Sur l'adaptation au contexte des réseaux de capteurs sans fil

Charbel Nicolas

THESE DE DOCTORAT CONJOINT TELECOM SUDPARIS et L'UNIVERSITE PIERRE ET MARIE CURIE

Spécialité : Informatique et Télécommunications

Ecole doctorale : Informatique, Télécommunications et Electronique de Paris

Présentée par

Charbel NICOLAS

Pour obtenir le grade de
DOCTEUR DE TELECOM SUDPARIS

Sur l'adaptation au contexte des réseaux de capteurs sans fil

Soutenue le 9/10/2012

devant le jury composé de :

Pr. Guy PUJOLLE	**Professeur, Université Pierre et Marie Curie**	Président
Pr. André-Luc BEYLOT	**Professeur, INP- ENSEEIHT**	Rapporteur
Pr. Imad MOUGHARBEL	**Professeur, Université Libanaise**	Rapporteur
Dr. Mahmoud DOUGHAN	**Maître de Conférences, Université Libanaise**	Examinateur
Pr. Michel MAROT	**Professeur Télécom SudParis**	Co-Directeur
Pr. Monique BECKER	**Professeur Télécom SudParis**	Directrice de thèse

Thèse n° 2012TELE0037

À ma protectrice éternelle, la sainte Marie

Remerciements

Au début de ce manuscrit de thèse, je profite de ces quelques lignes pour adresser mes plus vifs remerciements à toutes les personnes qui m'ont accompagné durant la thèse et qui m'ont aidé à accomplir ce travail.

Tout d'abord, je voudrais remercier Madame le Professeur Monique Becker, ma directrice de thèse, sans qui cette thèse n'aurait pas pu avoir lieu. Ces quelques mots ne suffiront pas pour exprimer toute ma gratitude et mon respect à son égard. La proximité d'un grand professeur est un privilège et un honneur. Durant cette thèse, Madame Becker fut toujours à coté de moi pour me soutenir et répondre à mes demandes. J'admire ses connaissances, et ses qualités humaines. Je lui dois d'avoir appris qu'on peut réaliser tout dans la vie si l'on veut vraiment.

C'est également du fond du cœur que je remercie le Monsieur le Professeur Michel Marot, qui ne m'a jamais abandonné durant les adversités que j'ai rencontrées. Dans ma vie personnelle, il est l'ami à qui je confie mes problèmes et mes soucis, dans ma vie de recherche il est le co-directeur de cette thèse qui m'a appris à devenir un bon chercheur. Sa clairvoyance, son énergie débordante, mais aussi et surtout ses conseils m'ont aidé à surpasser toutes les difficultés que j'ai pu rencontrer. Je n'oublierais pas les discussions à la cantine qui, parties du simple comportement d'un tout petit capteur sans fil ont pu atteindre les lois et les mécanismes qui gèrent le fonctionnement de l'univers jusqu'aux limites de l'univers et même au-delà pour atteindre la métaphysique et le spirituel !

Je tiens particulièrement à remercier Monsieur le Professeur Guy Pujolle, de l'Université Pierre et Marie Curie, pour avoir accepté de présider mon jury de thèse.

Je souhaite remercier Messieurs le Professeur André-Luc Beylot, Professeur à l'ENSEEIHT de Toulouse, et Monsieur le Professeur Imad Mougharbel, Professeur à l'Université Libanaise, pour l'intérêt qu'ils ont porté à cette thèse en étant mes rapporteurs, et pour le temps qu'ils ont accordé à la lecture de ce manuscrit et à l'élaboration de leur rapport.

Un grand merci également au Docteur Mahmoud Doughan d'avoir accepté de prendre part à mon jury.

Je remercie tout particulièrement mon laboratoire d'accueil, le laboratoire SAMOVAR, et le département Réseaux et Services Télécoms (RST) de Telecom SudParis ainsi que ses responsables qui m'ont permis de m'intégrer rapidement et de réaliser mes projets. Je me permets de remercier particulièrement Madame Françoise Abad qui a facilité mon travail et a résolu toutes les complexités des démarches administratives qui ne finissent jamais que ce soit un « simple » ordre de mission, un enregistrement à une conférence ou autre. Je Je n'oublie pas non plus Madame Céline Bourdais pour son aide précieuse, notamment lorsque nous avons reçu les différents équipements du CNRS.

Je remercie très sincèrement Docteur Vincent Gauthier, Maître de Conférences à Télécom SudParis, pour ses remarques utiles et ses conseils avisés.

Un grand merci à mes amis : Abdel mehsen Ahmad, Rashit Agarwal, Edward Chbat, le Docteur Ashish Gupta, Nabil Hachem et le Docteur Mazen Maarabani. Notez l'ordre alphabétique qui signifie, pour moi, que je vous aime tous autant. Je suis reconnaissant de votre immense soutien, et cette amitié sincère qui me lie à chacun de vous est un lien sacré qui m'accompagnera toute ma vie.

Finalement, je dois tout ce que je suis à mes parents, mon père Elias le sculpteur le peintre et l'architecte de ma vie ; Papa je te remercie pour tout ce que j'ai et je vais avoir dans ma vie ; ma mère Marlein à qui je dois toute ma vie. Quoi dire de ma mère qui en plus de tous les travaux qu'elle a à accomplir, a appris en un mois la langue anglaise et l'utilisation d'un PC seulement pour pouvoir me contacter et me voir durant mes séjours à l'étranger. Je remercie mes frères Eliad et Elie. Mes frères, dans nos vies, on ne choisit pas ses frères, mais si j'avais le choix c'est vous que je choisirais.

Résumé

Etant mobiles, pouvant changer d'environnements au cours du temps, tant en termes de milieu pour la transmission des données que de forme de topologie, les capteurs doivent s'adapter au contexte où ils se trouvent afin d'optimiser les mécanismes qu'ils mettent en œuvre, cette adaptation étant faite à partir de toute information qui peut être utilisée pour caractériser la situation des liens de communication entre les capteurs sans fil. Certains protocoles de routage, par exemple, se prêtent mieux à certaines topologies que d'autres. Le réseau de capteurs doit donc la reconnaître et utiliser le plus approprié. Les traitements basés sur la détection de contexte modifient le comportement d'un capteur à partir de sa perception de l'état du milieu et de ses environs. Proposer des méthodes permettant aux réseaux de capteurs de s'adapter dynamiquement en fonction du contexte est l'objet de cette thèse.

Dans la première partie, nous proposons un mécanisme qui permet d'adapter l'architecture d'un réseau de capteurs dynamiquement en fonction du contexte. La principale originalité de notre proposition réside dans le fait de changer dynamiquement de protocoles mais elle comprend: 1) la détection dynamique d'un changement de contexte, 2) la détection dynamique du nouveau contexte, 3) l'adaptation dynamique au niveau des trois couches responsables de la gestion des liens de communication en conséquence, et 4) le tout sous contrainte de consommation d'énergie. La solution développée s'avère plus générale que le contexte spécifique d'où elle est partie : la chaîne du froid. Nous avons alors généralisé notre contribution à travers la proposition d'un cadre conceptuel qui fournit, sous des hypothèses précises sur les situations possibles de visibilité des nœuds et les modes de communication, une panoplie de protocoles sélectionnés pour les niveaux routage, MAC et la couche physique ainsi qu'un mécanisme, CAM pour Contexte Aware Mechanism (mécanisme d'adaptation au contexte), qui passe dynamiquement de l'un à l'autre.

Le travail mené dans cette première partie a d'emblée posé la question de la détection du contexte. C'est une question assez difficile car elle est mal définie. Le contexte peut être détecté par la présence ou le changement de voisins mais aussi par la qualité des transmissions sans fil ou par d'autres critères concernant d'autres phénomènes physiques qui peuvent être le résultat des mesures elles-mêmes des capteurs. Dans la première partie de cette thèse, nous avons pris comme indicateur de changement de contexte une modification de l'ensemble des voisins, ce qui rend assez bien compte de la mobilité des capteurs et donc du changement de lieu. C'était assez bien adapté à l'application qui nous avons considéré puisque l'architecture dépend de la position dans le tronçon de la chaîne du froid et donc finalement du mouvement du capteur. Cependant, la notion de contexte peut être plus vaste et faire référence aux réseaux concurrents émettant dans le milieu dans lequel se trouve le réseau de capteurs que l'on considère. Par exemple, un réseau de capteurs peut être déployé dans un lieu où d'autres réseaux comme des réseaux WiFi sont déjà déployés. Il peut y avoir des fours micro-ondes, ou des équipements BlueTooth, ou toute autre source d'interférences. Détecter le contexte revient alors à détecter la cause des interférences. L'objet de la deuxième partie de cette thèse est justement d'aborder la reconnaissance à la volée de la technologie utilisée par les réseaux émettant du trafic concurrent au réseau de capteurs. Le mécanisme proposé, FIM, identifie la cause d'interférences à partir de modèles d'erreurs observées dans les paquets de données.

La détection du contexte permet aux nœuds du réseau de capteurs d'obtenir des informations sur l'environnement pour prendre la meilleure contremesure ou anticiper des dégradations de performances. Certains nœuds doivent avoir une connaissance plus fiable de l'environnement que d'autres. Se pose alors la question de savoir comment récupérer l'information de nœuds voisins, comment sélectionner ceux de qui on la récupère et comment ne garder que ce qui nous semble sûr et utile. Ce sont ces questions qui sont abordées dans la troisième partie. Nous proposons un mécanisme qui permet de décider dynamiquement si des mécanismes de docition doivent être utilisés ou pas.

Abstract

Being mobile, able to change from environments to others during time, sensors must adapt to the context where they are in order to optimize the mechanisms they use. This adaptation is done from any information which can be used to characterize the situations of the communication links between the sensors. Some routing protocols, for example, are more suitable to some topologies than others. Then, the sensor network must recognize and use the most suitable one. The processes based on context detection modify the behavior of the environment state and its surrounding. To propose methods allowing sensors to dynamically adapt in function of the context is the aim of this thesis.

In the first part, we design a mechanism allowing dynamically adapting the sensor architecture in function of the context. The main originality of our proposal resides in changing dynamically the protocols but it includes: 1) the dynamic detection of a context change, 2) the dynamic detection of the new context, 3) the dynamic adaptation at the level of the three layers in charge of the communication links management consequently, and4) by satisfying energy consumption constraints. The developed solution is more general than the specific context for which it has been designed: cold chain. Thus, we have generalized our contribution with a framework giving, under precise assumptions on possible situations of node visibility and communication modes, a panoply of selected protocols for the routing, MAC and physical levels as well as a mechanism, CAM for Contexte Aware Mechanism (mécanisme d'adaptation au contexte), which dynamically switches from one to another.

This work raises the question of context detection. It is a difficult question because it is not well defined. Context may be detected by change in the neighborhood but also by a change in the wireless transmissions quality or by changes in the sensed data them-selves. In the first part of this thesis, we have chosen as indicator of context change a modification in the neighborhood, which represents well sensor mobility and thus location changes. It was well suited to the application we considered since the architecture depends on node locations in the cold chain. However, the concept of context may be vaster and refer to networks concurrent to the sensor network. For example, a sensor network may be deployed in a location where WiFi networks are already or will be deployed later. Microwave owen or BlueTooth equipments, or any other interference sources may perturb the sensor network. To detect the context is then to detect the causes of the interferences. The aim of the second part is to allow sensor nodes to dynamically recognize, on the fly, the source of the interferences and to identify the corresponding technology in order to react at best.

Context detection allows nodes in the network to obtain information on the environment to take the best counter-measure or to anticipate performance degradations. Some nodes may have a better knowledge on the environments than others. The question to know how to get information from neighbors, how to select the neighbors and how to keep what seems useful and sure is then raised. These questions are addressed in the third part of this thesis. We propose a mechanism allowing to dynamically decide if docition mechanisms must be used or not.

Table des matières

Table des Figures

Chapitre 1. Introduction

Les réseaux de capteurs sans fil constituent un des domaines les plus actifs pour la recherche car il répond au besoin accru de surveillance et de contrôle des phénomènes physiques, biologiques ou autres pour de nombreuses applications. Ce type de réseaux est le résultat de la rencontre de deux domaines différents: celui des capteurs et celui des communications sans fil. Les réseaux de capteurs développés initialement pour des utilisations industrielles et militaires existent désormais dans la plupart des équipements que nous utilisons dans nos vies quotidiennes. Ces capteurs ont évolué de simples outils statiques de mesure pour se transformer en micro-ordinateurs qui peuvent faire des traitements et des analyses complexes, partager des informations et s'adapter d'une manière autonome à toute variation de l'environnement.

L'automatisation et la diffusion d'applications de hautes technologies omniprésentes dans la vie quotidienne depuis la fin du XXème siècle, et le besoin de les adapter à tout changement dans l'environnement, a conduit à la conception d'une grande variété de capteurs pour surveiller, interagir et propager l'information à ces différentes applications. Les applications des capteurs varient entre applications de surveillances médicale, militaires, de la faune, de la flore et de la géologie, capteurs utilisés dans les vêtements intelligents, surveillance des chaînes du froid et beaucoup d'autres encore. Ces applications, particulièrement dans le cas des vêtements intelligents ou de la surveillance de la chaîne du froid, nécessitent des capteurs à la fois mobiles et sans fil.

Bien qu'ayant des capacités infiniment plus grandes qu'il y a encore quelques dizaines d'années, et parce qu'ils utilisent les transmissions sans fil, ils sont sujets à plusieurs limitations. Leur ressource limitée en énergie léur nécessite de l'économiser. L'utilisation de l'air comme médium rend vulnérables les transmissions radio. Selon que la volatilité de l'environnement est attribuable à la mobilité ou à d'autres causes, comme la présence de réseaux concurrents, les réactions à entreprendre sont différentes. En détectant sa propre mobilité ou celle de ses voisins ainsi que les causes de perturbations, la radio peut s'adapter à l'état de l'environnement où elle se trouve.

Etant mobiles, pouvant changer d'environnements au cours du temps, tant en termes de milieu pour la transmission des données que de forme de topologie, les capteurs doivent s'adapter au contexte où ils se trouvent afin d'optimiser les mécanismes qu'ils mettent en œuvre, cette adaptation étant faite à partir de toute information qui peut être utilisée pour caractériser la situation des liens de communication entre les capteurs sans fil. Certains protocoles de routage, par exemple, se prêtent mieux à certaines topologies que d'autres. Le réseau de capteurs doit donc la reconnaître et utiliser le plus approprié. Les traitements basés sur la détection de contexte modifient le comportement d'un capteur à partir de sa perception de l'état du milieu et de ses environs.

Ce besoin d'adaptation du réseau a été constaté dans le contexte de la surveillance de la chaîne du froid au cours de notre participation au projet ANR CAPTEURS. Il existe des solutions adaptées spécifiquement à chaque parties de la chaîne mais, n'étant pas de bout en bout, il est nécessaire de disposer d'un mécanisme capable de détecter le contexte où un nœud se trouve et d'appliquer automatiquement le protocole approprié en fonction de celui-ci. Quand, comme c'est le cas dans le scénario adopté dans le contrat CAPTEURS, on ne peut pas avoir

d'infrastructure, la détection du contexte est rendue difficile. Il n'est pas possible d'installer de stations de base dans le camion ou dans l'entrepôt qui annoncent à chaque capteur son emplacement. Il est alors nécessaire de concevoir un système qui soit capable de s'adapter dynamiquement aux conditions de transport dans les camions ainsi qu'à celles du stockage en entrepôt. **C'est l'objet de cette thèse de proposer des méthodes permettant aux réseaux de capteurs de s'adapter dynamiquement en fonction du contexte.**

Dans la première partie, nous proposons un mécanisme qui permet d'adapter l'architecture d'un réseau de capteurs dynamiquement en fonction du contexte. La principale originalité de notre proposition réside dans le fait de changer dynamiquement de protocoles mais elle comprend: 1) la détection dynamique d'un changement de contexte, 2) la détection dynamique du nouveau contexte, 3) l'adaptation dynamique au niveau des trois couches responsables de la gestion des liens de communication en conséquence, et 4) le tout sous contrainte de consommation d'énergie. Un tel cadre, peut ensuite être implanté sous forme de kit de composants logiciels. La solution développée s'avère plus générale que le contexte spécifique d'où elle est partie : les protocoles retenus sont bien adaptés à certaines hypothèses sur la mobilité des nœuds qui dépassent le cadre restreint de la chaîne du froid. Nous avons alors généralisé notre contribution à travers la proposition d'un cadre conceptuel qui fournit, sous des hypothèses précises sur les situations possibles de visibilité des nœuds et les modes de communication, une panoplie de protocoles sélectionnés pour les niveaux routage, MAC et la couche physique ainsi qu'un mécanisme, CAM pour Contexte Aware Mechanism (mécanisme d'adaptation au contexte), qui passe dynamiquement de l'un à l'autre.

