs (comme il est représenté dans la figure 4.11), où chaque nœud emploie sa position indiquée par le module de localisation (tel que GPS) pour s’associer à un point dans la grille virtuelle.

Le diamètre de chaque grappe de la grille doit respecter les 2 critères suivant :

- 1- La plus faible portée de transmission doit au moins couvrir le diamètre d’une grappe pour garantir la communication intra-grappe.
- 2- La plus haute portée de transmission doit au moins couvrir le diamètre de deux grappes pour garantir la communication inter-grappe.

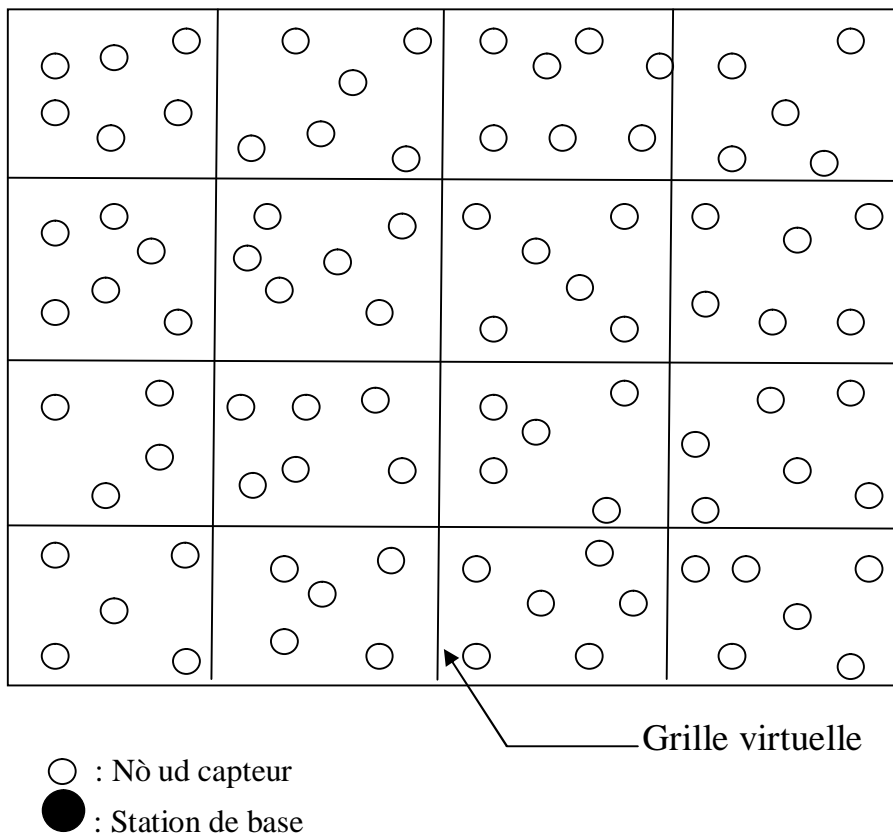


Figure 4.11 - Création de la grille virtuelle

types

La procédure pour choix des chefs de grappes est répéter chaque T second (la valeur de T est définie en fonction de la mobilité du réseau) pour choisir les nouveaux chefs de grappes.

Elle est comme suite :

1- Chaque capteur calcule sa probabilité de devenir un chef de grappe CHprob comme suit : **CH prob = E résiduelle / E max.**

ou E résiduelle : est l'estimation de l'énergie résiduelle du nœud.

E max : est la référence à l'énergie maximale (correspondre à une batterie pleine).

2- Chaque nœud envoie à ses voisins de la même grappe son CH prob, dans un paquet nommé : paquet de contrôle d'énergie (figure 4.12) en utilisant la communication intra-grappe.

3- Chaque nœud de la grappe compare son CH prob avec les CH prob des autres nœuds. Le nœud qui a la valeur du CH prob la plus élevée sera choisi comme chef de grappe.

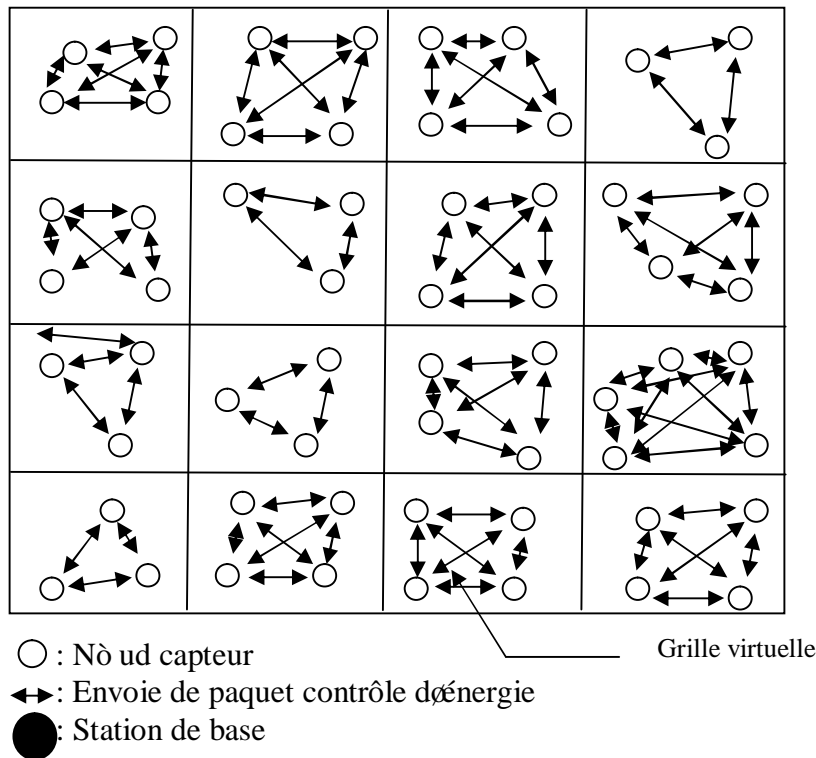


Figure 4.12 - Envoie de paquet contrôle d'énergie intra-grappe

chefs de grappes

Les nœuds ordinaires transmettent leurs données à leurs chefs de grappe (comme il est représenté dans la figure 4.13).

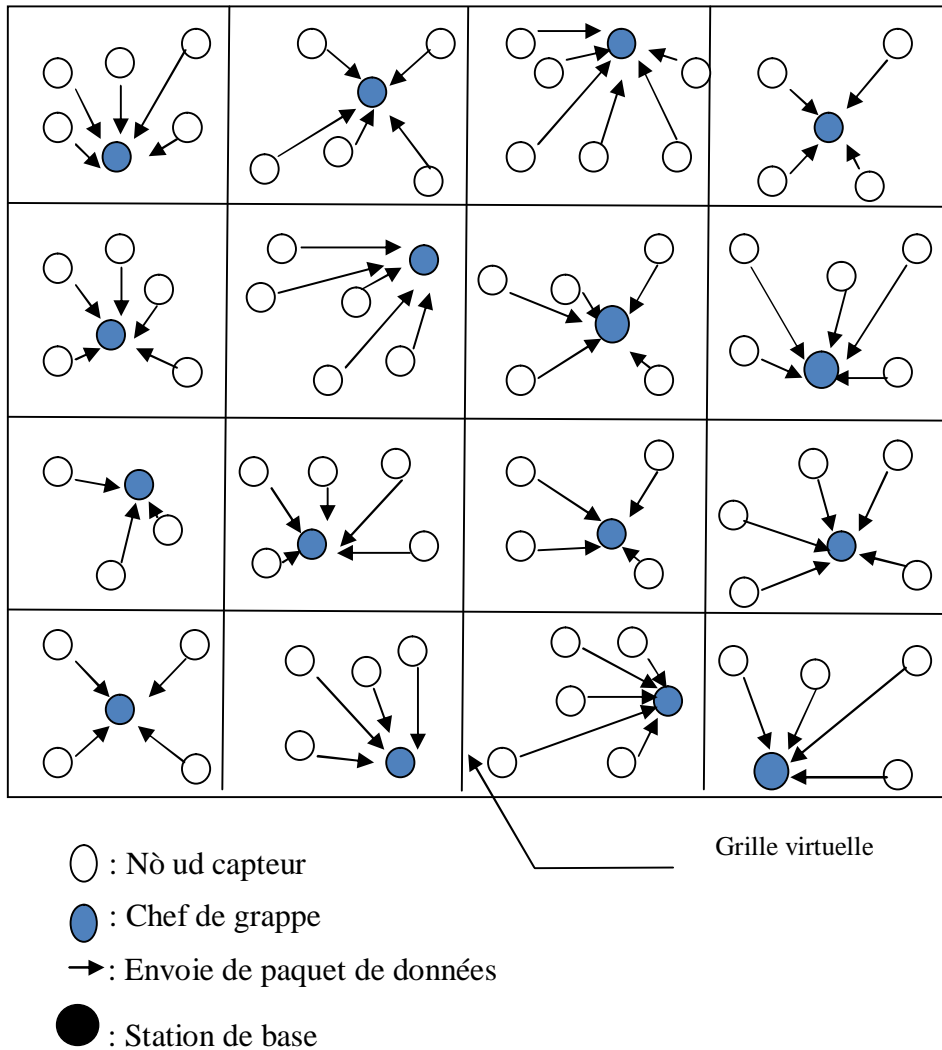
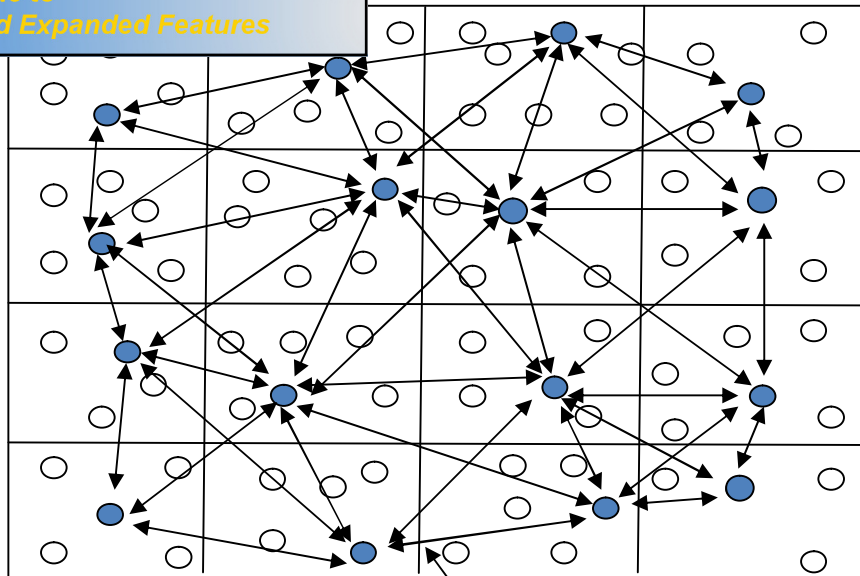


