



République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de La Recherche Scientifique
Université Mouloud MAMMERRI de Tizi-Ouzou
Faculté de Génie électrique et Informatique
Département Informatique

Projet de fin d'étude pour l'obtention du diplôme de Master
Option : Réseaux, Mobilité et Systèmes Embarqués

Système d'Ordonnancement Distribué et Auto-Organisé dans les réseaux de capteurs sans fil

Réalisé par :

Mr. Nacim HAMOUDI

Mr. Farid CHARCHAR

Encadrés par :

Mr. Mestapha LALAM

Dirigé par :

Président de jury : Mr.Daoui Mohamed

Promoteur : Mr.Lalam Mestapha

Examineurs : Mm.Aoudjit Rachida

Mm. Chemak Lynda

2012/2013

INTRODUCTION GENERALE	ERREUR ! SIGNET NON DEFINI.
I. ORGANISATION DU DOCUMENT	ERREUR ! SIGNET NON DEFINI.
CHAPITRE 1 : LES RESEAUX DE CAPTEURS SANS FIL : UNE NOUVELLE GENERATION DE RESEAUX SANS FIL	ERREUR ! SIGNET NON DEFINI.
INTRODUCTION	ERREUR ! SIGNET NON DEFINI.
I- PARTIE I : LES CATEGORIES DE RESEAUX SANS FIL	ERREUR ! SIGNET NON DEFINI.
I-1. <i>Le réseau personnel sans fil (WPAN)</i>	<i>Erreur ! Signet non défini.</i>
I-2. <i>Le réseau local sans fil (WLAN)</i>	<i>Erreur ! Signet non défini.</i>
I-3. <i>Le réseau métropolitain sans fil (WMAN)</i>	<i>Erreur ! Signet non défini.</i>
I-4. <i>Le réseau étendu sans fil (WWAN)</i>	<i>Erreur ! Signet non défini.</i>
II- PARTIE II : LES RESEAUX DE CAPTEURS SANS FIL (RCSF).....	ERREUR ! SIGNET NON DEFINI.
II-1. <i>Définition</i>	<i>Erreur ! Signet non défini.</i>
II-2. <i>Les principales caractéristiques des RCSF</i>	<i>Erreur ! Signet non défini.</i>
II-3. <i>Comparaison entre les RCSF et les réseaux sans fil classiques</i>	<i>Erreur ! Signet non défini.</i>
II-4. <i>Les domaines d'application</i>	<i>Erreur ! Signet non défini.</i>
II-5. <i>L'architecture d'un nœud capteur</i>	<i>Erreur ! Signet non défini.</i>
II-6. <i>La pile protocolaire des RCSF</i>	<i>Erreur ! Signet non défini.</i>
CONCLUSION	ERREUR ! SIGNET NON DEFINI.
CHAPITRE 2 :	ERREUR ! SIGNET NON DEFINI.
L'ACCES AU SUPPORT DANS LES RESEAUX SANS FIL	ERREUR ! SIGNET NON DEFINI.
INTRODUCTION	ERREUR ! SIGNET NON DEFINI.
I- PREMIERE PARTIE : LES TECHNIQUES DE CONTROLE D'ACCES DANS LES RESEAUX SANS FIL CLASSIQUES	ERREUR ! SIGNET NON DEFINI.
I-1. <i>L'accès multiple par répartition temporelle (TDMA)</i>	<i>Erreur ! Signet non défini.</i>
I-2. <i>L'accès multiple par répartition fréquentielle (FDMA)</i>	<i>Erreur ! Signet non défini.</i>
I-3. <i>L'accès multiple par répartition de codes (CDMA)</i>	<i>Erreur ! Signet non défini.</i>
I-4. <i>L'accès multiple avec écoute de la porteuse/ Evitement de collision (CSMA/CA)</i>	<i>Erreur ! Signet non défini.</i>
II- DEUXIEME PARTIE : LES PROTOCOLES MAC PROPOSES POUR LES RCSF	ERREUR ! SIGNET NON DEFINI.
II-1. <i>Les raisons d'adoption de nouveaux protocoles MAC pour les RCSF</i>	<i>Erreur ! Signet non défini.</i>
II-2. <i>Les caractéristiques d'un protocole MAC convenable aux RCSF</i>	<i>Erreur ! Signet non défini.</i>
II-3. <i>La consommation d'énergie au niveau de la couche MAC dans les RCSF</i>	<i>Erreur ! Signet non défini.</i>
II-4. <i>Le protocole Sensor-MAC</i>	<i>Erreur ! Signet non défini.</i>
II-5. <i>Le protocole TimeOut-MAC</i>	<i>Erreur ! Signet non défini.</i>
II-6. <i>Le protocole Wise-MAC</i>	<i>Erreur ! Signet non défini.</i>
II-7. <i>Le protocole TRAMA (Traffic-adaptive medium access protocol)</i>	<i>Erreur ! Signet non défini.</i>
II-8. <i>Le protocole Léger-MAC (LMAC)</i>	<i>Erreur ! Signet non défini.</i>
III- TROISIEME PARTIE : ETUDE COMPARATIVE DE QUELQUES PROTOCOLES MAC PROPOSES DANS LES RCSF	ERREUR ! SIGNET NON DEFINI.
III-1. LES CRITERES DE COMPARAISON.....	ERREUR ! SIGNET NON DEFINI.
III-2. <i>Le tableau comparatif</i>	<i>Erreur ! Signet non défini.</i>
CONCLUSION :	ERREUR ! SIGNET NON DEFINI.
CHAPITRE 3 : SYSTEME D'ORDONNANCEMENT DISTRIBUE ET AUTO-ORGANISE	ERREUR ! SIGNET NON DEFINI.
I. INTRODUCTION.....	ERREUR ! SIGNET NON DEFINI.
II. HYPOTHESES	ERREUR ! SIGNET NON DEFINI.
III. MOTIVATION ET MISE AU POINT	ERREUR ! SIGNET NON DEFINI.
IV. UN POINT DE VUE DE L'APPROCHE DOSA	ERREUR ! SIGNET NON DEFINI.
V. PRELIMINAIRES POUR AUTO-STABILISATION	ERREUR ! SIGNET NON DEFINI.
VI. DOSA : ALGORITHME D'ORDONNANCEMENT DISTRIBUE ET AUTO-ORGANISE	ERREUR ! SIGNET NON DEFINI.
VI.1 LES DETAILS DU SYSTEME DE SIMULATION	ERREUR ! SIGNET NON DEFINI.
VI.2 DEPENDANCE DE DOSA SUR LMAC.....	ERREUR ! SIGNET NON DEFINI.
VI.3 FONCTIONNEMENT GENERAL DE DOSA	ERREUR ! SIGNET NON DEFINI.
VI.3.1 <i>Exactitude de DOSA</i>	<i>Erreur ! Signet non défini.</i>

Sommaire

VI.3.2 Manipulation des messages corrompus.....	Erreur ! Signet non défini.
VII. PERFORMANCE DE DOSA.....	ERREUR ! SIGNET NON DEFINI.
VII.1 EFFICACITE DES DOSA EN TERMES DE GENERATION DE MESSAGES.....	ERREUR ! SIGNET NON DEFINI.
VII.2 EFFICACITE DES DOSA EN TERMES DE DUREE DE VIE DU RESEAU ET LA QUALITE DES DONNEES	ERREUR !
SIGNET NON DEFINI.	
VII.3 FAIRE FACE A UN NŒUD MORT	ERREUR ! SIGNET NON DEFINI.
VII.4 FAIRE FACE A UN NOUVEAU NŒUD.....	ERREUR ! SIGNET NON DEFINI.
CONCLUSION	ERREUR ! SIGNET NON DEFINI.
CONCLUSION GENERALE.....	ERREUR ! SIGNET NON DEFINI.
LISTE DES ABRÉVIATIONS.....	ERREUR ! SIGNET NON DEFINI.
BIBLIOGRAPHIE.....	ERREUR ! SIGNET NON DEFINI.

Introduction générale

Les réseaux de capteurs sans fil connaissent actuellement un engouement important dans le domaine de la recherche, du fait notamment des grands avantages qu'ils promettent en terme de flexibilité, de coût, d'autonomie et de robustesse. En plus, de tels réseaux trouvent une utilisation dans une grande variété d'applications, par exemple dans la collecte de données à distance, type surveillance de climat, activités sismiques, ou dans d'autres domaines tel que la domotique, le médical... Néanmoins, leurs inconvénients sont à la hauteur de leurs promesses. En effet, l'extraction des grandes quantités de données générées par la grande, haute densité déploiements de réseaux de capteurs peuvent provoquer un large éventail de problèmes. Cependant les déploiements WSN, ne sont pratiquement viables que si elles sont en mesure de fonctionner sans surveillance durant de longues durées. En outre, la bande passante limitée empêche toutes les lectures acquises de se propager avec succès vers le puits. Il en résulte une perte de paquets, qui à son tour a un impact négatif sur la qualité des données collectées.

L'objectif du projet est de présenter un algorithme d'ordonnancement complètement distribué qui permet à chaque nœud de choisir les ordonnancements de manière autonome en se basant uniquement sur les informations disponibles localement.

Cet Algorithme possède également des propriétés d'auto-stabilisation qui lui permettent de se rétablir en un temps fini quelles que soient les perturbations dans le réseau, tels que les changements de topologie ou des erreurs de communication.

Nous illustrons comment cet algorithme peut s'adapter rapidement aux changements de topologie grâce à son interaction étroite avec la couche sous-jacente MAC. L'algorithme améliore également l'efficacité énergétique en tirant parti des informations inter-couches fourni par le MAC.

Enfin, l'algorithme est également capable d'éliminer totalement les messages abandonnés causés par les dépassements de tampon.

I. Organisation du document

Ce document est organisé comme suit :

- Dans le chapitre 1, nous apportons, dans un premier temps, une vue d'ensemble des technologies des réseaux sans fil existantes actuellement. Dans un second temps, nous nous intéresserons aux RCSF. On étudiera alors leurs principales caractéristiques, leurs domaines d'application, l'architecture d'un nœud capteur et enfin les couches de leur pile protocolaire.
- Dans le chapitre 2, nous verrons dans une première partie les techniques d'accès utilisées dans les réseaux sans fil classiques. Dans une seconde partie, nous verrons un état de l'art des principaux protocoles MAC qui ont été proposés pour les réseaux de capteurs sans fil. Ce chapitre sera clôturé par une troisième partie consacrée à une étude comparative théorique des protocoles MAC évoqués dans la seconde partie.
- Dans le dernier chapitre, nous présenterons un algorithme d'ordonnancement complètement distribué, puis, nous prouvons que cet algorithme possède des propriétés d'auto-stabilisation, Nous illustrons en suite comment ce dernier est capable de s'adapter rapidement aux changements de topologie ; Enfin, nous présentons des estimations de performances théoriques de l'algorithme.

Chapitre 1 : Les réseaux de capteurs sans fil : Une nouvelle génération de réseaux sans fil

Introduction

Ce chapitre est scindé en deux parties. Dans la première partie, nous donnerons une vue d'ensemble des catégories des réseaux sans fil ainsi que leurs principales spécificités.

Dans la seconde partie, nous présenterons les RCSF (Réseaux de Capteurs Sans Fil), leurs caractéristiques, leur situation par rapport aux autres réseaux sans fil, leur pile protocolaire ainsi que leurs domaines d'applications.

I- Partie I : Les catégories de réseaux sans fil

Il existe plusieurs catégories de réseaux sans fil qui diffèrent par le périmètre géographique qu'ils couvrent ainsi que par les types d'applications supportées. Le schéma suivant illustre les catégories de réseaux sans fil.

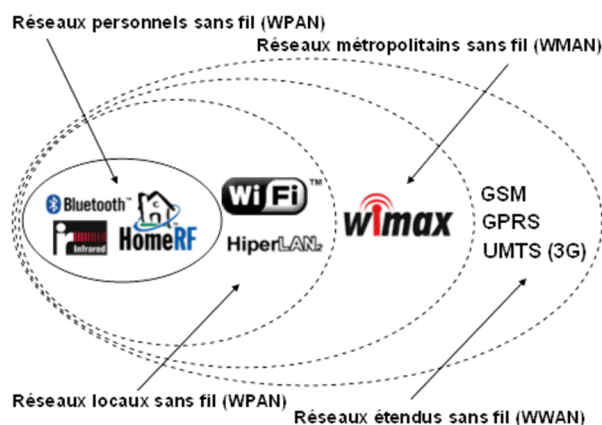


Figure 2.1 : Les catégories de réseaux sans fil [1]

I-1. Le réseau personnel sans fil (WPAN)

Il concerne les réseaux sans fil d'une faible portée : de l'ordre de quelques dizaines de mètres. Ce type de réseau sert généralement à relier des périphériques (imprimante, téléphone portable, appareils domestiques, PDA...). Il existe plusieurs technologies utilisées pour les WPAN :

- **La technologie Bluetooth :** Elle est connue aussi sous le nom de la norme IEEE 802.15.1, elle a été lancée par Ericsson en 1994, proposant un débit théorique de 1 Mbps lui permettant une transmission de la voix, des données et des images [2] d'une portée maximale d'une trentaine de mètres [1]. Bluetooth est une technologie peu onéreuse grâce à sa forte intégration sur une puce unique de 9 mm sur 9 mm [PUJ 05] ; Elle présente également l'avantage de fonctionner sur des appareils à faible puissance d'où une faible consommation d'énergie [3].
- **La technologie ZigBee :** Elle est connue aussi sous le nom de la norme IEEE 802.15.4 et permet d'obtenir des liaisons sans fil à bas prix et avec une très faible consommation d'énergie, ce qui la rend particulièrement adaptée pour être directement intégrée dans de petits appareils électroniques (capteurs, appareils électroménagers...) [1]. Les réseaux ZigBee permettent d'offrir des débits jusqu'à 250 Kbits/s dans la bande classique des 2,4GHz. Les RCSF constituent une des applications que cette norme peut couvrir [ZHE 04].
- **Les liaisons infrarouges :** Elles permettent de créer des liaisons sans fil de quelques mètres avec des débits pouvant monter à quelques mégabits par seconde. Cette technologie est largement utilisée dans la domotique (télécommandes), elle souffre toutefois des perturbations dues aux interférences lumineuses [1].

I-2. Le réseau local sans fil (WLAN)

C'est un réseau permettant de couvrir une portée d'environ une centaine de mètres. Il permet de relier entre-eux les terminaux présents dans la zone de couverture. Il existe deux technologies concurrentes :

- **Les réseaux Wi-Fi (Wireless-Fidelity) :** Ils proviennent de la norme IEEE 802.11, qui définit une architecture cellulaire. On y trouve principalement deux types de réseaux sans fil : Ceux qui travaillent à la vitesse de 11 Mbits/s à 2.4 GHz (IEEE 802.11b) et ceux qui montent à 54 Mbits/s à 5 GHz (IEEE 802.11 a/g) [PUJ 05].

- **Les réseaux HiperLAN 2 (High Performance LAN 2.0) :** Ils découlent de la norme européenne élaborée par l'ETSI (European Telecommunications Standards Institute). HiperLAN 2 permet d'obtenir un débit théorique de 54 Mbps sur une zone d'une centaine de mètres dans la gamme de fréquence comprise entre 5 150 et 5 300 MHz [1]. Ce type de réseau n'a pas reçu autant de succès que la technologie Wi-fi.

I-3. Le réseau métropolitain sans fil (WMAN)

Il est connu aussi sous le nom de Boucle Locale Radio (BLR). Il convient de rappeler que la BLR permet, en plaçant une antenne parabolique sur le toit d'un bâtiment, de transmettre par voie hertzienne de la voix et des données à haut débit pour l'accès à l'internet et à la téléphonie. Il existe plusieurs types de réseaux WMAN dont le plus connu est :

- **les réseaux Wimax (Worldwide interoperability for Microwave Access) :** ils émanent de la norme IEEE 802.16 et ont pour but de développer des liaisons hertziennes concurrentes aux techniques xDSL terrestres et offrent un débit utile de 1 à 10 Mbit/s dans la bande 10-66 GHz pour une portée de 4 à 10 kilomètres, ce qui destine principalement cette technologie aux opérateurs de télécommunication [PUJ 05].

I-4. Le réseau étendu sans fil (WWAN)

Il est connu sous le nom de réseau cellulaire mobile et il est le plus répandu de tous puisque tous les téléphones mobiles sont connectés à un réseau étendu sans fil. Les principales technologies sont les suivantes : GSM (Global System for Mobile Communication), GPRS (General Packet Radio Service) et UMTS (Universal Mobile Telecommunication System) [1].

II- Partie II : Les réseaux de capteurs sans fil (RCSF)

II-1. Définition

Un RCSF consiste en un nombre de capteurs connectés entre eux qui sont capables de sonder l'environnement dans lequel ils se trouvent et remonter l'information vers certains nœuds (puits) déployés qui sont en mesure de relayer l'information à grande échelle comme l'illustre le schéma suivant.

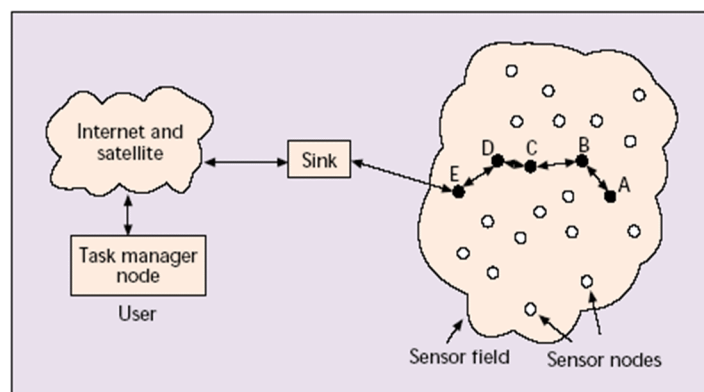


Figure 2.2 : Les RCSF dans leur contexte pratique [AKY 02]

Les RCSF forment une nouvelle génération de réseaux aux propriétés spécifiques, qui n'entrent pas dans les architectures classiques. Ils présentent un champ d'application très vaste et couvrent plusieurs domaines à caractère scientifique, logistique, militaire ou de santé.

II-2. Les principales caractéristiques des RCSF

- **La consommation réduite d'énergie :** Les nœuds capteurs utilisent des batteries de taille très petites comme ressources en énergie, ce qui limite leur durée de vie. La spécificité des applications des RCSF (militaires, sismiques et autres) fait que la recharge ou le remplacement de ces batteries est une tâche difficile ou presque impossible, ce qui nous mène à déduire que la durée de vie d'un nœud est essentiellement dépendante de la durée de vie de la batterie. Ainsi, la méthode de gestion de consommation d'énergie constitue une contrainte majeure dans ce type de réseau.

- **L'auto-configuration des nœuds capteurs :** Dans un RCSF, les nœuds sont déployés soit d'une manière aléatoire (missile, avion...), soit placés nœud par nœud par un humain ou un robot, et ceci à l'intérieur ou autour du phénomène observé (champ de guerre, surface volcanique, patient malade...) [AKY 02]. Ainsi, un nœud capteur doit avoir des capacités, d'une part, pour s'auto-configurer dans le réseau, et d'autre part pour collaborer avec les autres nœuds dans le but de reconfigurer dynamiquement le réseau en cas de changement de topologie du réseau [HOL 03].

Dans un RCSF, chaque nœud X possède une unité émettrice/réceptrice qui lui permet de communiquer avec les nœuds qui lui sont proches; En échangeant des informations avec ces

derniers, le nœud X pourra alors découvrir ses nœuds voisins et ainsi connaître la méthode de routage qu'il va adopter selon les besoins de l'application [CUL 04].

L'auto-configuration apparaît comme une caractéristique nécessaire dans le cas des RCSF étant donné que d'une part, leur déploiement s'effectue d'une manière aléatoire dans la majorité des applications, et d'autre part le nombre des nœuds capteurs est très grand.

- **La scalabilité** : Contrairement aux réseaux sans fil traditionnels (personnel, local ou étendu), un RCSF peut contenir un très grand nombre de nœuds capteurs (des centaines, des milliers...) [AKY 02].

Un réseau de capteur est scalable parce qu'il a la faculté d'accepter un très grand nombre de nœuds qui collaborent ensemble afin d'atteindre un objectif commun.

- **La tolérance aux pannes** : Dans le cas de dysfonctionnement d'un nœud (manque d'énergie, interférences avec l'environnement d'observation...) ou aussi en cas d'ajout de nouveaux nœuds capteurs dans le réseau, ce nœud doit continuer à fonctionner normalement sans interruption [AKY 02]. Ceci explique le fait qu'un RCSF n'adopte pas de topologie fixe mais plutôt dynamique.

- **Une densité importante des nœuds** : Les RCSF sont caractérisés par leur forte densité [FLE 03]. Cette densité peut atteindre, selon le type d'application, 20 nœuds/m² [AKY 02].

- **La capacité de communication** : Elle peut prendre deux aspects : Le multisaut ou à un seul saut [FLE 03]. Parce que le multisaut est moins énergivore, il reste le type de communication le plus sollicité par les applications de RCSF qui requièrent une faible consommation d'énergie.

- **Les types de communication** : Il existe différents types de communications utilisées dans les RCSF :

- **Unicast** : ce type de communication est utilisé pour échanger des informations entre deux nœuds sur le réseau.
- **Broadcast** : la station de base ou le nœud puits transmet des informations vers tous les nœuds du réseau. Ces informations peuvent être des requêtes de données bien précises (ex : la température dans la région A), des mises à jour de programmes ou des paquets de contrôle... [AKY 02]

- *Local Gossip* : ce type de communication est utilisé par des nœuds situés dans une région bien déterminée qui collaborent ensemble afin d'avoir une meilleure estimation de l'évènement observé et d'éviter l'émission du même message vers le nœud puits ce qui contribue à consommer moins d'énergie.
 - *Convergecast* : il est utilisé dans les communications entre un groupe de nœuds et un nœud bien spécifique (qui peut être le « puits »). L'avantage de ce type de communication est la diminution de contrôle d'entête des paquets (« *control overhead*») ce qui économise l'énergie au niveau du nœud récepteur [HOL 03].
 - *Multicast* : il permet une communication entre un nœud et un groupe de nœuds. Ce type de communication est utilisé dans les protocoles qui incluent la classification de données « clustering » dans lesquels, le « *Clusterhead* » s'intéresse à communiquer avec un groupe de nœuds [AKY 02].
- **Une architecture « data-centric »** : Du fait que le remplacement ou la recharge des batteries des nœuds capteurs est une tâche non pratique et difficile à réaliser, il est d'usage qu'on trouve des nœuds capteurs redondants (effectuant la même tâche dans la même région) ; L'importance d'un nœud particulier est, par conséquent, réduite par rapport à l'importance attribuée aux données observées par les nœuds. Ce type d'architecture diffère des architectures « node-centric » adoptées par les réseaux traditionnels où les nœuds possèdent une place importante (Exemple : un utilisateur qui veut connecter son laptop au serveur web X) [HOL 03].
- **Une collaboration entre les nœuds** : Les contraintes strictes de consommation d'énergie mènent les nœuds capteurs à détecter et traiter les données d'une manière coopérative afin d'éviter le traitement redondant d'une même donnée observée, source de la perte d'énergie [6].
- **La bande passante (ou capacité du canal)** : c'est une caractéristique beaucoup plus importante dans les réseaux cellulaires (GSM) et les réseaux locaux sans fils (WLAN), que dans les RCSF ; le débit étant en effet un objectif secondaire pour les RCSF [DEM 03]

II-3. Comparaison entre les RCSF et les réseaux sans fil classiques

Le tableau suivant illustre une comparaison entre les RCSF et les réseaux sans fil classiques. Cette comparaison s'appuie sur cinq critères : le nombre de nœuds, l'importance de la consommation d'énergie, l'importance de la QoS, l'identification des nœuds et les types de communication.