Certes, la nécessité d'adapter les protocoles ou architectures en fonction du contexte a bien déjà été ressentie mais cela n'a pas débouché sur des mécanismes qui s'adaptent dynamiquement. Les auteurs de [NMSYC07] ont analysé différentes situations que peut rencontrer un réseau de capteurs pour la surveillance du corps humain et ont conclu que dans les différents cas les architectures les plus adaptées sont différentes mais aucune proposition pour permettre de passer dynamiquement d'un cas à l'autre n'a été faite. De même, dans [NSYM09] on mesure par expérimentation l'efficacité de deux architectures de réseaux, en étoile d'une part et à plusieurs sauts d'autre part et l'on constate que chacune est efficace dans un contexte spécifique, mais il ne s'agit toujours pas de proposer une solution d'adaptation au contexte. Des travaux sur la détection de topologies de phénomènes physiques ont fait l'objet de plusieurs publications, comme dans [FZWN08] qui concerne la surveillance de phénomènes répartis sur une certaine zone géographique, comme les feux de forêts ou les marées noires. L'objet de ces travaux est de détecter dynamiquement les changements de ces topologies en vue d'une gestion dynamique du réseau. En revanche, cette question de la gestion dynamique des protocoles n'est pas vraiment abordée. Par exemple, si un protocole est plus adapté à une topologie qu'un autre, le fait d'en changer dynamiquement n'est pas évoqué.

Le travail mené dans cette première partie a d'emblée posé la question de la détection du contexte. C'est une question rendue assez difficile car elle est assez mal définie. Le contexte peut être détecté par la présence ou le changement de voisins mais aussi par la qualité des transmissions sans fil ou par d'autres critères concernant d'autres phénomènes physiques qui peuvent être le résultat des mesures elles-mêmes des capteurs. Dans la première partie de cette thèse, nous avons pris comme indicateur de changement de contexte une modification de l'ensemble des voisins, ce qui rend assez bien compte de la mobilité des capteurs et donc du

changement de lieu. C'était assez bien adapté à l'application qui nous avons considéré puisque l'architecture dépend de la position dans le tronçon de la chaîne du froid et donc finalement du mouvement du capteur. Cependant, la notion de contexte peut être plus vaste et faire référence aux réseaux concurrents émettant dans le milieu dans lequel se trouve le réseau de capteurs que l'on considère. Par exemple, un réseau de capteurs peut être déployé dans un lieu où d'autres réseaux comme des réseaux WiFi sont déjà déployés. Il peut y avoir des fours micro-ondes, ou des équipements BlueTooth, ou toute autre source d'interférences. Détecter le contexte revient alors à détecter la cause des interférences. **L'objet de la deuxième partie de cette thèse est justement d'aborder la reconnaissance à la volée de la technologie utilisée par les réseaux émettant du trafic concurrent au réseau de capteurs.**

Les réseaux de capteurs et ZigBee se basent sur le standard IEEE802.15.4. Ils constituent l'un des types de réseaux les plus utilisés et déployés dans les environnements industriels et médicaux. Ils partagent avec d'autres technologies la bande 2.4 GHz du spectre de fréquences connue comme bande dite industrielle, scientifique et médicale (ISM). Les technologies les plus présentes dans cette bande sont celles qui se basent sur Bluetooth et standard IEEE 802.11b/g. En raison de la coexistence dans la même bande ISM, lorsque qu'aucune planification radio n'est faite, les interférences imposées au réseau de capteurs par ces technologies sont inévitables. C'est un problème essentiel puisque les réseaux de capteurs sont très sensibles à l'environnement (cf. [BBDGKM09]) et ils se basent souvent sur les mesures de performance du réseau pour adapter leur algorithmes de configuration (niveau routage et ordonnancement). Le but de cette partie est de présenter un mécanisme de détection et d'adaptation permettant aux nœuds d'un réseau de capteurs de reconnaître dynamiquement la présence de différentes technologies utilisant la même bande de fréquence au même moment et d'adapter leurs modes de transmission en conséquence.

La source de la vulnérabilité à la coexistence des capteurs utilisant l'IEEE 802.15.4 est l'hétérogénéité des mécanismes des couches physiques et MAC. Cette hétérogénéité conduit à un phénomène similaire aux terminaux cachés et est accompagné de collisions et d'interférences. La coexistence avec le WiFi a un effet important sur les performances des réseaux de capteurs sans fil, surtout sur la prévention des collisions et l'équité entre les deux technologies. En raison de sa faible puissance d'émission et son faible débit nominal, le réseau de capteurs est affecté par les technologies qui ont des puissances de transmission et des seuils de détection plus élevés que les siens. Le protocole de la couche MAC le plus utilisé par ces technologies de communication sans fil est le CSMA/CA. Quand il a été mis au point, la diversité des technologies telles que le IEEE802.11 et le IEEE802.15.4 n'existait pas. En adaptant le CSMA/CA à ces technologies, des modifications ont été introduites sur ses seuils de sensibilité, les taux de transmission, etc. Cela a conduit, dans un environnement de coexistence, à la perte de l'équité et de la prévention des collisions initialement assurés par le CSMA/CA dans un contexte homogène.

Le problème du CSMA/CA est dû aux techniques utilisées pour faire l'évaluation de l'état libre du canal (le "clear channel assessment" ou CCA). Les différents types de CCA existants [RR07] sont: celui reposant sur la détection d'énergie (ED), celui sur la détection de préambule (PD) et enfin celui basé sur la décorrélation (DB). Les méthodes alternatives de détection de spectre utilisées par les radios cognitives, y compris l'estimation spectrale à fenêtres de pondération multiples, l'utilisation de la transformée en ondelettes, de la transformée de Hough,

et l'analyse temps-fréquence ne peuvent pas être appliquées par les technologies se basant sur l'IEEE802.15.4 en raison des limitations en complexité de calcul des capteurs et à cause des contraintes énergétiques. La détection de préambule ne peut pas être utilisée par l'IEEE802.15.4 pour détecter les transmissions des technologies utilisant l'IEEE802.11 en raison du coût énergétique et de la complexité des traitements (nécessité de taux d'échantillonnage élevé, filtrage, etc.). La détection basée sur la décorrélation est une combinaison de celles basées sur l'énergie et sur le préambule et hérite donc des mêmes limitations. La détection basée sur l'énergie n'est pas très efficace dans les cas de signaux large bande avec de l'étalement de spectre car la puissance de transmission étant proche du seuil de bruit [RR07] il est difficile de détecter la transmission. En outre, selon les canaux utilisés, le canal ZigBee peut chevaucher l'un des canaux de WiFi. Le canal ZigBee est d'une largeur de 2 MHz et le WiFi est de 20MHz. En raison de la puissance d'émission plus faible utilisée par le ZigBee et la moyenne faible de l'énergie reçue sur la bande passante WiFi 20Mhz, un équipement WiFi ne peut pas toujours détecter une transmission ZigBee.

En revanche, notre travail ainsi que [BGS08] montrent que les interférences avec le Bluetooth, grâce à son mécanisme de saut de fréquences, ont un effet moindre sur le réseau de capteurs. Ceci provient de ce que le Bluetooth n'utilise pas de mécanisme de détection de la puissance du canal pour déterminer si le canal est occupé ou pas, mais emploie à la place le FH/TDD pour l'accès au canal.

L'incompatibilité du CSMA/CA avec un environnement hétérogène et l'incapacité de déterminer la cause de la corruption conduisent les protocoles de la couche de liaison conçus pour un réseau de capteurs à réagir aveuglément à un paquet corrompu. Ignorer la nature du réseau concurrent conduit à l'échantillonnage excessif de la puissance sur le canal. Inversement, connaître la technologie qui occupe le canal de façon concurrente permet, si l'on connaît les caractéristiques de ses temps de silence (moyenne, distribution, etc.) d'optimiser l'échantillonnage et l'utilisation de la bande.

Si la coexistence ne peut être évitée, nécessairement des paquets corrompus sont reçus et le réseau doit alors s'adapter intelligemment, ce qui requiert de reconnaître la cause des interférences. Connaître la cause des interférences permet alors de cibler de manière fine la bonne réaction à entreprendre. L'adaptation du lien peut être faite au niveau de la couche de routage en changeant la structure du réseau ou bien au niveau des couches MAC et physique en changeant la puissance d'émission, le canal, le taux de transmission, en ajoutant des bits redondants, etc. Dans un réseau auto-organisé où l'énergie est une ressource limitée, l'analyse de la qualité et de la stabilité du canal est une procédure coûteuse en énergie et diminuant donc le rendement. Dans cette thèse, et c'est l'un des buts principaux de cette deuxième partie, nous affirmons que la cause exacte de l'erreur sur un paquet peut être déduite d'une simple analyse des erreurs sur ses bits. La meilleure contremesure peut ensuite être choisie. Lorsque les erreurs sur les paquets sont inévitables et si un mécanisme de répétition comme ARQ est utilisé, le paquet correct est finalement reçu tôt ou tard. Au lieu d'ignorer les paquets corrompus déjà reçus, nous suggérons de les conserver et de les comparer avec le paquet correct finalement reçu afin de détecter la forme des séquences d'erreur et d'utiliser cette information pour en déduire la cause des erreurs. Chaque cause doit produire une empreinte différente.

Connaître la cause des erreurs des paquets peut aider à prendre des décisions adéquates à la couche liaison. En identifiant une empreinte WiFi dans le modèle des octets corrompus des

paquets de ZigBee, un changement de canal peut être fait. Si la technologie Bluetooth est détectée, la contre-mesure appliquée pour le WiFi ne peut pas être utilisée puisque Bluetooth utilise le saut de fréquence. En revanche, des longueurs de paquets plus petites peuvent être utilisées. Les erreurs sur des transmissions peuvent aussi être dues au fait que l'émetteur est loin du récepteur, de sorte que le rapport signal sur bruit est petit. Dans ce cas, que nous appelons cas de lien faible, seule une faible quantité des bits des paquets transmis subit des erreurs. Des contremesures comme l'utilisation de codes FEC et de redondance de bits peuvent être appliquées. Les erreurs sur des paquets transmis peuvent aussi provenir de terminaux cachés appartenant au même type de réseau et, si elles sont reconnues, un mécanisme du type RTS/CTS ou une resynchronisation (si le réseau utilise le TDMA) peuvent être appliqués.

Une fois les technologies concurrentes détectées et reconnues, des décisions peuvent également être prises au niveau de la couche routage. Pour un réseau utilisant un mécanisme de routage en cluster, la sélection du chef du cluster peut dépendre des technologies qui l'entourent et de leurs effets sur sa communication. Par exemple, si du WiFi est détecté au voisinage d'un nœud ZigBee il y a une forte probabilité que ce nœud interfère pendant une longue durée avec le WiFi. Il est alors préférable de construire les feuilles d'une topologie à multiples sauts arborescente de telle sorte que les nœuds interférant avec d'autres technologies soient les feuilles de ces arbres, ou, au moins, ne soient pas les chefs de clusters. Si des slots de temps périodiques sont réservés pour les émissions de certains nœuds, on peut les modifier en fonction de la technologie concurrente détectée ou les mettre sur une liste noire.

La détection du contexte permet aux nœuds du réseau de capteurs d'obtenir des informations sur l'environnement pour prendre la meilleure contremesure ou anticiper des dégradations de performances. Certains nœuds doivent avoir une connaissance plus fiable de l'environnement que d'autres. **Se pose alors la question de savoir comment récupérer l'information de nœuds voisins, comment sélectionner ceux de qui on la récupère et comment ne garder que ce qui nous semble sûr et utile. Ce sont ces questions qui sont abordées dans la troisième partie.**

Un nouveau paradigme du domaine des réseaux coopératifs et distribués a émergé récemment : les réseaux docitifs [GGBD10]. Un réseau docitif est l'aboutissement naturel auquel devait arriver la recherche sur la radio cognitive [H05] : tandis que celle-ci utilise l'intelligence artificielle et des algorithmes d'apprentissage automatiques pour traiter les observations locales des canaux de communication, la radio docitive inclut aussi des informations collectées à partir des nœuds voisins. Le but de cet échange d'informations est d'accélérer et d'améliorer le processus de prise de décision. Le terme de docition dérive du mot latin « *docere* » signifiant enseigner, les radios « enseignant » les informations qu'elles considèrent importantes à d'autres radios [GGBD10]. La docition est donc un paradigme concernant le rapport entre enseignant et élève. L'intelligence est en effet impactée par le degré d'observation ou, plus précisément, de connaissance.

Tandis que par le passé la cognition et l'apprentissage à partir d'informations obtenues directement de son environnement par un nœud ont reçu beaucoup d'attention de la part de la communauté scientifique, le processus de transfert de connaissances, l'apprentissage, au moyen d'un support sans fil a fait l'objet de peu de travaux à ce jour. De même que pour la radio cognitive distribuée, la radio docitive a besoin de coopérer avec les radios voisines pour réaliser la docition, cependant dans le principe de docition l'utilisation des informations échangées n'est

pas systématique: l'enseignant n'enseigne pas les résultats finaux directement intéressant l'élève, mais propose les éléments des méthodes pour y parvenir. En d'autres termes, les problématiques de docition concernent la façon dont l'information est sélectionnée et transmise d'un nœud à un autre.

Le principe de docition peut être appliqué à des degrés divers, de l'absence totale de docition, c'est-à-dire du transfert systématique à tous les voisins de toute l'information dont disposent les nœuds, ce qu'on appelle encore radio distribuée, jusqu'à la docition parfaite où toute information est filtrée. Les auteurs de [GGBD10] évoquent ces différents degrés possibles mais supposent qu'ils sont statiques : un nœud docitif n'a pas la possibilité de choisir dynamiquement son propre degré de docition.

Pendant la docition, l'échange du tableau de « Q-learning » [HH00] est essentiel, car il contient les informations de docition. Ce tableau contient les informations relatives à l'état de l'enseignant or il est crucial que le nœud étudiant ait un état de l'environnement similaire à celui de l'enseignant. Or, pour que la docition permette au nœud apprenti une convergence rapide vers une prise de décision spécifique, une hypothèse forte est supposée par le paradigme : la cohérence entre les états de l'enseignant et ceux de l'élève. En effet, il n'existe pas de mesure prise dans le paradigme docitif pour s'assurer que l'enseignant et les nœuds étudiants ont des états cohérents. Les auteurs de [GGBD10] supposent que, par construction, puisque la docition est appliquée aux réseaux fixes, avec ou sans infrastructure, il n'y a pas de problème de cohérence d'information entre les nœuds voisins.

En revanche, dans le contexte de cette thèse, nous nous intéressons aux réseaux mobiles sans infrastructure tels que les MANETs et surtout les WSNs. Dans ce type de réseaux, les nœuds peuvent ne pas avoir de bases d'états cohérentes, du fait de la mobilité, de l'occupation de la bande ISM par des technologies et applications concurrentes variées ou tout autre raison. Nous appelons docition classique le principe de docition présenté jusqu'ici dans la littérature et utilisant un degré de docition statique pour les nœuds tout au long de la vie du réseau.

L'objet de cette troisième partie est par contre d'étendre ce concept classique en une docition dynamique qui permet aux nœuds enseignants et apprentis, dans tous les cas possibles de mobilité ou de causes diverses d'incohérences d'état entre voisins, de spécifier le niveau de docition dynamiquement en fonction du niveau de prévisibilité de l'environnement. Nous proposons alors d'ajouter une sonde de prévisibilité de l'environnement (SPE) comme nouvel élément à la docition classique. En fonction du résultat obtenu par l'SPE, si l'état de l'environnement est assez stable et un certain niveau de cohérence entre enseignants et apprentis est observé, des méthodes de docition sont appliquées sinon aucune docition n'est utilisée.