Figure 4.13 - Envoie de paquet de données aux chefs de grappes

Phase 4 : routage des données inter-grappe

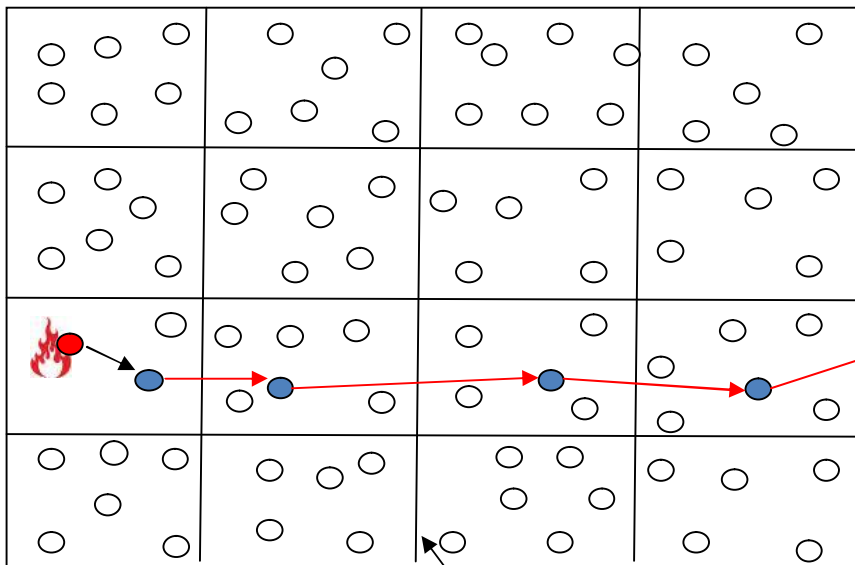
Dans cette phase les données seront routées à la station de base selon le protocole SPEED on utilisant la communication inter-grappe, seuls les chefs de grappes ont le droit de participer dans cette phase (figure 4.14.a-b).



- : Nœud capteur
- (blue) : Chef de grappe
- ↔ : Communication inter-grappe
- (black) : Station de base

Grille virtuelle

-a- envoi de paquet de contrôle par les chefs des grappes



- : Nœud capteur
- (red) : Nœud capteur qui a capté le feu
- (blue) : Chef de grappe
- : Communication intra-grappe
- (red) : Communication inter-grappe
- (black) : Station de base

Grille virtuelle

-b- routage des données en utilisant les chefs des grappes

Figure 4.13 - Routage des données inter-grappe



thme de routage EESPEED

I : création de la grille virtuelle

1. Définir(D) { D : L'intervalle entre chaque deux lignes de la grille}.
2. Définir(Pos_noeud) { Pos_noeud : La position géographique du noeud dans le réseau}
3. Définir(ID_grappe) { ID_grappe : a quelle grappe appartenant le noeud}

II : Choix des chefs des grappes

1. $CH\ prob \leftarrow E\ résiduelle / E\ max$
2. Envoyer ($CH\ prob, ID_grappe, ID_noeud$)
3. Recevoir (V) { V : Vecteur envoyé par un voisin}
4. Si mon $ID_grappe = V.ID_grappe$ Alors
5. $S_{CH} \leftarrow (V)$
6. $Mon_chef_de_grappe \leftarrow Max\ CH\ prob(S_{CH})$

III : envoi des données aux chefs de grappes

1. Si événement détecter Alors
2. Définir ($DATA$) { $DATA$: Les données de l'événement détecter}
3. Si $Mon_chef_de_grappe \neq ID_noeud$ Alors
4. Envoyer_a_Mon_chef_de_grappe (W) { W : Vecteur contenant les champs : $ID_noeud, Pos_noeud, DATA$ }
5. Sinon
6. Recevoir (W)

IV : routage des données inter-grappe

1. $SPEED (Y)$



Ce chapitre a fait le sujet d'une étude théorique de protocole de routage avec QoS SPEED. En effet, le protocole SPEED se caractérise essentiellement par la garantie des délais de bout de bout réduits. Cet aspect lui permet de répondre aux exigences des applications critiques et d'offrir une QoS temps réel satisfaisante. Cependant, l'utilisation de SPEED dans les réseaux de capteurs denses à grande échelle engendre plusieurs problèmes.

Le protocole que nous avons proposé EESPEED, qui est basé sur la technique d'agglomération (clustering) permet la résolution de ces problèmes.

Dans le chapitre suivant, nous allons voir les résultats des simulations de notre protocole EESPEED par rapport à SPEED.



Chapitre 5

Résultat Expérimentaux

5.1 Introduction

Ce chapitre a pour but de présenter tous les résultats des simulations effectuées dans le cadre de ce projet on utilisant le simulateur NS2 (Network Simulator), Ces résultats sont présentés sous forme de courbes calculées en fonction de cinq métriques. Ces métriques sont en fonction de deux variables : la densité des nœuds et trafic généré dans le réseau.

Nous commençons par présenter d'abord le simulateur NS2, en suite les paramètres de la simulation ainsi que les métriques et les variables qui nous ont permis d'établir les courbes représentatives.

5.2 Le simulateur NS2 (Network Simulator)

NS-2 est un logiciel libre de simulation par événements discrets très largement utilisé dans la recherche académique et dans l'industrie. Il est considéré par beaucoup de spécialistes des télécommunications comme le meilleur logiciel de simulation par événements discrets, en raison de son modèle libre, permettant l'ajout très rapide de modèles correspondant à des technologies émergentes. Il est basé sur l'utilisation de langages de scripts pour la commande des simulations (tcl/tk) alors que le cœur des simulations est implémenté avec le langage C++.

NS2 peut être compilé sur de multiples plateformes : Windows, Unix, Linux. Du fait de sa popularité, de nombreux protocoles sont à priori disponibles pour NS2.