	RCSF	Réseau WLAN	Réseau cellulaire	Réseau WPAN
Nombre de nœuds	Très élevé	Diminué	Elevé	1 nœud maître avec 7 nœuds esclaves (Cas de Bluetooth)
L'importance de la consommation d'énergie	Très élevé.	Diminué du fait que les nœuds peuvent être rechargés facilement.	Diminué du fait que les nœuds peuvent être rechargés facilement.	Diminué
Importance de la qualité de service	Diminué	Elevée	Elevée	Elevée
Identification des nœuds	Dépend de l'application (généralement pas de mécanismes d'identification pour éviter l'overhead)	Existe	Existe	Existe
Type de communication	broadcast, multicast, Convergecast...	Point à point	Du mobile vers la station de base et vice versa.	Du nœud maître vers le nœud esclave.

- *Tableau de comparaison entre les RCSF et les réseaux sans fil classiques* -

II-4. Les domaines d'application

Les RCSF couvrent un champ d'applications très vaste et varié. En effet, leurs spécificités lui ont permis de supporter des applications qui sont inappropriés pour d'autres types de réseaux sans fil. Parmi les domaines d'application de ce type de réseau, on peut citer les domaines militaire, médical, la sécurité civile, la domotique et autres.

Les RCSF sont utilisés dans le domaine militaire, pour la surveillance, la reconnaissance, la détection des mouvements de l'ennemi et autres.

Dans le domaine médical, ils peuvent être utilisés pour le monitoring des états de santé des patients... [AKY 02].

Dans le domaine de la sécurité civile, ils sont utilisés pour la détection des attaques biologiques, chimiques, nucléaires; comme dans la surveillance des grandes surfaces commerciales... [6].

Dans le domaine de l'environnement, ils peuvent être utilisés pour le monitoring des changements au niveau des forêts, des océans, des activités sismiques ...

Dans le domaine de la domotique (« home automation »), et avec la norme IEEE 802.15.4, il est possible que les appareils électroniques équipés de capteurs puissent communiquer entre-eux. A titre d'exemple, l'utilisateur pourra configurer son réseau domestique de façon que l'intensité de la lumière diminue dès que le poste de télévision commence à fonctionner, ou le poste de télévision se met en mode silencieux dès que le téléphone commence à sonner... [ZHE 04].

II-5. L'architecture d'un nœud capteur

II-5-1. Architecture matérielle

La principale tâche d'un nœud capteur dans un RCSF est de détecter, traiter et transmettre des données.

Un nœud capteur est un ensemble de quatre composants essentiels [AKY 02] qui sont:

- L'unité de capture ou « *sensing unit* » : elle se compose du capteur et du convertisseur analogique/numérique (ADC). En effet, le signal analogique produit par le capteur suite à un phénomène observé va être transformé par l'ADC en un signal numérique.
- L'unité de traitement ou « *processing unit* » : elle est composée d'un processeur (microcontrôleur) et d'une unité de stockage de faible taille. Elle permet au nœud la gestion des procédures de collaboration avec les autres nœuds dans le but d'accomplir la tâche demandée.
- L'unité émettrice-réceptrice ou « *transceiver unit* » : elle permet de connecter le nœud à l'ensemble du réseau. Grâce à cette unité, le nœud pourra émettre et recevoir des messages des autres nœuds.
- L'unité d'énergie ou « *power unit* » : elle constitue la source d'énergie du nœud capteur. Elle peut être associée ou alimentée par une unité génératrice d'énergie comme les cellules solaires.

Il existe des applications dont les besoins nécessitent d'autres composants qui s'ajoutent à ceux décrits précédemment, comme :

- Le système de localisation pour déterminer la position des nœuds.
- Le mobilisateur ou « *mobilizer* » pour déplacer un nœud d'un lieu à un autre.

Le schéma suivant illustre l'architecture matérielle d'un nœud capteur :

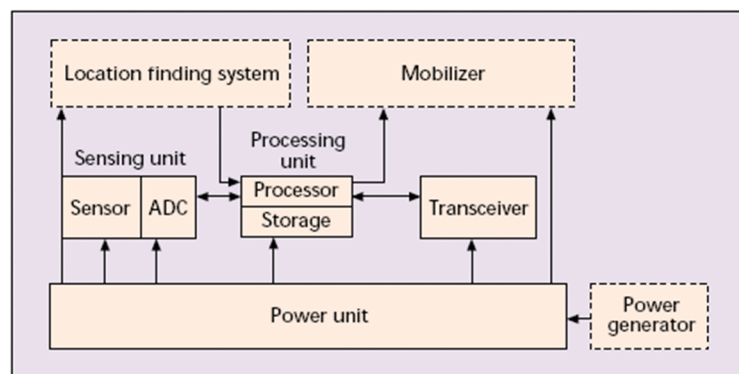


Figure 2.3 : L'architecture matérielle d'un nœud capteur [AKY 02]

II-5-2. Architecture logicielle

L'un des systèmes d'exploitation les plus connus dans le domaine des RCSF est « TinyOS ». Il est libre et est utilisé par une large communauté de scientifiques dans des simulations pour le développement et le test des algorithmes et protocoles réseau.

II-6. La pile protocolaire des RCSF

Cette pile se compose de :

- Une couche physique
- Une couche de liaison de données
- Une couche réseau
- Une couche transport
- Une couche application
- Un plan de gestion d'énergie
- Un plan de gestion de mobilité
- Un plan de gestion de tâches

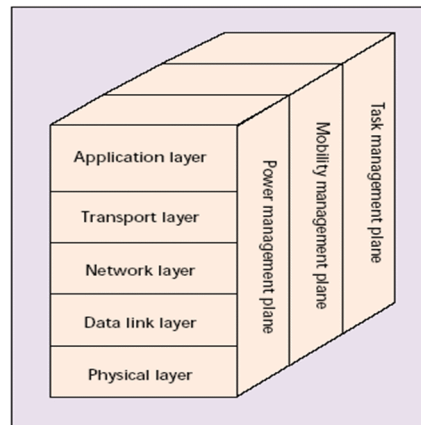


Figure 2.4 : La pile protocolaire des RCSF [AKY 02]

II-6-1. La couche physique

Elle est responsable de la sélection de fréquence, la génération de la fréquence porteuse, la détection du signal, la modulation/démodulation et le cryptage/décryptage des informations.

La consommation d'énergie au niveau de la couche physique peut être affectée par l'environnement de l'application, le choix du type de la modulation ou la bande de fréquence utilisée.

Il est avantageux en matière d'économie d'énergie que le concepteur de la couche physique choisisse une transmission à multi-sauts plutôt qu'une transmission directe qui nécessite une puissance de transmission très élevée [AKY 02].

II-6-2. La couche liaison de données

Elle est responsable de la détection des trames de données, le contrôle d'accès au support (MAC) et le contrôle d'erreurs. Elle maintient aussi la fiabilité des liaisons point à point ou multipoints dans les RCSF.

La couche liaison de données contient deux sous-couches qui sont :

- ***La sous-couche MAC*** : Dans un réseau RCSF, la couche MAC doit accomplir deux principales tâches qui sont celles de :

- établir des liaisons de communication entre les nœuds capteurs pour effectuer le transfert des données et permettre au réseau la capacité de s'auto-organiser.

- décider du moment et de la manière dont les nœuds capteurs peuvent accéder au canal avec un minimum de perte d'énergie [AKY 02].

- **La sous-couche de contrôle d'erreurs** : La technique de contrôle d'erreurs la plus utilisée dans les réseaux RCSF est le « *Forward error correction* » (FEC) ; Cette technique comporte de simples mécanismes de codage et de décodage (codes de contrôle d'erreurs simples) [AKY 02].

II-6-3. La couche réseau

La couche réseau gère les échanges (et éventuellement les connexions) au travers du RCSF.

Elle gère entre autre l'adressage et l'acheminement des données.

Les applications des réseaux RCSF requièrent le plus souvent des protocoles de routage à multi-sauts entre le nœud émetteur, le ou les nœuds relais et le nœud puits.

Les protocoles de routage traditionnels des réseaux ad hoc ne peuvent pas être utilisés dans les réseaux RCSF puisqu'ils ne satisfont pas les critères de conservation d'énergie et de scalabilité [LWA 04].

Les métriques considérées par les chercheurs pour déterminer la route la plus optimisée dans les réseaux RCSF sont :

- L'énergie nécessaire pour transmettre le paquet d'une manière fiable.
- L'énergie disponible dans chaque nœud capteur.

Les algorithmes de routage peuvent alors sélectionner les routes entre le nœud émetteur et le nœud puits en se basant soit sur le maximum d'énergie disponible au niveau des nœuds intermédiaires, soit sur la route qui consomme le moins d'énergie pour transmettre d'un nœud vers un autre. [AKY 02]

Le type d'adressage le plus utilisé dans les RCSF est l'adressage géographique, c'est-à-dire que chaque nœud capteur est identifié dans le réseau par sa localisation. D'ailleurs, l'adressage géographique est employé surtout dans les applications de monitoring (« *environmental monitoring* »...) [HOL 03].

II-6-4. La couche transport

Le rôle de cette couche intervient essentiellement lorsqu'on va accéder à partir de notre RCSF vers un autre RCSF ou vers Internet.

Le protocole de transport utilisé entre le nœud émetteur et le nœud puits peut être UDP. Il importe de mentionner que l'utilisation du protocole TCP est impossible vu la taille limitée des mémoires des nœuds capteurs qui ne leur permet pas d'enregistrer de grandes quantités d'informations pour la gestion des communications (mécanismes de fenêtres).

Les communications entre l'utilisateur et le nœud puits peuvent être gérées par TCP ou UDP via Internet ou satellite.

II-6-5. La couche application

Il existe plusieurs protocoles applicatifs qui ont été proposés. Parmi lesquels on peut citer le SMP (Sensor Management Protocol) qui permet à l'utilisateur d'exécuter des tâches administratives telles que la configuration du RCSF, la mise en marche/fermeture des nœuds, la synchronisation entre les nœuds, le déplacement des nœuds capteurs...

En plus du protocole SMP, on trouve SQDDP (Sensor Query and Data Dissemination Protocol) qui permet à l'utilisateur à travers des interfaces d'interroger le réseau en se basant non pas sur un système d'adressage particulier (interroger un nœud bien particulier) comme tel est le cas des réseaux sans fil classiques mais plutôt sur la localisation des nœuds [AKY 02].

II-6-6. Le plan de gestion d'énergie

Il gère la manière dont le nœud utilise son énergie. Par exemple, si le nœud capteur est faible en énergie, il pourra informer ses nœuds voisins par multicast qu'il ne pourra pas participer dans le routage des paquets [AKY 02].

II-6-7. Le plan de gestion de la mobilité

Il détecte les mouvements des nœuds et indique leurs placements. De cette manière, chaque nœud peut connaître les nœuds qui lui sont voisins (il pourra alors balancer ses tâches vers un autre nœud au cas où il manque d'énergie). Il doit aussi maintenir à n'importe quel instant la route séparant le nœud mobile du nœud puits [AKY 02].

II-6-8. Le plan de gestion des tâches

Il assure un ordonnancement des tâches de capture dans une région bien déterminée tout en évitant la redondance des tâches de capture à un même instant, et ceci dans le but d'économiser de l'énergie sur le réseau [AKY 02].

L'intérêt de ces trois plans réside dans le fait qu'ils assurent une gestion optimale de la consommation d'énergie, de la mobilité et des tâches au niveau de chaque nœud capteur.

Conclusion

Dans ce chapitre, nous avons donné une vue d'ensemble des catégories des réseaux sans fil ainsi que leurs principales spécificités et on a vu qu'ils possèdent des caractéristiques particulières qui les différencient des autres types de réseaux sans fil. Ces spécificités telles que la consommation d'énergie réduite, la scalabilité ou le routage incitent le besoin de concevoir de nouveaux protocoles d'accès au support, de routage, de transport ou d'application, qui s'adapteront aux caractéristiques des RCSF.

Dans ce qui suit, nous allons aborder les techniques d'accès utilisées dans les réseaux sans fil classiques, et nous donnerons ensuite une description de quelques protocoles MAC proposés dans les RCSF.

Chapitre 2 :

L'accès au support dans les réseaux sans fil

Introduction

Dans ce chapitre, nous aborderons les techniques d'accès utilisées dans les réseaux sans fil classiques. Nous donnerons ensuite une description de quelques protocoles MAC proposés dans les RCSF ; Enfin, nous brosserons une étude comparative des protocoles susmentionnés, fondée sur les critères d'allocation du canal, de notification, de gestion d'énergie et de QoS.

I- Première partie : Les techniques de contrôle d'accès dans les réseaux sans fil classiques

Un défi important dans les réseaux sans fil est la gestion des collisions dues à un transfert de données simultanée entre deux nœuds sur le même support.

Les protocoles de contrôle d'accès au support (MAC) ont été développés essentiellement pour essayer d'éviter ce genre de collisions en aidant les nœuds à décider quand et comment ils peuvent accéder au support.

A ce propos, nous allons essayer de dégager les diverses techniques d'accès au médium dans les réseaux sans fil qui sont :

- TDMA (Time Division Multiple Access).
- FDMA (Frequency Division Multiple Access).
- CDMA (Code Division Multiple Access).
- CSMA (Carrier Sense Multiple Access).

I-1. L'accès multiple par répartition temporelle (TDMA)

Cette technique est basée sur un multiplexage temporel (cas de la téléphonie) qui consiste à dire que les utilisateurs utilisent la même fréquence tout en occupant des slots de temps différents. Chaque nœud utilise toute la bande passante allouée par le système de transmission durant le slot (c'est lui seul qui occupe le support).

L'analyse énergétique de la technique TDMA :

Le fait que chaque nœud connaît d'avance le slot de temps qu'il va occuper, va lui permettre de passer à l'état « endormi » durant les slots inactifs. Ainsi, la perte d'énergie qui est due aux états de « sur-écoute » (Overhearing) et « écoute passive » (Idle) va être évitée.

Toutefois, le système TDMA demande un maintien constant des horloges de synchronisation à travers le réseau car une erreur introduite dans l'une des horloges peut entraîner des collisions ;

La station de base doit en effet, émettre périodiquement des paquets de synchronisation aux différents nœuds qui doivent impérativement les intercepter pour mettre à jour leurs horloges.

Cette réinitialisation de l'horloge effectuée à chaque fois par le nœud consomme une quantité considérable d'énergie malgré que le nœud ne transmette pas d'informations.

I-2. L'accès multiple par répartition fréquentielle (FDMA)

La technique FDMA est basée sur un multiplexage fréquentiel cela signifie que le spectre est divisé en canaux fréquentiels (ou bandes de fréquence). Chaque canal fréquentiel est affecté à un seul utilisateur.

La bande passante est partagée entre les différents canaux auxquels sont affectés les nœuds.

Dans un système FDMA pur, tous les utilisateurs peuvent transmettre leurs signaux simultanément.

L'analyse énergétique de la technique FDMA :

La technique FDMA élimine en fait le temps d'attente (dû à la réinitialisation de l'horloge de synchronisation) nécessaire au nœud avant qu'il puisse accéder au support (cas du TDMA) étant donné que dans un tel système, les nœuds peuvent communiquer simultanément.

Cette élimination du temps d'attente entraîne une sauvegarde d'énergie.

Les collisions sont minimisées puisque chaque nœud occupe sa propre bande de fréquence.

Cependant, en partageant la bande passante totale sur plusieurs nœuds, chaque nœud va avoir une assez étroite bande passante ce qui entraîne un temps de transmission élevé d'où l'augmentation de la consommation d'énergie.

I-3. L'accès multiple par répartition de codes (CDMA)

La technique CDMA (utilisé dans la norme IS95) est basée sur la technique du spectre étalé obtenu au moyen d'un code aléatoire unique à chaque utilisateur.

L'Analyse énergétique de la technique CDMA :

Dans un système CDMA, le nœud émetteur émet ses données à travers le canal de transmission en utilisant son code unique. Le nœud récepteur va alors regrouper les données reçues et essayer d'extraire seulement les données provenant du nœud émetteur.

Ce type d'échange peut réduire la bande passante du canal de transmission (Exemple : A émet à B 5Mbits de données, la ligne est à 1Mbits/s, il lui faut normalement 5s. On suppose qu'il y a 15Mbits de données émises par d'autres nœuds. Le canal transporte alors 20Mbits en total, il nous faudra alors un temps =20s) d'où l'augmentation du temps de transmission qui entraîne une augmentation de la consommation d'énergie.

I-4. L'accès multiple avec écoute de la porteuse/Evitement de collision (CSMA/CA)

Contrairement aux techniques TDMA, FDMA et CDMA qui sont des techniques « programmées d'avance » [YE 03] et dans lesquelles les nœuds sont assignés à des canaux partitionnés (temps, fréquence, code) pour éviter les collisions, CSMA/CA constitue une technique aléatoire dans laquelle chaque nœud doit rester à l'écoute du médium avant de transmettre ses données.

En effet, les terminaux d'un même BSS (groupe de terminaux munis d'une carte d'interface réseau 802.11 et interconnectés entre eux) peuvent écouter l'activité de toutes les stations qui s'y trouvent. Lorsqu'une station envoie une trame, les autres stations l'entendent et, pour éviter les collisions, mettent à jour un « Timer », appelé NAV permettant de retarder toutes les transmissions prévues. Le NAV est calculé par rapport à l'information située dans le champ durée de vie, ou TTL contenu dans les trames qui ont été envoyées. Les autres stations n'ont la capacité de transmettre qu'après la fin du NAV [PUJ 05].

L'analyse énergétique de la technique CSMA/CA :

L'utilisation de CSMA/CA oblige les nœuds d'être éveillés pour l'écoute du médium ce qui accroît leur consommation d'énergie. En outre, si on utilise cette technique dans un réseau à haute densité de nœuds comme les RCSF, on peut accroître le risque de collisions dans ce réseau,

provoquer la perte des données transmises et engendrer d'avantage de consommation d'énergie lors de la retransmission.

II- Deuxième partie : Les protocoles MAC proposés pour les RCSF

II-1. Les raisons d'adoption de nouveaux protocoles MAC pour les RCSF

Les caractéristiques des RCSF qu'on a décrites précédemment, ainsi que les techniques d'accès MAC utilisées dans les réseaux sans fils classiques et qui sont non adaptées aux besoins des applications des RCSF, ont poussé la communauté des chercheurs à proposer de nouveaux protocoles MAC spécifiques aux réseaux.

En effet, l'objectif essentiel du protocole MAC dans un réseau cellulaire est de fournir une bonne qualité de service avec une bande passante efficace. Cependant, l'économie d'énergie dans un tel réseau ne constitue pas une contrainte importante prise en compte par le protocole MAC étant donné que l'utilisateur peut recharger les batteries de son combiné lorsqu'il le voudra.

Pour le cas de Bluetooth, il adopte une topologie en étoile dans laquelle un nœud « maître » interagit avec sept nœuds « esclave » pour former un « pic-réseau ». La technique d'accès utilisée par chaque « pico-réseau » est TDMA. La puissance de transmission est de l'ordre de 20dBm et la portée de transmission est de l'ordre d'une dizaine de mètres [AKY 02].

Contrairement à ces systèmes sans fils, le RCSF possède un nombre plus grand de nœuds, la puissance de transmission est de l'ordre du 0dBm, la portée des transmissions est très inférieure à celle de Bluetooth et l'économie d'énergie constitue l'objectif primordial des RCSF.

Toutes ces caractéristiques nous mènent à déduire que les protocoles MAC de Bluetooth, de MANET ou du GSM ne peuvent pas être utilisés directement par les RCSF.

La question qui se pose alors est la suivante :

Quelles doivent être les caractéristiques d'un protocole MAC convenable aux RCSF ?

II-2. Les caractéristiques d'un protocole MAC convenable aux RCSF

Afin de concevoir le protocole MAC le mieux adapté aux spécificités des RCSF, on doit prendre en considération les propriétés suivantes [DEM 03] :

- **L'optimisation d'énergie** : cette propriété est la plus importante de toutes dans le cas des RCSF. En effet, le fait qu'il est difficile de changer ou de recharger les batteries des nœuds, constitue un vrai handicap qui limite leur durée de vie.

Comme la couche MAC contrôle les activités de la couche radio qui à son tour consomme le plus d'énergie, alors on peut déduire que la couche MAC peut gérer cette consommation en essayant d'empêcher les pertes de cette énergie.

- **L'évitement des collisions** : Cette caractéristique constitue la mission principale de tous les protocoles MAC qu'ils s'agissent des réseaux filaires ou des réseaux sans fil.

- **L'adaptation au changement** : Les RCSF sont des réseaux dynamiques au niveau de leur taille, leur densité ou leur topologie ; Alors dans ce cas, un protocole MAC efficace doit gérer rigoureusement ces changements sans qu'il y ait un dysfonctionnement du réseau.

- **Le rendement (Throughput)** : c'est la quantité de données transmises avec succès entre un émetteur et un récepteur dans un temps bien déterminé. Il constitue une caractéristique assez importante dans le cas des applications qui requièrent un bon rendement.

- **L'équité (Fairness)** : Elle reflète la capacité des nœuds capteurs à partager le canal d'une façon équitable. Dans le cas des RCSF, cette propriété n'est pas prise en considération puisque tous les nœuds collaborent ensemble, indépendamment de la quantité d'informations émises par les différents nœuds, afin de remplir une tâche commune.

Cette propriété reste cependant très importante dans les réseaux sans fil classiques du fait que chaque nœud désire avoir la même chance que les autres nœuds pour l'émission ou la réception des données.

- **Le temps d'attente ou latence** : C'est le délai entre l'instant d'émission d'un message et l'instant de sa réception avec succès. L'importance de cette caractéristique est dépendante du type d'application.

Pendant que les protocoles MAC classiques sont conçus de telle sorte qu'ils maximisent le rendement, minimisent la latence et assure une égalité des chances de transmission (l'équité). La conception du protocole MAC des RCSF se focalise essentiellement sur la minimisation de la consommation d'énergie [VAN 03].

La question qui se pose alors est la suivante: Comment est consommée l'énergie au niveau de la couche MAC dans les RCSF ?

II-3. La consommation d'énergie au niveau de la couche MAC dans les RCSF

On essayera dans ce qui suit d'analyser les raisons de perte d'énergie au niveau de la couche MAC dans les RCSF [Ye 03]:

- **Les collisions** : dans le cas d'une collision entre 2 ou plusieurs paquets, ces derniers vont être rejetés et par conséquent retransmis par leurs émetteurs. Cette retransmission va augmenter la consommation d'énergie des nœuds capteurs émetteurs.