Pour évaluer la pertinence et les performances de la docition dynamique, nous l'appliquons au cas d'une situation de coexistence entre les technologies IEEE802.15.4 (capteurs sans fil) et IEEE802.11b/g (WiFi), où les nœuds capteurs sont mobiles. Pour échapper aux interférences avec le WiFi, les capteurs exploitent l'existence des périodes de silences dans le trafic WiFi, silences modélisés par une loi de Pareto. Cette modélisation est proposée et validée dans [HXZZ10]. Nous la prenons comme hypothèse, qui pourrait être affinée au demeurant mais cela ne devrait pas modifier grandement notre étude. Le scenario qui nous intéresse est semblable à celui d'une radio cognitive qui s'adapte en tant qu'utilisateur sans licence (connu sous le nom

d'utilisateur secondaire) pour coexister avec un usager ayant une licence (connu sous le nom d'utilisateur principal) [M98]. Plus précisément, nous cherchons à donner aux technologies « faibles » (alimentation électrique limitée, faibles capacité de traitements, puissances et taux de transmission) comme celles utilisant le standard IEEE802.15.4 les moyens d'adaptation pour coexister avec les technologies « fortes » comme l'IEEE802.11 (alimentation électrique suffisante, taux et puissance de transmission élevés). L'application de notre proposition de docition dynamique dans ce scénario améliore l'efficacité de la consommation d'énergie et assure un temps de convergence des nœuds plus rapide vers la meilleure prise de décision.

Dans le chapitre suivant, un aperçu du domaine est présenté. Le troisième chapitre présente le mécanisme d'adaptation au contexte qui fit l'objet de la première partie de la thèse. Le mécanisme de détection des technologies concurrentes à partir d'empreintes spécifiques fait l'objet du chapitre quatrième. Le cinquième est dédié à la docition et le sixième au bilan de la thèse et à ses perspectives.

Chapitre 2. Etat de l'art

Les réseaux de capteurs sans fil constituent un des domaines les plus actifs pour la recherche car il répond au besoin accru de surveillance et de contrôle des phénomènes physiques, biologiques ou autres pour de nombreuses applications. Ce type de réseaux est le résultat de la rencontre de deux domaines différents: celui des capteurs et celui des communications sans fil. Les réseaux de capteurs développés initialement pour des utilisations industrielles et militaires existent désormais dans la plupart des équipements que nous utilisons dans nos vies quotidiennes. Ces capteurs ont évolué de simples outils statiques de mesure pour se transformer en micro-ordinateurs qui peuvent faire des traitements et des analyses complexes, partager des informations et s'adapter d'une manière autonome à toute variation de l'environnement.

Dans ce chapitre, on commence par discuter de la principale faiblesse des capteurs sans fil à savoir leur approvisionnement en énergie, ou plus exactement leur nécessité de l'économiser, et de sa cause à savoir le fait que justement ils ne sont pas filaires (§2.1). Nous décrivons ensuite les différentes composantes d'un capteur sans fil (§.2.2). Les différentes applications des réseaux de capteurs sont listées au §.2.3, puis les faiblesses de la partie radio sont mises en relief au §.2.4. La vulnérabilité des transmissions radio est principalement causée par l'état de l'environnement §.2.5. Celui-ci détermine les différents états possibles des canaux de communication. Selon que la volatilité de l'environnement est attribuable à la mobilité (§.2.6) ou pas (§2.7), les réactions à entreprendre sont différentes. En détectant sa propre mobilité ou celle de ses voisins, la radio peut s'adapter à l'état de l'environnement où elle se trouve. D'autres méthodes d'adaptations sont à mettre en place pour la radio quand l'environnement varie sans que cette variation soit attribuable à une quelconque mobilité §.2.7. Le §2.7.1 décrit les principales causes de volatilité de l'environnement, les plus récentes solutions d'adaptation à ces types de variations sont présentées aux §§2.7.2 et 2.7.3. Enfin, un aperçu général est donné sur les principaux simulateurs et le système d'exploitation le plus accepté au §2.8 avant de conclure 2.9.

2.1 Les capteurs filaires et les capteurs sans fil

Les communications filaires dans les réseaux de capteurs permettent une communication fiable, grâce à différents protocoles comme par exemple Ethernet, Modbus (pour les automates programmables industriels) ou via différents ports séries comme les ports USB. Il y aura toujours des situations où une liaison filaire est plus adaptée qu'un lien sans fil, mais les capteurs sans fil deviennent de moins en moins coûteux et plus fiables, ce qui les rend préférables dans la plupart des applications modernes. En outre, des études ont montré que les réseaux filaires peuvent être utilisés pour un faible nombre de nœuds, en revanche pour un grand nombre il est plus efficace d'utiliser un réseau de capteurs sans fil ([AARA06]).

La raison pour laquelle le coût de la communication filaire reste élevé est due au coût du fil, des connecteurs, et au travail nécessaire pour installer l'infrastructure qui connecte les nœuds du réseau. En revanche, le coût des communications sans fil a chuté d'une façon spectaculaire suivant la loi de Moore, qui stipule que « la densité des transistors dans les microprocesseurs double tous les deux ans et que, en conséquence, les machines électroniques deviennent de moins en moins coûteuses et de plus en plus puissantes ». En même temps, les différentes

améliorations dans le fonctionnement cognitif des émetteurs-récepteurs les rendent plus fiables contre les interférences et les distorsions des canaux partagés.

Les réseaux sans fil sont plus fiables que les filaires dans des applications spécifiques. Nous donnons ci-après quelques exemples. Dans les cas de mobilité, les capteurs ne peuvent pas être connectés par des câbles or on cherche de plus en plus à surveiller des systèmes ou des objets mobiles. Les capteurs attachés aux vêtements et au corps humain pour enregistrer des mesures médicales, les capteurs surveillants la chaîne du froid, les capteurs maritimes surveillant le niveau de pollution dans la mer, etc. sont de tels exemples.

Les systèmes sans fil sont particulièrement appréciés dans les cas de coupure volontaire ou involontaire des câbles ! Dans un environnement industriel la section d'un câble par accident lors du déplacement d'une cargaison lourde n'est pas impossible. En outre, des coupures de câble volontaires dans des actes de sabotages peuvent aussi se produire, mais avant que certains malfaiteurs puissent couper une connexion, ils doivent savoir que cette connexion existe. Contrairement aux connexions filaires, les connexions sans fil sont invisibles, ce qui offre une protection importante contre les attaques malveillantes. Les capteurs sans fil sont aussi bien utiles dans les domaines de surveillance où les zones sont nuisibles ou toxiques pour la santé humaine ou qui ne peuvent pas être atteintes par l'homme pour faire la maintenance ou la récolte de données.

Cette thèse se focalise sur les capteurs sans fil. À cause de l'absence de connexion physique à une source d'alimentation permanente, qui existait dans le cas d'un réseau de capteurs filaire, les capteurs sans fil ont besoin d'être efficaces au niveau de leur consommation d'énergie et donc de devenir plus intelligent dans leur choix de lien de communication, la façon d'adapter leur transmission, celle de choisir leurs durées du rapport du temps passé en état de veille par rapport à celui en état de sommeil, etc.

Au §.2.2 on présente l'architecture d'un capteur sans fil avec une attention particulière sur la consommation d'énergie associée à chacune de ses composantes ce qui permet de mettre en relief le taux élevé de la consommation d'énergie reliée à la partie radio.

2.2 Architecture d'un capteur sans fil

Un capteur sans fil est principalement composé de 5 unités principales : l'unité de mesure ou capteur proprement dit, l'unité de traitement, l'unité de stockage de donnée, l'unité de transmission et l'unité de gestion d'énergie.

L'unité de mesure (capteur)

Le composant principal d'un capteur sans fil est le capteur lui-même. C'est un dispositif transformant l'état d'une grandeur physique observée en une grandeur utilisable. Il s'agit d'un récepteur et d'un transducteur (convertissant le signal du récepteur en signal électrique). Le capteur fournit des signaux analogiques, à partir du phénomène observé, au convertisseur Analogique-Numérique. Ce dernier transforme ces signaux en un signal numérique compréhensible par l'unité de traitement.

L'unité de traitement

Elle comprend un processeur qui représente le centre décisionnel de toutes les fonctionnalités d'un capteur sans fil. Elle est gérée par un système d'exploitation léger en termes de complexité d'exécution et d'allocation de mémoire (typiquement TinyOS). Elle implante et exécute divers protocoles et mécanismes de communications. En outre, elle peut effectuer des traitements et des analyses de données pour optimiser le fonctionnement global du réseau de capteurs.

L'unité de stockage

A cause de la mobilité, l'importance de l'unité de stockage a augmenté ces dernières années. Elle doit pouvoir sauvegarder tous les différents événements qui peuvent arriver durant la durée de surveillance. Le besoin de stockage provient de la mobilité d'un capteur sans fil qui peut se trouver dans le cas où il est déconnecté totalement des réseaux de capteurs existant, et doit pourtant assurer la préservation les données collectées jusqu'à l'établissement d'une connexion à un réseau voisin ou à une station de base.

L'unité de transmission

L'unité de transmission effectue toutes les émissions et réceptions des données sur un médium. Elle peut être utilisée pour faire une transmission filaire ou sans fil. En accentuant sur la partie sans fil, cette unité de transmission de type radio-fréquence exécute des tâches complexes de modulation, démodulation, filtrage et multiplexage, ce qui impose une consommation élevée d'énergie. En outre pour qu'un nœud ait une portée de communication suffisamment grande, il est nécessaire d'utiliser un signal assez puissant et donc une énergie consommée importante (cf. Figure 2.1).

L'unité de gestion d'énergie

Un capteur sans fil est équipé d'une ressource énergétique de petite taille, cette ressource énergétique étant limitée et généralement non remplaçable. L'unité de gestion d'énergie constitue donc une partie essentielle du système. Elle répartit l'énergie disponible d'une manière optimale en réduisant les dépenses inutiles et en mettant en veille les composants inactifs.

La Figure 2.1 présente la consommation élevée d'énergie par la composante radio quand elle est activée relativement aux autres composantes du capteur sans fil.

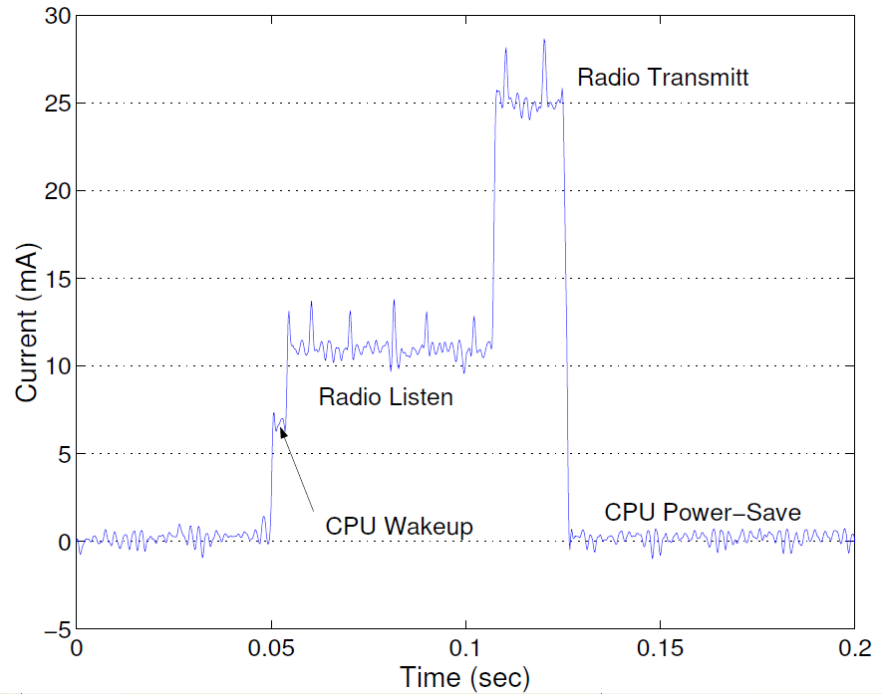


Figure 2.1 Consommation de courant mesurée pour transmettre un message radio unique avec une puissance maximal d'émission par un nœud Mica2 (extrait de [SHCWW04])

La plupart des fabricants de capteurs sans fil, sur le marché, se basent sur ces concepts.

Les fabricants les plus connus sont :

Sun-SPOT de Sun Microsystems [SSW12]

Sun SPOT est un capteur sans fil développé par Sun Microsystems. La partie radio de Sun Spot est basée sur la norme IEEE 802.15.4. Contrairement aux autres capteurs sans fil, Sun SPOT est basé sur la machine virtuelle Java Squawk. Il est composé de quatre parties : la couverture de protection, le composant capteur, le composant microcontrôleur et les piles électriques (cf. Figure 2.2).

Figure 2.2: solution Sun-Spot

WiEye d'EasySen [EWSB09]

EasySen est un composant capteur pour faire de la surveillance. Il est conforme à TelosB (cf. Figure 2.3)

Figure 2.3: La carte électronique supérieure est le capteur EasySen et la carte inferieur est le capteur sans fil TelosB [EWSB09]

JENNIC [JWM]

Les capteurs sans fil développés par JENNIC se caractérisent par leur très faible consommation d'énergie assurant ainsi une longue durée de vie.

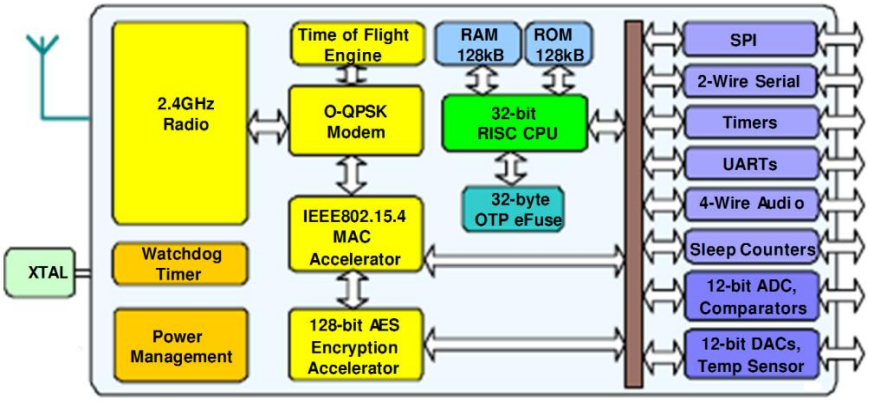


Figure 2.4 : pile protocolaire de JENNIC

Crossbow[Cross]

Crossbow a développé le capteur sans fil "Micaz" et ce capteur est accompagné par un connecteur permettant l'intégration d'un composant capteur (cf. Figure 2.5)

Figure 2.5 : unité de captage (lumière) sur mote Crossbow Micaz

Tmote Sky de Moteiv [TSM07]

Pour nos expériences, nous avons choisi d'utiliser les capteurs sans fil Tmote Sky de Moteiv. Tmote Sky opère avec deux piles de type AA. C'est une solution qui contient un microcontrôleur qui fonctionne à une fréquence de 8 MHz, avec une mémoire ROM de capacité 48 KB et une mémoire RAM de 10 KB. Ce capteur sans fil est équipé d'une composante radio CC2420 [CC2420] qui est conforme à la norme IEEE 802.15.4. Elle a un débit de 250Kbps, et fonctionne dans la bande de fréquence 2.4 GHz. De plus, Tmote sky est équipé d'une interface USB permettant de programmer facilement le capteur et de collecter les données enregistrées durant la surveillance. Tmote Sky est équipé de différents composants capteurs : un capteur de lumière, capteur de mouvement, un capteur d'humidité et peut être équipé d'autres types de capteurs (cf. Figure 2.6).