La figure suivant montre les étapes de déroulement d'une simulation sous ns2 :

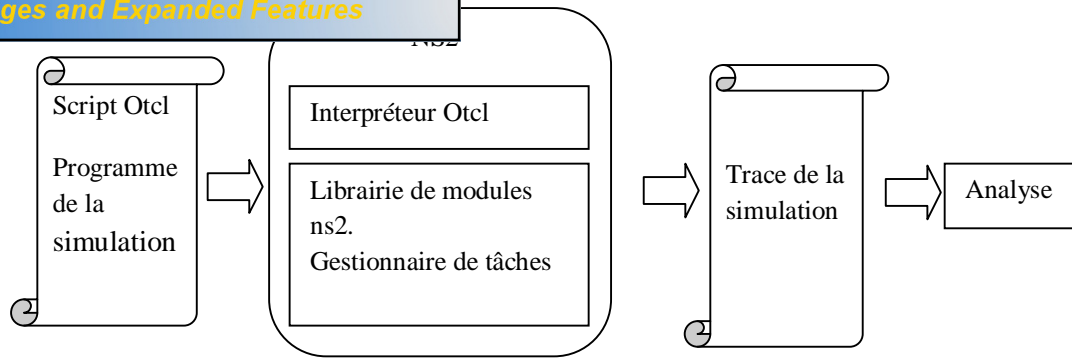


Figure 5.1 - Le déroulement d'une simulation sous ns2

1 ère étape : Ecrire un script Otcl qui initie le gestionnaire de tâches événementiel.

2 ème étape : Ajouter au script le scénario de la simulation => fichier simu.tcl par exemple.

3 ème étape : Lancer la simulation avec la commande `ns simu.tcl`.

4 ème étape : Analyser la trace.

NAM (*Network AniMator*) est un outil graphique fournis avec ns2 qui permet, la visualisation des résultats de simulation (Figure 5.2)

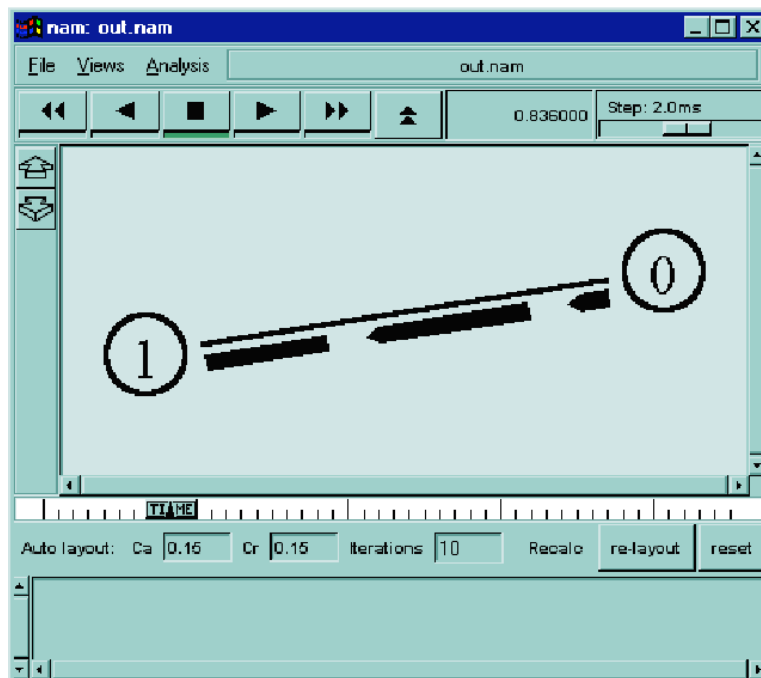


Figure 5.2 - L'outil de visualisation NAM



ux

utiliser pour la simulation des réseaux de capteurs comme : OPNET, OMNet++, JSIM, QUNALNET í .

OPNET (Optimum Network Performance) est un outil de simulation de réseaux très puissant et très complet. Basé sur une interface graphique intuitive, son utilisation et sa prise en main est relativement aisée.

OMNet++ est un simulateur d'évènement basé sur le langage C++, destiné principalement à simuler les protocoles réseau et les systèmes distribués. Il est totalement paramétrable et modulaire. C'est une application open source et sous licence GNU, développée par Andras Varga, chercheur à l'université de Budapest. OMNet++ est destiné avant tout à un usage académique et est l'intermédiaire entre des logiciels de simulation comme NS, destiné principalement à la recherche et OPNET qui est une alternative commerciale de OMNet++.

JSIM est un outil de simulation libre à temps discret, développé en Java qui utilise (TCL/ Jacl) pour la mise en place de scénario de simulation. Il est basé sur la notion de composants autonomes.

QUNALNET est un outil professionnel de modélisation des réseaux. Il comprend également un outil permettant de décrire le comportement du réseau sous la forme d'un automate à états finis.

5.3 Caractéristiques matérielle et logiciels de la machine

Les caractéristiques de la machine utilisée sont :

Matérielle : Un ordinateur portable acer Extensa 5510 avec un processeur Intel Core 2 Duo 1.66 GHz et une RAM de 1 Go.

Logiciels : Le système d'exploitation est Windows xp Service pack 2.

La version du simulateur NS est 2.32, installé sous Windows via Cygwin qui est un environnement UNIX pour Windows.

5.4 Paramètres de la simulation

Dans cette partie nous allons présenter les paramètres de nos simulations, le modèle de topologie, la propagation du signal radio, le trafic des données, la mobilité des nœuds et le modèle de l'énergie utilisé par chacun des nœuds.

La topologie utilisée est une zone carrée de 1000 m × 1000 m, la taille de chaque grappe est de 50m × 50m.

5.4.2 Le modèle de propagation

Le modèle de propagation radio utilisé est appelé « TwoRayGround » qui emploie une atténuation de $1/r^4$ pour les grandes distances. Le type d'antenne radio NS choisie est « OmniAntenna » qui représente les antennes omnidirectionnelles ou l'émission est en 360°.

Les nœuds que nous avons utilisés dans SPEED ont la même configuration avec un rayon de connexion radio : 70 mètres. Les nœuds utilisés dans EESPEED ont la même configuration avec deux rayons de connexion radio :

- Connexion intra-cluster : 70 mètres.
- Connexion inter-cluster : 140 mètres.

5.4.3 Le modèle de trafic

Le modèle de trafic utilisé est de type UDP, avec taille de paquet fixé à 32 octet.

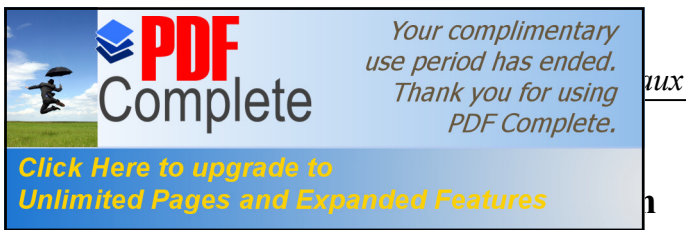
5.4.4 Le modèle de mobilité

Les nœuds ont le droit de se déplacer dans la zone aléatoirement avec une vitesse aléatoire aussi dans l'intervalle [0,1] en mètres par seconde.

5.4.5 Le modèle d'énergie

Le modèle d'énergie utilisé est celui implémenté dans NS et qui attribue aux nœuds une énergie initiale que nous avons fixé à 100 joules, les énergies consommées sont les suivants :

- Pour une transmission (rayon de 140m) : 0.9 joules
- Pour une transmission (rayon de 70m) : 0.6 joules
- Pour une réception : 0.3 joules
- énergie initial : 1000 joules



Chacune des métriques que nous avons calculées dans nos simulations vont nous aider à trouver les écarts entre les deux algorithmes simulés. Ci-dessous nos cinq métriques.

5.5.1 Les paquets de control

Détermine le nombre des paquets émis par les nœuds dans le but de gérer le réseau (identification, recherche de route, maintien de la table de routage, maintenance de lien rompu, etc).

Avec cette métrique nous allons voir le quelle de ces deux algorithmes utilise le minimum de paquets de contrôle pour un meilleur acheminement de paquets et une meilleure visibilité de la topologie du réseau à n'importe quel instant.

5.5.2 Les paquets de contre pression

Détermine le nombre des paquets émis par les nœuds dans le but de gérer le routage si au cours de route, on rencontre des nœuds congestionnés.

Avec cette métrique nous allons voir le quelle de ces deux algorithmes utilise le minimum de paquets de contre pression pour un meilleur acheminement de paquets

5.5.3 Les paquets perdus

Détermine le nombre de paquets de contrôle ou de données perdus physiquement dans le réseau. Ces pertes sont issues de trafic important ou de temps d'attente assez élevé. Les nœuds routeurs perdent des paquets de données utiles ou même de contrôle quand les liaisons sont perdues à cause de déplacement des nœuds récepteur ou la sortie de ces derniers du rayon de propagation de leurs émetteurs.