- **Le phénomène d'« idle-listening » ou écoute passive** : Elle apparaît quand le nœud reste à l'écoute du médium pour recevoir des données possibles. Elle est très coûteuse en énergie notamment dans le cas des applications qui ne nécessitent pas pratiquement un grand échange de données.

Le coût de la consommation d'énergie dans les communications de type radio dépend à la fois du matériel d'émission/réception et de la distance. En effet, si cette distance est grande, (Cas des WLAN, WWAN) le coût de consommation dû à l'écoute et à la réception est négligeable comparativement à celui dû à la transmission.

Cependant, dans les RCSF là où la distance est petite, le coût de consommation d'énergie dû à l'écoute passive est presque du même ordre de grandeur que celui dû à la réception et à l'émission [Ye 03].

- **Le phénomène d'« Overhearing » ou « Sur-écoute »** : cela signifie que le nœud reçoit des paquets qui sont normalement destinés à d'autres nœuds. Ce phénomène peut constituer une cause importante de perte d'énergie dans le cas d'une zone à forte densité avec un trafic assez volumineux.

- **Le phénomène d'« overemitting » ou « Sur-émission »** : il est causé par la transmission d'un message vers un nœud qui n'est pas encore prêt à recevoir des données.

La synthèse de cette partie nous amène à déduire que pour les RCSF qui se caractérisent généralement par leur forte densité et leur trafic non important, le phénomène d'« idle listening » ou écoute passive constitue la cause principale de la perte d'énergie dans les nœuds capteurs.

II-4. Le protocole Sensor-MAC

Sensor-MAC est un protocole MAC spécialement conçu pour les RCSF. L'objectif majeur de ce protocole est de réduire les pertes d'énergie dues aux causes que l'on a identifiées précédemment.

Il supporte les quatre mécanismes suivants :

- Les états périodiques "actif" et "endormi"
- L'évitement de collision
- L'évitement du phénomène de « sur-écoute »
- Le "Message passing".

II-4-1. Les séquences d'états périodiques "actif" et "endormi"

D'après notre analyse sur la consommation d'énergie au niveau de la couche MAC dans les RCSF, nous avons constaté que l'écoute passive constitue la cause principale de perte d'énergie.

L'idée apportée par Sensor-MAC pour limiter au maximum cette écoute passive est d'entraîner les nœuds dans un état endormi périodique [HEI 02] en se basant sur un « duty-cycle » fixe (égale au rapport de la durée de la période « actif » sur la somme des périodes « actif » et « endormi »).

En effet, chaque nœud s'endort pendant un laps de temps puis se réveille et se met à l'écoute pour voir s'il y a un autre nœud voulant initier une communication avec lui ou s'il veut lui-même

initier une communication. Durant l'état endormi, le nœud éteint sa « radio » et déclenche un temporisateur pour son réveil plus tard.



Figure 3.1 : Principe des états périodiques “actif” et “endormi” [HEI 02]

La durée des états « actif » et « endormi » varie d'une application à une autre.

Chaque nœud est libre de choisir sa propre séquence d'état « actif/endormi ». Toutefois, pour réduire le temps d'attente, chaque nœud doit synchroniser sa séquence d'états « actif/endormi » avec les nœuds qui lui sont proches [Ye 03].

Avant que chaque nœud ne commence une séquence d'états périodiques, il doit d'abord choisir sa propre séquence et l'échanger avec ses voisins ; Il doit maintenir alors une table de séquences qui enregistre les séquences des nœuds voisins.

Afin de choisir sa propre séquence et établir la table des séquences, chaque nœud doit suivre les étapes suivantes :

- Le nœud commence par écouter le support, s'il n'intercepte aucune séquence d'un nœud voisin alors il va choisir immédiatement sa propre séquence et va l'émettre dans un paquet SYNC vers tous les nœuds voisins.
- Si un nœud A reçoit une séquence d'un nœud voisin B et annonce sa propre séquence, alors A doit adopter la séquence de B. Une fois la séquence a été choisie, le nœud A doit émettre cette séquence vers les nœuds voisins [Ye 03].

Si un nœud A reçoit une séquence, d'un nœud voisin B, différente de la sienne. Deux cas peuvent se produire :

- Si A n'admet que B comme voisin alors A doit détruire sa propre séquence et suivre la séquence de B.
- Si A admet un ou plusieurs voisins avec lesquels il a déjà échangé une séquence, alors A doit adopter à la fois sa propre séquence et la séquence de B. Ainsi, le nœud A sera réveillé pendant les intervalles « actif » des deux séquences [HEI 02].

II-4-2. L'évitement de collision

Si plusieurs nœuds voisins veulent communiquer avec le même nœud en même temps, ils vont essayer d'émettre leurs données quand ce nœud entamera sa période « actif ». Cette opération va entraîner une collision de leurs requêtes.

Le principe d'évitement de collision dans Sensor-MAC est le même que celui utilisé dans DCF (Distributed Coordinated Function) pour le cas de IEEE 802.11 qui utilise l'échange de RTS/CTS et l'écoute virtuel/physique de la porteuse.

En effet, dans chaque paquet transmis, il existe un champ qui indique le temps de transmission restant. Dans ce cas, si un nœud reçoit un paquet destiné à autrui, il va connaître grâce à ce champs, le temps qu'il restera silencieux. Il enregistrera cette valeur dans son compteur NAV et déclenchera un temporisateur. Le NAV sera alors décrémenté jusqu'à ce qu'il atteigne la valeur zéro.

Si cette valeur diffère de zéro alors le nœud conclura que le support est occupé. Cette opération est dite écoute virtuelle de la porteuse [HEI 02].

II-4-3. L'évitement du phénomène d'Overhearing

Etant donné que les RCSF sont caractérisés par leur forte densité, alors il est évident qu'un nœud reçoit de ses nœuds voisins des paquets qui ne lui sont pas destinés.

Le phénomène d' « Overhearing » peut entraîner une importante perte d'énergie, surtout lorsque le trafic est très chargé.

Sensor-MAC essaie de remédier à cet inconvénient en entraînant les nœuds voisins dans une phase « endormi » juste après qu'ils « sur-entendent » un paquet RTS ou CTS.

Dans la figure suivante, les nœuds A, B, C, D, E et F forment un réseau à multi-saut dans lequel chaque nœud ne peut entendre que les nœuds qui lui sont immédiatement voisins.

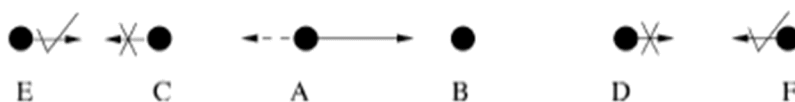


Figure 3.2 : L'évitement du phénomène d'Overhearing [HEI 02].

On suppose que A est entrain d'émettre un paquet DATA à B, quels sont alors les nœuds qui doivent s'endormir durant cette transmission ?

Comme les collisions ne se passent qu'au niveau du récepteur, alors le nœud D doit s'endormir puisqu'une transmission émanant de lui peut interférer avec le paquet reçu par B à partir de A.

Les nœuds E et F ne produisent pas d'interférence donc ils n'ont pas besoin de s'endormir.

Concernant le nœud C qui est à deux sauts de B, il peut transmettre vers E et A sans se soucier d'une interférence avec la transmission reçue par B. Cependant, C ne doit pas recevoir de requête émanant de E car une telle requête va entrer en collision avec celle (paquet DATA) émanant de A vers C. En plus, après que A finit son émission vers B, il va attendre l'acquittement (ACK) de B. A ce moment, une transmission de C vers A peut entrer en collision avec l'ACK de B.

⇒ C doit s'endormir car ses transmissions n'ont aucun effet [HEI 02].

Pour récapituler, les nœuds immédiatement voisins à l'émetteur et au récepteur doivent s'endormir dès qu'ils entendent un paquet RTS ou CTS respectivement de l'émetteur ou du récepteur. Ils ne pourront émettre des données que lors de leur prochain état « actif » avec un compteur NAV à 0.

II-4-4. Le « Message Passing »

La transmission d'un long message en un seul paquet peut coûter beaucoup d'énergie à son émetteur car, en cas où des erreurs surviennent lors de cette transmission, l'émetteur doit retransmettre tout le paquet.

Cependant, dans le cas où on transmet ce long message en plusieurs petits paquets, on aura un retard de transmission important car, les paquets RTS et CTS sont obligatoires pour chaque petit paquet envoyé.

L'approche utilisée dans Sensor-MAC est de fragmenter le long message en de petits fragments qui seront transmis ensemble en utilisant un seul RTS et un seul CTS grâce auxquels le support va être réservé pendant toute la transmission de ces fragments.

Chaque petit fragment envoyé par l'émetteur doit être acquitté par le récepteur. Dans le cas échéant, l'émetteur doit réémettre ce petit fragment non acquitté, et augmenter le temps de transmission.

Les paquets RTS et CTS contiennent chacun un champ qui indique le temps nécessaire pour transmettre les petits fragments de données et les paquets ACK.

Ainsi, dans le cas où un nœud voisin entend un paquet RTS ou CTS, il connaîtra automatiquement la période durant laquelle il restera endormi. Cette période n'est autre que le temps nécessaire pour transmettre les petits fragments de données et les paquets ACK.

Ce mécanisme de « Message Passing » constitue donc une source d'économie d'énergie au niveau des nœuds capteurs [HEI 02].

II-5. Le protocole TimeOut-MAC

La description de ce protocole est basée sur un article publié par Tijs Van DAM et al. [VAN 03].

Le protocole TimeOut-MAC est un protocole qui a été conçu afin de remédier aux faiblesses du protocole Sensor-MAC en matière de charge de trafic variable.

L'idée que le protocole TimeOut-MAC a apportée est de réduire le phénomène d'écoute passive en rendant le « duty-cycle » (cyclique) variable et dépendant du volume du trafic, contrairement au protocole Sensor-MAC qui adopte un cyclique fixe.

II-5-1. Fonctionnement de Timeout-MAC

Chaque nœud se réveille périodiquement pour communiquer avec ses voisins puis retourne à son état endormi jusqu'au début de la prochaine séquence. Entre temps, les messages destinés à leur récepteur seront stockés dans son « buffer ».

Pendant la période « active », un nœud reste à l'écoute du support et pourrait potentiellement transmettre des paquets durant cette période.

La période « active » se termine quand il n'y a plus aucun événement de réception de message pendant une durée TA (Timeout Activity) qui détermine la durée d'écoute par séquence actif/endormi. Par conséquent, la période active est adaptée à la charge du trafic.

Les nœuds communiquent entre eux en utilisant les paquets RTS, CTS, DATA et ACK

La figure suivante illustre le fonctionnement de TimeOut-MAC qu'on a décrit précédemment :

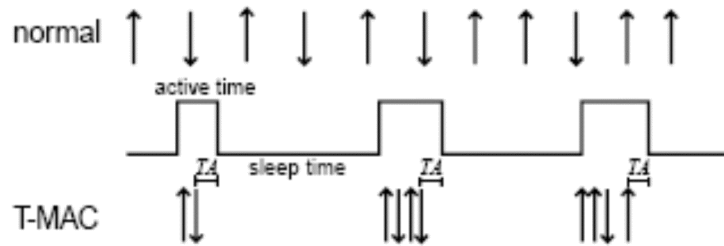


Figure 3.3 : le fonctionnement du protocole TimeOut-MAC [VAN 03]

II-5-2. La Synchronisation entre les nœuds

La synchronisation des séquences s'est inspirée de la méthode décrite dans le protocole Sensor-MAC.

Le schéma de synchronisation décrit avec Sensor-MAC et adapté par TimeOut-MAC pousse les nœuds à former des clusters de telle sorte que chaque cluster est décrit par une séquence d'états. Ceci permet une communication efficace entre les nœuds et évite un maintien d'informations pour chaque nœud.

II-5-3. Détermination de TA (Timeout-Activity)

Un nœud ne doit pas s'endormir pendant que ses voisins communiquent puisqu'il peut être à tout moment le récepteur d'un message.

Du fait qu'un nœud C peut ne pas entendre, en raison de la portée limitée d'émission, un paquet RTS émis par un nœud A, l'intervalle TA doit être suffisamment large pour que C puisse recevoir au minimum la date de l'émission du paquet CTS (entre la réception d'un paquet et la date de son émission, il y a une différence du fait que le récepteur est à l'écoute du support).

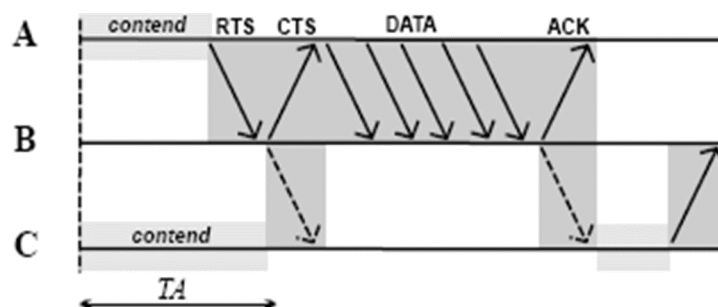


Figure 3.4 : Choix du paramètre TA dans le protocole Timeout-MAC [VAN 03]

Le fait de choisir un intervalle TA très large peut avoir des conséquences négatives puisque l'augmentation du TA implique une augmentation de la phase d'écoute passive donc une augmentation de la consommation d'énergie.

II-5-4. L'évitement du phénomène d'Overhearing

Le protocole TimeOut-MAC quant à lui, considère l'évitement de la « sur-écoute » comme une option dont il peut ne pas tenir compte du fait qu'il peut perturber les communications entre les nœuds dans le cas d'applications qui requièrent le maximum de rendement. En effet, pendant la période où le nœud A va entrer en phase « endormi », il peut manquer la réception de paquets RTS ou CTS destinés vers lui et va donc perturber les communications avec autrui lors de son réveil. Par conséquent, le rendement va diminuer.

II-6. Le protocole Wise-MAC

Wise-MAC utilise la technique de « Preamble Sampling » (prise d'échantillons préliminaires) pour minimiser la perte d'énergie due à l'écoute passive.

La technique de prise d'échantillons préliminaires consiste à écouter le canal périodiquement pendant des périodes assez courtes pour vérifier s'il y a une activité sur le canal.

Si le canal est occupé, le récepteur continue son écoute périodique dans l'attente d'un paquet qui lui est destiné ou jusqu'à ce que le canal retourne à son état libre [DEC 03].

Au niveau de l'émetteur, un préambule est transmis avant chaque message pour s'assurer que le récepteur sera à un état « actif » lorsque le message va lui arriver.

Ce préambule va consommer de l'énergie que ce soit au niveau de l'émetteur ou du récepteur alors que le transfert de données n'a pas encore commencé [DEC 03].

Afin de remédier à cette perte d'énergie, Wise-MAC offre une méthode qui permet de déterminer dynamiquement la longueur de ce préambule de telle sorte qu'il soit le plus petit possible. Cette méthode consiste à connaître les séquences « endormi » des voisins directs de l'émetteur.

En connaissant ainsi la séquence « endormi » du destinataire, l'émetteur va émettre son préambule pendant une période minimum T_p juste avant que le récepteur débute sa nouvelle période d'écoute [DEM 03].

La figure suivante montre et explique le fonctionnement de base du protocole Wise-MAC :

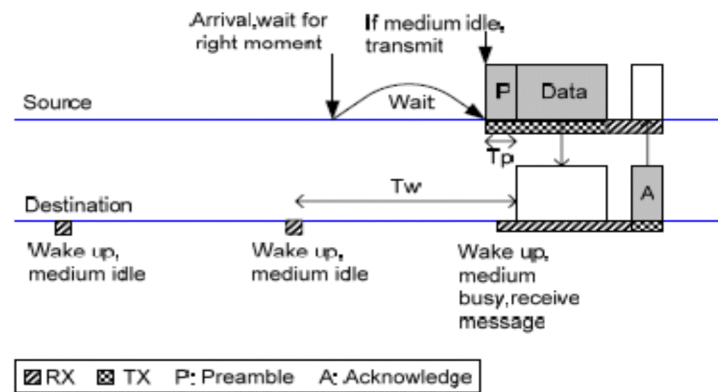


Figure 3.5 : Le fonctionnement de base du protocole Wise-MAC [HOI 04]

Chaque nœud maintient une table contenant les séquences « endormi » des voisins directs, qui sera lue et mise à jour par le nœud lui-même et ceci grâce au paquet ACK qui lui est renvoyé et qui non seulement acquitte son envoi mais aussi contient la durée restante au récepteur pour débiter son prochain écoute [HOI 04].

II-7. Le protocole TRAMA (Traffic-adaptive medium access protocol)

La description de ce protocole figure dans un article publié par Rajendran V. et al [RAJ 03].

TRAMA a été conçu dans le but de réduire la consommation d'énergie dans les RSCF.

Il se base sur une approche TDMA qui consiste à partager le temps en plusieurs slots qui ne seront alloués qu'aux nœuds qui ont des informations à transmettre ce qui diminue le temps d'attente des autres nœuds.

II-7.1- Fonctionnement du protocole TRAMA

TRAMA utilise un algorithme d'élection distribué basé sur l'état du trafic au niveau de chaque nœud. Cet algorithme, qui sera traité par la suite, permet de sélectionner les récepteurs potentiels selon les plannings annoncés par les émetteurs.

Les nœuds utilisant le protocole TRAMA échangent les plannings de transmission (spécifiant les récepteurs potentiels des messages à émettre, dans un ordre chronologique ainsi que des informations sur le trafic à émettre) ainsi que des informations sur leur voisinage, avec leurs homologues situés à deux sauts d'eux.

Grâce à ses informations échangées, le protocole TRAMA va déterminer les nœuds susceptibles d'émettre ou de recevoir des données durant chaque slot de temps.

La figure suivante illustre l'organisation des slots de temps dans le protocole TRAMA :

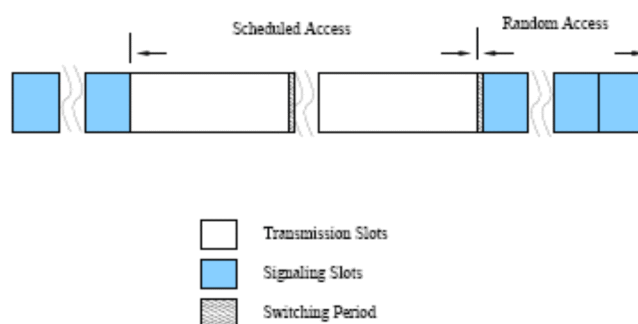


Figure 3.6 : Organisation des slots de temps dans le protocole TRAMA [RAJ 03]

D'après cette figure, on remarque qu'il existe deux types d'accès au support en fonction des slots de temps :

- Un accès aléatoire (possibilité de collision) lors des slots de temps destinés à la signalisation.
- Un accès déterministe (pas de collision) lors des slots de temps destinés à la transmission.

Le protocole TRAMA se décompose de trois composants :

- Le protocole voisin ou Neighbor Protocol (NP).
- Le protocole d'échange de planning ou Schedule Exchange Protocol (SEP).
- L'algorithme d'élection adaptée ou Adaptive Election Algorithm (AEA).

Les deux premiers protocoles NP et SEP permettent à un nœud d'échanger des informations sur son voisinage ainsi que son planning avec ses voisins situés à deux sauts de lui.

Quant à l'algorithme AEA, il utilise les informations échangées afin de sélectionner les émetteurs et les récepteurs pour le slot de temps courant, et permet aux autres nœuds d'entrer ainsi en mode basse consommation.

II-8. Le protocole Léger-MAC (LMAC)

La description de ce protocole est basée sur un article publié par Van Hoesel L. et al. [HOE04].

Le protocole LMAC est basé sur la technique TDMA. Le temps est divisé en des slots de temps qui peuvent être utilisés par les nœuds pour transmettre des données sans avoir à écouter le canal. A chaque slot de temps, LMAC assigne un nœud qui sera le contrôleur de ce slot de temps.

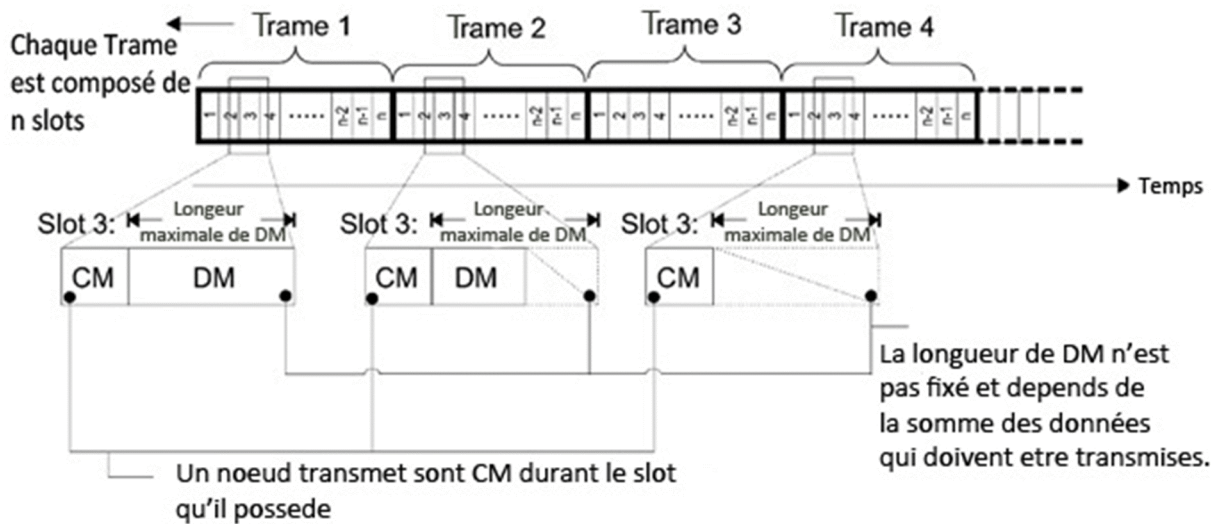


Illustration des frames et les slots dans LMAC

Le temps dans LMAC est divisé en trames, dont chacune est divisée en un nombre fixe de slots de temps. Chaque nœud choisit son propre slot en utilisant un algorithme distribué qui utilise les informations disponible localement. Un nœud est autorisé à choisir n'importe quel emplacement tant qu'elle n'est pas détenue par un autre nœud dans son voisinage à deux sauts. Ce mécanisme permet effectivement d'éviter le problème du nœud caché (hidden-terminal), car elle rend impossible pour les deux nœuds qui sont à deux sauts l'un de l'autre de transmettre des données en même temps. Elle empêche également tous les slots d'être utilisés, (puisque LMAC assure que deux nœuds qui sont au moins trois sauts les uns des autres de réutiliser le même intervalle de temps).

Un slot de temps est constitué de deux sections, le message de contrôle (CM) et le message de données (DM). Le CM contient des informations de commande et dispose d'une partie de

longueur fixe. Il est diffusé par un nœud à ses voisins pendant son slot de temps, une fois que chaque trame possède des données à envoyer. Le CM contient une table qui identifie les emplacements qui sont occupés par lui-même et par ses voisins d'un seul saut ainsi que d'autres informations de contrôle. Chaque nœud maintient une table des voisins qui stocke les informations sur ses voisins à un seul saut, comme Identification (ID), slot occupé, nombre de sauts, et ainsi de suite. Les emplacements occupés sont marqué avec un 1, alors que celles inoccupées sont marquées avec un 0. Un nœud joignant le réseau, écoute d'abord le CMS de tous ses voisins, puis choisit un des slots qui est marqué comme étant inoccupés, en effectuant une opération OU. (Ce mécanisme sera illustré dans une section du chapitre qui suit).