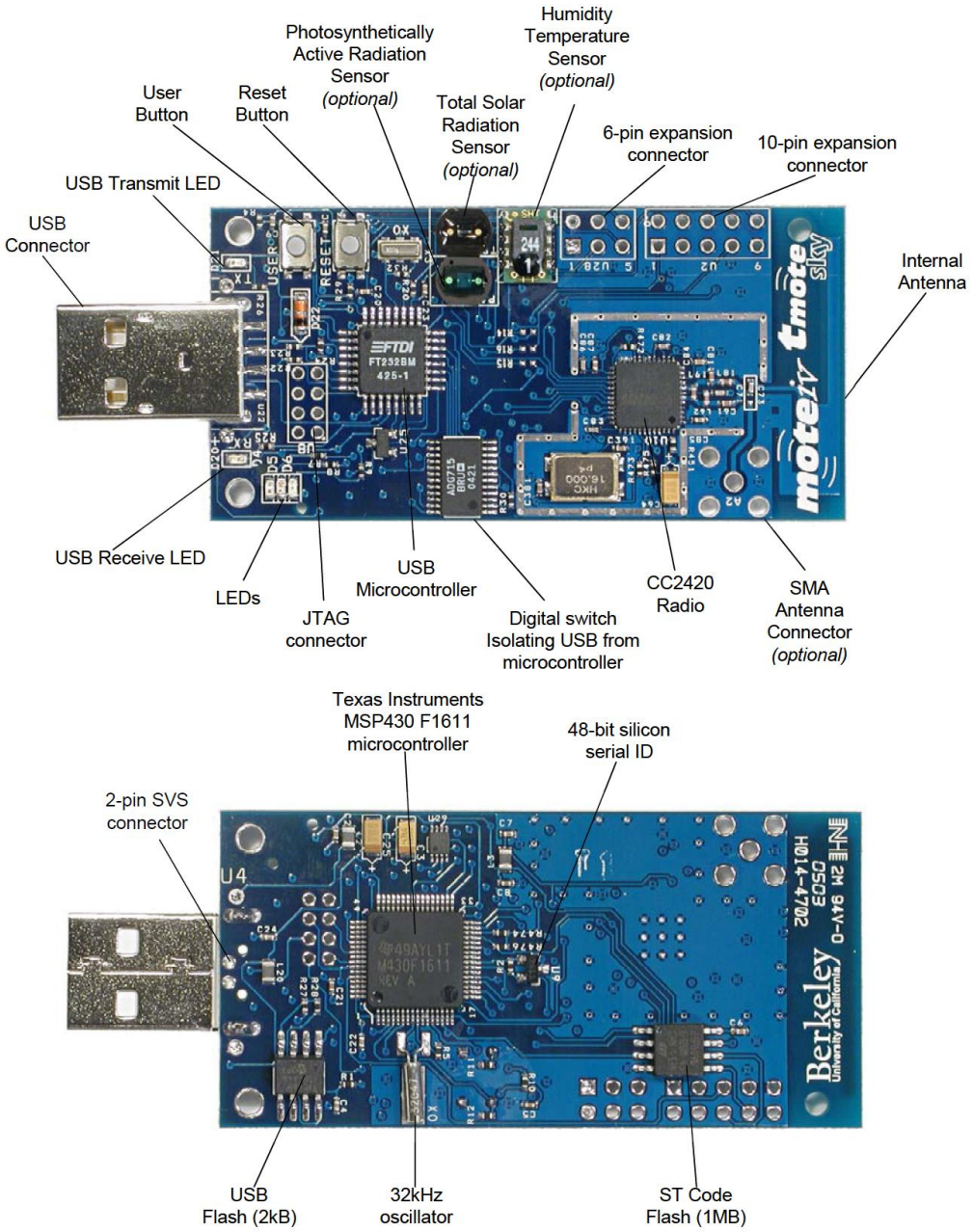


Figure 2.6: module Tmote Sky

Il existe encore d'autres fabricants de capteurs sans fil. Nous n'avons cité que les plus importants. La présence de ces différents fabricants sur le marché n'est qu'un indicateur de la grande demande de capteurs sans fil. À cause de cette demande, une grande variété de capteurs est développée pour répondre aux besoins reliés aux caractéristiques des différentes applications.

2.3 Applications et exigences

Dès leur apparition, les capteurs ont évolué considérablement, d'un simple mécanisme pour collecter des mesures à un système complexe capable de construire des réseaux dynamiquement, de faire des traitements et de s'adapter aux différents obstacles qu'ils peuvent rencontrer. Cette évolution est due aux vastes domaines d'application des capteurs qui demandent des solutions assez différentes.

Spécifiquement, dans les applications militaires, un capteur sans fil est sujet à un environnement hostile. Ils sont dispersés à partir d'un avion, d'une manière aléatoire, dans un champ de bataille,... Ils doivent construire un réseau qui assure une bonne diffusion des données, crée des chemins de secours pour éviter les attaques d'interférences et l'arrêt imprévisible d'un capteur dans le réseau. De plus, il ne faut pas oublier la mission principale d'un capteur sans fil qui est la récolte de données sur l'environnement. Les données collectées peuvent être la détection de la présence des ennemis, des agents chimiques, biologiques ou de radiations.

La sécurité est une autre application. Dans cette application, le système fonctionne en mode temps réel. Le réseau construit doit supporter un trafic élevé, à cause du nombre potentiellement élevé d'alarmes déclenchées en même temps par différents capteurs dès la détection d'intrusion.

Les applications médicales et la surveillance du corps humain sont des applications de plus en plus répandues. Elles consistent à surveiller les signaux émis par le corps humain ainsi que son comportement dans différentes circonstances. Plusieurs capteurs sont attachés aux habits du sujet surveillé et ils échangent différents types de données collectées comme le rythme cardiaque, le taux de sécrétion de sueur, celui de sucre dans le sang, etc. Ces capteurs sont positionnés dans différents milieux, par exemple près du cœur, près de la cuisse, etc. Ils échangent les données entre eux car, à cause d'effets d'atténuations causés par le corps surveillé ou bien d'autres obstacles, tous les nœuds ne peuvent pas forcément se connecter à un autre réseau ou à une station de base pour transmettre les données collectées à l'établissement concerné. Dans le cas de la détection d'un nouveau réseau dans un contexte de mobilité, une adaptation au niveau radio entre les nœuds qui se connectent doit s'exécuter et en même temps une autre adaptation au niveau du routage doit se faire entre le nouveau réseau et l'ancien. La surveillance de la chaine de froid est une autre application dont les conditions sont proches de la surveillance du corps. Dans cette application, les nœuds doivent s'adapter dynamiquement d'une part pour optimiser la consommation d'énergie à cause des longues durées de surveillance et, d'autre part, pour s'adapter à la mobilité. Dans ce cas, la mobilité se présente sous le fait de transporter un ensemble de palettes à chacune desquelles un capteur est attaché, dans un camion par exemple. A cause de l'isolement ces capteurs forment alors un petit réseau coupé de l'extérieur, puis ils sont insérés plus tard dans un autre entrepôt qui contient beaucoup de nœuds. À cause de cette mobilité tous les nœuds doivent s'adapter et se reconfigurer pour construire un réseau convenable et efficace pour l'application.

2.4 Limitations des composants radio dans les capteurs sans fil

Même si en principe tous les types de technologies de communication sans fil peuvent être combinés avec les capteurs pour former des capteurs sans fil, les plus efficaces au niveau de la consommation d'énergie sont les technologies basées sur la norme IEEE 802.15.4. C'est le cas de la plupart des composants radio des capteurs sans fil du commerce (Figure 2.7).

Bande de fréquence utilisée par les capteurs	Débit en Kb/s	Débit de symboles	Modulation

868.0-868.6 MHz	20	20	BPSK
902.0-928.0 MHz	40	40	BPSK
2.4-2.4835 GHz	250	62.5	DSSS

Figure 2.7 : IEEE 802.15.4 - Paramètres de modulation

Comme la qualité du lien dépend fortement de la composante radio, il est important de sonder les caractéristiques des radios généralement employées dans les capteurs sans fil. Dès le début, on s'est attelé à la question de l'énergie. Les premières versions des composants radio comme Chipcon CC1000 et RFM TR1000 nécessitent une faible consommation d'énergie dans les deux modes de transmission ou réception. Néanmoins, le faible taux de transmission réalisable par ces dispositifs empêche leur utilisation dans des scénarios où un taux de transmission élevé est requis. Le besoin de débits de données supérieurs a motivé la conception des composants radios fonctionnant dans la bande ISM à 2.4 GHz, comme par exemple les familles CC2400 et CC2500. On plafonne malgré tout à 250kb/s.

Par ailleurs, les capteurs sans fil sont souvent livrés avec des antennes à faible gain intégrées dans la carte électronique. Même si l'antenne est sensée être omnidirectionnelle, le diagramme de rayonnement réel est irrégulier (cf. Figure 2.8, Figure 2.9). Ceci limite les mécanismes au niveau MAC et routage, qui supposent traditionnellement que le rayon de couverture est uniforme et les liens de communication symétriques.

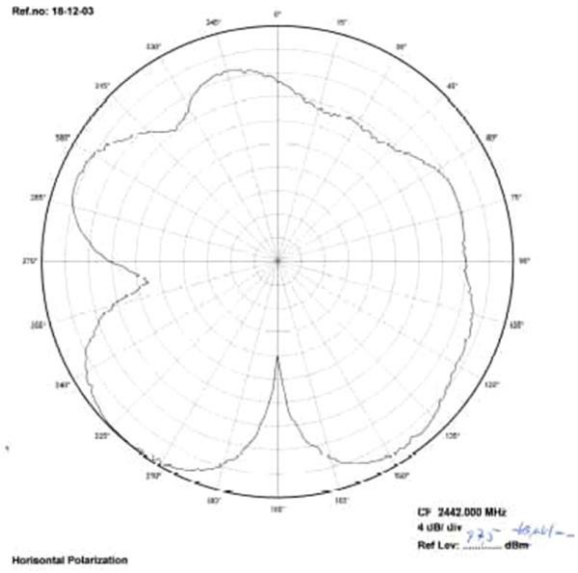


Figure 2.8 : diagramme de rayonnement de l'antenne en F-inversé au montage horizontal [TSM07]

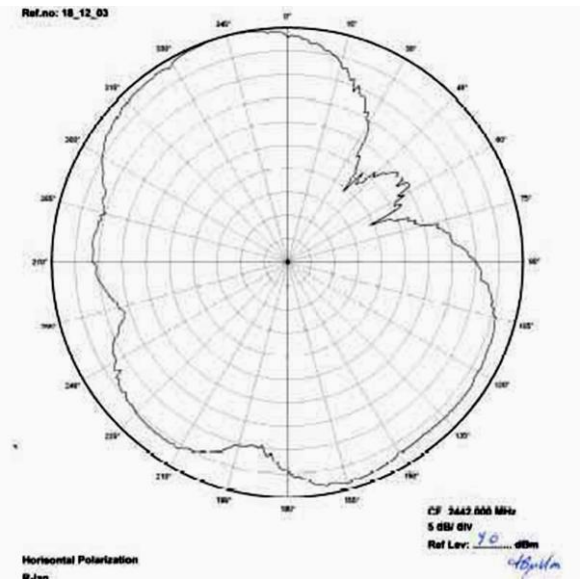


Figure 2.9: diagramme de rayonnement de l'antenne en F-inversé au montage vertical [TSM07]

La qualité de liens est extrêmement variable. Par exemple, elle est très dépendante de la position de la radio. Dans [BBDGKM09] les auteurs ont examiné l'influence de la topologie et l'environnement sur les caractéristiques de la radio. Ils ont montré que s'il y avait beaucoup d'obstacles à l'entourage, les pertes de paquet peuvent atteindre 45% (cf. Figure 2.10). En tout cas, la qualité du lien est très volatile dans le temps. Ils ont aussi montré que les pertes de paquets sont très élevées avec leurs capteurs si les nœuds sont placés par terre, en revanche, à 80cm au-dessus du sol, le taux de perte devient moins élevé.

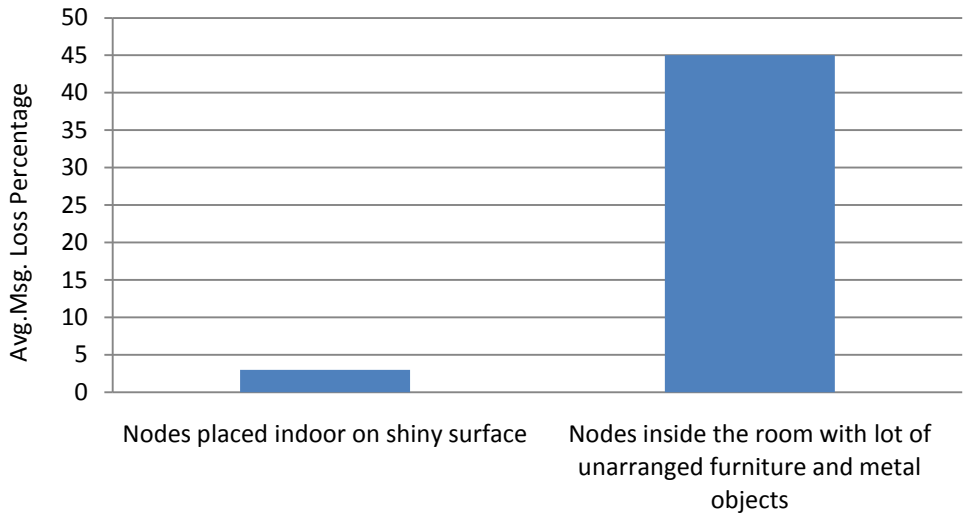


Figure 2.10 taux de perte de paquets dans différentes milieux selon [BBDGKM09]

Beaucoup d'analyses ont été faites sur le composant radio des capteurs sans fil. Des travaux ont examiné de nouvelles métriques [BKM12] pour évaluer les performances des liens formés. D'autres concernent l'implémentation de ces métriques dans les différents mécanismes de la couche MAC ou les protocoles de routage, comme dans [GSMB10].

La constatation de ces limites a motivé les travaux présentés dans la suite pour les dépasser.

2.5 Variation de l'état de l'environnement des capteurs

La composante radio d'un capteur sans fil permet de moduler différentes fréquences du spectre 2.4 GHz ainsi que de les écouter. Les modifications de l'environnement que perçoit la composante radio peuvent être attribuées en première approximation à deux causes : la mobilité du capteur qui se déplace d'un lieu à un autre, et la variation de l'état de l'environnement causée par une source d'interférence qui modifie l'environnement. Idéalement, la composante radio d'un nœud doit pouvoir détecter et distinguer ces différentes causes pour pouvoir s'adapter à chacune car, la connaissant, la meilleure contremesure peut être prise. Toute variation imprévisible de l'environnent peut impliquer une perte de paquet et donc un gaspillage d'énergie.

Dans le cas où l'unique cause de variation de l'état de l'environnement est la mobilité, les nœuds passent par un état transitoire après un déplacement, état où des messages de signalisation sont échangés entre les nœuds pour s'adapter au niveau couche liaison et au niveau routage. La mobilité selon son degré impacte les différentes couches de la pile protocolaire. En effet, ce n'est pas seulement l'action d'un déplacement physique, mais aussi la coupure ou la formation des liens avec les voisins et cela dépend fortement des caractéristiques de la composante radio déjà décrites dans le §2.4. Ceci revient à dire que le degré de mobilité est relatif à la vitesse d'établissement et de coupure de liaison entre les nœuds voisins. Plus ce degré est élevé plus il est difficile de former un réseau consistant. L'efficacité des protocoles de routage, en plus de leur capacité à construire une architecture efficace, est fonction de leur capacité à s'adapter le plus vite possible à la mobilité. Des propositions récentes, dont le but est d'accélérer l'adaptation à la mobilité, utilisent des méthodes de prédiction de position par apprentissage pour concevoir un algorithme de routage proactif (cf. [RS12], [DT12], [J12],

[CCSM12]). Malheureusement, ces méthodes consomment beaucoup d'énergie dont le coût n'est intéressant que pour un gain qui n'apparaît que dans un environnement mobile. En revanche, dans un environnement statique la complexité des traitements devient une source considérable de gaspillage d'énergie.

La variabilité de l'environnement radio peut ne pas être due à une quelconque mobilité mais à des phénomènes d'interférences. Ceux-ci sont typiquement dus aux autres technologies coexistantes sur la même bande (BlueTooth, fours micro-ondes, etc.), ou aux collisions de paquets transmis par d'autres nœuds du même réseau sans fil à cause de phénomènes de congestion, de terminaux cachés, etc. Le bruit blanc, plus ou moins important selon le milieu, est aussi bien sûr une cause de variabilité de l'environnement. Pour échapper à ces interférences plusieurs méthodes ont été proposées pour les couches physique et MAC.