5.5.4 Le délai bout en bout

Détermine le délai moyen de bout en bout pour le routage des paquets de données de la source à la destination.

voir le quelle de ces deux algorithmes utilise le minimum délai bout en bout pour le routage des paquets.

5.5.5 L'énergie consommée

Détermine l'énergie totale consommée dans le réseau par chaque nœud durant toute la simulation.

Avec cette métrique nous allons voir le quelle de ces deux algorithmes consomme le minimum d'énergie.

5.6 Variables de la simulation

Pour bien représenter nos métriques. Il nous fallait les schématiser par rapport à des variables qui soient représentatives sur le plan quantitatif et qualitatif. Deux algorithmes de routage peuvent avoir les mêmes valeurs au niveau des métriques parce qu'elles sont consolidées. Une fois, ces valeurs éclatées en plusieurs variables, le contraste des limites et des différences de ces protocoles sera plus accentué. Ci-dessous sont présentées nos variables de simulation.

5.6.1 La densité des nœuds

L'augmentation du nombre des nœuds dans le réseau génère beaucoup de contrôle. Il est important d'étudier le comportement des protocoles et l'impact de la densité des nœuds sur les 2 algorithmes de routage.

Le tableau ci-dessous liste les valeurs de la densité utilisé dans la simulation exprimer en nombre de nœud / Km.

Densité (Nbr nœud/Km)							
200	400	600	800	1000	1200	1400	1600

TAB 5.1 - Valeurs de la densité

5.6.2 Nombre de trafic UDP

Pour varier le nombre de trafic UDP, nous avons varié le nombre de sources émettrices afin d'étudier la charge du réseau.

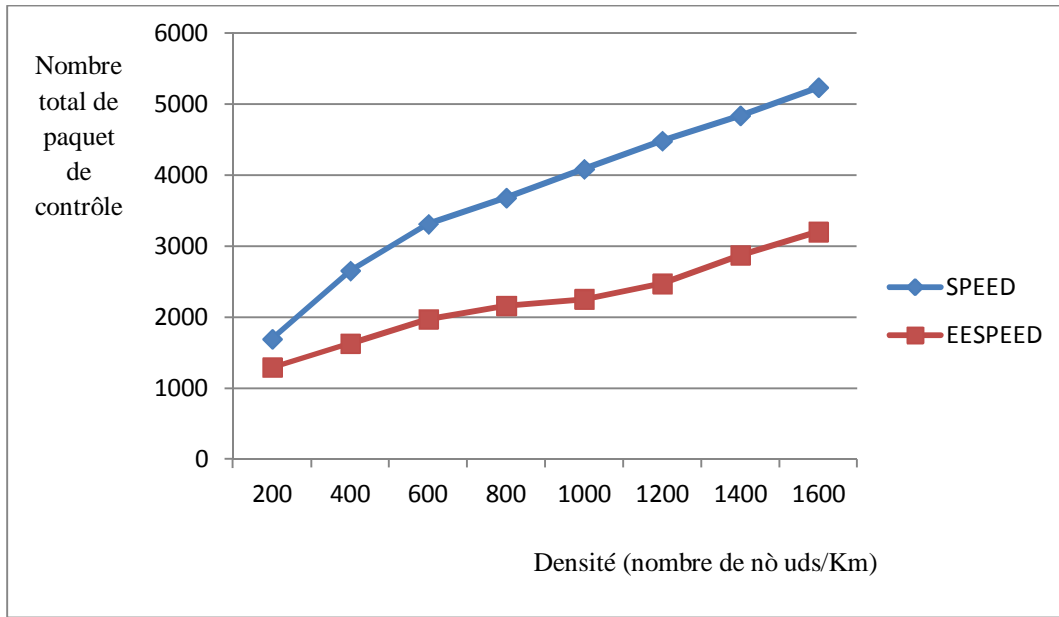
Les valeurs utilisées dans nos simulations sont 3, 6, 9, 12 et 15 trafic UDP que nous pouvons appeler aussi agents UDP, Un agent UDP est lié qu'à un seul nœud source.

ère des paquets de données UDP chaque 6 second pendant 5 minutes (5min représente le temps de la simulation).

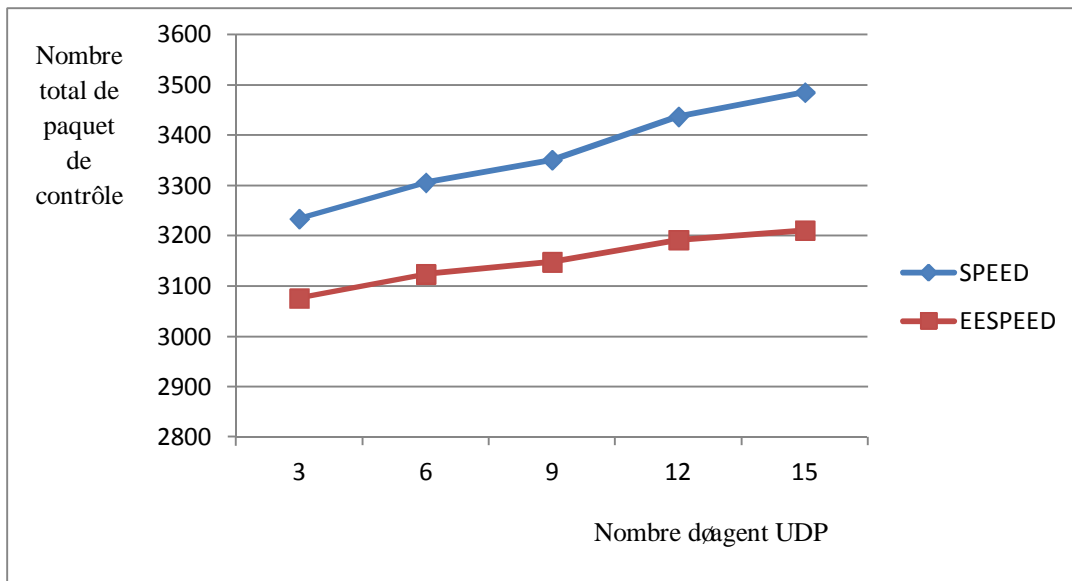
5.7 Résultats et discussions

5.7.1 Paquets de control (nombre total de paquet de contrôle)

Pour ce scénario nous avons deux courbes. La première illustre le nombre total de paquet de contrôle en fonction de la densité (**Figure 5.3-A**) et la deuxième illustre le nombre total de paquet de contrôle en fonction du trafic UDP sortant (**Figure 5.3-B**).



-A- : En fonction de la Densité



-B- : En fonction du trafic UDP

Figure 5.3 - Le nombre total de paquet de contrôle

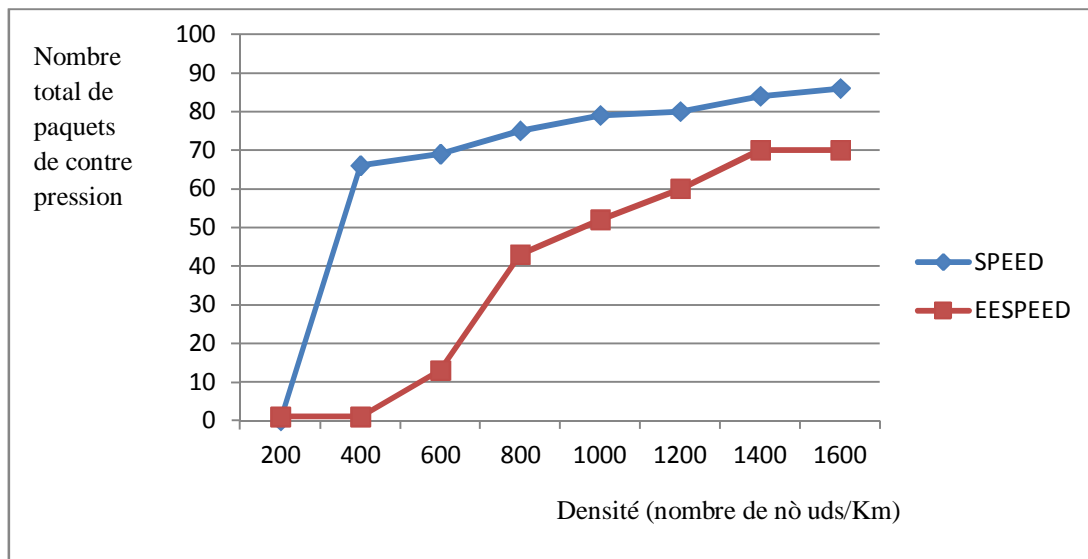
figure la courbe du protocole SPEED positionnée au dessus de la courbe du protocole EESPEED. Lorsque la densité est petite l'écart entre les deux protocoles est petit, mais avec l'augmentation de la densité l'écart devient grand.