II-8-1. L'évitement de collision

Afin d'éviter les collisions, les nœuds maintiennent des tables contenant les identifiants des slots alloués aux nœuds situés dans un périmètre de trois sauts.

Il existe une possibilité (probabilité faible) du même choix du slot de temps entre deux ou plusieurs nœuds. Dans ce cas, les nœuds informent leurs voisins qu'une collision entre les messages de contrôle a eu lieu.

Les nœuds qui ont émis ces messages de contrôle vont alors stopper leur contrôle aux slots utilisés et rechoisir aléatoirement d'autres slots (à part ceux qui ont été choisis) après un temps de recule dépendant de l'identifiant (ID) du nœud.

III- Troisième partie : Etude comparative de quelques protocoles MAC proposés dans les RCSF

III-1. Les critères de comparaison

Pour réaliser cette étude comparative, nous nous sommes basés sur les quatre critères suivants :

- L'allocation du canal radio.
- La notification
- La gestion d'énergie
- La qualité de service.

III-1-1. L'allocation du canal radio

Dans les communications radio fréquence, s'il existe plus qu'un nœud qui veut transmettre des données sur le même canal et en même temps, alors des problèmes de communication tels que les collisions ou la distorsion, peuvent surgir.

Afin d'éviter de tels problèmes, une partie de la bande passante est allouée à chaque nœud.

Cette allocation peut être soit statique, soit dynamique :

- ***Allocation statique*** : cette technique d'allocation divise la bande passante en N parties. Chaque partie est allouée à un nœud. Les techniques de multiplexage utilisées pour diviser la bande passante ont été décrites dans la première partie de ce chapitre et sont : TDMA, FDMA et CDMA.

En général, les protocoles MAC dans les RCSF, qui emploient une allocation statique du canal, utilisent la technique TDMA du fait que FDMA et CDMA ne rencontrent pas les contraintes de consommation d'énergie imposées dans les nœuds capteurs. Cette technique requiert une synchronisation entre les nœuds afin de permettre à chaque nœud d'identifier ses slots de temps.

La synchronisation dans le cas des RCSF est de type distribué où chaque nœud ou groupe de nœuds génère sa propre séquence d'états qui sera ajusté périodiquement.

La synchronisation centralisée n'est pas applicable dans les RCSF car ce genre de réseau souffre d'un temps d'attente élevé et une perte de paquets assez fréquente.

Donc, dans le cas d'un retard ou d'une perte du signal de synchronisation, le réseau sera perturbé.

- ***Allocation dynamique*** : Dans cette technique d'allocation, il n'existe pas de bande passante allouée d'une manière prédéfinie pour chaque nœud. Tout nœud voulant accéder au canal doit gagner la contention. Avec ce type d'allocation, il existe une forte probabilité de collision.

III-1-2. La notification

Afin de réussir la communication entre émetteur et récepteur, ce dernier doit être à l'écoute du canal au moment où la transmission commence. Ainsi, il sera notifié de l'existence d'une transmission sur le canal. Cette notification peut être classée en deux types :

- ***Par réservation*** : Ce type de notification est utilisé par les protocoles basés sur une allocation statique du canal, là où les nœuds possèdent des slots prédéterminés pour l'émission ou la réception. Léger-MAC est un exemple de protocole qui emploie ce type de notification.

- ***Par écoute du canal***: Dans les protocoles utilisant une allocation dynamique du canal, il n'existe pas de slots prédéterminés pour émettre ou recevoir des données.

Un nœud peut être toujours à l'écoute du canal en attente de recevoir une transmission qui lui est destinée. Malgré que cette méthode d'écoute puisse augmenter les chances de réception du message, cette méthode est trop coûteuse en énergie.

Afin d'éviter de telles pertes, les nœuds changent périodiquement d'états « endormi » et « actif ». L'écoute du canal peut être synchrone ou asynchrone :

- ***Synchrone*** : la séquence d'états « actif/endormi » est déterminé par un échange de messages de synchronisation. Chaque nœud connaît quand est-ce que ces nœuds voisins sont à l'état actif. Ainsi, le nœud émetteur attend jusqu'à ce que le récepteur entre en état actif pour lui transmettre son message.

Sensor-MAC et TimeOut-MAC sont des protocoles qui emploient une écoute synchrone du canal.

- ***Asynchrone*** : Les nœuds ne connaissent pas quand est-ce que leurs voisins sont actifs. Ils se mettent alors périodiquement à l'écoute du canal pour vérifier s'il y a une transmission qui va avoir lieu. Cette méthode est connue sous le nom de « prise d'échantillons préliminaires ». Wise-MAC utilise ce type d'écoute du canal.

III-1-4. La qualité de service

Contrairement aux réseaux classiques là où les composantes de base de la qualité de service sont la bande passante, l'équité et le temps d'attente. Ces composantes sont, pour la majorité des protocoles MAC proposés pour les RCSF (à l'exception du protocole MAC de la norme IEEE 802.15.4), sacrifiées aux dépens de l'optimisation de la consommation d'énergie des nœuds capteurs.

Cela ne veut pas dire que la qualité de service n'est pas tenue en compte dans ce type de réseau, sauf qu'elle est dépendante essentiellement du type d'application qui tourne au niveau du RCSF. En effet, les concepteurs de Sensor-MAC, Time-Out MAC ou Wise-MAC avaient pour premier objectif, la réduction de consommation d'énergie pour maximiser la durée de vie du réseau ce qui convenait avec les applications qu'ils utilisaient (militaire...).

Cependant, et pour le cas du protocole MAC de la norme IEEE 802.15.4 (norme utilisée à des fins d'applications pour le grand public), la bande passante et le temps d'attente par exemple sont des paramètres de qualité de service fortement tenus en compte.

III-2. Le tableau comparatif

Le tableau suivant illustre une classification des protocoles MAC proposés pour les RCSF, selon les quatre critères qu'on a décrit précédemment (L'allocation du canal radio, La notification, La gestion d'énergie, La qualité de service).

L'accès au support dans les réseaux sans fil

Notification	Avantages	Inconvénients	Qualité de Service
<p>Écoute synchrone du canal</p>	<p>- protocole économique en consommation d'énergie grâce aux séquences périodiques « endormi ».</p>	<p>- Les périodes « endormi » et « actif » sont prédéfinies à l'avance, ce qui limite l'efficacité de l'algorithme Sensor-MAC dans le cas d'une charge de trafic variable => un faible rendement en cas de forte charge de trafic.</p> <p>- Les paquets de données de type « Broadcast » n'utilisent ni RTS, ni CTS ce qui augmentent la probabilité de collision dans ce genre de transmission.</p> <p>- Problème du sommeil anticipé : Le nœud s'endort avant la réception des données qui lui sont destinées. => Le temps d'attente devient important. En plus, il s'accumule à chaque fois qu'on passe d'un saut à un autre.</p>	<p>Absente</p>
<p>Écoute synchrone du canal</p>	<p>- protocole économique en consommation d'énergie grâce aux séquences périodiques « endormi ».</p> <p>- Les périodes « endormi » et « actif » sont déterminés en fonction du trafic : TimeOut-MAC ajuste sa consommation d'énergie,</p> <p>dans le contexte d'un trafic</p>	<p>- Problème du sommeil anticipé.</p>	<p>Absente</p>

L'accès au support dans les réseaux sans fil

	variable, grâce au Time-Out Timer (TA). => Adaptation au trafic.		
Écoute asynchrone du canal	- L'ajustement dynamique de la longueur du préambule (de telle sorte qu'il soit le plus petit possible) permet des économies de consommation d'énergie.	- L'utilisation de préambule « Wake-up » va consommer de l'énergie (Overhead) que ce soit au niveau de l'émetteur ou du récepteur alors que le transfert de données n'a pas encore commencé.	Absente
Par réservation	- Protocole basé sur la technique TDMA => probabilité de collision faible.	- Lors du choix aléatoire du slot de temps, il y a une chance que deux ou plusieurs nœuds choisissent le même slot. A ce moment, ils doivent supprimer leurs premiers choix et rechoisir une deuxième fois ce qui consomme plus d'énergie. - Les nœuds doivent être toujours à l'écoute lors des sections de contrôles.	Absente
Par réservation	- protocole basé sur la technique TDMA => probabilité de collision faible. - Les nœuds qui n'ont pas à	- Pour chaque slot de temps, le nœud calcule les priorités de ses nœuds voisins situés jusqu'au deuxième saut.	Absente

L'accès au support dans les réseaux sans fil

transmettre ou à recevoir des données vont fermer leurs « radio » et entrer en mode «endormi». => Pas de période d'écoute passive => Gain d'énergie.	=> traitement interne élevé au niveau du capteur => consommation d'énergie élevée.	
---	--	--

Le tableau comparatif des protocoles MAC proposés pour les RCSF

Conclusion :

Dans ce chapitre, nous avons essayé de faire une synthèse de quelques protocoles MAC proposés dans les RCSF. Cette synthèse a été clôturée par une étude comparative qui nous a permis d'avoir une vision globale regroupant leurs principales caractéristiques, leurs avantages et inconvénients.

Dans ce qui suit, nous allons présenter un algorithme d'ordonnancement complètement distribué et prouver que cet algorithme possède des propriétés d'auto-stabilisation, Nous allons illustrer en suite comment il est capable de s'adapter rapidement aux changements de topologie ; Enfin essayer de présenter des estimations de performances théoriques majorants pour les performances de celui ci.

Chapitre 3 : Système d'Ordonnancement Distribué et Auto-Organisé

I. Introduction

Dans ce chapitre, nous présentons un algorithme d'ordonnancement complètement distribué. Nous montrons également que cet algorithme possède des propriétés d'auto-stabilisation. Nous illustrons ensuite comment il est capable de s'adapter rapidement aux changements de topologie ; Enfin, nous présentons des estimations de performances théoriques de cet algorithme.

II. Hypothèses

Sur la base de notre scénario d'application, nous avons fait quelques hypothèses sur les données qui seront recueillies, et sur le réseau lui-même. Tout d'abord, comme il y aura un grand nombre de nœuds (~ 100) et, comme il peut être nécessaire d'obtenir des mesures à une fréquence élevée, on peut s'attendre qu'une grande quantité de données circule à travers le réseau. Compte tenu de la bande passante limitée et la capacité de mémoire de nœuds capteurs individuels, en supposant que les nœuds transmettent des données via un arbre de diffusion vers le nœud puits, les nœuds qui sont plus proche du nœud puits seront sujets à des débordements de tampon. Cela se traduira par la perte de messages, ce qui réduira considérablement la qualité des données collectées. Puis on peut s'attendre à ce que des mesures entre nœuds voisins soient corrélées au cours de la majeure partie de la journée. Nous supposons que la topologie du réseau est relativement statique. Cependant, nous devons prendre en considération le fait que la topologie du réseau peut changer de temps en temps puisque les nœuds sont sujets à l'échec (par exemple, en raison de l'environnement hostile ou à des piles mortes), ou des nouveaux nœuds peuvent être ajoutés pour étendre le réseau.

III. Motivation et Mise au point

Profitant des corrélations des nœuds entre nœuds voisins dans l'espace permettraient de filtrer les données redondantes, ce qui à son tour, contribuerait à réduire des problèmes telles que l'utilisation excessive d'énergie, les dépassements de tampon, et une réduction de la qualité de données. Plutôt que de transmettre chaque mesure de nœud vers le nœud puits, un nœud qui découvre une corrélation avec ses nœuds voisins, ne transmet que les données de corrélation, suivie de ses propres mesures. Ainsi, le nœud récepteur peut alors prévoir les valeurs des nœuds voisins en utilisant les données de corrélation et les mesures transmises à partir du nœud lui-même. Ceci est illustré dans la Figure 4(b).

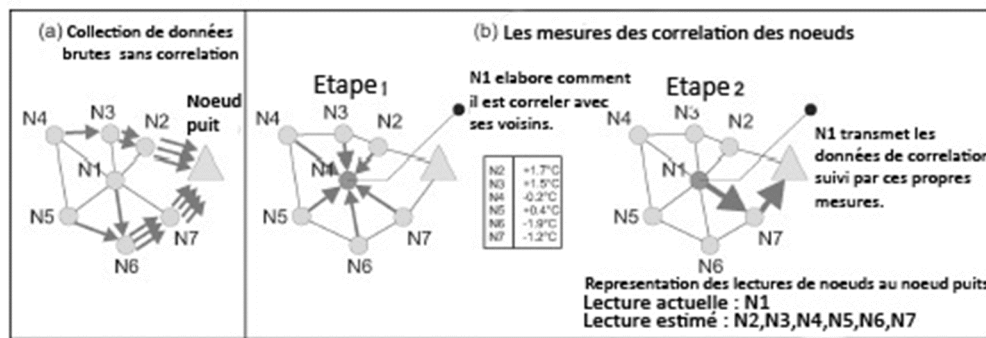


Fig. 4. Avantage de l'utilisation des données de corrélation (b) au lieu de transmettre les données brutes (a).

L'approche qui consiste à tirer parti des corrélations spatiales et temporelles des mesures du capteur comporte deux aspects qui doivent être abordés:

Identifier des corrélations et maintenir à jour des informations de corrélation. Il est important de noter que la corrélation n'est pas un attribut statique. Une corrélation entre deux capteurs voisins peut exister seulement à certains moments de la journée. Ainsi, un nœud doit être en mesure de déterminer si une corrélation peut se poser, et elle a aussi besoin de faire en sorte que les données de corrélation dont il dispose sont mises à jour. Naturellement, si les tendances des mesures de capteurs changent très rapidement, un tel système entraînerait une surcharge très importante qui dépasserait le coût de la collecte des données brutes à partir du réseau à cause de fréquentes mises à jour de l'information de corrélation. Cependant, les mesures préliminaires obtenues ont montré que des changements brusques dans les tendances de mesures du capteur ne sont pas particulièrement communs. En fait, pendant la majeure partie de la journée, les capteurs placés géographiquement proches les uns des autres ont tendance à afficher un comportement similaire. L'approche utilisée n'est pas conçue pour des applications où les corrélations fluctuent

rapidement. Ainsi, il ne serait pas sensé que tous les nœuds envoient des informations de corrélation au nœud puits simultanément car cela impliquerait l'envoi de plus d'informations que même la transmission brute mesure. Quand un nœud est le transmetteur de données de corrélation, les nœuds voisins devraient s'abstenir de le faire. Cela implique que tous les nœuds de transmission sont représentés au nœud puits par leurs propres mesures, leurs voisins sont représentés par les mesures qui sont estimés sur la base de données de corrélation transmis par les nœuds de corrélation. Ainsi, deux nœuds voisins ne doivent pas agir en tant que nœuds de corrélation au même temps. En outre, il est important de s'assurer qu'à tout moment, chaque nœud du réseau est représenté au niveau du nœud puits soit par une lecture réelle ou estimée par une mesure. Cela signifie que si un nœud n'est pas un nœud de corrélation à un moment donné, il doit être connecté à au moins un nœud de corrélation voisin.

Avoir un schéma d'ordonnancement statique qui fixe les nœuds de corrélation pour toute la vie du réseau n'est pas souhaitable. C'est parce que, bien qu'il y aurait un certain nombre de nœuds de corrélation envoyant leurs propres mesures en plus de leurs données de corrélation. Ainsi, un tel régime serait sujet à des erreurs dans le cas où le nœud de corrélation échoue pour une raison quelconque et commence à envoyer des informations de corrélation erronée au nœud puits. Ainsi, afin d'avoir un système plus robuste, chaque nœud du réseau doit avoir la possibilité d'être un nœud de corrélation. Cela permettrait au nœud puits de déclencher une alarme au cas où il remarque que les valeurs réelles d'un nœud indiquent une caractéristique très différente par rapport aux valeurs estimées du même nœud. Ceci implique clairement qu'il doit y avoir un schéma d'ordonnancement qui décide quand un certain nœud doit être en charge de l'envoi d'informations au cas où il existe une corrélation.

Le travail que nous présentons dans ce chapitre se concentre sur cette dernière question et présente une distribution et une auto-organisation d'algorithme d'ordonnancement (DOSA), ce qui permet aux nœuds de la grille de se réattribuer de manière autonome si un changement de topologie est détecté, si elle est due à une défaillance ou à un ajout de nœuds.

IV. Un point de vue de l'approche DOSA

Comme nous l'avons mentionné dans la section précédente, l'objectif principal de DOSA est d'aider à décider quand un nœud particulier doit agir en tant qu'un nœud de corrélation et donc être mis en charge de représenter les valeurs des capteurs de son voisinage à 1 saut.

Notez que lorsqu'un nœud est un nœud de corrélation, le nœud transmet d'abord des informations de corrélation vers le nœud puits suivie par sa propre mesure. Aucun des nœuds à 1 saut du nœud de corrélation ne transmet ses données au nœud puits pendant cette période.

Puisque DOSA est destinée à résoudre un problème d'ordonnancement, nous faisons usage d'un algorithme de coloration distribué pour attribuer les ordonnancements des nœuds individuels. Ainsi, d'un point de vue théorie des graphes, il n'ya pas deux nœuds adjacents qui peut servir en tant qu'un nœud de corrélation simultanément, tous les nœuds choisis par DOSA doivent être corrélés pour former un ensemble indépendant. En outre, les nœuds de corrélation à un instant particulier ont besoin de former un ensemble dominant puisque chaque nœud non corrélé doit être associé à au moins un nœud de corrélation par une arête. A noter également que le sous-ensemble de nœuds qui sont à la fois indépendants et dominants est connu comme un ensemble indépendant maximal. Un ensemble indépendant maximal ne peut pas être étendu par l'addition de tous les autres nœuds du graphe.

Ce sont ces exigences qui nous aident à définir les contraintes, plus loin dans la section 6, que DOSA suit afin de s'acquitter de sa tâche prévue. Afin d'accélérer la vitesse à laquelle l'ordonnancement des nœuds sont affectés, DOSA utilise les informations fournies par LMAC, En d'autres termes, au lieu d'avoir à colorer tous les nœuds à partir de zéro, DOSA tire parti des ordonnancements (ou couleurs) déjà attribués par LMAC et construit par la suite sur cette attributions afin de s'assurer que les exigences de DOSA sont remplies. Un autre avantage de cette forme d'optimisation inter couche est que moins de messages doivent être transmis à tous les ordonnancements affecter correctement, car nous utilisons des informations déjà existantes.

V. Les préliminaires d'auto stabilisation

Comme nous illustrons plus tard comment DOSA s'initialise lors du démarrage et comment il est capable de se réorganiser à partir des changements de topologie provoqués par l'ajout ou l'enlèvement de nœuds, nous suivons l'approche auto-stabilisation [Dijkstra, 1974; Dolev 2000] pour formaliser des propriétés d'auto-organisation de l'algorithme.

L'auto-stabilisation permet à un système qui entre dans un état illogique (par exemple, en raison de la survenance des défauts fugitifs) à converger vers un état logique au sein d'un temps fini sans aucune intervention extérieure. Nous présentons maintenant quelques préliminaires de l'auto-stabilisation.

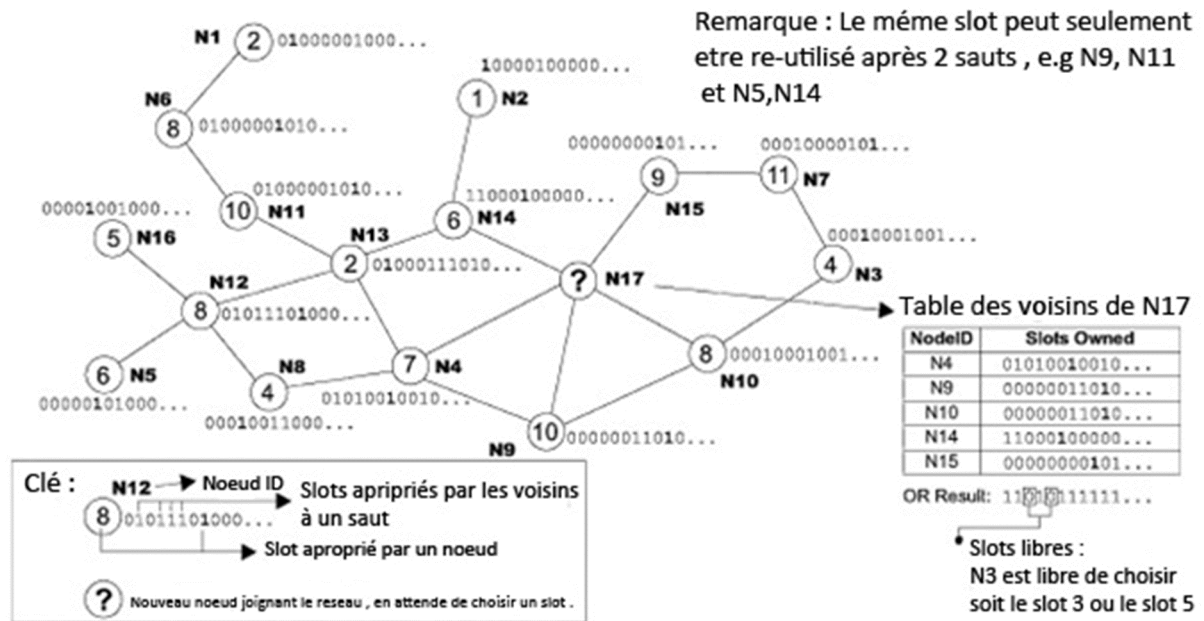


Fig. 6. Fente distribué des ordonnancements de slots dans LMAC.

Tous les nœuds du réseau sont supposés avoir des identifiants uniques et une connaissance de leurs voisins adjacents. Chaque nœud possède un état qui est spécifié par ses variables locales. L'état de l'ensemble du système est appelé « l'état global » ou « configuration » et représente l'union des états locaux de tous les nœuds.

L'objectif du système est d'atteindre un état final global souhaitable appelé un état logique. L'état d'un système peut être logique ou illogique. Nous utilisons **S** pour désigner **l'ensemble de tous les états possibles**.

Afin que le système se rétablisse des fautes transitoires, tous les nœuds affectés exécutent à plusieurs reprises un morceau de code comprenant un ensemble fini de règles ayant la forme **(label) [garde]: <instruction>**; La partie Déclaration de la règle est la description de l'algorithme utilisé pour calculer les nouvelles valeurs pour les variables locales.

Une règle est *activée* lorsque sa protection est vraie. L'exécution d'une règle activée détermine la nouvelle valeur de l'état d'un nœud en utilisant l'algorithme décrit par la partie d'instruction de la règle.

On note **l'ensemble des états logiques** par **L** tel que $L \subseteq S$. On note **l'ensemble de règles** en utilisant **R**, où $R \in S \times S$ tel que $(s_i, s_j) \in R$. Une exécution de e est une séquence maximale d'états, $e = s_i, s_{i+1}, \dots, s_j$ tel que $\forall i \geq 1, s_i \in S$, et s_i est atteint de s_{i-1} par l'exécution d'une règle particulière.