Dans les deux paragraphes suivants, on présente les solutions les plus récentes proposées pour adapter les réseaux de capteurs à différents cas de variation de l'environnement : mobilité (§.2.6) ou interférences (§.2.7).

2.6 Adaptation à la mobilité

Les techniques d'adaptation sont assez variées: certaines sont « bio-inspirées », d'autres reposent sur des mécanismes de prédiction de mobilité, certaines sont propres à une seule couche tandis que d'autres sont multicouches, etc.

2.6.1 Structures et topologies existantes

Les topologies dans les réseaux de capteurs sont soit à infrastructure soit sans et dépendent de l'application et des contraintes imposées par l'utilisateur. Dans le cas de réseau à infrastructure, il y a une station de base qui est équipée de suffisamment de ressources et d'énergie pour pouvoir gérer toutes les fonctionnalités du réseau comme l'organisation des communications, la configuration des nœuds et le paramétrage de l'algorithme de routage, mais aussi qui est le point critique qui doit recevoir tous les messages du réseau. Il y a trois inconvénients à cette structure. Dans les topologies multi-sauts les nœuds les plus proches de la station de base épuisent rapidement leur énergie, ce qui accélère la fin du réseau. Si la connexion est directe avec la station de base les nœuds les plus distants épuisent aussi leur capacité énergétique puisqu'ils transmettent avec des puissances élevées pour l'atteindre. Enfin, en cas de mobilité et s'il y a une connexion en multi-sauts, prendre une décision pour inclure un nœud mobile prend du temps puisque toutes les décisions sont prises par la station de base. Dans cette thèse, nous nous intéressons à des réseaux sans infrastructure pour limiter leur coût de déploiement.

Dans les réseaux sans infrastructure, les nœuds doivent s'auto-organiser. En particulier, ils doivent s'accorder sur l'ordonnancement des communications et le routage. L'inconvénient de ce type de réseau est la complexité des algorithmes utilisés et le besoin d'une intelligence élevée pour faire les traitements complexes qui doivent garantir des solutions optimales pour la conservation d'énergie et l'adaptation à la mobilité.

Les topologies les plus courantes dans les réseaux de capteurs sont: la chaîne, l'étoile, la topologie maillée, l'arbre ou encore celles basées sur les clusters (qui sont souvent des arbres) [BTTM11].

Le principal avantage de la topologie en chaine est qu'elle met souvent en œuvre des protocoles simples, plutôt qu'un mécanisme de routage complexe par exemple, elle a une faible consommation d'énergie et nécessite peu de signalisation. En revanche, elle implique de longs délais, et pose des problèmes de passage à l'échelle.

La topologie en étoile est relativement simple à appliquer avec un potentiel pour réaliser une faible latence et une bande passante élevée. En revanche, si le point central est atteint d'une défaillance il y a une perte de tout le réseau. Elle ne passe pas à l'échelle et la communication est indirecte entre les nœuds feuilles.

Une topologie maillée est une topologie avec une connectivité complète entre les nœuds. Elle est tolérante aux pannes mais a un coût élevé de communication puisqu'en cas de densité élevée les nœuds doivent communiquer avec un grand nombre de voisins. L'utilisation d'une topologie de maillage est une considération primordiale dans tous les scénarios dans lesquels la fiabilité des communications et leur flexibilité sont prioritaires sur l'efficacité énergétique et la longévité du réseau [BGMS10].

Dans une topologie en arbre, les connexions entre les nœuds sont hiérarchiquement structurées, ce qui signifie que chaque nœud peut être un enfant d'un nœud de niveau supérieur et parent d'un nœud de niveau inférieur. Les topologies en arbre et hybrides arbre-maillé présentent une alternative à la topologie de maillage dans le cas où l'on veut optimiser les connections pour diminuer la consommation en énergie. Les topologies en arbre et en arbre-maillé présentent une bonne couverture, une bonne tolérance aux pannes, une faible latence et la possibilité de bande passante élevée. Toutefois, les parents (tête de cluster) peuvent consommer beaucoup d'énergie. Le choix d'un protocole de routage adapté aux caractéristiques du réseau (mobilité, densité, connectivité, etc.) est important, un protocole qui a besoin de signalisation complexe pouvant souffrir de délais de construction et d'une consommation élevée d'énergie.

2.6.2 Couche MAC pour les capteurs sans fil et techniques de réveil à la demande

Couche mac pour les capteurs sans fil

Les couches routages et MAC sont très liées dans les réseaux de capteurs. Par exemple, le fait que ceux-ci soient « endormis » et « réveillés » périodiquement impacte les décisions à prendre au niveau routage.

Les sources de gaspillage d'énergie dans les réseaux de capteurs sans fil sont connues: les collisions, les écoutes des messages destinés à d'autre destinataires, les écoutes excessives du canal, le coût spécifique de signalisations diverses, etc. Selon les différentes sources de gaspillage d'énergie, les chercheurs ont proposé différents types de protocoles MAC pour améliorer les économies d'énergie pour optimiser la durée de vie du réseau de capteurs. Dans [DF09] on présente les différentes catégories de mécanismes et protocoles utilisés dans la couche liaison qui optimisent la consommation d'énergie : mécanismes basés sur la contention, mécanismes basés sur le TDMA, mécanismes hybrides, et les mécanismes multi-couches.

Les mécanismes de la couche liaison basés sur la contention sont principalement du type CSMA ou CSMA/CA. Quand un nœud doit envoyer des données il est alors en concurrence avec d'autres sur le canal sans fil. Les nœuds utilisant des mécanismes basés sur la contention

n'ont pas besoin de se coordonner entre eux pour accéder au canal. En cas de collision les nœuds impliqués font un « backoff » pour une durée de temps aléatoire avant de tenter d'accéder au canal de nouveau. Les mécanismes et protocoles principaux basés sur la contention sont S-MAC [YHE02], T-MAC [DL03], et UMAC [SHE05]. S-MAC est un protocole qui se base sur un cycle périodique d'endormissement et de réveil des capteurs pour optimiser le coût énergétique. Pendant le cycle, un nœud a une étape de travail et une étape de sommeil. T-MAC est basé sur S-MAC, l'amélioration ajoutée est d'utiliser une période qui s'adapte aux différentes conditions: tous les messages sont transmis en rafales de longueur variable et les longueurs de rafales sont déterminées dynamiquement. UMAC fournit trois améliorations à S-MAC: la possibilité d'affecter aux différents nœuds des périodes de durées différentes, la longueur étant modifiée selon l'utilisation, des endormissements sélectifs peuvent être appliqués après la transmission. Dans ces protocoles de la couche liaison basés sur la contention, les nœuds sont autorisés à accéder indépendamment au médium partagé et ils n'ont pas besoin de former de cluster. De même, ils sont scalables et supportent l'insertion de nouveaux nœuds et l'extraction d'anciens. Ils adoptent différents mécanismes pour réduire le gaspillage d'énergie causé par les différentes sources de perte. Toutefois, l'efficacité énergétique des protocoles de la couche liaison basée sur la contention reste faible en raison des collisions, des écoutes excessives du canal et du coût ajouté de la signalisation.

Contrairement aux protocoles et mécanismes de la couche liaison basés sur la contention, les techniques basées sur l'ordonnancement des communications, du type TDMA donc, offrent par construction un schéma de communication libre de collisions en attribuant des slots de temps uniques à chaque nœud pour envoyer ou recevoir des données. Le premier avantage du TDMA est qu'il évite les interférences entre des liaisons sans fil adjacentes. Ainsi, le gaspillage d'énergie provenant de la collision des paquets est-il réduit. Deuxièmement, le TDMA peut résoudre le problème des terminaux cachés sans surcharge de messages supplémentaires (e.g. RTS/CTS) parce que les nœuds voisins transmettent à des instants différents. Les principaux protocoles de ce type sont µ-MAC [BRS05], DEE-MAC [SKJ05], SPARE MAC [CCC07]. Bien que le gaspillage d'énergie causé par les collisions soit évité, il y a un certain nombre d'inconvénients qui persistent. Le cluster, qui est largement utilisé par ces protocoles, a beaucoup de difficultés à modifier dynamiquement la longueur de trame et les affectations des slots de temps, ainsi peut-il difficilement passer à l'échelle. Le fait qu'un nœud soit une tête de cluster exige que ce nœud soit plus performant que les nœuds ordinaires, particulièrement au niveau des capacités de puissance de transmission et de calcul.

Des propositions de mécanismes et protocoles hybrides ont été faites, qui combinent les avantages des protocoles de la couche liaison basés sur la contention avec ceux des approches TDMA. Tous ces protocoles divisent le canal en deux parties. Les paquets de contrôle sont transmis sur le canal par accès aléatoire, et ceux de données dans les slots de temps prévus à cet effet. L'ordonnancement nécessite l'échange de paquets de contrôle. Les protocoles hybrides peuvent gagner en économies d'énergie et offrent une meilleure scalabilité et flexibilité que n'importe quel protocole à contention seul ou TDMA pur. Les plus récents sont Z-MAC [RWAP05], A-MAC [LN07] et IEEE 802.15.4 [STDS03]. Dans ces protocoles hybrides, la signalisation est importante et consomme beaucoup d'énergie. En outre, pour ces protocoles une latence élevée est introduite par la transition de l'état de signalisation à l'état de transmission de données et vice versa.

Aucune de ces approches n'est multi-couches mais toutes sont prévues pour fonctionner indépendamment des autres couches. La pile protocolaire traditionnelle responsable de la gestion du réseau est simple, cependant cela se traduit par un manque de flexibilité et une faible efficacité.

Dans [KP06], la conception d'un mécanisme multi-couches qui utilise le codage FEC et qui détermine les périodes de veille et sommeil pour les réseaux de capteurs sans fil à bande étroite est présentée. Cette conception prend en compte, de manière conjointe, les caractéristiques des couches physique et liaison. Un nouveau protocole multicouches "liaison-routage" a été présenté dans [CYD06] appelé MAC-CROSS. Les informations de routage de la couche réseau sont utilisées par la couche MAC pour optimiser la durée du sommeil de chaque nœud. Principalement, l'objectif de MAC-CROSS est de désactiver les composants radio des nœuds qui ne sont pas inclus dans le chemin de routage. Dans [SH07] une solution pour la détection d'intrusion est présentée. Dans cette solution, les interactions directes entre la couche application et les couches liaison et physique ont été exploitées. La couche réseau traditionnelle et la couche transport ont été supprimées, ce qui simplifie la pile protocolaire. Les fonctionnalités de la couche application sont fusionnées avec celles de la couche liaison. En se basant sur la détection de nouveaux noeuds la couche application contrôle les réveils et les endormissements du composant radio. Dans [KDB09] un protocole nommé PLACIDE pour la surveillance de la chaine de froid est développé. Il fonctionne au niveau de la couche liaison et routage pour consommer le minimum d'énergie dans ce contexte de chaîne du froid. L'idée est de ne s'éveiller que quelques millisecondes toutes les vingt minutes pour transmettre des informations captées. On utilise la propriété d'inertie thermique des denrées surveillées pour adapter le temps d'endormissement à vingt minutes. Par contre, rester éveillé aussi peu de temps requiert la mise en place d'un anneau bien synchronisé entre les nœuds. B-MAC [PHC04] est un protocole qui se base sur un cycle périodique d'endormissement et de réveil des capteurs. C'est un protocole de couche liaison mais B-MAC surpasse les performances des autres protocoles (ex : S-MAC) grâce à la reconfiguration, la rétroaction, et des interfaces bidirectionnelles avec les services des couches supérieures. Dans [JSH07], un mécanisme multi-couches appelé CLMAC est proposé. Le protocole se base sur un cycle périodique d'endormissement et de réveil des capteurs et, comme B-MAC, adapte dynamiquement ses temps de veille et de sommeil, et il comprend la distance de routage (nombre de sauts) dans le préambule du B-MAC et est donc un protocole multi-couches en ce sens. Le nombre de sauts indique la distance pour atteindre la station de base et par suite choisir le chemin optimal pour l'atteindre. En outre, sans grande table de routage, il permet aux nœuds de réduire le trafic de contrôle de routage.

La couche physique affecte la couche liaison lorsqu'elle change sa puissance d'émission et le type de modulation utilisé. La couche routage choisit les liaisons sans fil à garder comme relais de paquets à la destination, de sorte que la décision de routage change le niveau de contention de la couche liaison. Le contrôle de flux et le taux de congestion changent au niveau de la couche transport le volume de trafic sur chaque lien de communication tandis que les types de trafic ont un impact important sur la couche liaison. Les mécanismes ou protocoles multi-couches sont donc des moyens possibles d'amélioration des performances et par suite ils constituent une piste très importante de recherches.

Dans [CK10] les auteurs étudient et analysent le problème de la conception d'une couche liaison dans le contexte de minimisation de l'énergie des communications de capteurs sans fil.

Les deux protocoles MAC bien connus utilisés pour de nombreuses applications, l'accès aléatoire et le TDMA, ont été étudiés. En outre ils ont fait une comparaison entre L-MAC [HH04] et B-MAC en simulant leur comportement dans OMNET++. Leur étude a montré que, malgré de nombreuses propositions, aucune proposition parfaite n'a été publiée. Cependant, les solutions multi-couches et qui s'adaptent peuvent conduire à obtenir à la fois de hautes performances et une faible consommation d'énergie en même temps. D'après leur étude, les auteurs de [CK10] sont venus à la conclusion que la conception de protocole optimal au niveau liaison pour les capteurs sans fil avec des paramètres optimaux doit prendre en entrée les spécifications de l'application (la topologie du réseau et le taux de paquets générés), les exigences relatives aux consommations d'énergie demandées par une application, les retards et la fiabilité, et les contraintes de la couche physique (la consommation d'énergie et le taux de transmission).

Technique de réveil à la demande

De nouveaux mécanismes ont été développés pour optimiser la consommation d'énergie en évitant les écoutes à vide du canal imposées par la couche liaison. Des composants électroniques (radios de réveil) sont utilisés par un nœud pour déclencher un signal pour réveiller un nœud voisin quand sa radio de transmission de données est en mode arrêt [CLY+12].

Les équipements radios de réveil qui ont été proposés pour les réseaux de capteurs sans fil peuvent être classés en deux catégories principales:

- les équipements passifs: le récepteur n'utilise que l'énergie reçue de l'émetteur pour s'activer. Ils utilisent des diodes passives pour redresser le signal RF reçus et le convertir en impulsion envoyée, sur une broche du microprocesseur central, provoquant une interruption qui, à son tour, active la carte radio endormie en vue de l'envoi des données. Certains d'entre eux utilisent des circuits de type pompe à diode pour accumuler l'énergie du signal RF ([KCX+10], [Intelleflex10], [KL07], [SYQ07]).

- les équipements actifs: ils ont une alimentation autonome. Ils utilisent des filtres, amplificateurs, et des méthodologies de modulations spécifiques, tels PPM ou PWM, pour amplifier le signal RF désiré et supprimer le bruit pour améliorer la sensibilité. L'amplificateur représente une majeure partie de la dissipation de puissance dans cet équipement de réveil. Plusieurs travaux ([LR10], [KV10], [PGR09], [YLSL08], [DSB+09], [ATMEL12]), utilisent ce type de radio pour faire la signalisation puisqu'elle assure une meilleur portée de transmission. Des propositions récentes visent à utiliser les composants radio prévus pour la transmission des données aussi pour ces signaux de réveil au lieu de nécessiter une carte dédiée ([PGR09], [DSB+09], [ATMEL12], [SJL+11]). Celui développé dans [PGR09] nécessite un émetteur spécifique qui fonctionne dans la bande 2 GHz et peut aussi être utilisé comme radio de transmission de données. Cependant, ([DSB+09], [ATMEL12]) peuvent utiliser des radios basées sur IEEE 802.15.4 sans aucune modification nécessaire pour être utilisée comme radio émetteur de signaux de réveil.

Les couches MAC et protocoles développés dans la littérature n'utilisent pas les possibilités offertes par ces dernières avancées. Nous proposons justement dans cette thèse un mécanisme qui en tire parti.