SPEED engendre périodiquement pour chaque nœud dans le réseau deux types de paquet de contrôle : contrôle de localisation et contrôle de délai, donc l'augmentation de la densité des nœuds fait générer plus de paquets de contrôles, cependant dans EESPEED ces deux type de paquet de contrôle sont engendrer seulement par les chef de grappe, ce qui signifie que la densité des nœuds n'influence pas sur ces paquets de contrôles, seul les paquets contrôle d'énergie sont engendrés périodiquement pour chaque nœud dans le réseau.

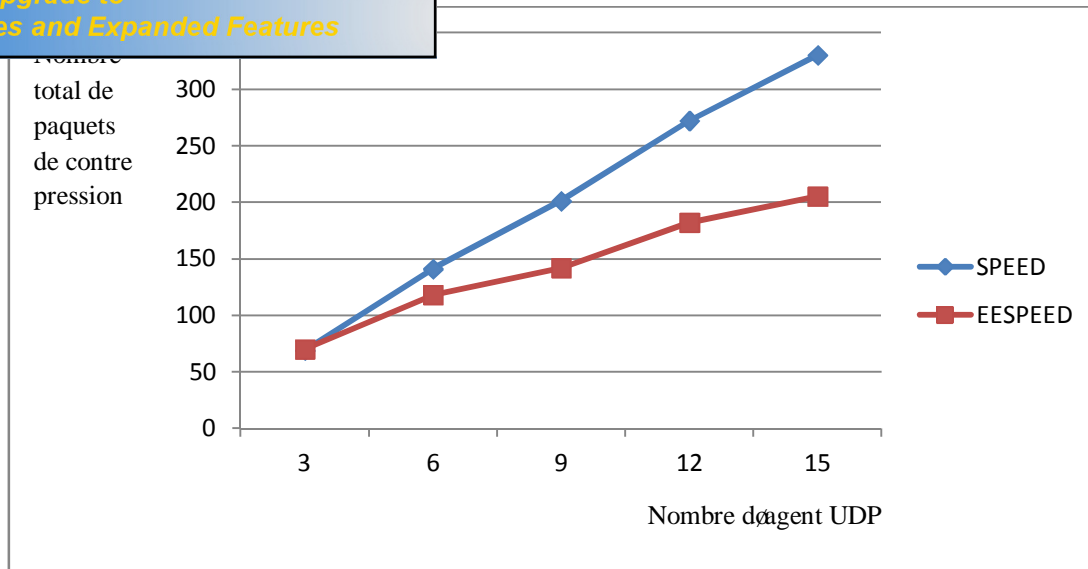
Pour la deuxième figure, SPEED maintient la barre haute au dessus de EESPEED, les deux protocoles sont presque stables en augmentant le flux sortant, parce que le trafic UDP n'influence pas beaucoup sur le nombre total de paquet de contrôle générés.

5.7.2 Les paquets de contre pression

Pour ce scénario nous avons deux courbes. La première illustre le nombre total de paquets de contre pression en fonction de la densité (**Figure 5.4-A**) et la deuxième illustre le nombre total de paquets de contre pression en fonction du trafic UDP sortant (**Figure 5.4-B**).



-A- : En fonction de la Densité



-B- : En fonction du trafic UDP

Figure 5.4 - Le nombre total de paquets de contre pression

Dans la première figure l'augmentation de la densité des nœuds fait augmenter aussi le nombre total de paquets de contre pression des deux protocoles.

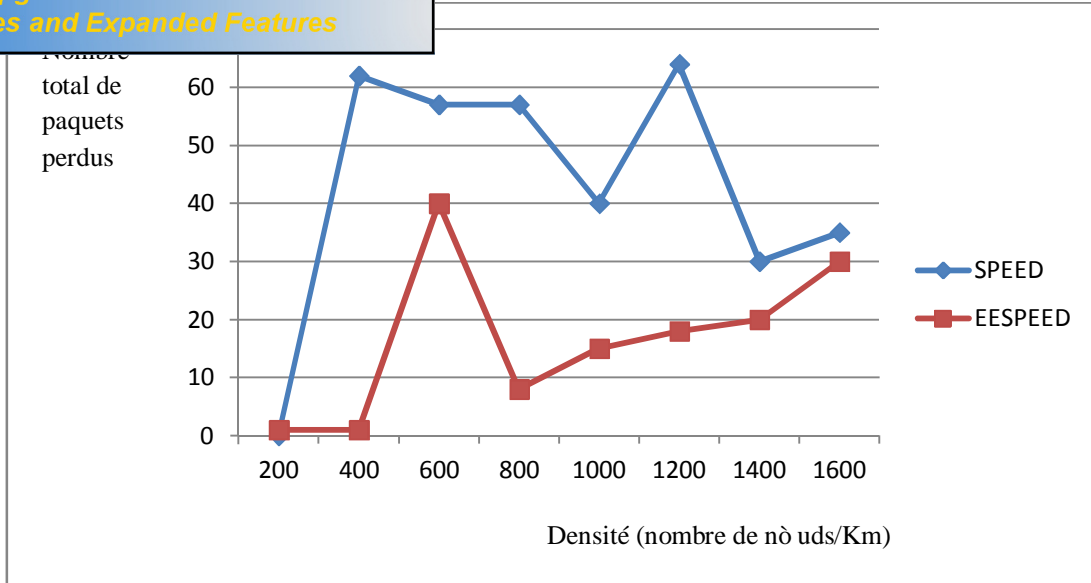
Pour la deuxième figure l'augmentation du trafic UDP fait augmenter aussi le nombre total de paquet de contre pression des deux protocoles.

SPEED engendre plus de paquet de contre pression par rapport à EESPEED, parce que le nombre total de paquets de contrôle générés dans SPEED est grand par rapport à EESPEED ce qui surcharge le réseau et crée des nœuds congestionnés.

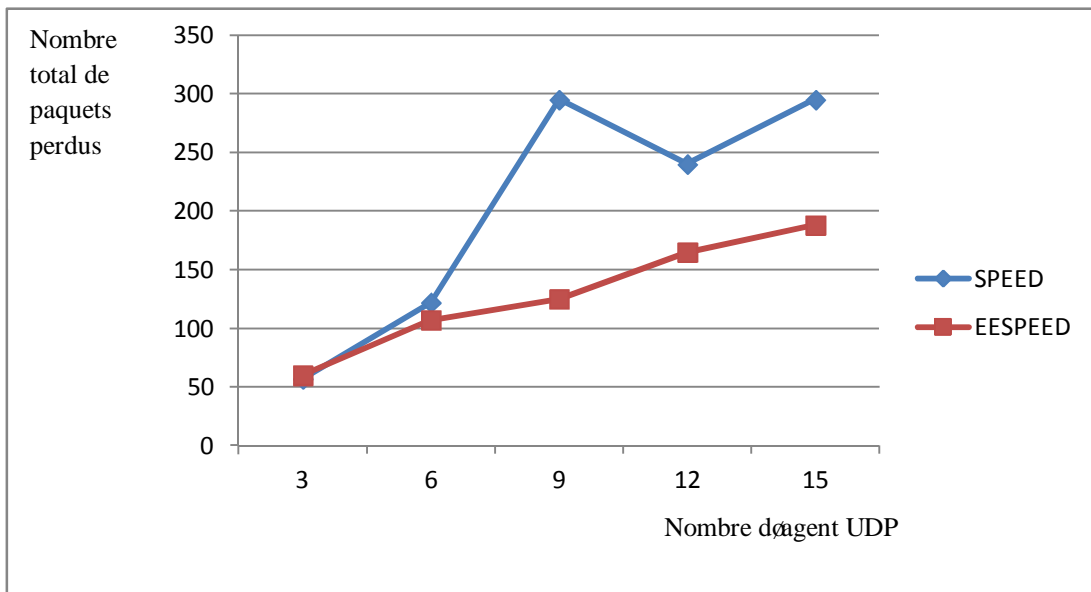
5.7.3 Les paquets perdus

Pour ce scénario nous avons deux courbes. La première illustre le nombre total de paquets perdus en fonction de la densité (**Figure 5.5-A**) et la deuxième illustre le nombre total de paquets perdus en fonction du trafic UDP sortant (**Figure 5.5-B**).