Un système peut être considéré comme un système auto-stabilisé si les deux conditions suivantes sont satisfaites:

-**Fermeture:** Si $s \in L$ et $s \rightarrow \mathbf{s}$ alors $\mathbf{s} \in L$. signifie donc la propriété de fermeture que, lorsque le système est dans un état logique, l'état suivant est toujours un état logique indépendamment de la règle exécutée.

-**Convergence:** A partir de n'importe quelle configuration $s \in S$, chaque exécution atteint L dans un nombre fini de transitions.

Les préliminaires présentés ainsi sont utilisés dans les sections suivantes pour illustrer comment DOSA permet de démarrer correctement et comment il peut également se rétablir lorsque le système rencontre certains défauts.

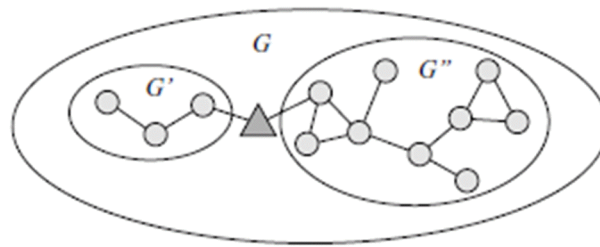


Fig. 7. Deux composantes indépendantes dans G .

VI. DOSA : Algorithme d'Ordonnancement Distribué et Auto-Organisé

DOSA utilise une méthode de coloration de graphe distribué pour décider quand un nœud particulier doit être un nœud de corrélation. Chaque couleur appartenant à un nœud représente une trame particulière de temps pendant laquelle un nœud doit servir en tant qu'un nœud de corrélation. Bien que l'approche de la coloration de graphe de DOSA assure que les nœuds adjacents dans le réseau ne possèdent pas les mêmes couleurs, elle diffère dans le sens où chaque nœud est autorisé à posséder plusieurs couleurs. De plus, le nombre de couleurs utilisées dans DOSA est fixe et il est égal au nombre de slots qui sont affectés à une trame LMAC.

Nous modélisons la topologie du réseau comme un graphe non orienté G , où $G = (V, E)$.

V représente les sommets ou nœuds dans le réseau, tandis que deux nœuds sont connectés par une arête E si elles se sont à portée d'une transmission radio l'un de l'autre. K représente l'ensemble des couleurs utilisées pour colorer tous les nœuds. Ainsi, $|K|$ est égale au nombre de slots par trame dans LMAC. En outre, on note le voisinage fermé d'un nœud $v \in V$ par $\Gamma(v)$:

$$\Gamma(v) = \{u \in V \mid (u, v) \in E\} \cup \{v\}.$$

En d'autres termes, le voisinage fermé de V comprend non seulement son côté voisins, mais aussi le v (nœud) lui-même. En utilisant la distance du domaine mathématique de la théorie des graphes $d_G(u, v)$, qui représente le nombre d'arêtes sur un chemin le plus court entre les sommets u et v , nous pouvons définir le voisinage $r^{\text{ième}}$ de v comme :

$$r(v) := \{u \in V \mid d_G(u, v) \leq r\}.$$

De même, nous définissons le voisinage ouvert d'un nœud v par Γ tel que :

$$\Gamma(v) := \{u \in V \mid (u, v) \in E\}.$$

Nous nous référons à C_v comme l'ensemble des couleurs détenue par le nœud v , Pour C_v il peut facilement être vu que :

$$0 < |C_v| < (|K| - |\Gamma^c(v)|)$$

Étant donné qu'un sous-graphe induit est un sous-ensemble des nœuds d'un graphe G avec arêtes dont les extrémités sont à la fois dans cette partie, nous définissons un composant comme un sous-graphe induit de nœud d'un sous-ensemble de nœuds. Par ailleurs, nous appelons deux composantes indépendantes si elles ne sont pas reliées par une arête. Ainsi, G' et G'' sont deux composantes indépendantes de G . Avant de décrire les détails de l'opération de DOSA, nous posons d'abord les contraintes des exigences énoncées à la section 4, qui définit son comportement. Les deux contraintes suivantes doivent être remplies lorsque deux nœuds u et v sont adjacents:

$$\text{Contrainte 1: } C_v \cap C_u = \emptyset$$

En d'autres termes, deux sommets adjacents ne peuvent pas posséder les mêmes couleurs. C'est parce que deux sommets adjacents ne doivent pas être affectés comme nœuds de corrélation au même temps.

$$\text{Contrainte 2: } C_{\Gamma(v)} = K$$

Toutes les couleurs doivent être présentes dans le voisinage du nœud v à un saut, ainsi, si le nœud v ne possède pas une couleur particulière lui-même, la couleur doit être présente dans un de ses nœuds voisins.

VI.1 Les détails du système de simulation

Afin de faciliter la comparaison, nous présentons les résultats de simulation immédiatement après la description des limites des performances théoriques de DOSA dans chaque paragraphe qui suit. Ainsi, nous parlerons d'abord des détails importants des dispositifs de simulations et ensuite poursuivre dans le reste des sections.

Toutes les simulations sont mises en œuvre dans Matlab [2006]. Les résultats de simulation sont moyennés sur plus de 100 topologies réseaux générés aléatoirement pour une connectivité moyenne des nœuds. Chaque topologie se compose de 100 nœuds répartis au hasard dans une zone de 100x100 de l'unité. La connectivité moyenne a été variée entre 5 et 11 en définissant les différentes distances de transmission pour les nœuds. Les nœuds sont statiques et homogènes dans le sens où ils ont tous les mêmes rayons de transmission. Le nombre de slots par trame dans la mise en œuvre LMAC est de 32.

VI.2 Dépendance de DOSA sur LMAC

Tel que mentionné dans le chapitre précédent, LMAC attribue un slot à chaque nœud du réseau. DOSA commence son système de coloration distribuée en considérant l'affectation initiale de LMAC comme une entrée. L'attribution de slots dans LMAC correspond aux attributions de couleurs partielles dans DOSA. Ainsi, alors que LMAC attribue à chaque nœud une seule couleur, DOSA attribue les couleurs restantes qui assurent le respect des contraintes 1 et 2. On peut alors affirmer que $C_v = C_{v\text{LMAC}} \cup C_{v\text{DOSA}}$ où $C_{v\text{LMAC}}$ se réfère à la couleur correspondante au slot LMAC détenue par le nœud v , et $C_{v\text{DOSA}}$ se réfère aux couleurs attribuées au nœud v par DOSA. De même, les couleurs appartiennent aux nœuds adjacents au nœud v , $(C_{\Gamma(v)})$ sont également composée des couleurs de LMAC et DOSA. Ainsi, nous pouvons affirmer : $C_{\Gamma(v)} = C_{\Gamma(v)\text{LMAC}} \cup C_{\Gamma(v)\text{DOSA}}$.

La dépendance de DOSA sur LMAC permet aux nœuds de s'adapter de manière autonome et immédiate aux changements de topologie du réseau. Par exemple, l'ajout ou la suppression d'un nœud résulte dans le changement qui se reflète dans la prochaine table LMAC.

DOSA détecte les changements dans la table des voisins de LMAC et effectue une réaffectation des ordonnancements si l'un des nœuds voisins ne répondent pas aux contraintes mentionnées ci-dessus.

Nous faisons également l'hypothèse que le degré maximal d'un seul nœud dans le réseau est toujours connu avant le déploiement. Cette information est utilisée pour choisir le nombre

approprié de slots dans une trame dans LMAC. Au cas où, le degré maximal des nœuds ne peut être délimité avec suffisamment de précision, LMAC offre également une fonctionnalité d'exploiter les nœuds passivement, qui est, sans posséder un intervalle de temps, lorsque le réseau devient dense.

Toutefois, pour faciliter la notation et l'argumentation, nous considérons seulement les nœuds actifs qui sont supposés acquérir un emplacement libre dans l'exercice de l'attribution de slots. Ainsi, le bon fonctionnement de LMAC garantit également le bon fonctionnement de DOSA.

VI.3 Fonctionnement général de DOSA

DOSA utilise une approche intéressante à attribuer des couleurs aux nœuds. Le coloriage est effectué en utilisant deux types de couleurs: les couleurs LMAC et les couleurs de DOSA. Les couleurs LMAC se réfèrent aux couleurs qui ont été affectées par LMAC, en raison de la répartition des slots. Les couleurs de DOSA correspondent aux couleurs supplémentaires qui sont affectées par DOSA pour s'assurer que contraintes 1 et 2 sont remplies. Cela se produit après l'attribution des couleurs LMAC.

DOSA n'a pas de contrôle sur la couleur LMAC d'un nœud puisque cela dépend uniquement de l'affectation des ordonnancements effectué par LMAC. En fait, ce contrôle n'est pas nécessaire. Par conséquent, dans ce qui suit, nous nous référons aux couleurs DOSA simplement comme couleurs.

Les couleurs sont acquises sur la base d'une priorité calculée. Un nœud calcule sa priorité dans son voisinage à 1 saut en fonction de son degré et de son ID de nœud. Si deux nœuds voisins ont le même degré, la priorité est calculée sur la base d'un ID unique de nœud, le nœud avec le plus grand ID aura la priorité. Cette priorité calculée est effectuée dans la ligne 4 de l'algorithme 1.

Une fois tous les nœuds ont acquis leurs slots LMAC, un message `BeginSecondPhase` est injecté dans le réseau par le nœud puits, en demandant aux nœuds de commencer la phase de coloration DOSA. A ce stade, tout nœud recevant un message `BeginSecondPhase` ne disposant que d'une couleur LMAC et ainsi ne satisfait pas les contraintes mentionnées précédemment. Ainsi, un seul nœud atteint le statut Satisfait quand il répond au message, un nœud diffuse son message `NodeStatus`.

Ce message contient les informations sur le degré du nœud, son statut (par exemple, satisfait/insatisfait), et la liste des couleurs appropriés. Le champ `ColorsOwned` est une chaîne de bits de $|K|$ où chaque couleur appartenant à un nœud est marqué avec un 1. Le reste des bits sont marqués par un 0. Initialement, un seul nœud marque sa propre couleur de LMAC 1 en raison de

la première attribution de slot LMAC. Un nœud voisin qui reçoit le message NodeStatus effectue la coloration à l'aide de DOSA tel que décrit dans l'algorithme 1. Notez que le message NodeStatus est le seul message qui est utilisé pour l'opération DOSA.

Algorithm 1. *DOSA* - Normal Initialization

Input: NodeStatusMSG(SatisfiedStatus(TRUE/FALSE), ColoursOwned)
Output: NodeStatusMSG(SatisfiedStatus(TRUE), ColoursOwned)/ NIL

```

1: UPDATE(LocalInfoTable, v)
2: if LocalInfoTable contains entries from ALL adjacent nodes then
3:   if SatisfiedStatus(v)=FALSE then
4:     Compute PRIORITY(v)
5:     if PRIORITY(v)=Highest then
6:        $C_v \leftarrow K \setminus C_{\Gamma'(v)}$ 
7:       ColoursOwned  $\leftarrow C_v$ 
8:       SatisfiedStatus  $\leftarrow TRUE$ 
9:       UPDATE(LocalInfoTable, v)
10:      BROADCAST NodeStatusMSG(Degree, SatisfiedStatus, ColoursOwned)
11:    end if
12:  end if
13: end if

```

Algorithme d'initialisation DOSA

Nous décrivons maintenant brièvement le fonctionnement de DOSA tel que décrit dans l'algorithme 1.

Dès la réception d'un message NodeStatus, le nœud met à jour sa LocalInfoTable (Ligne 1). Cette table stocke toutes les informations contenues dans le NodeStatus les messages reçus à partir de tous les nœuds adjacents. Une fois un nœud reçoit Messages NodeStatus de tous ses voisins immédiats (ligne 2), si son statut n'est pas satisfait (ligne 3), le nœud procède à calculer sa priorité. La fonction PRIORITY calcule la priorité d'un seul nœud parmi ses voisins insatisfaits (ligne 4), et doit prendre en compte un plus petit nombre de nœuds voisins. La plus haute priorité est donnée au nœud avec le plus grand degré parmi ses voisins adjacents Insatisfait. Si plus d'un nœud possède le même degré, alors la plus haute priorité est donnée au nœud Insatisfait avec le plus grand NodeID.

Le nœud qui a la priorité la plus élevée parmi tous ses voisins immédiats insatisfaits, acquiert toutes les couleurs qui ne sont pas détenues par l'un de ses voisins adjacents (ligne 7). Puisque le nœud a alors satisfait les deux contraintes de DOSA, il passe à l'état Satisfait, met à jour sa propre LocalInfoTable, et informe tous ses voisins à travers une opération de diffusion (lignes 8-10).

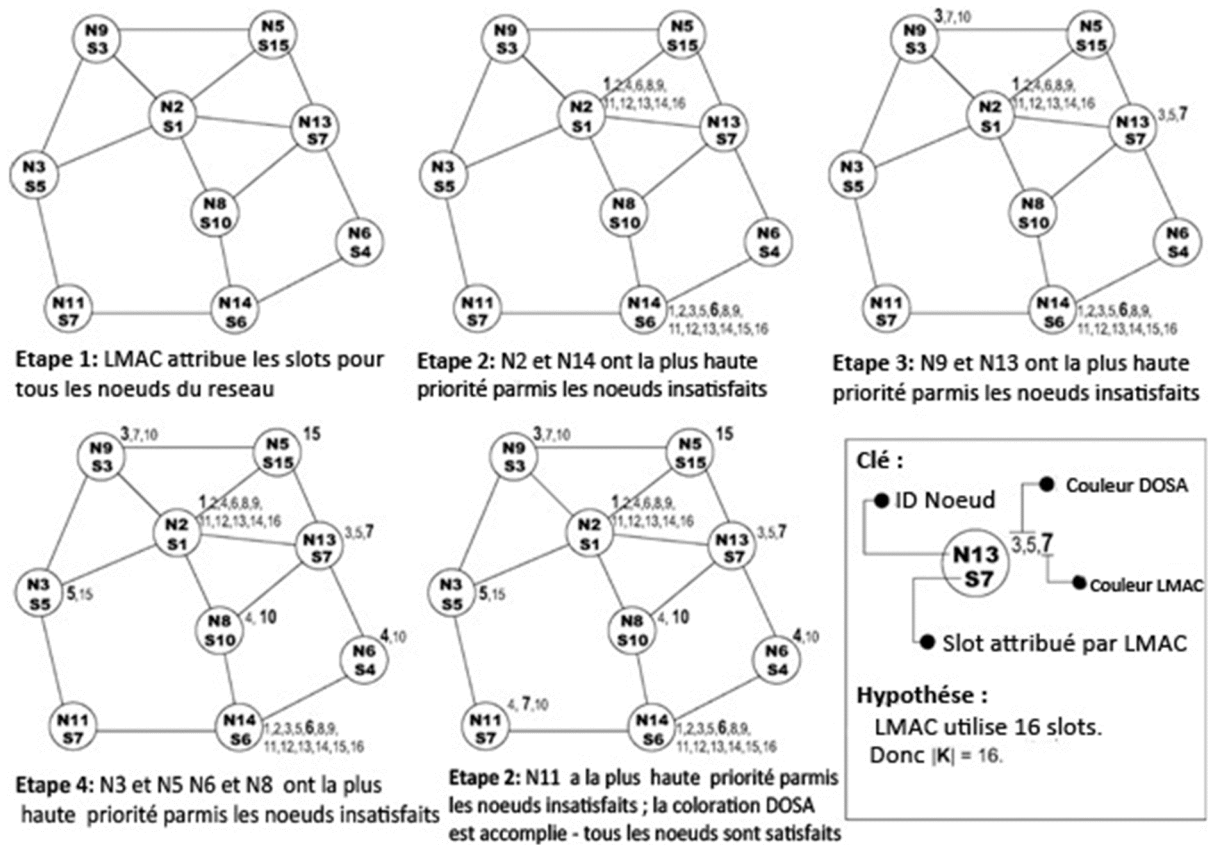


Figure 8 donne un exemple étape par étape comment l'algorithme DOSA assigne couleurs aux nœuds d'un réseau. Nous faisons l'hypothèse que dans l'exemple LMAC utilise 16 slots.

VI.3.1 Exactitude de DOSA

Dans ce qui suit, nous illustrons comment DOSA est capable de mener à bien l'initialisation de n'importe quel réseau choisi dans un temps donné. Nous supposons initialement qu'aucune erreur de transmission ne se produit tout au long de la phase d'initialisation, mais nous décrivons ensuite comment ces questions sont traitées dans la section VI.3.2.

Pour que DOSA fonctionne correctement, il est absolument impératif que chaque nœud ait toujours des informations d'état mises à jour sur ses voisins immédiats. Si un nœud n éprouve un certain changement d'état (par exemple, un changement de Satisfait à Insatisfait) et n'informe pas un voisin adjacent du changement, ce nœud voisin pourrait exécuter certaines mesures inappropriées basé sur son information d'état qui n'est plus à jour pour le nœud n . Cette erreur peut empêcher DOSA de se stabiliser dans un temps fini. Il est donc essentiel pour DOSA de posséder la propriété du cache cohérent [Herman, 2003].

Que chaque nœud $v \in V$ dans le réseau de capteurs a une variable, C_v indique les couleurs détenues par le nœud v . Pour chaque $(u, v) \in E$, u possède une variable $\diamond_u C_v$ qui désigne une version mise en cache de C_v . Nous pouvons appeler un système cache cohérent si $\forall u, v : (u, v) \in E : \diamond_u C_v = C_v$ [Herman, 2003].

Cela signifie que chaque fois que v attribue une valeur à C_v , le nœud v diffuse également la nouvelle valeur à tous ses voisins. Le moment où un nœud u reçoit une valeur actualisée de C_v , il met à jour $\diamond_u C_v$ instantanément et automatiquement.

Si l'on considère le fonctionnement de LMAC seul, la propriété de la cohérence de cache ne tient pas. Prenons le cas où deux nœuds adjacents v et u possèdent les slots i et j respectivement, où $j > i$. Supposons que v diffuse premièrement sa mise à jour d'informations d'états à u durant son propre slot i . Considérons maintenant le cas où l'état de v change de slot q où $i < q < j$. Dans ce cas, v sera incapable de diffuser sa nouvelle mise à jour d'état pour u , puisque le moment où il peut transmettre sera en slot $i + n$ où n est le nombre d'intervalles dans une trame unique, et pour cela, v devrait attendre toute une trame. Ce retard dans la transmission empêche la propriété de cohérence de cache d'exister.

VI.3.2 Manipulation des messages corrompus

Jusqu'à présent, nous avons supposé que toute communication est exempte d'erreurs. Cependant, pour rendre notre analyse réaliste, nous décrivons maintenant les mesures prises par DOSA pour s'assurer qu'il continue à fonctionner normalement même en cas d'erreur de transmission, dues à la mauvaise qualité de la liaison ou des changements de topologie qui se produisent.

Un nœud utilise le champ d'accusé de réception dans la section CM d'un slot dans LMAC pour indiquer si elle a bien reçu un message entrant. Rappelons que, puisque ce domaine se trouve dans la section de CM, chaque nœud transmet une fois par trame. Le nombre de bits dans le champ d'accusé de réception correspond au nombre total de slots utilisés dans une trame. Ainsi, si un nœud n reçoit un message avec succès à partir d'un voisin m particulier de slot i , un 1 est placé dans le i ème bit du champ d'accusé de réception dans la section de CM. De même, un '0' est placé dans le i ème bit si le message entrant reçu dans le slot i devient corrompu. Le nœud m peut

renvoyer le message, s'il constate un 0 dans le ième bit du champ d'acquittement du CM reçu du nœud n .

Formellement, nous affirmons que chaque nœud n utilise une Booléen $b_n(m)$ pour chaque voisin m . Pour passer d'un état G à A dans DOSA, nous pouvons alors affirmer $(\forall m: (n, m) \in E: b_n(m)) \wedge G \rightarrow A$. Si n reçoit un message correctement d'un voisin m , n affecte $b_n(m) = \text{true}$. Si le message est corrompu, $b_n(m) = \text{false}$ pour tout m . Ainsi n bloque l'exécution de DOSA le moment où il reçoit un message corrompu et ne continue à exécuter le programme qu'une fois qu'il a bien reçu les messages de tous les voisins.

En outre, jusqu'à présent, nous n'avons supposé qu'aucun changement de topologie survient au cours du processus d'initialisation. Nous tenons à souligner que cette hypothèse a été faite simplement pour permettre au mécanisme d'initialisation à s'expliquer d'une manière plus simple. Si un changement de topologie se produit, par exemple, un nœud disparaît ou réapparaît, DOSA utilise les algorithmes décrits dans les Sections VII.3 et VII.4 afin de s'assurer que le système continue à fonctionner correctement.

VII. Performance de DOSA

Dans cette section, nous étudions d'abord l'efficacité de DOSA de plusieurs façons. Tout d'abord, nous observons la réduction du nombre de nœuds générant des mesures par rapport la collecte de données brutes. Nous illustrons aussi à travers des simulations, comment cette réduction dans les transmissions de message traduit en une plus grande durée de vie d'un réseau et aussi l'amélioration de la qualité des données. Par la suite, nous décrivons le comportement de DOSA quand un nœud meurt ou quand un nœud est ajouté au réseau.

VII.1 Efficacité de DOSA en termes de génération de messages

L'efficacité de DOSA peut être évaluée en observant le nombre de nœuds de corrélations à tout moment et en la comparant avec le modèle de collecte de données brutes, dans lequel chaque nœud est impliqué dans la transmission de valeurs brutes de capteurs, la figure 10 (a). Considérons deux graphiques dans les figures 10 (b) et (c). Les nœuds noirs représentent les nœuds de corrélation dans les deux graphes à partir des ensembles indépendants maximaux.

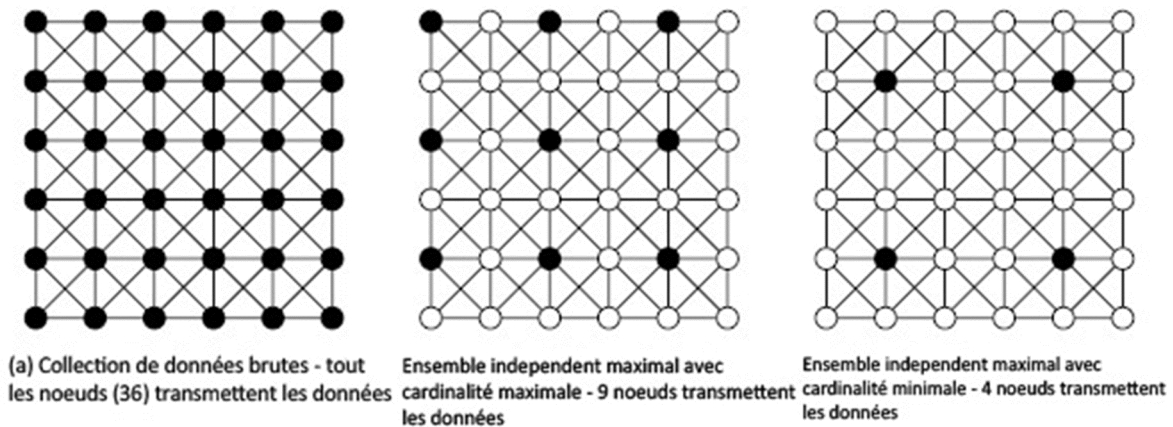


Fig. 10. Impact du cardinal de jeu indépendant maximal.