2.6.3 Protocoles d'auto-organisation et méthodes de prédictions pour les réseaux de capteurs

Auto-organisation :

À cause de sa nature distribuée, la formation d'un réseau de capteurs sans infrastructure pose le problème de la façon de choisir une structure optimale pour sa construction. Plusieurs mécanismes et protocoles distribués ont été développés et proposés pour faire la gestion des réseaux de capteurs sans fil. Ils se répartissent en deux catégories: organisation sans clusters, totalement distribuée, et avec clusters, regroupement des nœuds dans des ensembles gérés par un des nœuds de cet ensemble, lequel tient lieu de station de base dans le cluster.

L'utilisation de clusters est très commode pour l'agrégation de données dans le cas d'un réseau très dense. L'utilisation des clusters est naturelle aussi dans le cas où le réseau contient des nœuds puissants et d'autres moins, les nœuds puissants pouvant former les clusters et en devenir les chefs. Ces derniers peuvent gérer toutes les ressources de leurs clusters et reconfigurer les paramètres des nœuds leur appartenant. Le fait de construire des réseaux en clusters doit optimiser la consommation des ressources des nœuds constituant ces réseaux et est surtout un moyen d'assurer le passage à l'échelle.

La complexité qui se trouve derrière le choix du bon nombre et de la bonne taille des clusters ainsi que le choix des chefs de clusters elles-mêmes sont les principaux inconvénients des réseaux en clusters. Les clusters de petites tailles créent des congestions et des clusters de grandes tailles épuisent rapidement les ressources de la tête de cluster. LEACH [HCB00] est un exemple de ce type de protocoles, et l'un de plus connus, pour former des clusters. C'est un protocole hiérarchique basé sur les clusters qui cherche à optimiser le nombre de chefs des clusters et aussi à répartir entre les nœuds la consommation d'énergie spécifique à la fonction de tête de cluster.

L'intérêt des architectures à clusters et sans clusters est examiné dans [VX06]. Les auteurs ont trouvé que les réseaux à clusters ne sont pas nécessairement plus performants que ceux sans clusters. La condition qui assure une performance supérieure pour les réseaux à clusters est le fait que les clusters formés doivent exister dans les isoclusters du phénomène surveillé, c'est-à-dire qu'il y ait une relation entre les clusters naturels des mesures captées et les clusters logiques du réseau. En revanche, ils ont montré que la circonférence des clusters ne doit pas nécessairement être égale à la circonférence de l'isocluster.

[KJT11] présente un état de l'art des algorithmes de clusterisation pour les réseaux de capteurs. Il présente une taxonomie des algorithmes efficaces en consommation d'énergie. En outre [KJT11] décrit chronologiquement Leach et ses descendants dans les réseaux de capteurs.

LCA [BE81] est un des plus anciens protocoles de clustérisation. [BE81] indique que LCA fut développé pour les réseaux de capteurs filaires puis modifié pour fonctionner avec les capteurs sans fil. Dans LCA chaque nœud dispose d'un numéro d'identification unique et les chefs de clusters sont choisis en se basant sur celle-ci. Le nœud qui a l'ID le plus élevé dans le cluster, et dont aucun de ses voisins n'est une tête de cluster, est élu tête de cluster. LCA se basant sur le TDMA pour ordonnancer les communications entre tous les nœuds, LCA est applicable uniquement pour les petits réseaux mais pour les réseaux les plus grands, il entraîne

des retards élevés sur les communications. Les auteurs proposent l'algorithme LCA2 afin d'éliminer l'élection d'un trop grand nombre de chefs des clusters, défaut de LCA.

PEGASIS [LR02] est un algorithme de sélection des chefs de clusters et de construction des clusters. Il présente une amélioration par rapport à LEACH. PEGASIS est plus efficace que LEACH. Dans PEGASIS, la communication entre les nœuds est en chaîne : chaque nœud communique seulement avec un de ses voisins les plus proches puis, à tour de rôle, un nœud communique directement avec la station de base, ce qui élimine une grande partie de l'énergie gaspillée par les en-chefs.

La littérature contient beaucoup d'autres protocoles (cf. Figure 2.11), chacun adapté à des conditions précises, mais jusqu'à maintenant il n'existe pas de protocole parfait optimal pour toutes les conditions et toutes les applications. Les recherches actuelles se concentrent sur l'adaptation, voire le changement, dynamique de protocole en fonction des conditions du réseau. Dans cette thèse, nous explorons justement la voie du changement dynamique de protocoles.

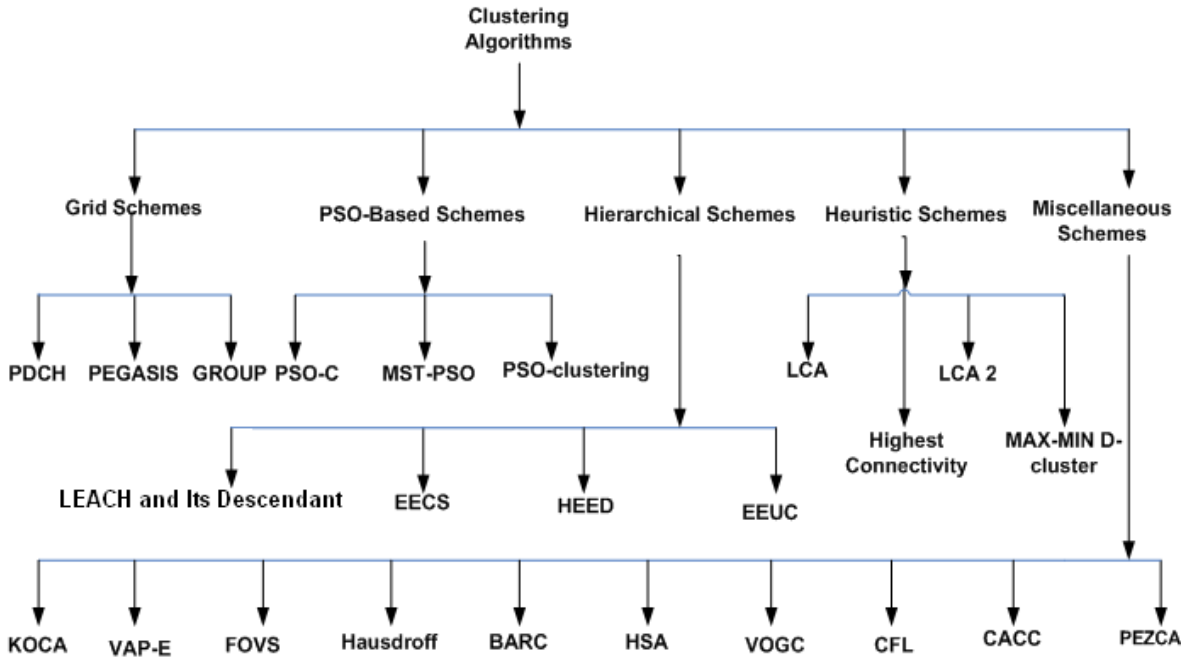


Figure 2.11: taxonomie des algorithmes de clusterisation, extrait de [KJT11]

Pour compléter ce paragraphe, il faut mentionner les méthodes bio-inspirées (ex : [GHF05], [SSS07], [DA10]). Il est à craindre que celles-ci, avec toute l'intelligence de leurs algorithmes, ne soient pas très efficaces dans les capteurs : un algorithme bio-inspiré a besoin de temps pour converger, ce qui demande une signalisation entre voisins qui consomme de l'énergie et la réservation d'une grande espace mémoire pour le stocker lui-même. Il n'y a pas aujourd'hui, à notre connaissance, d'implantation de telles propositions.

Dans [BTTM11] un travail intéressant propose une classification qui permet, sur la base de plusieurs critères, de déterminer dans une situation donnée les protocoles adéquats à utiliser. Il est contemporain au nôtre ([NMB11]) et ressemble par certains côtés dans la mesure où il nous a fallu aussi lister les différents contextes que traverse le réseau de capteurs que nous considérons dans [NMB11] et déterminer des protocoles adaptés selon les situations mais la

différence majeure est que les auteurs ne proposent pas de mécanisme pour repérer ces situations à la volée et changer dynamiquement de protocole.

Méthodes de prédictions de mobilité en vue de l'amélioration de l'adaptation des protocoles de routage :

[RS12] propose une solution pour résoudre le problème de la mobilité des chefs de clusters ,. Cette approche utilise une technique de prédiction de mobilité basée sur la moyenne glissante exponentielle pour identifier le mouvement des chefs de clusters. Chaque nœud du réseau échange des messages avec les voisins et met à jour l'algorithme de prédiction des connections qui se forment.

Dans [DT12] une solution est proposée pour les réseaux cellulaires pour améliorer le « hand over» entre les nœuds mobiles et les stations de bases. Cette solution propose l'enregistrement des coordonnées des nœuds mobiles puis la construction d'un modèle de mobilité. La complexité de cette construction et le besoin d'un grand espace mémoire pour stocker les informations de localisation rendent cette approche difficilement applicable dans les réseaux de capteurs.

La proposition de [CCSM12] repose sur une technique de prédiction de position future des nœuds des réseaux MANETs qui utilise des méthodes d'apprentissage automatique qui se basent sur la régression des différentes positions d'un nœud. Cette approche exige que la position des nœuds soit connue.

Ces solutions utilisant l'apprentissage ont l'inconvénient majeur de présenter un coût élevé d'acquisition et de stockage des informations dont ils ont besoin pour avoir une bonne approximation du modèle de mobilité.

2.7 Adaptation à la variation de l'état de l'environnement

Pour éviter la perte de paquets à cause des interférences, une grande variété de solutions est proposée. Beaucoup de techniques ont été développées pour filtrer les bruits de différentes sources comme les bruits thermiques, cosmique, etc. la solution consistant à supprimer ces bruits quand ils sont de faible puissance concerne la conception de la couche physique et le développement des filtres [S11b]. Nous nous intéressons dans cette thèse à la détection des interférences qui peuvent modifier totalement un signal et ne peuvent pas être supprimées par des filtres à cause de leur forte puissance, et, plus précisément, celles qui provoquent des erreurs sur les paquets reçus et qui proviennent des technologies qui coexistent sur la même bande de fréquence et qui sont les plus abondants : WiFi, BlueTooth, ZigBee.

Une analyse sur l'impact de différentes sources d'interférences est d'abord présentée puis on aborde les différentes solutions pour les éviter.

2.7.1 Sources d'interférences et leur impact

Dans [ASL+06], les auteurs ont étudié par simulation l'impact de la coexistence d'un réseau de capteurs avec le WiFi, le BlueTooth et les fours micro-ondes sur les systèmes IEEE 802.15.4. Les résultats ont montré que même un faible trafic WiFi a un grand impact sur l'IEEE802.15.4 contrairement aux équipements BlueTooth qui ont un faible effet. Les fours à micro-ondes

présentent une source d'interférence très puissante mais les résultats ont montré que cet effet est fortement lié aux canaux utilisés.

Dans [TS09], les auteurs on fait une analyse de la probabilité de collision entre l'IEEE 802.15.4 et l'IEEE 802.11b, par simulation, et suivant différentes topologies. Leur analyse a montré que les collisions augmentent linéairement avec le nombre de réseaux IEEE802.11b.

Dans [HXB+09] des mesures expérimentales ont montré que l'effet des interférences du BlueTooth est faible, le taux de perte de paquets ne dépassant pas 4%. L'effet du WiFi peut être de moins de 10% s'il y a une bonne méthode de sélection de canal. Quant au four à micro-ondes, les pertes peuvent atteindre 8% si la distance qui sépare le nœud du micro-ondes est inférieure à 1,5m. Les auteurs ont pu donner un modèle de perte intéressant et présenté Figure 2.12. Leur taux de perte de paquets ZigBee en présence de BlueTooth est présenté Figure 2.13, leur taux de perte de paquets en présence de WiFi est présenté Figure 2.14 et celui de perte de paquets en présence d'un four à micro-ondes est présenté Figure 2.15.

$$BER = \begin{cases} Q(\sqrt{11SINR}) & ,for 802.11b\ with\ 1Mb/s \\ Q(\sqrt{5.5SINR}) & ,for 802.11b\ with\ 2Mb/s \\ \left(\frac{8}{15}\right)\left(Q\left(14\sqrt{8SINR}\right)+Q\left(\sqrt{16SINR}\right)\right) & ,for 802.11b\ with\ 5.5Mb/s \\ \left(\frac{128}{255}\right)\left(24Q\left(\sqrt{4SINR}\right)+16Q\left(\sqrt{6SINR}\right)+174Q\left(\sqrt{8SINR}\right)\right. & \\ \left.+16Q\left(\sqrt{10SINR}\right)+24Q\left(\sqrt{12SINR}\right)+Q\left(\sqrt{16SINR}\right)\right) & ,for 802.11b\ with\ 11Mb/s \\ \left(\frac{1}{2}\right)\exp\left(\frac{-SINR}{2}\right) & ,for 802.15.1 \\ \left(\frac{8}{15}\right)\left(\frac{1}{16}\right)\left(\sum_{i=2}^{16}(-1)^i C_{16}^i \exp\left(-20SNIR\left(1-\frac{1}{i}\right)\right)\right. & ,for 802.15.4 \end{cases}$$

Figure 2.12 : taux d'erreur binaire [HXB+09]

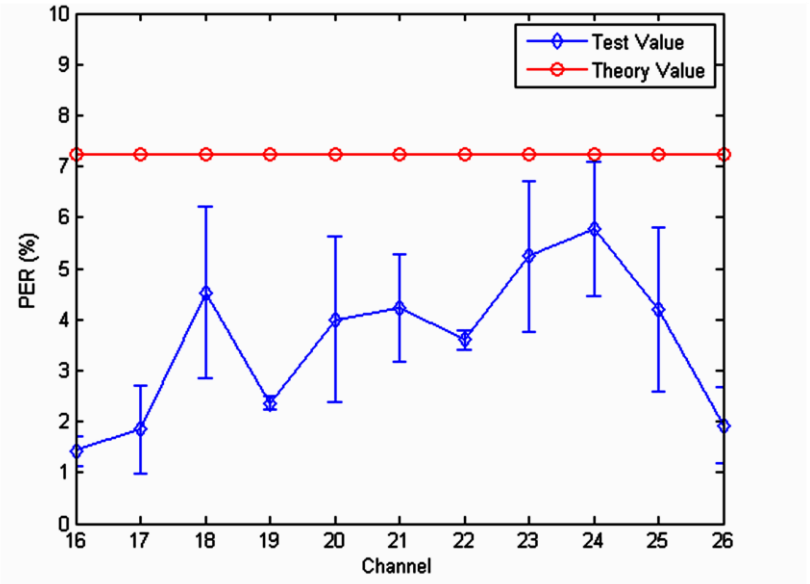


Figure 2.13 taux de paquets ZigBee subissant des erreurs à cause de la coexistence avec BlueTooth

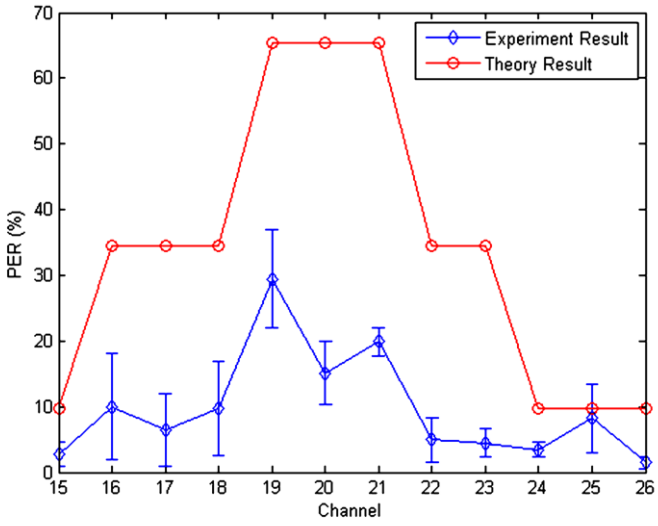


Figure 2.14 taux de paquets ZigBee erronés à cause de la coexistence avec WiFi

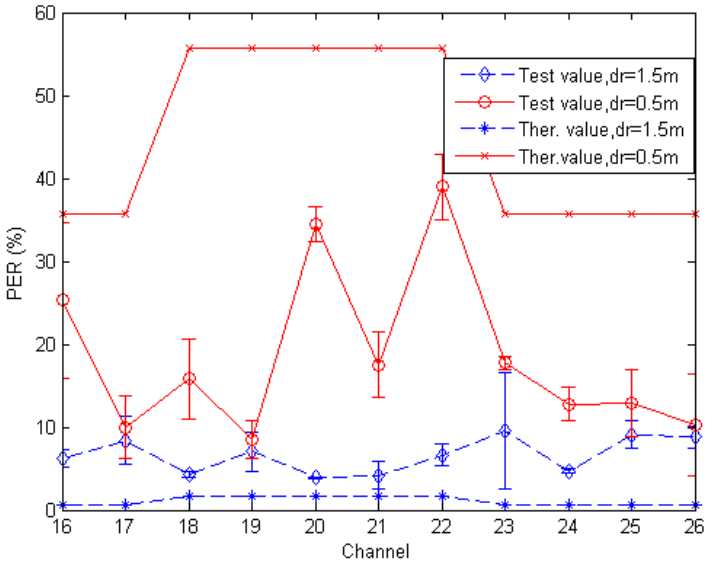


Figure 2.15 taux de paquets ZigBee subissant des erreurs à cause de la coexistence avec un four à micro-ondes

Les corruptions dans un paquet transmis sont causées par les interférences. L'importance et la forme de ces corruptions dépendent de la bande de fréquences utilisée, de la durée de transmission d'un paquet, du type de modulation, de la puissance de transmission et de l'instant de la collision (au début, au milieu, à la fin d'un paquet, etc.). La Figure 2.16 et la Figure 2.17 présentent les spécifications et les caractéristiques du WiFi, du BlueTooth et de l'IEEE802.15.4.