La différence est bien visible sur les deux courbes entre les deux protocoles. Sur la première figure avec l'augmentation de la densité des nœuds SPEED perd plus de paquets, tandis que EESPEED perd moins de paquets.



-A- : En fonction de la Densité



-B- : En fonction du trafic UDP

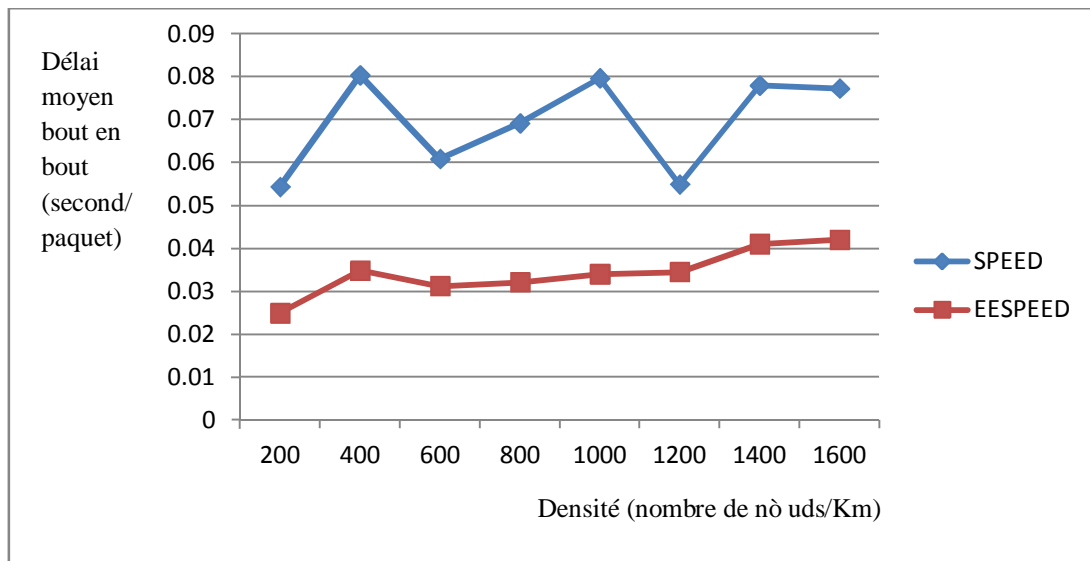
Figure 5.5 - Le nombre total de paquets perdus

Nous pouvons presque appliquer la même analyse à la deuxième figure, ou avec l'augmentation des flux sortants, SPEED perd plus de paquets. Sa moyenne de perte est nettement supérieure à celle du protocole EESPEED.

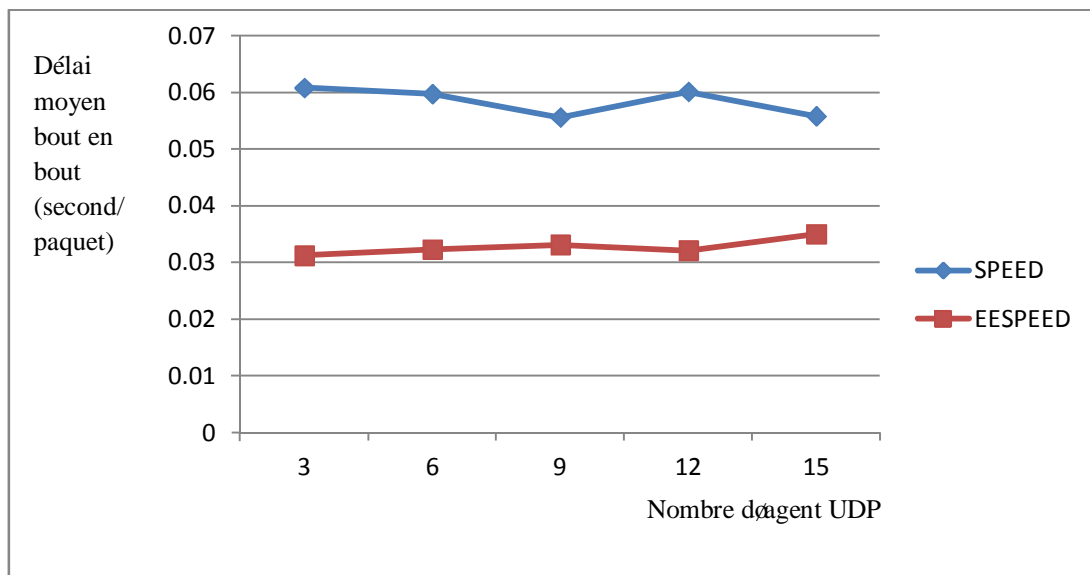
contrôle ou de données) par apport a EESPEED, parce que le nombre de paquet de contrôle générés dans SPEED et grand par apport a EESPEED ce qui surcharge le réseau et provoque la perte de paquets.

5.7.4 Le délai bout en bout

Pour ce scénario nous avons deux courbes. La première illustre le délai moyen bout en bout en fonction de la densité (**Figure 5.6-A**) et la deuxième illustre le délai moyen bout en bout en fonction du trafic UDP sortant (**Figure 5.6-B**).



-A- : En fonction de la Densité



-B- : En fonction du trafic UDP

Figure 5.6 - Le délai moyen bout en bout

protocoles sont presque stables, donc l'augmentation de la densité des nœuds n'influence pas beaucoup sur le délai moyen de bout en bout.

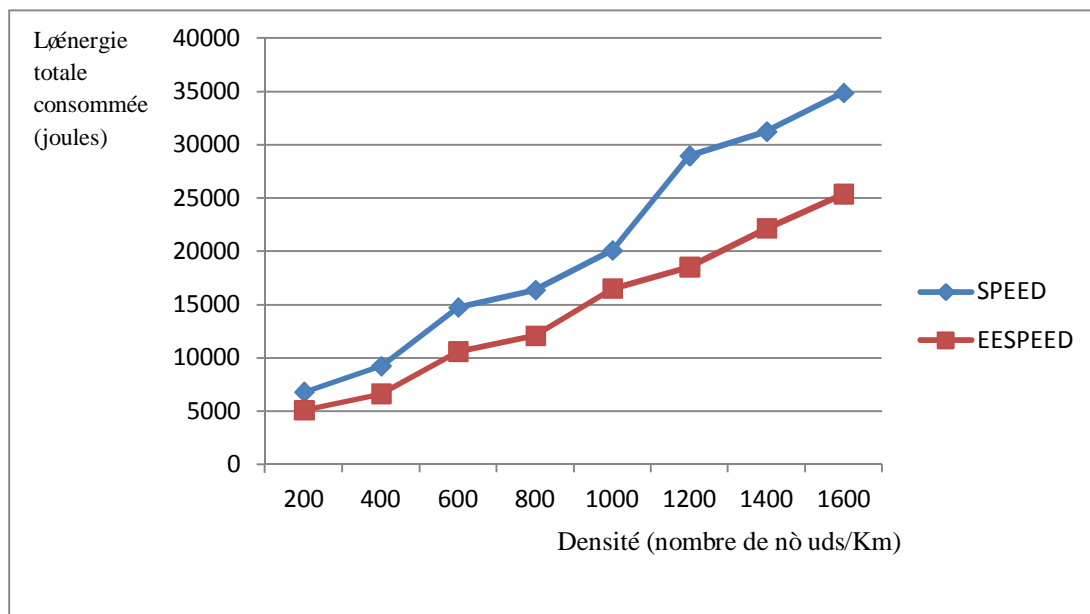
La même chose peut être dite sur la deuxième figure, où l'augmentation du trafic UDP n'influence pas beaucoup sur le délai moyen de bout en bout.

La courbe du protocole EESPEED est au dessous de la courbe du protocole SPEED parce qu'il utilise moins de routage que ce dernier.