Néanmoins, on peut voir que le cardinal d'ensemble indépendant maximal peut varier considérablement en fonction de l'ensemble des nœuds choisis. Il en résulte divers degrés d'efficacité énergétique puisqu'un grand cardinal signifie moins d'efficacité par rapport à la collecte de données brutes.

Cela nous donnerait essentiellement une estimation de la performance de DOSA au cas pire.

Lemme VII.1. *Le pire des cas de performance de DOSA peut être garanti à entraîner une réduction de messages d'au moins $(\frac{2nr^2}{xy} - 1) \times 100\%$ par rapport à la collecte données brutes, dans lequel n nœuds sont distribués de manière uniforme dans un espace de dimensions $x \times y$ et chaque nœud dispose d'un rayon de transmission circulaire de r .*

PREUVE. Divisons la zone $x \times y$ en m carrés où,

$$m = \frac{xy}{2r^2} \quad (1)$$

Puisque les nœuds sont supposés être distribués de façon aléatoire, on peut raisonnablement supposer que les nœuds sont présents dans tous les carrés m , Figure 11. Notez que cela entraîne une estimation pessimiste. En outre, nous supposons qu'exactly un nœud dans chaque carré fait partie d'un ensemble indépendant maximal. Nous voyons immédiatement qu'il n'est pas possible d'avoir plus d'un nœud qui fait partie de l'ensemble indépendant maximal dans un seul carré, car ces nœuds supplémentaires seraient à portée du premier nœud choisi. Cela implique par conséquent que le cardinal de l'ensemble indépendant maximal serait m . Il serait impossible d'augmenter la taille plus loin en ajoutant des nœuds. Nous pouvons donc conclure que la

cardinalité maximale de l'ensemble indépendant maximal créé par DOSA est m . Ainsi, le pourcentage de réduction de message de DOSA par rapport à la collecte de données brutes serait, le $n-m/m \times 100$. Cela peut ensuite être simplifié $(\frac{2nr^2}{xy} - 1) \times 100\%$.

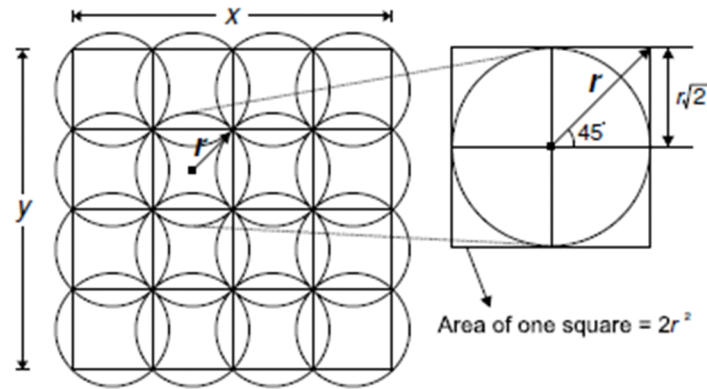


Fig. 11. L'estimation de la cardinalité de l'ensemble maximal maximale indépendant générée par DOSA.

Comme indiqué dans Bulusu et al. [2001], la densité réseau μ peut être définie comme suit :

$$\mu = \frac{n\pi r^2}{xy}. \quad (2)$$

En utilisant les équations 1 et 2, on peut alors affirmer,

$$|I| \leq \frac{n\pi}{2\mu} \quad (3)$$

où I est un ensemble indépendant calculer par DOSA. Nous aimerions cependant indiquer que la densité du réseau est approximativement égale à la connectivité moyenne telle que,

$$\frac{n\pi}{2\mu} \approx \frac{n\pi}{2(\rho-1)} \quad (4)$$

où ρ est la connectivité moyenne. Ce résultat est utilisé pour tracer le graphe de la Figure 12 (b).

Le résultat de simulation présentée dans la figure 12 (a), montre que même pour un grand cardinal, le nombre de nœuds de corrélation n'est jamais supérieur à environ 31%, ce qui se traduit par une réduction du nombre de messages transmis d'environ 69% par rapport à la collecte de données brutes à partir de chaque nœud dans le réseau. Cela est vrai dans le cas où la connectivité moyenne du réseau est très faible. Comme on peut le constater sur la figure 12 (a), le cardinal de l'ensemble indépendant maximal réduit davantage puisque la connectivite moyenne du

réseau est augmenté. C'est assez intuitif car un nœud peut être utilisé pour représenter un plus grand nombre de voisins adjacents étant donné que la connectivité augmente.

La réduction moyenne des transmissions de message dû à DOSA par rapport à la collecte de données brutes, va jusqu'à environ 85% lorsque la connectivité est augmenté à 11.

Le schéma de hiérarchisation utilisé dans DOSA a également un impact important sur l'exécution de l'algorithme. On peut observer deux caractéristiques du fait que DOSA donne la plus haute priorité aux nœuds avec la plus grande connectivité.

Tout d'abord, comme les nœuds qui ont le plus haut degré dans leur voisinage à un saut acquièrent les premières couleurs, le cardinal d'ensemble indépendant maximal tend vers l'indépendant maximal minimum défini.

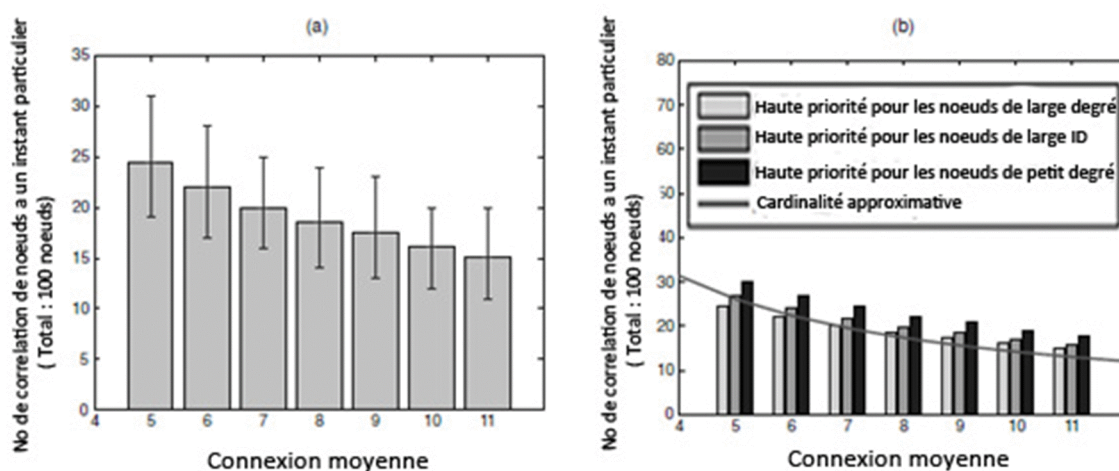


Fig. 12. (a) Impact de la connectivité moyenne sur le nombre de nœuds de corrélation à un instant particulier (nombre total de nœuds dans le réseau = 100), (b) Effet du mécanisme de priorisation sur cardinal d'ensemble indépendant maximal.

Dans la figure 12 (b), nous illustrons les effets de l'utilisation de trois priorités différentes : (1) la priorité absolue donnée au nœud avec le plus grand degré, (2) Plus de priorité accordée au nœud avec le plus grand ID de nœud, et (3) La plus grande priorité accordée à un nœud avec le plus petit degré. En suivant le même raisonnement que dans le schéma (1), le schéma (3) résulte un ensemble indépendant maximal qui a une cardinalité qui est plus près de la cardinalité de l'ensemble indépendant maximal maximale. Néanmoins, le schème (2), en raison de son caractère aléatoire, résulte toujours dans un ensemble indépendant maximal, mais ne tend pas vers la valeur minimale ou la cardinalité maximale. Notez que la différence entre le cardinal estimé et les résultats réels peuvent être attribués à des effets de bord. Il est important de noter cependant que, si l'ensemble indépendant maximal minimum aboutirait à une solution optimale (ie, le plus petit nombre de nœuds de corrélation), et donc semble être le plus efficace en termes d'efficacité d'énergie.

VII.2 Efficacité des DOSA en termes de durée de vie du réseau et la qualité des données

Comme mentionné précédemment, la transmission des valeurs brutes du capteur a un compromettant impact sur la durée de vie du réseau et aussi sur la qualité de données. La réduction dans la génération de message décrit dans le paragraphe précédent conduit naturellement à l'amélioration de ces deux facteurs.

Dans ce paragraphe, nous illustrerons les avantages de DOSA en termes de durée de vie du réseau et la qualité des données d'après les simulations.

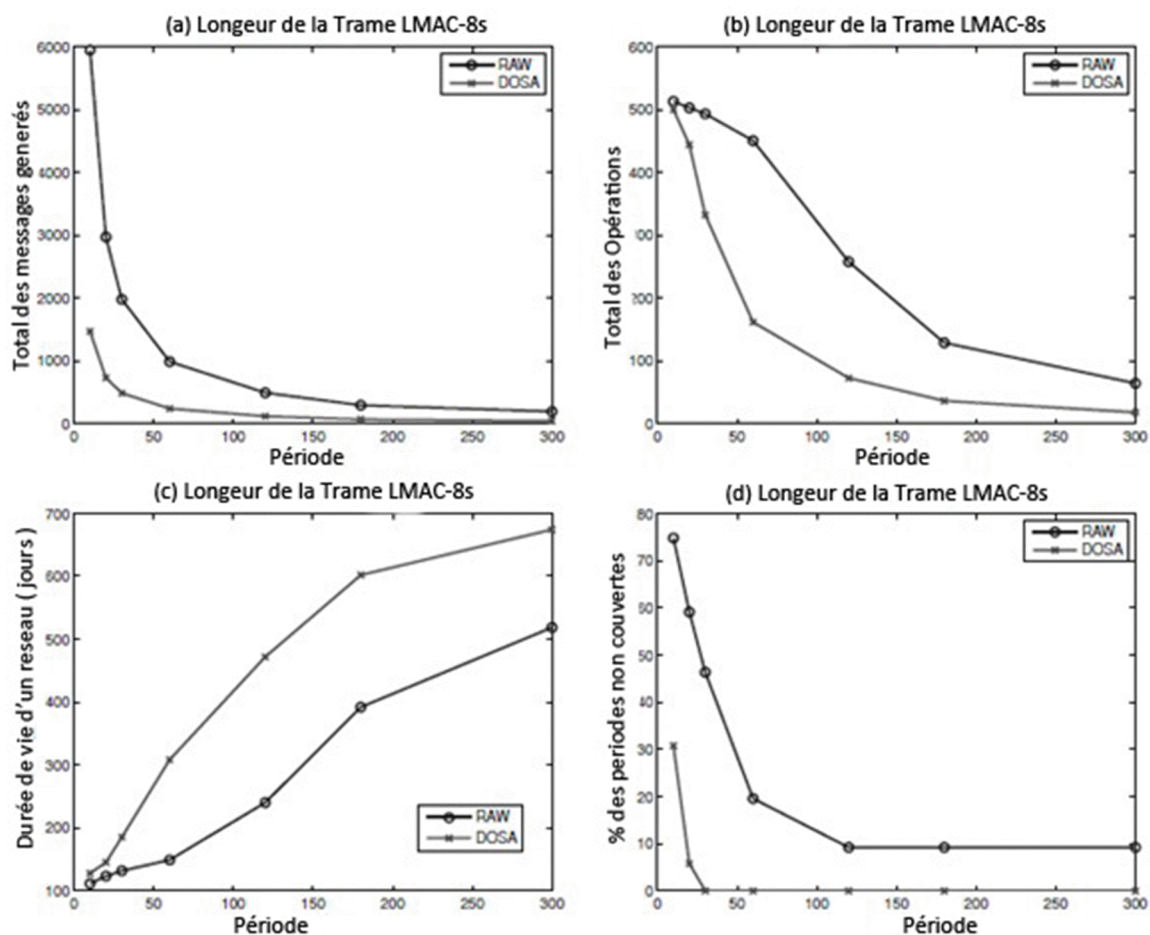


Fig. 13. (a) Nombre total de messages générés, (b) Nombre total d'opérations de transmission, (c) durée de vie du réseau, (d) Pourcentage des périodes découverts.

Notez que nous définissons la durée de vie du réseau comme le temps total pris avant la mort du premier nœud du réseau. Dans les simulations, LMAC utilise une longueur de trame de 8 secondes. Nous supposons que les mesures des nœuds de corrélation restent constantes pendant

cet intervalle. Les mesures pour les différents graphiques ont été recueillies à des époques suivantes (en secondes): 10, 20, 30, 60, 120, 180, 300.

La figure 13 (a) représente le nombre total de mesures de capteur qui sont générés pendant un intervalle de 10 minutes en utilisant les deux techniques de collecte de données. Figure 13 (b) indique le nombre total d'opérations d'émission exécutées par tous les nœuds du réseau pendant toute la durée de la simulation. On peut clairement voir que les figures 13 (a) et 13 (b) n'ont pas de formes similaires. C'est principalement parce que à la fois la collecte des données brutes et DOSA subissent des pertes de messages lourds dû au haut taux d'échantillonnage. Le côté gauche des graphes de la figure 13 (b) tend l'un vers l'autre puisque la limite du débit maximal de LMAC est presque atteinte.

C'est cette même caractéristique qui produit la forme de la durée de vie du réseau graphique de la figure 13 (c). Comme le nombre total de transmissions de messages est presque le même pour les deux méthodes de collecte de données à des taux d'échantillonnage élevé, la durée de vie du réseau est également très similaire. Il peut être vu à partir de la figure 13 (c) que DOSA peut aider la durée de vie du réseau de s'améliorer de près de 83,5% (Période = 120s) par rapport à la collecte de données brutes.

En plus d'aider à améliorer la durée de vie du réseau, DOSA a aussi un important impact positif sur la qualité des données recueillies. Lors de l'analyse de messages abandonnés pour les deux scénarios de collecte de données, il est important de réaliser que chaque message généré par DOSA comporte beaucoup plus de poids qu'un seul message dans le processus de collecte de données brutes. C'est parce qu'une seule lecture de capteur transmis par un nœud n dans DOSA représente non seulement la lecture de n mais aussi ceux de ses voisins immédiats. Pour cette raison, nous analysons la qualité des données, en observant le nombre de périodes qui ne sont pas représentés au nœud puits au lieu de compter le nombre de messages abandonnés. À titre d'exemple, Supposons qu'un message généré par le nœud n représentant sa propre lecture et celle de ses voisins, q , r et s pour la période E est perdu sur le chemin du nœud puits en raison d'un événement de dépassement de capacité de tampon. Cela signifie que pendant la période E , le nœud puits n'aurait aucune valeur des nœuds n , q , r et s . Sur la base de cet exemple, nous présentons les résultats de la qualité des données sur la figure 13 (d). Au taux d'échantillonnage élevé, par exemple, lorsque la période est 10s, la collecte de données brutes en résulte dans environ 75% à période non couvert tandis que le résultat de DOSA en résulte seulement dans 30% à période non couvert. Le pourcentage des périodes non couverts sous DOSA réduit rapidement à 0 et y reste tant que la fréquence d'échantillonnage est réduite. Pour la collecte de

données brutes toutefois, le pourcentage des niveaux de périodes non couverts descendent à environ 10%.

Habituellement, un nœud perd des messages lorsque ses tampons se remplissent. Ainsi, plus le taux d'échantillonnage est élevé, plus la proportion de nœuds dans le réseau éprouve des débordements de tampon. Ceci a naturellement augmenté également le nombre de messages perdus et à son tour le pourcentage de périodes non couvert. Cependant, comme la cadence d'échantillonnage est réduite, le nombre de nœuds connaissent des dépassements de tampon et ne pourrait pas continuer à diminuer jusqu'à zéro. Dans la plupart des topologies, en raison de la production simultanée de messages par tous les nœuds du réseau, il y aura un certain ensemble de nœuds qui seront toujours confrontés aux débordements de tampon et ne cela ne garantira pas qu'un nombre fixe de messages d'arriver avec succès jusqu'au nœud puits. Ainsi, pour des taux d'échantillonnage faibles, à chaque période, seul un nombre fixe de messages atteindra le nœud puits indépendamment de la période choisie.

On peut admettre que les résultats des graphes présentés dans les figures 13 (a) – (d) montrent clairement que DOSA a un avantage seulement pour les applications qui nécessitent un faible taux d'échantillonnage, pourtant ce n'est pas le cas. Pour les applications qui nécessitent un grand taux d'échantillonnage et de débits de données élevées donc, LMAC peut facilement être réglés comme une trame a une longueur de 2 secondes au lieu de 8 secondes. Nous illustrons le résultat de durée de vie du réseau et le pourcentage de périodes non couvert dans les figures 14 (a), et (b). Notez que ces graphes affichent également les mêmes caractéristiques mentionnées précédemment.

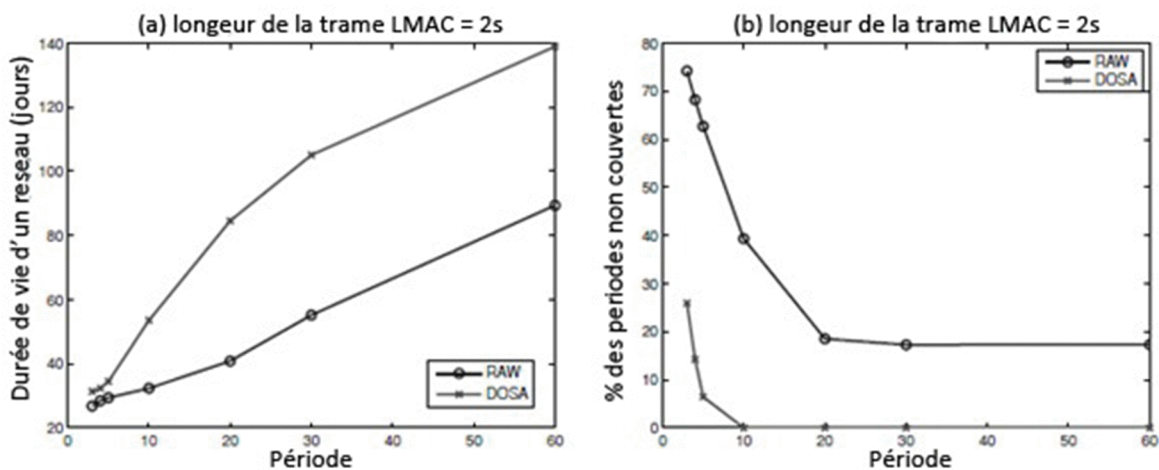


Fig. 14. (a) durée de vie du réseau, (b) Pourcentage des périodes non couverts.

VII.3 Faire face à un nœud mort

Parce que la mort d'un nœud peut être un phénomène courant dans les réseaux de capteurs, il est important que n'importe quel algorithme conçu pour les réseaux de capteurs puisse faire face à de tels événements.

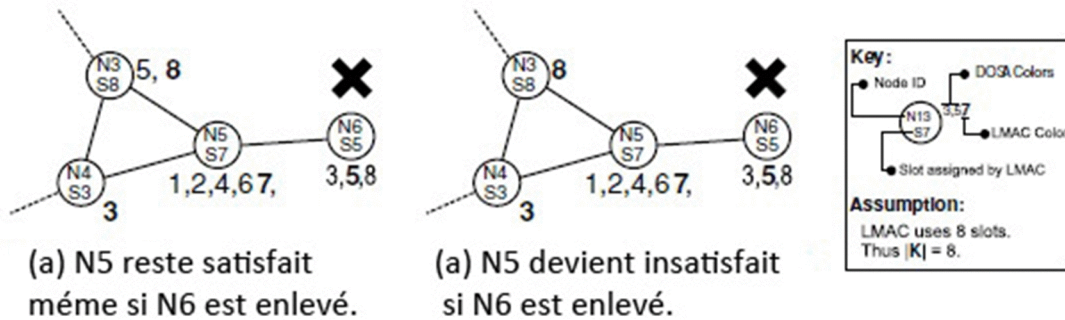


Fig. 15. Deux scénarios possibles quand un nœud meurt

DOSA assure qu'un nœud est capable de réorganiser l'algorithme d'ordonnement à l'intérieur d'une quantité de temps limitée de manière autonome, au moment où un nœud voisin disparaît à partir du réseau. Il fait ceci en récupérant des informations inter-couches du protocole LMAC, ainsi, la mort d'un nœud déclenche une mise à jour dans la table des voisins LMAC.

La mort d'un nœud entraîne la disparition des couleurs qui étaient détenues par le nœud mort. Cela peut conduire à deux scénarios possibles. Tout d'abord, il peut être possible où un ou plusieurs voisins du nœud morts satisfont encore les contraintes 1 et 2 puisque les couleurs qui ont disparu avec le nœud mort sont également présents dans les nœuds voisins. Ceci est illustré dans la figure 15 (a). Dans ce cas, les nœuds voisins satisfaits continuent à maintenir leurs ordonnancements existant et ne transmettent aucun message. Notez que, si leurs affectations de couleur sont invariantes, le degré des voisins du nœud morts se réduit d'une unité. Cela est important que les nœuds qui sont à un saut du voisin nœud mort soient informés de ce changement de degré, car cette information est nécessaire au cas où les ordonnancements doivent être réaffectés à l'avenir en raison de certaines perturbations du réseau. Toutefois, puisque cette conception tire profit des informations inter-couches de LMAC, les transmissions de messages explicites ne sont pas requises pour transmettre les informations concernant un changement de degré d'un nœud.

Cette information est automatiquement diffusée grâce la diffusion périodique de la section CM du protocole LMAC. Rappelons que la section CM transmis par un nœud contient une liste d'emplacement occupé, qui répertorie les emplacements occupés par le nœud et ses voisins. Ainsi, cette information peut également être utilisée pour déduire le degré d'un nœud.

Dans le second scénario, illustré à la figure 15 (b), la mort d'un nœud peut entraîner un ou plusieurs nœuds voisins de se retrouver avec certaines couleurs manquantes.

Puisque ce nœud ne répond plus aux contraintes 1 et 2, le nœud passe à l'état insatisfait et diffuse ce changement d'état à ses voisins immédiates. Le nœud attend ensuite une trame pour voir s'il existe d'autres nœuds voisins qui sont également à l'état insatisfait. Notez que l'attente d'une trame permet au nœud d'entendre tous ses voisins au cas où ils ont tous un changement de statut à signaler. Après avoir attendu une trame, si le nœud avec la ou les couleurs perdus a la priorité la plus élevée parmi tous les nœuds insatisfaits il acquerra toutes les couleurs qui lui manquent. Ce processus est décrit dans l'algorithme 2. Si un nœud manque une couleur mais n'a pas la plus haute priorité, il continue d'attendre jusqu'à ce que tous ses voisins avec priorité élevés non satisfaits soient devenus satisfaits. En d'autres termes, le nœud continue d'exécuter l'algorithme 1 chaque fois qu'il reçoit un message NodeStatus jusqu'à ce qu'il acquière finalement l'état satisfait.