	IEEE 802.15.4	**IEEE 802.11b**	**IEEE 802.11g**
Durée de transmission de paquet	4ms	1ms	2ms

SIFS	192µs	10µs	10 µs
Durée de BackoffTimeslot	320 µs	20 µs	9 µs
CWmin	7	31	15
CCA	128 µs	-	-
ACK	-	14 octets[STDW99]	14 octets [STDW99]
DIFS	-	50 µs	28 µs
Puissance de Transmission	0dBm	20dBm	20dBm
Sensibilité du récepteur	-85dBm	-76dBm	-82dBm
Largeur de bande	2 MHz	22MHz	22 MHz
Débit de transmission	250 Kbps	11 Mbps	6 Mbps
Fréquence centrale	2410MHz	2412 MHz	2412 MHz
Taille de paquet	128 Octets	1500 Octets	1500 Octets

Figure 2.16: caractéristiques des standards IEEE802.15.4, IEEE802.11b et g importantes pour la compréhension des phénomènes de collisions.

Standard	BlueTooth	ZigBee	WiFi
IEEE spec.	802.15.1	802.15.4	802.1 1a/b/g
Bande de fréquence	2.4 GHz	868/915 MHz; 2.4 GHz	2.4 GHz; 5 GHz
Débit Max	1 Mb/s	250 Kb/s	54 Mb/s
Couverture nominale	10m	10 - 100 m	100 m
Puissance de TX nominale	0 - 10 dBm	(-25) - 0 dBm	15 - 20 dBm
Nombre de canaux RF	79	1/10; 16	14 (2.4 GHz)
Largeur de bande d'un canal	1 MHz	0.3/0.6 MHz; 2 MHz	22 MHz
Type de modulation	GFSK	BPSK (+ ASK), O-QPSK	BPSK, QPSK
Etalement	FHSS	DSSS	COFDM, CCK, M-QAM DSSS, CCK, OFDM
Mécanisme d'accès	Adaptive freq. hopping	Dynamic freq. selection	Dynamic freq. selection,transmit power control (802.1 1 h)
Cellule de base	Piconet	Star	BSS
Extension de cellule de base	Scatternet	Cluster tree, Mesh	ESS

Nombre max de noeuds par cellule	8	> 65000	2007
Méthode de cryptage	EQ stream cipher	AES block cipher (CTR, counter mode)	RC4 stream cipher (WEP),AES block cipher
Authentification	Shared secret	CBC-MAC (ext. of CCM)	WPA2 (802.11i)
Protection de données	16-bit CRC	16-bit CRC	32-bit CRC

Figure 2.17: caractéristiques du WiFi, BlueTooth et 80215.4 importantes pour la compréhension des phénomènes de collisions.

2.7.2 Méthodes de détection de coexistence

Suite à l'analyse de l'impact des interférences (§ précédent 2.7.1), plusieurs solutions ont été proposées. Dans [HLL+07] les auteurs ont modélisé un scénario de coexistence entre l'IEEE802.15.4 et l'IEEE802.11b et ils ont constaté que les performances des systèmes basés sur l'IEEE802.15.4 se dégradent en présence d'IEEE802.11b. Ils ont proposé un algorithme pour éviter les interférences en faisant des sauts de fréquences selon la puissance des signaux qui interfèrent.

Dans [YLN10] et [BGS07] le seuil de puissance servant à déterminer par l'écoute une occupation du canal pendant la phase de contention de ZigBee est ajusté afin de minimiser la perte de paquets. Dans [YLN10] les auteurs ont simulé leur proposition sur OPNET tandis que [BGS07] présente une validation par expérimentations sur plate-forme réelle. Pour les deux approches la modification du seuil diminue les pertes de paquets causées par l'inhibition de transmissions mais ne résout pas le problème de collisions et d'interférences entre les différentes technologies.

Les auteurs de [PPSG09] analysent l'énergie du spectre en présence de WiFi et Bluetooth pour sélectionner les meilleurs canaux pour la communication. Plus précisément, la densité spectrale de puissance du WiFi et de Bluetooth sont analysées en utilisant un capteur. En se basant sur les résultats de l'analyse, ils ont proposé un modèle qui détermine la capacité du canal et, par suite, si cette capacité dépasse un certain niveau, il faut choisir un autre canal. Les analyses concernent le WiFi et le BlueTooth mais la méthode proposée pour détecter la capacité du canal n'identifie pas les sources d'interférences et par conséquent, si l'interférence est causée par une forte contention des nœuds IEEE802.15.4, tous les nœuds utilisant cette méthode feront des sauts perpétuels de fréquences, conduisant à une consommation très élevée d'énergie.

Dans [LPL+10], on présente une analyse sur les interférences et les corruptions causées par le WiFi qui peuvent affecter les paquets de ZigBee. Les nœuds ZigBee peuvent se trouver dans une région où leur transmission n'est pas détectable par les nœuds WiFi et, par suite, à cause de leur forte puissance, les transmissions WiFi peuvent corrompre d'une manière uniforme n'importe quel bit des paquets ZigBee. Pour annuler les corruptions [LPL+10] présente BuzzBuzz, mécanisme qui ajoute des bits de redondance.

Dans [HXZZ10] les auteurs ont proposé un modèle de trafic WiFi, à partir de mesures de trafic réel. Ils ont trouvé que les trafics WiFi ont une durée d'inter-arrivées des rafales de

paquets qui suit une distribution de Pareto. Ils proposent alors de tirer parti de la connaissance de la forme de cette loi pour adapter les transmissions des capteurs sans fil. En particulier, ils adaptent dynamiquement la taille des paquets en fonction de la longueur des temps de silence WiFi. Cette idée est intelligente mais a des limites. La méthode proposée pour détecter le modèle de trafic repose sur les valeurs de RSSI échantillonné à partir du canal. Le fait d'utiliser le RSSI fait que les nœuds ne peuvent pas distinguer les différents types du trafic WiFi. De plus, l'échantillonnage fréquent du canal entraîne une consommation d'énergie élevée et, finalement, cela occupe aussi le composant radio et l'empêche de transmettre ou d'écouter pendant ces périodes d'échantillonnage.

Pour contrer l'impact des interférences les diverses méthodes consistent à ajouter de la redondance de transmission, utiliser la diversité de fréquences, la diversité temporelle et spatiale, utiliser du FEC ou des mécanismes de retransmissions automatiques (ARQ). Ces solutions proposées ne sont que des traitements topiques or il serait intéressant de connaître la source de l'interférence pour déterminer l'adaptation ou la contremesure la plus adéquate.

Le mécanisme ZiFi proposé dans [ZXX10] cherche à déterminer la présence d'un réseau WiFi spécifiquement au moyen du composant radio d'un capteur mais le but n'est pas d'éviter les interférences mais de proposer une solution peu consommatrice d'énergie par rapport aux méthodes actuelles pour détecter la présence d'un réseau WiFi pour des équipements à faibles ressources comme des PDAs afin de leur permettre de se connecter à ce réseau WiFi. Cette méthode demande moins d'énergie que des écoutes ou des recherches actives via le protocole 802.11 et elle permet de détecter la signature spécifique des balises WiFi à partir de mesures de RSSI sur un composant ZigBee mais les échantillonnages périodiques qu'elle nécessite requièrent encore trop d'énergie pour pouvoir détecter à la volée un réseau WiFi concurrent pendant la vie d'un capteur. De plus, elle ne permet pas de distinguer les paquets WiFi de paquets ZigBee.

Les solutions basées sur l'échantillonnage de la puissance du canal souffrent d'au moins un des problèmes suivants. 1) Ils sont basés sur la détection de la puissance du canal physique et donc la transmission des nœuds ZigBee occupant le canal ne peut pas être différenciée de la transmission de WiFi ou de Bluetooth. 2) Un taux d'échantillonnage élevé est nécessaire pour détecter les paquets WiFi, au moins deux fois plus élevé que la durée de transmission d'un paquet, ce qui nécessite un coût énergétique élevé et des temps de traitement relativement longs pour les nœuds ZigBee. 3) Ces approches nécessitent l'occupation du composant radio du capteur sans fil pour l'échantillonner pendant un temps dédié et demandent aussi du temps pour converger.

2.7.3 Radio cognitive distribuée et coopération dans le réseau

Les travaux présentés au §.2.7.2 visent à développer des méthodes intelligentes pour pouvoir accéder au médium partagé et, finalement, à développer une certaine forme de cognition dans le réseau. Elles ressemblent beaucoup à celles développées pour la radio cognitive [H05]. La cognition est plus performante quand un nœud coopère avec ses voisins et lorsque celui-là se coordonne avec ceux-ci.

La grande densité des nœuds dans certains réseaux de capteur fait d'eux de bons objets d'applications des méthodes de coopérations et d'algorithmes distribués. Les seules préoccupations concernent les dépenses énergétiques :

1- Il ne faut pas échanger trop de messages de signalisation entre les nœuds puisqu'ils causent beaucoup de dépenses d'énergie.

2- l'information échangée ne doit pas être utilisée directement sans vérifier préalablement qu'elle améliore les performances des voisins autrement il y a risque de gaspillage d'énergie.

La cognition est généralement définie comme « un processus impliqué dans les processus d'acquisition de connaissances et de compréhension, y compris la pensée, le savoir, le souvenir, le jugement, et la résolution de problèmes » [H05]. Une radio cognitive apprend de l'environnement en analysant le médium de communication et tire des décisions intelligentes (cf. §.2.7.2 pour des exemples). Ce processus d'apprentissage est souvent un processus long et complexe en soi, avec une complexité croissante avec la taille de l'espace d'observation.

La problématique étudiée dans le contexte de la radio cognitive est généralement de mettre au point des méthodes pour permettre à un nœud qui n'a pas de licence particulière garantissant son accès à une fréquence de l'utiliser si aucun utilisateur licencié n'a besoin d'y accéder. Se pose alors des questions comme celle du meilleur échantillonnage du spectre, de repérer la fréquence qui peut être utilisée, de minimiser le taux de collision, de prédire l'occupation du spectre, etc. (ex : [WR11], [DSB12], [AFS12]). Ces méthodes ont été appliquées aux réseaux de capteurs. Dans [VA12] les auteurs présentent une analyse sur les radios cognitives distribuées utilisées par les capteurs sans fil. Spécifiquement, ils distinguent trois topologies de cognitions distribuées, qui sont déduites des différentes approches et implémentations, connues sous le nom topologie en arbre, en série et parallèle (cf. Figure 1.18, Figure 1.20 et Figure 1.21).

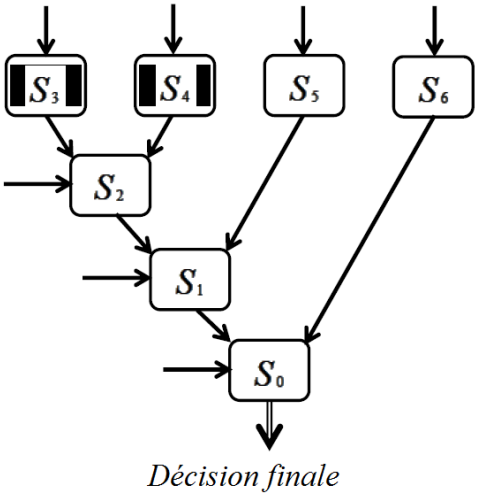


Figure 2.18 : Décision distribuée utilisant une topologie en arbre, extrait de [VA12]

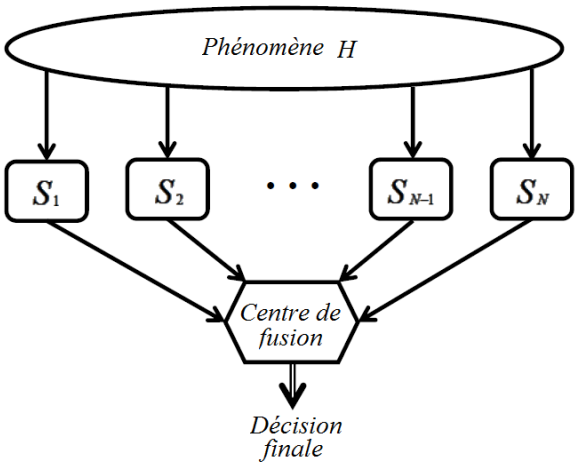


Figure 2.19 : Topologie en parallèle avec un centre d'agrégation de données, extrait de [VA12]

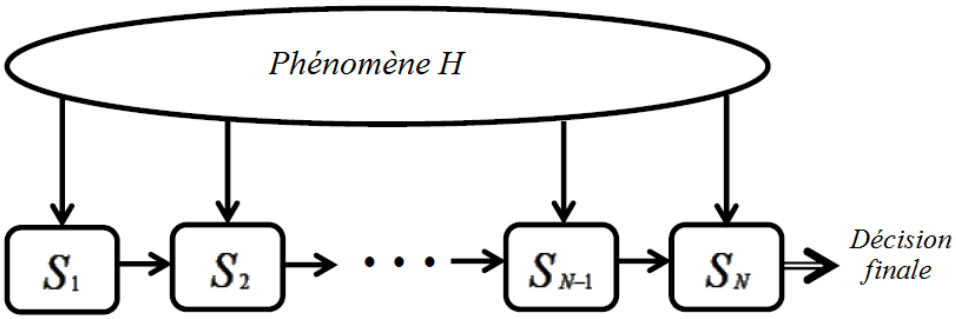


Figure 2.20 : décision distribuée utilisant une topologie en série, extrait de [VA12]

[VBI11] présente une enquête sur des techniques de cognition appliquées sur les réseaux de capteurs et propose un cadre pour la radio cognitive des réseaux de capteurs pour assurer l'accomplissement des objectifs, de bout en bout, précisés par l'application. Dans le cas où plusieurs objectifs sont demandés par les différentes couches gérant la communication des nœuds, le cadre proposé assure une performance globale optimale du réseau selon ces objectifs.

Dans [UV08] les auteurs proposent une méthode pour les radios cognitives qui se base sur la coopération entre les nœuds pour la détection de l'énergie d'un canal, et s'assure que les utilisateurs secondaires accèdent à un canal qui soit libre d'un utilisateur primaire. Cette détection est accomplie par une observation reposant sur un modèle log-normal de la puissance reçue et la corrélation des observations entre les capteurs voisins. Le problème des méthodes coopératives existantes est que les nœuds impliqués dans les opérations pour prendre une décision sont obligés de faire leur propre analyse du canal et de considérer l'avis des voisins. Cette complexité de traitement est importante et nécessaire dans le cas où il y a un utilisateur primaire qui a une licence pour utiliser un canal et un utilisateur secondaire non licencié, ce qui n'est pas le cas pour les réseaux de capteurs qui utilisent une bande dont l'accès ne nécessite pas une licence mais un moyen pour échapper aux interférences.