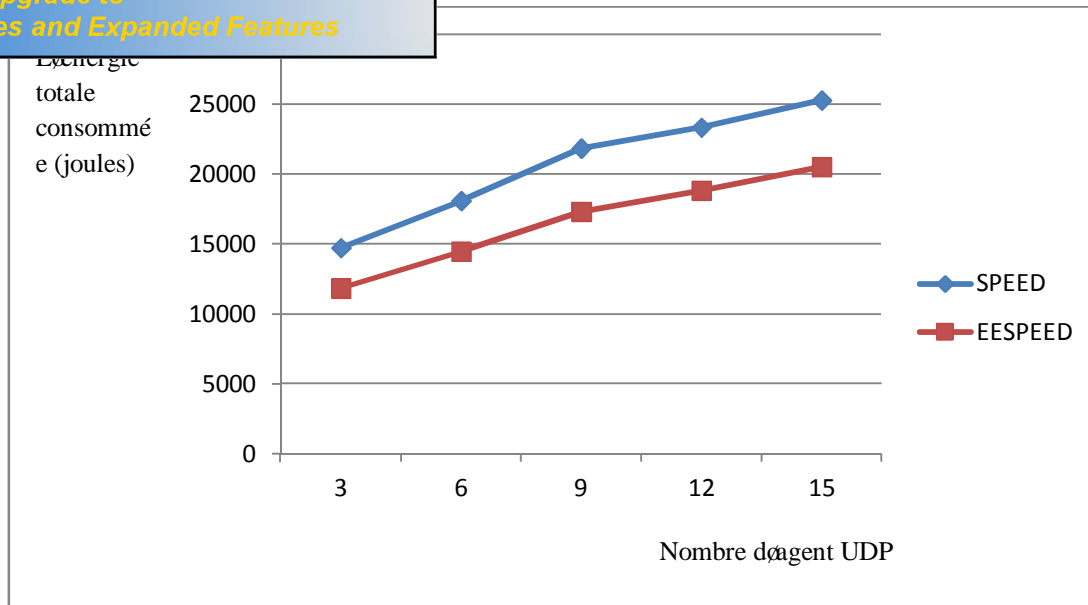
5.7.5 L'énergie consommée

Pour ce scénario nous avons deux courbes. La première illustre l'énergie total consommée dans le réseau en fonction de la densité (**Figure 5.7-A**) et la deuxième illustre l'énergie total consommée dans le réseau en fonction du trafic UDP sortant (**Figure 5.7-B**).

Dans la première figure la courbe du protocole SPEED positionnée au dessus de la courbe du protocole EESPEED. SPEED consomme plus d'énergie que l'autre protocole, et avec l'augmentation de la densité des nœuds l'écart entre les deux protocoles devient grand.



-A- : En fonction de la Densité



-B- : En fonction du trafic UDP

Figure 5.7 - L'énergie moyenne consommée

Les paquets de contrôle occupent une grande partie du trafic circulant dans le réseau, donc le protocole qui engendre moins de contrôle consomme moins d'énergie, c'est le cas du protocole EESPEED.

Pour la deuxième figure la courbe du protocole SPEED est aussi positionnée au dessus de la courbe du protocole EESPEED. L'augmentation du trafic UDP fait augmenter aussi la consommation d'énergie avec un écart presque stable entre les deux protocoles.

EESPEED consomme moins d'énergie que SPEED parce qu'il engendre moins de contrôle et utilise moins de routage que ce dernier.

5.8 Conclusion

Nous venons de voir par simulation dans ce chapitre que le protocole EESPEED permet la minimisation du nombre total des paquets de contrôle générés dans le réseau par rapport à SPEED. Cette minimisation permet l'amélioration des métriques suivantes : le nombre total de paquets perdus, le délai de bout en bout, le nombre total de paquets de congestion et la consommation totale d'énergie dans le réseau.



PDF Complete

Your complimentary use period has ended.
Thank you for using PDF Complete.

[Click Here to upgrade to Unlimited Pages and Expanded Features](#)

aux

ns les 2 cas suivants :

1^{er} cas : Lorsque plusieurs nœuds appartenant à la même grappe veulent transmettre des paquets de données au même temps. Le nœud chef de la grappe sera congestionné par ce que tous les paquets de données doivent passer par ce nœud.

2^{ème} cas : Lorsque la mobilité des nœuds dans le réseau est grande l'intervalle de temps entre deux re-clusterisation devient petit ce qui provoquera des retards dans la livraison et augmentera le taux de perte des paquets.



Conclusion générale

Les réseaux de capteurs présentent une solution adéquate pour servir les applications critiques telles que les alertes de catastrophes naturelles, la détection des intrusions, etc. Pour répondre aux exigences temps réel de ce type d'applications, il a fallu développer de nouveaux protocoles de routage qui garantissent la QoS temps réel et qui tiennent compte de certaines contraintes spécifiques de ces réseaux, comme la densité importante des nœuds capteurs, leurs mobilités, leurs autonomies énergétiques limitées, leurs durées de vie limitées...

C'est dans cette optique que nous avons mené nos travaux dans ce projet. En effet, nous nous sommes intéressés aux protocoles de routage basés sur la QoS pour les réseaux de capteurs à savoir le protocole SPEED. Pour la résolution des problèmes créés par SPEED lorsqu'il est utilisé comme protocole de routage pour un réseau de capteur dense à grande échelle, nous avons proposé un nouveau protocole de routage, appelé EESPEED (Energy-aware clustering SPEED). Ce qui constitue notre principale contribution. Le protocole EESPEED permet d'optimiser d'une manière plus efficace que SPEED, les performances : nombre total des paquets perdus, délai de bout en bout, nombre de paquets routés et la consommation totale d'énergie des réseaux de capteurs.

Le protocole SPEED se caractérise essentiellement par la garantie des délais de bout en bout réduits, mais, l'utilisation de ce protocole dans les réseaux de capteurs dense à grande échelle fait augmenter le nombre total des paquets de contrôle générés périodiquement (contrôle de localisation et contrôle de délai), ce qui fait diminuer les performances du protocole SPEED.

Nous avons, alors, exploité ce protocole pour minimiser le nombre total des paquets de contrôle générés périodiquement. En effet, nous avons introduit la technique d'agglomération (clustering) pour créer des grappes statiques, ou les paquets de



PDF Complete

*Your complimentary use period has ended.
Thank you for using PDF Complete.*

[Click Here to upgrade to Unlimited Pages and Expanded Features](#)

de délai ne seront générés que par les chefs des
ces paquets sont générés par tous les nœuds du
réseau. Ceci fait l'idée de notre nouveau protocole EESPEED. Les simulations effectuées, dans le cadre de notre projet, ont confirmé la fiabilité du protocole EESPEED par rapport au protocole SPEED pour les réseaux de capteurs denses à grande échelle en fonction des cinq métriques (nombre de paquets de contrôle, nombre de paquets perdus, délai de bout en bout, nombre de paquets de contre-pression et la consommation d'énergie dans le réseau).

En conclusion, le nouveau protocole, EESPEED, s'avère plus performant que le protocole SPEED pour les réseaux de capteurs denses à grande échelle.



PDF
Complete

*Your complimentary
use period has ended.
Thank you for using
PDF Complete.*

[Click Here to upgrade to
Unlimited Pages and Expanded Features](#)

Perspectives

Comme très souvent dans le monde de la recherche, le travail que nous avons effectué ouvrent de nouvelles perspectives, permettant de le compléter de différentes manières.

Une première perspective consistera à trouver une solution pour la congestion du nœud chef de grappe dans le cas où plusieurs nœuds appartenant à cette grappe **veulent** transmettre des paquets de données au même temps.

Une deuxième perspective visera l'amélioration des performances du protocole EESPEED dans le cas où la mobilité des nœuds dans le réseau est grande ce qui provoquera des retards dans la livraison et augmentera le taux de perte des paquets à cause de la diminution de l'intervalle de temps entre chaque deux re-clusterisations.



Bibliographie

- [1] Weiser, M. The Computer for the Twenty-First Century, Scientific American Paper, Vol. 265, No. 3, pp.94-104. September 1991.
- [2] Pujolle, G. Les réseaux sans fil et l'internet ambiant. In DNAC, Paris, France. 2003
- [3] International Organization for Standardization. Information processing systems, OSI reference model. Norme 7498-1, ISO/IEC. 1994.
- [4] ZigBee Standards Organization. ZigBee specification. Norme 053474r06, Version 1.0, San Ramon, Canada. 2005.
- [5] IEEE Standards Association. Standard 802.11 part 11: wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. 1999.
- [6] European Telecommunications Standards Institute (ETSI). Broadband Radio Access Networks (BRAN), High Performance Radio Local Area Network (HIPERLAN) Type 2, Requirements and architectures for wireless broadband access. Rapport technique 101 031 V2.2.1, Sophia-Antipolis, France. 1999.
- [7] Garelli, R., Royères, N., & Tschopp, C. *802.11 vs Hyperlan*. Mémoire de master en informatique, Université Montpellier II, Montpellier, France. 2005.
- [8] Trezentos, D. Standard pour réseaux sans fil : IEEE 802.11. In *Traité Télécoms*, volume TE 7 375. Techniques de l'ingénieur. 2002.
- [9] Corson, S., & Macker, J. Mobile Ad hoc Networking (MANET): Routing protocol performance issues and evaluation considerations. RFC 2501, IETF - Network Working Group. 1999.