Algorithm 2. *DOSA* - Coping with the loss of a node

Input: LMAC Neighbor Table indicates at least one missing node

Output: NodeStatusMSG(SatisfiedStatus(FALSE & TRUE), ColoursOwned)/NIL

```

1: UPDATE(LocalInfoTable, v)
2: if MissingColours(v) = TRUE (i.e. SatisfiedStatus(v)=FALSE) then
3:   BROADCAST NodeStatusMSG(Degree,SatisfiedStatus(FALSE), ColoursOwned)
4:   WAIT one frame
5:   Compute PRIORITY(v)
6:   if Priority(v)=Highest then
7:      $C_v \leftarrow \mathbf{K} \setminus C_{I'(v)}$ 
8:     ColorsOwned  $\leftarrow C_v$ 
9:     SatisfiedStatus  $\leftarrow TRUE$ 
10:    UPDATE(LocalInfoTable, v)
11:    BROADCAST NodeStatusMSG(Degree, SatisfiedStatus(TRUE), ColoursOwned)
12:  end if
13: end if

```

Afin d'expliquer les limites temporelles de DOSA quand un nœud meurt, on peut étendre le lemme suivant :

Lemme VII.2. *Quand un nœud v avec x voisins meurt, le délai maximal pour tous les nœuds de converger vers l'état satisfait est $x + 1$ trames où $x \leq |K| - 1$*

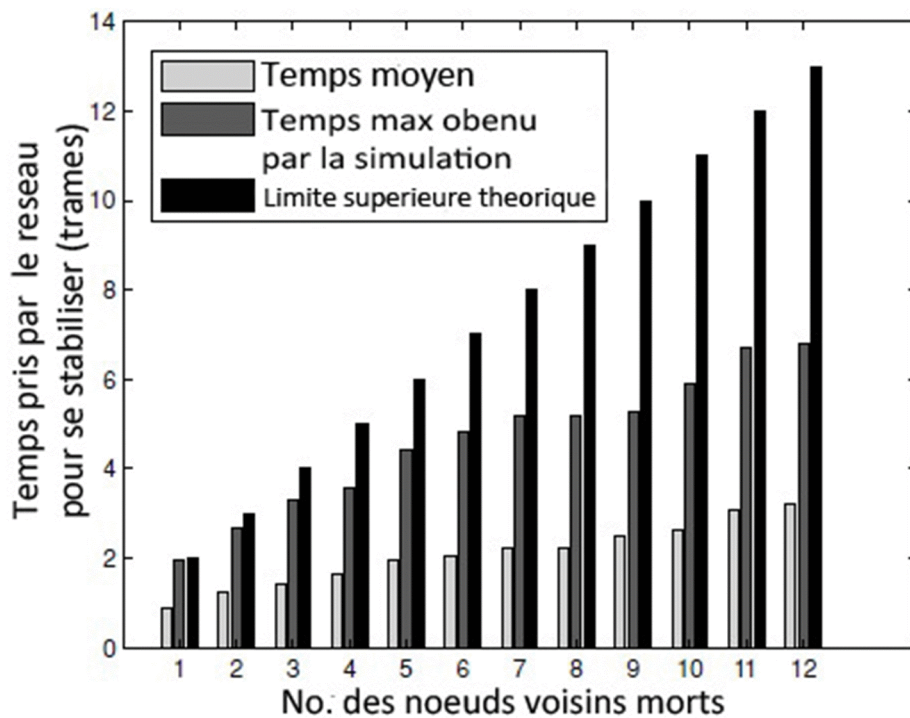


Fig. 16. Le temps nécessaire pour un réseau de se stabiliser une fois qu'un nœud a été supprimé du réseau.

PREUVE. Dans le pire des cas, tous les nœuds d'un voisin mort passent à l'état insatisfait et diffusent ce changement d'état. Chaque voisin insatisfait attend ensuite sa plus haute priorité de voisin insatisfait pour passer à l'état satisfait avant d'acquiescer l'état Satisfait lui-même.

Les simulations ont été faites pour comparer les temps de stabilisation d'un réseau spécifique où un nœud est supprimé, avec les limites présentées ci-dessus. Pour chaque topologie de 100 nœuds (dont un nœud puits), on a enlevé d'abord un nœud, puis attendu que le réseau se stabilise, puis ajouté à nouveau nœud au réseau. Cette opération a été réalisée pour tous les 99 nœuds dans chaque topologie, donc il y avait 9900 nœuds. Les résultats présentés dans les sections suivantes ont été obtenus au cours de ces 9900 cycles. Notez que la connectivité moyenne des nœuds dans chaque topologie est 8.

La figure 16 présente les temps prises par le réseau pour se stabiliser une fois qu'un nœud a été supprimé du réseau. En règle générale, le temps moyen de stabilisation augmente avec le nombre de voisins du nœud mort. C'est également vrai pour les deux temps de stabilisation maximale et la limite majorants théorique présenté précédemment. Toutefois, comme le nombre de voisins du

nœud mort augmente, le taux d'augmentation des durées moyennes et maximales diminue. C'est parce que la probabilité d'avoir un grand nombre de nœuds organisés de manière croissante réduit le nombre de voisins augmentés. Ainsi, dans les milieux de la vie réelle, un réseau de plus haute densité n'a pas nécessairement une reprise plus lente quand un nœud est supprimé. En fait, selon les résultats de la simulation, le cas le plus défavorable enregistré au cours d'une simulation dans laquelle le nœud mort a 12 voisins, serait d'environ 50% du majorant théorique.

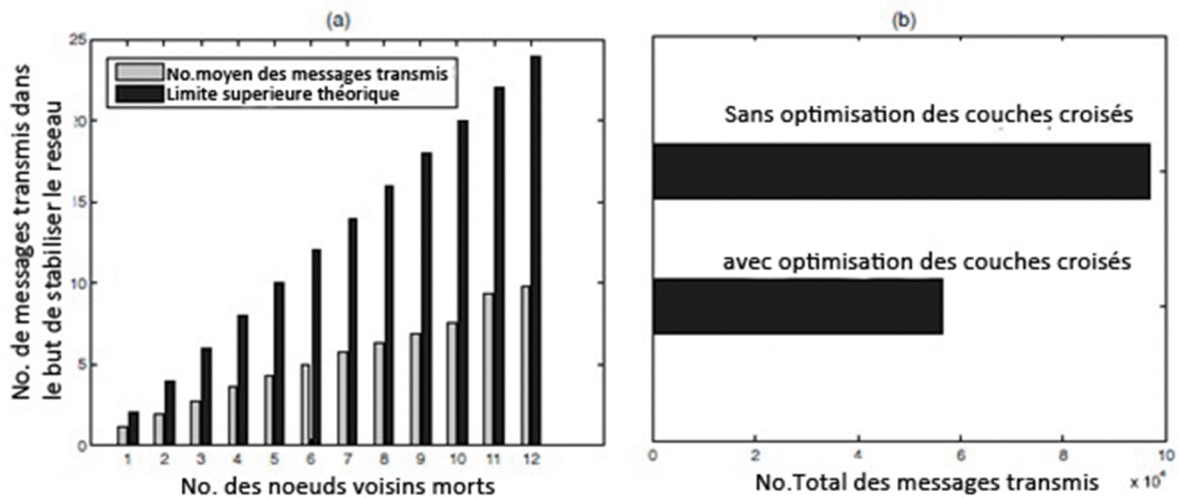


Fig. 17. (a) Nombre de messages transmis afin que le réseau se stabilise une fois un nœud meurt, (b) Nombre de messages transmis sur 9900 exécutions avec et sans les informations de couche croisé.

Lemme VII.3. Quand un nœud v avec x voisins meurt, le maximum nombre possible de messages pouvant être transmis est $2x$, où $x \leq |K| - 1$.

PREUVE. Comme indiqué dans le lemme précédant, dans chaque cas pire, tous les x voisins peuvent devenir insatisfaits quand un nœud v meurt. En règle générale, chaque nœud affecté transmet d'abord un message de NodeStatus, avec l'état mis à l'état Insatisfait au moment où le nœud v meurt. Enfin, quand un nœud acquiert l'état Satisfait, il transmet un autre message NodeStatus qui reflète ce changement. Notez qu'une fois un nœud particulier acquiert l'état Satisfait, il reste dans cet état indéfiniment. Ainsi, le nombre maximum de messages qui peuvent être transmis est $2x$.

La figure 17 (a) montre le nombre moyen de messages transmis lorsqu'un nœud avec un nombre particulier de voisins meurt. Notez que si tous les voisins deviennent insatisfaits en raison de la mort du nœud, chaque voisin unique devrait transmettre deux messages, comme expliqué

précédemment. Dans une topologie aléatoire, le nombre moyen de messages transmis quand un nœud meurt est inférieure à 50% du maximum majorant théorique. Les résultats de simulation présentés dans la figure 17 (b) montrent l'avantage de DOSA d'avoir utilisé l'information inter-couche de LMAC. Le nombre total des messages transmis par tous les nœuds ont été comparées sur 9900 suppressions de nœuds, avec et sans informations inter-couche étant utilisée. Quand il n'est pas utilisé, chaque voisin du nœud mort doit transmettre un message NodeStatus, indépendamment de son statut. Les résultats indiquent une économie de jusqu'à 42% lors de l'utilisation d'information inter-couche.

Lemme VII.4. *Quand un nœud v meurt, seulement ses premiers voisins de commande peuvent être atteints, ainsi, il peut passer de l'état satisfait à l'état insatisfait.*

PREUVE. La mort d'un nœud v ne peut résulter que les nœuds adjacents connaissent des couleurs manquantes, puis de passer à l'état insatisfait. Les nœuds insatisfaits occupent alors les couleurs qui leur font défaut et ainsi faire en sorte que leur choix de couleurs ne posera pas de collisions de couleurs avec leurs voisins. En outre, un nœud qui est satisfait et reçoit un message NodeStatus, ne change pas son statut aussi longtemps que les contraintes 1 et 2 sont remplies. Ainsi, les nœuds qui sont à deux ou plusieurs sauts du nœud v ne peuvent pas connaître un changement d'état lorsque le nœud v meurt.

VII.4 Faire face à un nouveau nœud

Comme nous l'avons montré dans le paragraphe précédent, quand un nœud meurt, DOSA peut seulement exécuter un ensemble fixe d'étapes pour s'assurer que les schémas d'ordonnancement se stabilise dans un laps de temps fini. L'opération d'addition de nœuds est un peu plus impliquée parce que l'ensemble des mesures prises par DOSA dépend des événements qui se produisent lorsqu'un nouveau nœud v est ajouté au réseau. Par exemple, le nœud v peut détecter une collision LMAC, ou peut causer la collision ou la perte de couleurs des nœuds voisins, ou peut même causer une combinaison de ces événements. Les différentes permutations et combinaisons de ces événements peuvent pousser le réseau à réagir de plusieurs façons. Donc qu'il est impossible d'analyser la performance limites de chaque séquence particulière d'événements qui pousse le réseau à réagir d'une certaine manière. Au lieu de cela, dans le but de simplifier les choses, nous classons tous les permutations et les combinaisons d'événements selon jusqu'où la perturbation de réseau se propage lorsqu'un nœud v est ajouté au réseau. Par exemple, il peut y

avoir une certaine combinaison d'événements qui provoquerait des nœuds qui sont jusqu'à deux sauts du nœud v pour passer à l'état insatisfait. De même, il peut y avoir d'autres événements susceptibles d'entraîner la perturbation du réseau pour se propager au 3ème ordre de voisinage de commande du nœud v , nous commençons d'abord par décrire les différents événements qui pourraient se produire lorsque le nœud v est ajouté. Nous avons inclus un exemple de la figure 18 pour illustrer comment les différents événements peuvent se produire. (Note: Le terme «slot LMAC» et «couleur LMAC» sont équivalentes et peuvent donc être utilisés de façon interchangeable) :

(1) Collision entre slots LMAC. Cela se produit lorsque le nouveau nœud v détecte une collision entre deux ou plusieurs de ses voisins adjacents. Chaque collision voisine doit alors abandonner le slot et choisir un nouveau.

(2) Collision entre les couleurs LMAC et les couleurs DOSA: Quand un nœud n qui est à d sauts du nœud v choisit une nouvelle couleur LMAC, il provoque une collision à un nœud m adjacent qui est à $d + 1$ sauts du nœud v , en supposant ce nœud m possède la couleur DOSA qui est égale à la nouvelle couleur LMAC choisi par le nœud n . Notez que si $d = 0$, $n = v$ Aussi $0 \leq d \leq 1$ en utilisant LMAC, le nœud v peut seulement détecter les collisions de slots parmi ses voisins du premier ordre.

(3) Les couleurs DOSA manquantes: Un nœud m qui est à $d + 1$ sauts à partir du nouveau nœud v éprouve des couleurs DOSA manquantes si un nœud adjacent n qui est à d sauts du nœud v , abandonne une couleur DOSA due à une collision de couleur. Ainsi, une collision de couleur d'un nœud qui est à d sauts à partir de v ne peut causer des couleurs manquantes à des voisins adjacents qui sont $J + 1$ sauts plus loin. Puisque un événement manquant de couleur d'un nœud qui est à $d + 1$ sauts à partir de v peut seulement arriver en combinaison avec les événements de collision de couleurs et un nœud qui est à d saut de v , et puisque une collision de couleur peut seulement se produire dans le 1ère ordre du voisinage de v , on peut conclure que $d \geq 1$ si un événement de couleur manquante se produit.

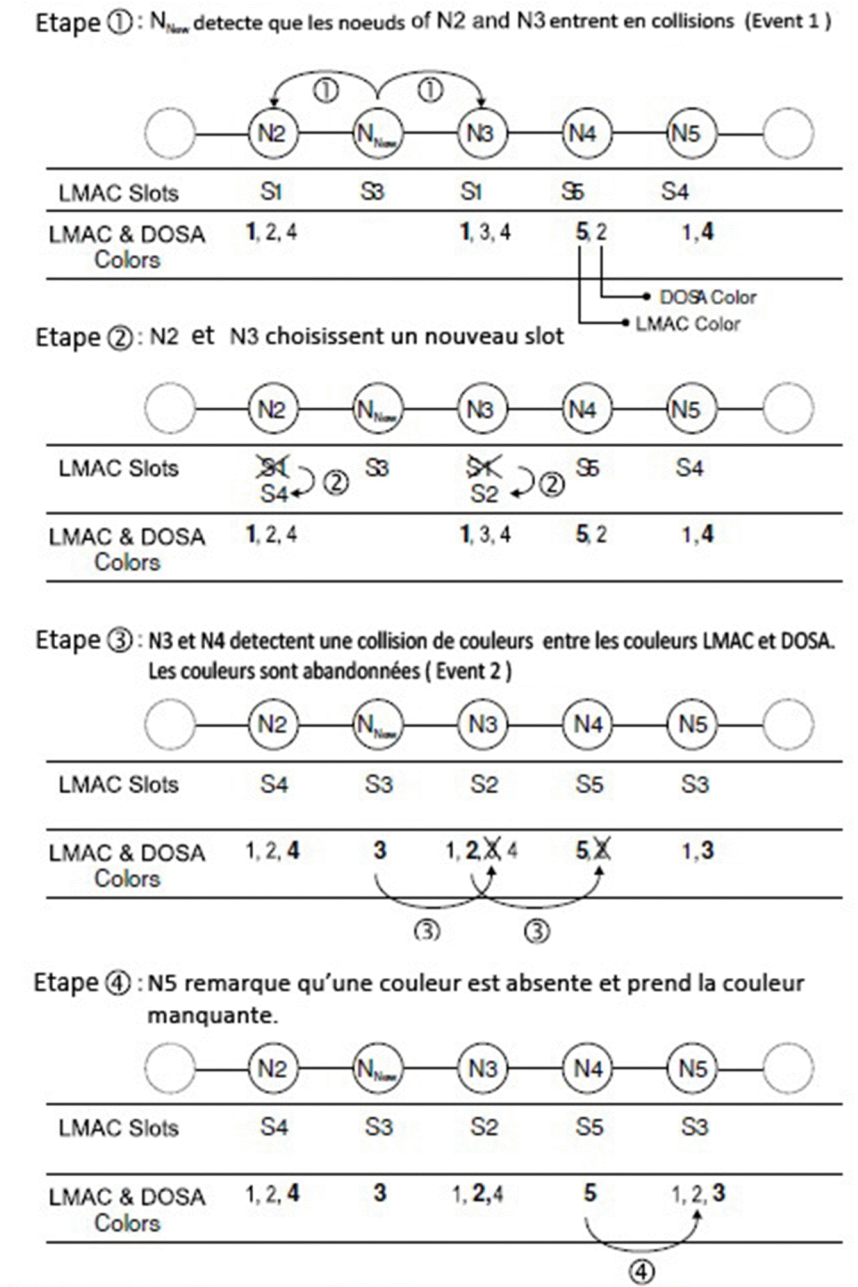


Fig. 18. Un exemple de la manière dont certains événements se produisent quand un nouveau nœud est ajouté.

(4) Un nœud obtient la priorité la plus élevée (en raison du plus large degré dans le voisinage local). Un nœud n qui est à d sauts à partir du nouveau nœud v , réalise qu'il a le plus haut degré dans son voisinage local après l'ajout du nœud v . Cela permet au nœud n d'obtenir la plus haute priorité et ainsi acquérir toutes les couleurs sauf les couleurs LMAC de ses voisins immédiats. Comme cet événement peut se produire soit au nouveau nœud lui-même ou à un nœud qui est adjacent à v nous pouvons conclure que $0 \leq d \leq 1$.

Toutefois, l'ajout d'un nœud ne provoque pas un effet dans DOSA, et cela est expliqué dans le lemme suivant :

Lemme VII.5. *Quand un nœud v est ajouté, tous les nœuds au-delà du voisinage de 3^{ème} ordre de v peuvent être garantie inchangés, il y a des nœuds qui sont à plus de trois sauts et ils le resteront toujours dans l'état satisfait, indépendamment de la séquence des événements qui se produisent après l'ajout du nœud v .*

PREUVE. Nous savons par les quatre événements énumérés dans la figure 18 qu'un nœud peut passer à l'état insatisfait quand il subit soit une collision de couleur ou un événement de couleur manquante. Comme expliqué précédemment, une couleur manquante peut seulement se produire à 1 saut d'une collision de couleur. Nous savons aussi qu'une collision de couleur peut se produire au maximum jusqu'à deux sauts de v . Cela implique qu'un événement de couleur manquante ne peut se produire dans un nœud qui est de trois sauts de v . Ainsi, les nœuds de plus de trois sauts de v ne peuvent pas être touchés par son addition.

Alors **Lemme VII.5** montre qu'un nœud ajouter ne peut pas affecter l'ordonnancement DOSA et d'être dérangé au niveau de trois sauts du nœud nouvellement ajouté, nous avons également effectué des simulations pour analyser les effets réels de plus de nœud. Les simulations ont été faites dans plus de 100 topologies composées chacune de 100 nœuds placés au hasard. Pour chaque topologie, nous ajoutons un nœud aléatoire au réseau et recueillir les statistiques requises, par exemple, le temps de stabilisation du réseau, la profondeur de la perturbation du réseau, et ainsi de suite. Cette procédure est effectuée pour 100 nœuds par topologie. Ainsi, les résultats suivants ont été présentés moyenné sur 10.000 additions de nœud. Les résultats présentés dans la figure 19 indiquent que dans environ 92% des simulations, la perturbation du réseau a été limitée à l'intérieur du deuxième d'ordre du voisinage du nœud nouvellement ajouté. Dans 8% des simulations, aucun des voisins ont été touchés. Les voisins de troisième ordre ont été touchés en moins de 1% des simulations. Quelle que soit la séquence d'événements qui se produit une fois qu'un nouveau nœud rejoint le réseau, il ya quelques étapes communes que DOSA prend. Une fois ces étapes communes sont terminées, la prochaine série de mesures prises dépend de jusqu'où la perturbation du réseau se propage. Nous expliquons d'abord les étapes communes initiales ci-dessous.

Quand un nouveau nœud n est ajouté au réseau, LMAC assure que le nœud n occupe un ordonnancement qui n'est pas utilisée par un autre nœud à deux sauts de n (Figure 20, étape 1). Le nœud n commence alors la diffusion de sa section de CM. Les nœuds voisins détectent alors le nœud n et ajoute son entrée dans les prochaines tables LMAC (Figure 20, étape 2). Nous expliquons les étapes restantes prises par DOSA en se référant à un nœud voisin du nœud n . Ceci est expliqué dans l'algorithme 3.

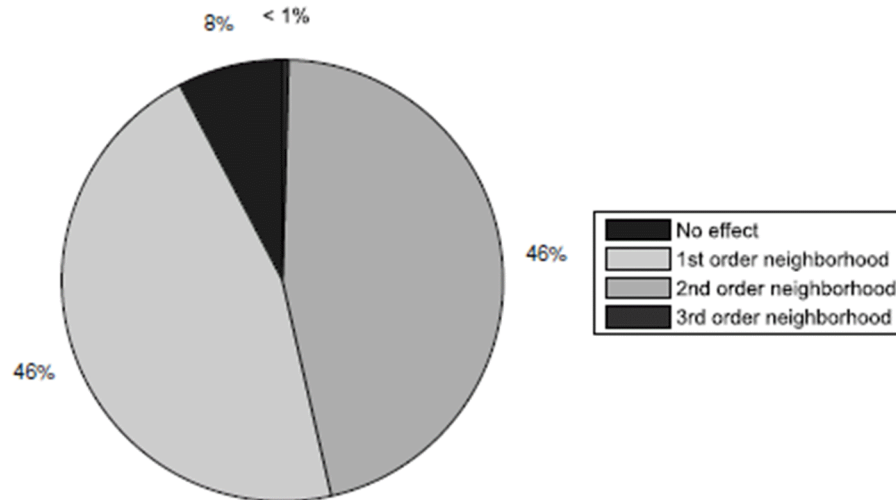


Fig. 19. Les résultats des simulations montrent comment un nœud nouvellement ajouté affecte les nœuds voisins qui sont de 1 à 3 sauts du nouveau nœud.

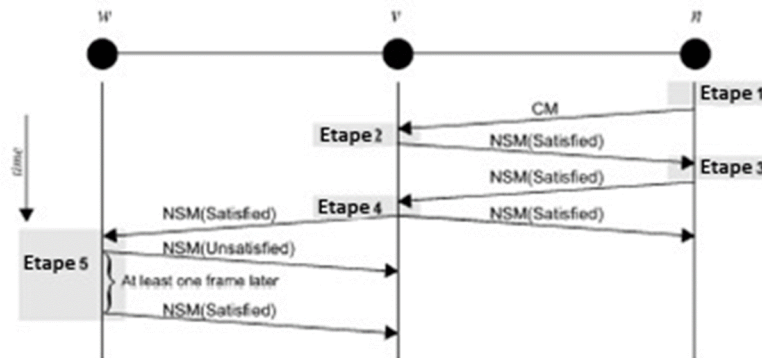


Fig. 20. Diagramme de temps pour l'addition d'un nouveau nœud, n (le nœud v est adjacent au nœud n et w est égal à deux sauts à partir de n.).