PDF Complete
 Your complimentary use period has ended.
 Thank you for using PDF Complete.

[Click Here to upgrade to Unlimited Pages and Expanded Features](#)

Wireless networks and mobile computing, Chapitre
 Mobile ad hoc networks. Wiley Interscience Publication. 2002.

[11] Perkins, C. E. "Ad hoc networking". Addison-Wesley. 2001

[12] Chlamtac, I., Conti, M., & Liu, J. "Mobile ad hoc networking: Imperatives and challenges". *Ad Hoc Networks Journal* vol. 1, N. 1. 2003

[13] CHEE-YEE, C., & SRIKANTA P. K. "Sensor Networks: Evolution, Opportunities, and Challenges". *Proceedings of the IEEE*, vol. 91, no. 8, pp. 1247-1256, August 2003.

[14] Akyildiz, I.F., Sankarasubramaniam, Y., & Cayirci, E. "Wireless sensor networks: a survey". *Broadband and Wireless Networking Laboratory, School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, USA*. 2001.

[15] Archana, B., & Vijay A. "Sensor Networks: An Overview". Department of Computer Science University of California. 2002.

[16] Raileanu, L., & Nastaran, F. « Les Réseaux de Senseurs », Haute école d'ingénierie et de gestion du Canton de Vaud, Suisse. 2006.

[17] Dazhi, C., & Varshney, P. K. "QoS Support in Wireless Sensor Networks: A Survey". In *Proceedings of International Conference on Wireless Networks*. pp. 227-233. U.S.A. 2004.

[18] Hill, J. & Culler, D. MICA: A Wireless Platform for Deeply Embedded Networks. In *Micro IEEE*, Vol.22, No. 6, pp. 12 - 24. 2002.

[19] Hill, J., Szewczyk, R., Woo, A., Hollar, S., Culler, D. E., & K. S. J. Pister. System Architecture Directions for Networked Sensors. In *Proceedings of the 9th International Conference on Architectural Support for Programming Languages and Operating Systems*, Cambridge, MA. 2000

[20] Karl, H., & Willig, A. "Protocols And Architectures For Wireless Sensor Networks". Copyright John Wiley & Sons Ltd. England. 2005.

survey on routing protocols for wireless sensor networks. Elsevier Journal of Ad Hoc Networks. Vol. 3, No. 3. pp. 325-349. 2005.

[22] Al-Karaki, J. N., & Kamal, A. E. Routing Techniques in Wireless Sensor Networks: A Survey. IEEE Wireless Communications. Vol. 11, No. 6. pp. 6-28. 2004.

[23] Heinzelman, W., Kulik, J. & Balakrishnan, H. "Adaptive protocols for information dissemination in wireless sensor networks," in the *Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom99)*, pp. 174-85, Seattle, WA, USA. 1999.

[24] Intanagonwiwat, C., Govindan, R., & Estrin, D. "Directed diffusion: A scalable and robust communication paradigm for sensor networks", in the *Proceedings of the 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'00)*, pp. 56-67, Boston, MA, USA. 2000.

[25] Hedetniemi, S., & Liestman, A. "A survey of gossiping and broadcasting in communication networks," *Networks Journal*, Vol. 18, No. 4, pp. 319-349. 1988.

[26] Ganesan, D., & al. "Highly Resilient, Energy Efficient Multipath Routing in wireless Sensor Networks" in *Mobile Computing and Communications Review (MC2R)*, Vol. 1, No. 2. 2002.

[27] Shah, R., & Rabaey, J. "Energy Aware Routing for Low Energy Ad Hoc Sensor Networks", in the *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC)* Vol. 1, pp. 350- 355. Orlando, FL. 2002.

[28] Braginsky, D., & Estrin, D. "Rumor routing algorithm for sensor networks," Proceedings of the First Workshop on Sensor Networks and Applications (WSNA), SESSION: Transport and Routing Protocols, Pages: 22 - 31. Atlanta, GA. 2002.

[29] Schurgers, C., & Srivastava, M.B. "Energy efficient routing in wireless sensor networks" in the *MILCOM Proceedings on Communications for Network-Centric Operations: Creating the Information Force, (MILCOM '01)*, vol. 1, pp. 3576361., McLean, VA. 2001.



PDF Complete
 Your complimentary use period has ended.
 Thank you for using PDF Complete.

[Click Here to upgrade to Unlimited Pages and Expanded Features](#)

ao, F. "Scalable information-driven sensor querying and routing for ad hoc heterogeneous sensor networks," *The International Journal of High Performance Computing Applications* Vol. 16, No. 3, pp.293-313. 2002.

[31] Yao, Y., & Gehrke, J. "The cougar approach to in-network query processing in sensor networks," In *SIGMOD Record*, Vol. 31, No. 3, pp. 9-18. 2002.

[32] Sadagopan, N., & al. "The ACQUIRE mechanism for efficient querying in sensor networks," in the *Proceedings of the First International Workshop on Sensor Network Protocol and Applications*, pp. 149-155, Anchorage, AK, USA. 2003.

[33] Heinzelman, W., Chandrakasan, A., & Balakrishnan, H. "Energy-efficient communication protocol for wireless sensor networks," in the *Proceeding of the Hawaii International Conference System Sciences*, Vol. 8, p.8020 Hawaii. 2000.

[34] Lindsey, S., & Raghavendra, C. S. "PEGASIS: Power Efficient Gathering in Sensor Information Systems," in the *Proceedings of the IEEE Aerospace Conference*, pp.1-6. Big Sky, Montana, USA. 2002.

[35] Manjeshwar, A., & Agrawal, D. P. "TEEN: A Protocol for Enhanced Efficiency in Wireless Sensor Networks," in the *Proceedings of the 1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing*, p. 189. San Francisco, CA. 2001.

[36] Subramanian, L., & Katz, R. H. "An Architecture for Building Self Configurable Systems," in the *Proceedings of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing*, pp. 63-73. Boston, MA, USA. 2000.

[37] Rodoplu, V., & Ming, T.H. "Minimum energy mobile wireless networks," *IEEE Journal of Selected Areas in Communications*, Vol. 17, No. 8, pp. 1333-1344. 1999.

[38] Xu, Y., Heidemann, J., & Estrin, D. "Geography-informed energy conservation for ad hoc routing," in the *Proceedings of the 7th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom '01)*, pp. 70-84. Rome, Italy. 2001.



PDF Complete
Your complimentary use period has ended.
Thank you for using PDF Complete.

[Click Here to upgrade to Unlimited Pages and Expanded Features](#)

- [43] A. R. Rebai, R. "Geographical and Energy-Aware Routing: A Recursive Data Dissemination Protocol for Wireless Sensor Networks," *UCLA Computer Science Department, Technical Report UCLA/CSD-TR-01-0023*, USA. 2001.
- [40] Chang, J. H., & Tassiulas, L. "Maximum Lifetime Routing in Wireless Sensor Networks," in the *Proceedings of the Advanced Telecommunications and Information Distribution Research Program*, Vol. 12, No. 4, pp. 609-619. College Park, USA. 2004.
- [41] Kalpakis, K., Dasgupta, K., & Namjoshi, P. "Maximum lifetime data gathering and aggregation in wireless sensor networks," in the *Proceedings of IEEE International Conference on Networking (NETWORKS '02)*, pp. 685-696, Atlanta, Georgia. 2002.
- [42] Chu, M., Haussecker, H., & Zhao, F. "Scalable Information-Driven Sensor Querying and Routing for ad hoc Heterogeneous Sensor Networks," *The International Journal of High Performance Computing Applications*, Vol. 16, No. 3, pp. 293-313. 2002.
- [43] Akkaya, K., & Younis, M. "An Energy-Aware QoS Routing Protocol for Wireless Sensor Networks," in the *Proceedings of the IEEE Workshop on Mobile and Wireless Networks (MWN 2003)*, Providence, Rhode Island. 2003.
- [44] He, T. & al. "SPEED: A stateless protocol for real-time communication in sensor networks," in the *Proceedings of International Conference on Distributed Computing Systems*, pp. 46- 55, Providence, RI. 2003.
- [45] Kurose, J. F., Ross, K. W. "Computer Networking A Top-Down Approach Featuring the internet," Addison Wesley Longman Inc. 2000.
- [46] Rebai, A. R. "Optimisation Globale de la Qualité de Service dans les réseaux locaux sans fils de type IEEE 802.11 : Mise en œuvre de nouveaux mécanismes de gestions de QoS pour la couche d'accès". 2007.