Algorithm 3. *DOSA—Coping with a new node*

Input: NodeStatusMSG(Degree, SatisfiedStatus(TRUE), ColoursOwned)

Output: NodeStatusMSG(Degree, SatisfiedStatus(TRUE), ColoursOwned)

- 1: UPDATE(LocalInfoTable, n)
 - 2: if LocalInfoTable contains entries from ALL adjacent nodes then
 - 3: Compute PRIORITY(n)
 - 4: if PRIORITY(n) = Highest then
 - 5: $C_n \leftarrow K \setminus C_{\Gamma_{LMAC}^v(n)}$
 - 6: else
 - 7: $C_n \leftarrow K \setminus C_{\Gamma^v(n)}$
 - 8: end if
 - 9: UPDATE(LocalInfoTable, n)
 - 10: BROADCAST NodeStatusMSG(Degree, SatisfiedStatus(TRUE), ColoursOwned)
 - 11: end if
-

Dès que le nœud v (qui est déjà dans l'état Satisfait) détecte la présence du nœud n, il envoie un message NodeStatus au nœud n (Figure 20, étape 2). Le nœud n attend ensuite de recevoir des messages des états des nœuds de tous ses voisins immédiats (Figure 20, étape 3). Notez qu'à ce

stade, n ne connaîtrait pas l'existence de tous ses voisins immédiats car sinon il n'aurait pas été en mesure d'obtenir un slot LMAC. A partir de ce point, les mesures prises par DOSA sont dépendantes de la séquence d'événements qui se produit. Une fois n a reçu des messages de NodeStatus de tous ses voisins immédiats, il vérifie pour voir si elle a la plus haute priorité au sein de son voisinage immédiat. Si n estime qu'il dispose de la plus haute priorité, il acquiert toutes les couleurs sauf les couleurs LMAC des nœuds voisins adjacents. Cela aide de veiller à ce qu'au fil du temps, même si la topologie du réseau change, le cardinal de l'ensemble indépendant maximal continue d'être faible. En d'autres termes, le nœud puits serait en mesure de prédire les lectures d'un plus grand nombre de nœuds lorsqu'un nœud avec un plus haut degré est choisi pour effectuer les corrélations. Cela conduit à de plus grandes économies d'énergie.

Si le nœud n se rend compte qu'il n'a pas la priorité la plus élevée, il suffit d'acquiert toutes les couleurs qu'il lui manque. Puisque le nœud n satisfait maintenant les contraintes 1 et 2, il diffuse un NodeStatus indiquant qu'il est satisfait.

A ce stade, un nœud voisin v qui reçoit le message NodeStatus à partir de n , peut détecter que certaines couleurs sont en collision (algorithme 4, ligne 3). Cela signifierait que la contrainte 1 n'est pas satisfaite. Ainsi le nœud v abandonne les couleurs qui sont en collision avec le nœud n , atteint l'état Satisfait, mises à jour sa propre LocalInfoTable, et informe tous ses voisins par le biais d'une opération de diffusion (Figure 20, étape 4).

Algorithm 4. *DOSA—Colliding colors due to a new node*

```

1:  UPDATE(LocalInfoTable,  $n$ )
2:  if LocalInfoTable contains entries from ALL adjacent nodes then
3:    if  $C_n \cap C_v \neq \phi$  then
4:       $C_v \leftarrow C_v \setminus (C_n \cap C_v)$ 
5:      UPDATE(LocalInfoTable,  $v$ )
6:      BROADCAST NodeStatusMSG(Degree, SatisfiedStatus(TRUE), ColoursOwned)
7:    end if
8:  end if

```

Comme v a eu un changement de couleurs, il est possible qu'un nœud w , qui est adjacent à v mais pas à n (ie, w est de deux tronçons du n), peut devenir Insatisfait (en raison le message d'état de nœud transmis à l'étape 4 de la figure 20). Le nœud peut alors résoudre la situation en exécutant l'algorithme 2, ce qui lui permet de récupérer les couleurs lorsque ces dernière se trouvent être manquantes (Figure 20, étape 5).

Ensuite, nous présentons les limites majorants de DOSA en termes de quantité du temps pris par le réseau pour se stabiliser et du nombre de transmissions de message lorsqu'un nouveau nœud est ajouté. Puisque l'ajout d'un nœud peut entraîner l'apparition de plusieurs événements, nous décomposons l'analyse en 5 groupes possibles, sur la base de la profondeur de propagation de la perturbation du réseau, comme représenté sur la Table 1.

	No effect (Group 1, 8%)	1st order (Group 2, 46%)
Event type	-	Color collision
Max. time (Frames)	≤ 1	≤ 1
Max Msgs Tx	$= \Gamma'_1(v) + 1$	$\leq 2 \Gamma'_1(v) + 1$
	2nd order	
Event type	Color collision (Group 3, <1%)	Missing color (Group 4, 46%)
Max. time (Frames)	≤ 2	$2 + \Gamma'_2 \setminus \Gamma'_1 $
Max Msgs Tx	$\leq 2 \Gamma'_1(v) + 1 + \Gamma'_2 \setminus \Gamma'_1 $	$\leq 2 \Gamma'_1(v) + 1 + 2 \Gamma'_2 \setminus \Gamma'_1 $
	3rd order	
Event type	Missing color (Group 5, <1%)	
Max. time (Frames)	$3 + \Gamma'_3 \setminus \Gamma'_2 $	
Max Msgs Tx	$\leq 2 \Gamma'_1(v) + 1 + 2 \Gamma'_2 \setminus \Gamma'_1 + 2 \Gamma'_3 \setminus \Gamma'_2 $	

Tableau I. limites majorants pour le temps et transmission de messages quand un nœud est ajouté

Notez que ces cinq groupes englobent toutes les séquences possibles d'événements qui peuvent se produire en raison de l'ajout d'un nouveau nœud, par exemple, collidingLMACslots, un nouveau nœud acquiert la priorité la plus élevée, et ainsi de suite. Aussi pour le 3ème ordre, l'événement de collision de couleur n'est pas répertorié dans le tableau 1 car un tel événement peut se produire seulement pour les raisons indiquées dans la liste des événements présentés précédemment dans cette section.

Nous nous abstenons d'expliquer les dérivations pour la partie théorique majorants pour la stabilisation du réseau indiqués dans le tableau I, car ils ont été obtenus en utilisant les mêmes arguments présentés plus tôt. Toutefois, afin de présenter une explication plus concise, nous présentons les limites théoriques majorants pour le nombre de transmissions de message en utilisant les cinq règles ci-dessous:

Règle 1: Quand un nœud qui a déjà acquis les couleurs DOSA détecte un nouveau nœud v , il envoie d'un message NodeStatus au nœud v .

Règle 2: Un nouveau nœud v diffuse un message de NodeStatus une fois qu'il a acquis son emplacement LMAC, a résolu toutes les collisions entre LMAC et ses voisins et a reçu des messages NodeStatus de tous ses voisins.

Règle 3: Un nœud qui acquiert une nouvelle couleur LMAC qui ne figure pas dans sa liste des couleurs DOSA existantes diffuse un seul message NodeStatus.

Règle 4: Un nœud qui subit une collision de couleur transmet un message NodeStatus.

Règle 5: Un nœud qui subit un événement de couleur manquante transmet deux messages NodeStatus: le premier à indiquer que le nœud n'est pas satisfait en raison de la couleur manquante (s), et le deuxième nœud pour indiquer qu'il est Satisfait après avoir acquis les couleurs appropriées.

Nous illustrons maintenant comment ces règles peuvent être utilisées pour travailler sur la borne supérieure pour le nombre de transmissions de message pour le 3ème ordre en cas de couleur manquante.

Étape 1: Les voisins de premiers ordres du nouveau nœud v transmettent un message NodeStatus après l'avoir détecté. ($|\Gamma'_1(v)|$ messages, règle 1)

Étape 2: Un nouveau nœud transmet un message NodeStatus après l'acquisition de couleurs. (1 message, la règle 2)

Étape 3: Chaque voisin du premier ordre acquiert de nouvelles couleurs et des émissions d'un NodeStatus message. ($|\Gamma'_1(v)|$ messages, règle 3)

Étape 4: Chaque voisin du second ordre connaît un événement de collision de couleur et diffuse un message de NodeStatus. ($|\Gamma'_2(v) \setminus \Gamma'_1(v)|$ messages, règle 4)

Étape 5: Chaque voisin du troisième ordre éprouve un événement de couleur qui manque et diffuse deux messages NodeStatus. ($2(|\Gamma'_3(v) \setminus \Gamma'_2(v)|)$ messages, règle 5)

Ainsi, la limite majorant pour le nombre total de transmissions de message pour le 3ème ordre, *couleurs manquantes* = $2(|\Gamma'_1(v)|) + 1 + |\Gamma'_2(v) \setminus \Gamma'_1(v)| + 2(|\Gamma'_3(v) \setminus \Gamma'_2(v)|)$.

Les simulations montrent que les groupes 2 et 4 du tableau I se produisent dans 92% de toutes les 10.000 simulations tandis que le groupe 1 se produit dans 8% des cas. Les groupes 3 et 5 cependant, se produisent dans moins de 1% des cas. Ainsi, nous présentons les résultats de simulation uniquement pour les groupes 2 et 4, car ils représentent un plus important pourcentage des différents événements qui pourraient survenir.

Considérons d'abord les premiers résultats des collisions de premier ordre. La figure 21 (a) montre que quel que soit le nombre de voisins du 1^{er} ordre qu'un nouveau nœud peut avoir, le temps de stabilisation du réseau reste de moins 1 trame. Cela coïncide avec les limites indiquées dans le tableau I. La figure 21 (b) montre que seulement 1% de toutes les couleurs de collision de 1^{er} ordre ont donné lieu à des scénarios dans lesquels le nombre de messages transmis a été d'environ 90 à 100% de la limite majorant pour la transmission de messages lorsqu'un nouveau nœud est ajouté. Dans près de 50% des cas, le nombre de messages transmis a été d'environ 60% de la limite majorant. La figure 21 (c) montre qu'environ 92% du temps, la quantité de temps nécessaire à la stabilisation du réseau quand les nœuds de second ordre découvrent un événement de couleur manquante était moins de 40% de la limite majorant. La figure 21 (d) montre que dans presque 90% des cas, le nombre de messages transmis a été inférieur à 60% de la limite majorant. Remarquer que les résultats de la figure 21 (b) sont généralement plus proches de la limite majorant que celles présentées à la figure 21 (d). C'est parce que, pendant que les résultats de la

figure 21 (b) exige seulement que les nœuds du premier ordre qui seront concernés, les résultats de la figure 21 (d) impliquent à la fois les nœuds du premier et second ordre. Naturellement, la probabilité d'affecter les nœuds dans les deux premier et second ordres est inférieure à celui des nœuds dans du premier ordre. La performance globale de DOSA pour plus de nœud est présenté dans les figures 21 (e) et 21 (f). La figure 21 (e) et la figure 21 (f) montrent les distributions du nombre de messages transmis et la quantité de temps nécessaire pour que DOSA se stabilise une fois qu'un nouveau nœud est ajouté au réseau.

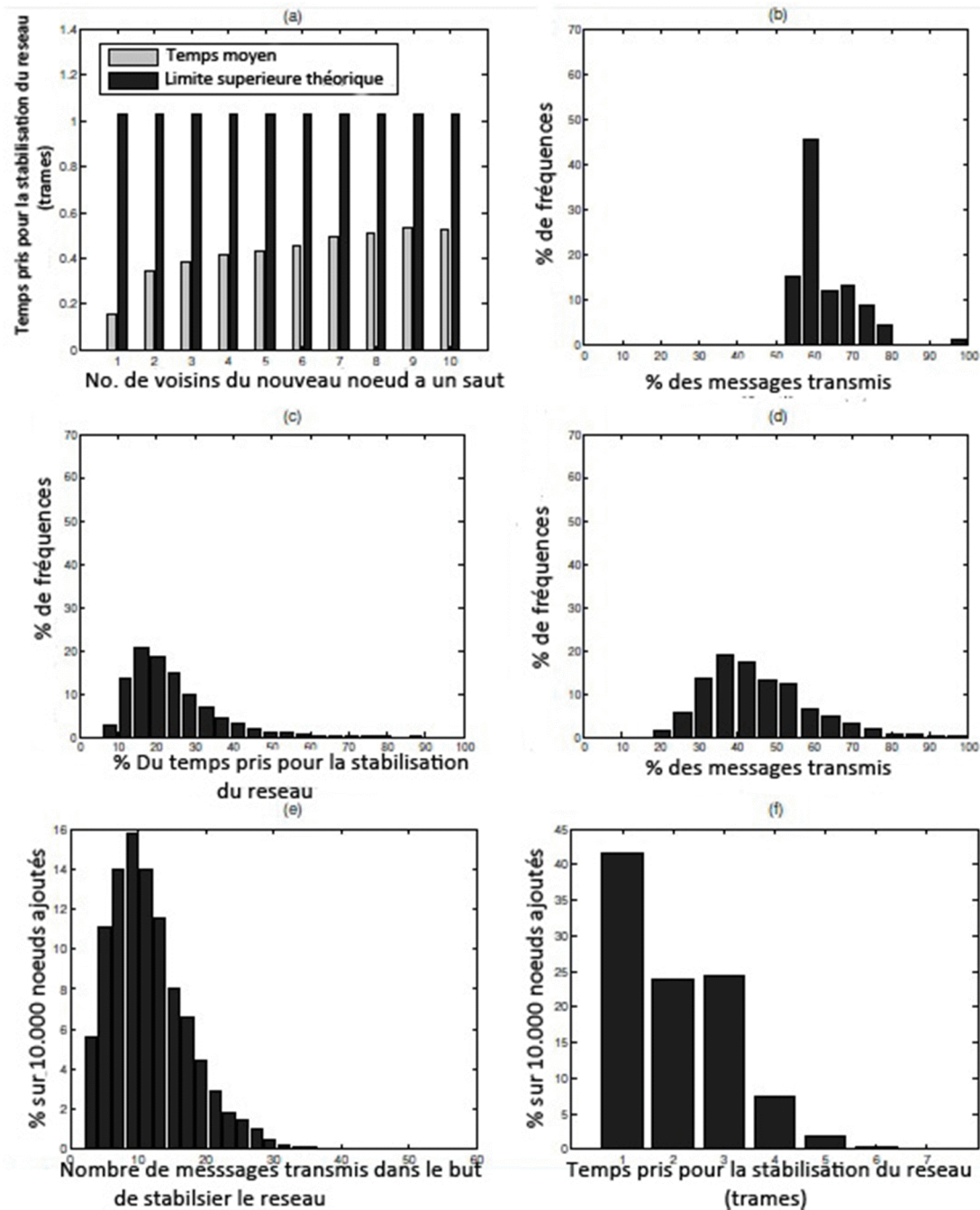


Fig. 21. (a) Le temps nécessaire pour un réseau de se stabilise une fois qu'un nœud a été ajouté au réseau, (b) combien de fois la limite majorant du nombre de messages transmis par le premier ordre événement de

collision de couleur est atteint quand un nouveau nœud est ajouté, (c) Combien de fois la limite majorant du temps nécessaire à la stabilisation du réseau pour le 2ème ordre événement de couleur manquante est atteint quand un nouveau nœud est ajouté, (d) Combien de fois la limite majorant du nombre de messages transmis pour le 2ème ordre manquant si la couleur est atteint quand un nouveau nœud est ajouté (e) Répartition du nombre de messages transmis lorsqu'un nouveau nœud est ajouté au réseau, (f) la distribution de temps nécessaire pour stabiliser réseau lorsqu'un nouveau nœud est ajouté au réseau.

Conclusion

Suite aux résultats obtenus, nous pouvons dire que DOSA tire parti des corrélations spatiales des nœuds à proximité et tire parti des informations inter-couches de LMAC protocole, Aussi DOSA résulte dans 80% d'économies d'énergie par rapport aux données brutes connectées.

Les travaux en cours sur les stratégies pour identifier des corrélations et maintenir des modèles de corrélation mises à jour.

Au cours de ce projet de fin d'études, on a eu l'occasion d'approfondir nos connaissances dans le nouveau domaine des réseaux de capteurs sans fil qui, d'après le MIT's technology Review, constitue l'une des dix nouvelles technologies qui bouleverseront le monde et notre manière de vivre et de travailler.

Nous avons essayé d'analyser grâce à une étude comparative à plusieurs critères les principaux protocoles MAC destinés aux RSCF.

Nous avons présenté un algorithme d'ordonnancement distribué, DOSA qui permettra de recueillir des données brutes d'une manière économe en énergie par tirant parti des corrélations spatiales qui existent entre les lectures du capteur des nœuds adjacents. L'algorithme est complètement auto-organisation dans le sens où les nœuds sont en mesure de choisir des nouveaux ordonnancements de manière autonome quand il y a changement topologie dans le réseau. Ceci est possible grâce à l'étroite intégration de DOSA avec la underlying MAC protocol. Cette approche couche croisée entraîne également d'importants économies d'énergie. Nous avons présenté à la fois la performance théorique limites et les résultats de simulation. Les résultats de simulation indiquent une réduction un message transmissions jusqu'à 85% et une augmentation de durée de vie du réseau de haut à 92% par rapport à la collection de données brutes. L'algorithme est également capable éliminer complètement de messages ont été rejetés par dépassement de mémoire tampon, ce qui l'amélioration de la qualité des données collectées.

Liste des abréviations

ACK : Acknowledgment

BSS : Basic Service Set

CDMA : Code Division Multiple Access

CSMA/CA : Carrier Sense Multiple Access/Collision Avoidance

CTS : Clear To Send

FDMA : Frequency Division Multiple Access

NAV : Network Allocation Vector

RCSF : Réseau de capteurs sans fil

RTS : Request To Send

TDMA : Time Division Multiple Access

TRAMA : Traffic-adaptive medium access protocol

WLAN : Wireless Local Area Network

WMAN : Wireless Metropolitan Area Network

WPAN : Wireless Personal Area Network

WWAN : Wireless Wide Area Network

MAC : Medium Access Control

LMAC : Lightweight Medium Access Control

DOSA : Distributed and Self-Organizing Scheduling Algorithm

Bibliographie

[PUJ 05] Pujolle G., « Les réseaux Editions 2005 », éditions Eyrolles, 2005.

[ZHE 04] Zheng J., Myung L., « Will IEEE 802.15.4 make ubiquitous networking a reality ? », The city college of CUNY, IEEE Communications Magazine, juin 2004.

[AKY 02] Akyildiz I., Su W., Sankarsubramaniam Y., Cayirci E., «A Survey on Sensor Networks», Georgia Institute of Technology, IEEE Communications Magazine, Aout 2002.

[HOL 03] Holger K., Willig A., « A short survey of wireless sensor networks », Technical university Berlin, Telecommunication Networks Group, Octobre 2003.

[CUL 04] Culler D., Estrin D., Srivastava M., « Overview of sensor networks », University of California, Berkeley, IEEE Computer Society, Aout 2004.

[FLE 03] Fleury E., Chelius G., Mignon T., « minimisation de l'énergie dans les réseaux de capteurs », Laboratoire CITI/INSA de Lyon, 2003.

[DEM 03] Demirkol I., Ersoy C., Alagöz F., « MAC Protocols for Wireless Sensor Networks: a Survey », 2003

[LWA 04] Lwakabamba B., « Performance analysis experiments for the wireless sensor networks integrated into the C6 virtual reality environment », Iowa State University, 2004.

[HEI 02] Heidemann J., Ye W., Estrin D., « An Energy-Efficient MAC Protocol for Wireless Sensor Networks », IEEE Infocom, Juin 2002.

[VAN 03] Van Dam, Langendoen K., « An Adaptive EnergyEfficient MAC Protocol for Wireless Sensor Networks », Faculty of Information Technology and Systems, Delft University of Technology, Pays-Bas, 2003.

[YE 03] Ye W., Heidmann J., « Medium Access Control in Wireless Sensor Networks? », USC/ISI Technical Report ISI-TR-580, Octobre 2003.

[DEC 03] Decotignie J. D., El-Hoiydi A., Enz C., Le Roux E., « WiseMAC, an Ultra Low Protocol for the WiseNET Wireless Sensor Network », ACM SenSys'03, Los Angeles, USA, Novembre 2003.

[HOI 04] El-Hoiydi A., Decotignie J.D., « WiseMAC : An Ultra low power MAC Protocol for the downlink of Infrastructure Wireless Sensor Networks », IEEE Symposium on Computers and Communication, pages 244-251, Egypte, Juin 2004.

[HOE 04] Van Hoesel L.F.W., Havinga P.J.M., « A Lightweight Medium Access Protocol (LMAC) for Wireless Sensor Networks: Reducing Preamble Transmissions and Transceiver State Switches », INSS, Japan, Juin 2004.

M. Kubale, *Graph Colorings*, American Mathematical Society, 2004

J. H. van Lint et R. M. Wilson, *A Course in Combinatorics*, Cambridge University Press, 2001

Y. Z. Supriyo Chatterjea, Tim Nieberg and P. Havinga, "Energy-efficient data acquisition using a distributed and self-organizing scheduling algorithm for wireless sensor networks," 2007.

S. Chatterjea, T. Nieberg, N. Meratnia, and P. J. M. Havinga, "A distributed and self-organizing scheduling algorithm for energy-efficient data aggregation in wireless sensor networks," Technical Report TR-CTIT-07-10, Enschede, February 2007.

L. van Hoesel and P. Havinga, "A lightweight medium access protocol (lmac) for wireless sensor networks: reducing preamble transmissions and transceiver state switches," in Proceedings of the International Conference on Networked Sensing Systems (INSS), 2004.

K. P. J. Zhang and P. H. Bauer, "A distributed self-organization algorithm for ad-hoc sensor networks," 2003.

Résumé

L'objectif du projet est de présenter un algorithme d'ordonnement complètement distribué qui permet à chaque nœud de choisir les ordonnancements de manière autonome en se basant uniquement sur les informations disponibles localement. Cet Algorithme possède également des propriétés d'auto-stabilisation qui lui permettent de se rétablir en un temps fini quelles que soient les perturbations dans le réseau, tels que les changements de topologie ou des erreurs de communication. Nous illustrons comment cet algorithme peut s'adapter rapidement aux changements de topologie grâce à son interaction étroite avec la couche sous-jacente MAC. L'algorithme améliore également l'efficacité énergétique en tirant parti des informations inter-couches fourni par le MAC. Enfin, l'algorithme est également capable d'éliminer totalement les messages abandonnés causés par les dépassements de tampon. Ceci nous a permis d'approfondir nos connaissances dans le nouveau domaine des réseaux de capteurs sans fil qui, d'après le MIT'stechnologyReview, constitue l'une des dix nouvelles technologies qui bouleverseront le monde et notre manière de vivre et de travailler. Nous avons essayé d'analyser grâce à une étude comparative à plusieurs critères les principaux protocoles MAC destinés aux RCSF. Nous avons présenté un algorithme d'ordonnement distribué, DOSA qui permettra de recueillir des données brutes d'une manière économe en énergie par tirant parti des corrélations spatiales qui existent entre les lectures du capteur des nœuds adjacents. L'algorithme est complètement auto-organisation dans le sens où les nœuds sont en mesure de choisir des nouveaux ordonnancements de manière autonome quand il y a changement topologie dans le réseau. Ceci est possible grâce à l'étroite intégration de DOSA avec la underlyingMACprotocol. Cette approche couche croisée entraîne également d'importants économies d'énergie. Nous avons présenté à la fois la performance théorique limites et les résultats de simulation. Les résultats de simulation indiquent une réduction un message transmissions jusqu'à 85% et une augmentation de durée de vie du réseau de haut à 92% par rapport à la collection de données brutes. L'algorithme est également capable éliminer complètement de messages ont été rejetés par dépassement de mémoire tampon, ce qui l'amélioration de la qualité des données collectées.