Un nouveau concept étendant celui de radio cognitive coopérative et nommé docition est proposé dans [GGBD10]. La docition se base sur le paradigme enseignant-élève. L'enseignant n'est pas (seulement) censé enseigner à l'élève les résultats finaux (ex: sous forme de «je sens que le spectre est occupé »), mais plutôt les éléments des méthodes d'y arriver. En même temps, ces informations ne sont pas imposées à l'élève, mais il peut les considérer comme les

ignorer. Ce paradigme a été proposé dans le contexte d'un réseau cellulaire ayant une infrastructure qui, de plus, est fixe. La cognition étant basée sur l'apprentissage de la dynamique de l'environnement, en tenant compte des états du système présents et passés, modélise le système en utilisant le « Q-Learning» [HH00]. La docition utilise cette modélisation dans l'intelligence distribuée et échange les Q-tables. Elle introduit donc l'apprentissage au cœur même du processus d'échange au lieu de se contenter seulement de l'échanges de mesures brutes. Ce type d'informations échangées donne la liberté à l'élève de prendre une décision plus dépendante de sa propre situation que de celle de son enseignant. Une fois qu'un élève a accompli son apprentissage, il peut alors prendre l'action qui optimise le gain selon sa situation particulière. Il serait intéressant d'investiguer son applicabilité dans les réseaux de capteurs sans fil qui n'ont pas d'infrastructure et sont mobiles.

La grosse problématique dans les réseaux docitifs est l'optimisation de la transmission d'information minimale. Des méthodes avancées voient le jour en ce moment qui visent à adapter les instants d'échantillonnage et de ne transmettre que le minimum d'information. Par exemple, dans [FGM11] une méthode permet d'adapter dynamiquement les instants de mesures en fonction de l'historique des mesures. Comme le récepteur connaît la méthode appliquée par l'émetteur qui sonde l'environnement, il n'est plus nécessaire que ce dernier envoie au récepteur les instants de mesures.

2.8 Simulateurs et système d'exploitation TinyOs

2.8.1 Simulateurs

Après avoir développé un nouveau concept, il faut choisir un bon simulateur qui peut rendre compte autant que possible du cas étudié, reflétant les caractéristiques dont on a besoin dans son étude et présentant le moins de complexité possible aussi bien pour la programmation que pour l'analyse. Une variété de simulateurs et leur comparaison sont présentées dans [EVMPG05]. Il y a trois types de simulateurs : simulateurs à événements discrets, simulateurs à temps continu, simulateurs hybrides.

Beaucoup de simulateurs existent sur le marché, soit dédiés spécifiquement aux réseaux de capteurs, soit généraux et incorporant des bibliothèques de modèles permettant de simuler différentes types de réseaux.

Dans la première catégorie, on compte des simulateurs comme OMNET++ [OM12], JiST [BHR04] et SSFN [SSF12] ou encore NS2 [NS212]. Les trois premiers ont des bibliothèques de modèles de protocoles moins étendues que NS-2, ce qui augmente le temps de développement. La qualité de NS2 laisse aussi parfois à désirer en termes de « propreté du code ». Quant à NS3 [NS312], il est développé avec plus de rigueur et mieux intégré mais n'en est qu'à ses débuts et donc n'a que peu de modèles disponibles. Si le développement démarre de zéro les logiciels J-Sim [SCH+05] ou Ptolemy II [PTO12] offrent le maximum de souplesse puisqu'ils offrent des APIs simples à invoquer.

En ce qui concerne les performances d'exécution, on peut s'attendre à de meilleures performances des simulateurs dont les moteurs sont développés en C/C++ que de leurs homologues Java. Toutefois, les auteurs de simulateurs récents comme JIST/SWAN affirment que leurs performances sont meilleures que celles de NS-2 ou GloMoSim [GMI12] (dans sa version séquentielle). Les simulations parallèles doivent mieux passer à l'échelle que les

simulations séquentielles. L'inconvénient est l'augmentation de complexité de programmation. Les simulateurs parallèles comme GloMoSim (dont l'objectif est la performance plutôt que le passage à l'échelle) peut simuler jusqu'à près de 10.000 nœuds sans fil. DaSSF [DSSF12], outil parallèle, dont l'objectif principal est le passage à l'échelle, autorise la simulation de topologies de réseaux dont le nombre de nœuds peut atteindre100.000 éléments filaires. Tous les simulateurs fournissent une interface graphique. NS2, OMNET++, NCTUns2.0 [NCT12], J-Sim et Ptolémée offrent de puissantes bibliothèques graphiques pour l'animation, le traçage et le débogage.

Dans la catégorie des simulateurs dédiés aux réseaux de capteurs on trouve TOSSIM [TOS03], EMTOS [EMS04] ou ATEMU [PBM+04]. Ils sont capables de faire de la simulation en intégrant le code réel qui est prêt à être implémenté dans un capteur. TOSSIM utilise TinyViz comme outil de visualisation. TinyViz est une application Java qui fournit des informations utiles de débogage. En outre, elle peut contrôler et piloter les éléments de simulation. Les utilisateurs peuvent développer leurs propres composants, qui écoutent à partir de TinyViz les événements de TOSSIM et par suite réagir. EmView est un outil très similaire, dans ce cas écrit en C, pour EMTOS. TOSSIM a été conçu pour simuler le comportement d'un réseau de capteurs au niveau applicatif mais pas spécifiquement pour la simulation d'une couche radio. Il n'a donc qu'un modèle extrêmement simplifié de la couche radio. Par exemple, les liens radios sont considérés comme des liens dans un graphe et les interférences entre transmissions ne sont pas prises en compte dynamiquement.

Dans la première partie de cette thèse, nous avons choisi de développer nous même en C notre propre simulateur pour des raisons de performance de l'exécution de la simulation d'une part et car les modèles dont nous avions besoin n'existaient pas dans les simulateurs existants. Dans la deuxième partie, nous avons choisi de ne plus utiliser de simulateur du tout : notre proposition a été validée directement sur plate-forme réelle de capteurs. La troisième partie est validée avec MATLAB [MAT12], outil de calcul mathématique mais qui dispose d'un module de couche physique radio.

2.8.2 Systèmes d'exploitation

Bien qu'il y ait de nombreux systèmes d'exploitation efficaces pour les capteurs sans fil comme, par exemple, Contiki [COS12], ERIKA Enterprise [EE12], Nano-RK [NRK12], MantisOS [MO12], RETOS, Senses, Cormos, LiteOS, NanoQplus, etc., TinyOS [PMP+05] reste le plus connu dans le domaine de la recherche. Développé dans les laboratoires de Berckley, TinyOS est un système d'exploitation open source qui contient tous les pilotes nécessaires, des mécanismes divers et des applications qui sont prêtes à être implémentées directement. Il respecte les contraintes de mémoire propres aux capteurs sans fil et utilise le minimum de ressources et, par conséquent, il assure une consommation d'énergie optimale. Dans cette thèse nous avons testé et expérimenté nos mécanismes en utilisant la plate-forme TinyOS 1.x. L'expérience a été satisfaisante, le seul inconvénient étant qu'il n'y avait pas de mécanisme pour installer la même application sur différent capteurs en même temps, ce qui demande beaucoup de temps pour répéter la même tâche au fur et à mesure.

2.9 Conclusion

Après une présentation des capteurs sans fil, de leur structure, des principaux types et de leurs limitations, nous avons passé en revue les grandes problématiques actuelles sur le sujet.

Les recherches actuelles visent à mettre en place des systèmes s'auto-organisant en fonction du contexte. Les réseaux de capteurs sont déployés dans des environnements qui peuvent changer radicalement, et sont bien souvent sans infrastructure. Nous passons en revue les principaux topologies, protocoles MAC ou architectures de routage concernant les réseaux de capteurs. Il apparaît que ce qui a été développé l'a été dans des contextes spécifiques, pour répondre à des besoins spécifiques, que, par exemple, dans certains contextes les réseaux ont plutôt une topologie complètement maillée mais que dans d'autres ce n'est plus le cas, et qu'il faut alors que les réseaux soient capables de changer dynamiquement d'un protocole à un autre en fonction du contexte. Par ailleurs, ceci requiert de détecter le contexte dans lequel se trouve un capteur, ce qui peut être difficile si tout le voisinage est endormi or, depuis une dizaine d'année, de nouveaux systèmes de réveil à la demande ont été conçus. Dans la partie suivante de cette thèse, nous proposons justement un mécanisme permettant de changer dynamiquement de protocoles, mécanisme rendu possible par ces nouveaux moyens de réveil à la demande.

Toujours sur l'auto-organisation, un sujet actif de recherche concerne l'adaptation à l'environnement et plus particulièrement à la coexistence avec d'autres réseaux concurrents d'autres technologies. Après avoir examiné l'impact de différentes sources d'interférences, nous avons listé les travaux récents pour aider les réseaux à y faire face. Nous constatons que les approches proposées conjuguent plusieurs limitations, en particulier celle de nécessiter des écoutes régulières du canal, ce qui est coûteux en termes de consommation énergétique et aussi celle de ne pas permettre d'identifier explicitement la cause de l'interférence. Or, la connaître doit permettre de déclencher la réaction la plus adaptée. Dans cette thèse, nous explorons la possibilité de détecter et d'identifier des réseaux concurrents au réseau de capteurs déployé, à partir non pas d'écoutes fréquentes du canal mais des paquets que l'on reçoit. Au lieu de les ignorer, puisqu'on les a reçus, nous proposons de les analyser pour déterminer la source des erreurs qui peuvent s'y trouver. C'est un moyen de repérer des signatures de réseaux concurrents, de capteurs ou d'autres technologies.

L'auto-organisation pose la question de la mise en commun d'informations possédées par les capteurs et de la manière de la récupérer. Par exemple, la détection d'un réseau concurrent gagnerait à être transmise à des capteurs « amis » du même réseau. Les techniques de la radio cognitive peuvent être utiles dans ce but. Les réseaux docitifs se situent dans le prolongement naturel de la radio cognitive en explorant les meilleures façons d'échanger les données et aussi de sélectionner celles qui sont utiles et fiables. Nous avons montré dans cet état de l'art que les travaux sur les réseaux docitifs ont été menés dans le contexte de réseaux cellulaires avec une infrastructure, mais que, dans un réseau de capteurs mobiles sans infrastructure concevoir des mécanismes de docition efficaces est beaucoup plus complexe. Dans la dernière partie de cette thèse, nous abordons cette question et proposons un mécanisme de docition pour la détection des paramètres de la loi de Pareto modélisant les temps de silence du trafic de réseaux WiFi sous la couverture desquels se trouvent des nœuds de capteurs. La difficulté vient du fait que les capteurs, étant mobiles, peuvent se trouver dans des endroits couverts par peu de points d'accès WiFi et donc de grands silences puis, quelques instants plus tard, dans d'autres très chargés en trafic WiFi. Se pose alors la question de la fraîcheur de l'information, et de l'opportunité de transmettre ou recevoir cette information d'autres nœuds lorsqu'on bouge.

Enfin, la question de la validation de mécanismes réseaux étant fondamentale, nous donnons un bref aperçu des outils qui peuvent être utilisés pour les études de performances. Dans la première partie de la thèse (chapitre suivant), nous avons choisi de développer nous-mêmes

notre propre simulateur en C car les mécanismes que nous utilisons ne sont déjà codés dans aucun simulateur. Dans la deuxième partie, présentée au chapitre 3, notre proposition est validée à partir de mesures sur un réseau de capteurs réels. Notre dernier travail est développé en MATLAB.

Chapitre 3. Mécanisme d'adaptation au contexte et d'auto-organisation

3.1 Introduction

L'automatisation et la diffusion d'applications de hautes technologies omniprésentes dans la vie quotidienne depuis la fin du XXème siècle, et le besoin de les adapter à tout changement dans l'environnement, a conduit à la conception d'une grande variété de capteurs pour surveiller, interagir et propager l'information à ces différentes applications. Les applications des capteurs varient entre applications de surveillances médicale, militaires, de la faune, de la flore et de la géologie, capteurs utilisés dans les vêtements intelligents, surveillance des chaînes du froid et beaucoup d'autres encore. Ces applications, particulièrement dans le cas des vêtements intelligents ou de la surveillance de la chaîne du froid, nécessitent des capteurs à la fois mobiles et sans fil. Etant mobiles, pouvant changer d'environnements au cours du temps, tant en termes de milieu pour la transmission des données que de forme de topologie, les capteurs doivent s'adapter au contexte où ils se trouvent afin d'optimiser les mécanismes qu'ils mettent en œuvre, cette adaptation étant faite à partir de toute information qui peut être utilisée pour caractériser la situation des liens de communication entre les capteurs sans fil. Certains protocoles de routage, par exemple, se prêtent mieux à certaines topologies que d'autres. Le réseau de capteurs doit donc la reconnaître et utiliser le plus approprié. Les traitements basés sur la détection de contexte modifient le comportement d'un capteur à partir de sa perception de l'état du milieu et de ses environs.

Ce travail répond à un besoin d'adaptation du réseau constaté dans le contexte de la surveillance de la chaîne du froid au cours de notre participation au projet ANR CAPTEURS. Il existe des solutions adaptées spécifiquement à chaque partie de la chaîne mais, n'étant pas de bout en bout, il est nécessaire de disposer d'un mécanisme capable de détecter le contexte où un nœud se trouve et d'appliquer automatiquement le protocole approprié en fonction de celui-ci. Comme, dans le scénario adopté dans le contrat CAPTEURS, on ne peut pas avoir d'infrastructure, la détection du contexte est rendue difficile. Il n'est pas possible d'installer de station de base dans le camion ou dans l'entrepôt qui annonce à chaque capteur son emplacement. Nous avons alors conçu un système qui soit capable de s'adapter dynamiquement aux conditions de transport dans les camions ainsi qu'à celles du stockage en entrepôt.

La solution développée s'avère plus générale que le contexte spécifique d'où elle est partie : les protocoles retenus sont bien adaptés à certaines hypothèses sur la mobilité des nœuds qui dépassent le cadre restreint de la chaîne du froid. Nous avons alors généralisé notre contribution à travers la proposition d'un cadre conceptuel qui fournit, sous des hypothèses précises sur les situations possibles de visibilité des nœuds et les modes de communication, une panoplie de protocoles sélectionnés pour les niveaux routage, MAC et la couche physique ainsi qu'un mécanisme, CAM pour Contexte Aware Mechanism (mécanisme d'adaptation au contexte), qui passe dynamiquement de l'un à l'autre. La principale originalité de notre proposition réside dans le fait de changer dynamiquement de protocoles mais elle comprend: 1) la détection dynamique d'un changement de contexte, 2) la détection dynamique du nouveau contexte, 3) l'adaptation dynamique au niveau des trois couches responsables de la gestion des

liens de communication en conséquence, et 4) le tout sous contrainte de consommation d'énergie. Un tel cadre, peut ensuite être implanté sous forme de kit de composants logiciels.

Certes, la nécessité d'adapter les protocoles ou architectures en fonction du contexte a bien déjà été ressentie mais cela n'a pas débouché sur des mécanismes qui s'adaptent dynamiquement. Les auteurs de [NMSYC07] ont analysé l'efficacité de différentes architectures, pour l'application spécifique de la surveillance du corps humain. Les réseaux utilisés pour accomplir cette tâche sont appelés les réseaux de capteurs corporels. Leurs résultats suggèrent que, même si une architecture en étoile avec des nœuds fonctionnant à de faibles niveaux de puissance peut suffire dans un environnement intérieur encombré, les nœuds dans un environnement ouvert en extérieur doivent fonctionner à des niveaux de puissance plus élevés ou bien passer à une architecture à plusieurs sauts permettant des taux acceptables d'acheminement de paquets. En revanche, on ne fait pas dans cet article de proposition pour permettre de passer dynamiquement d'un cas à l'autre.

De même, dans [NSYM09] on mesure par expérimentation l'efficacité de deux architectures de réseaux, en étoile d'une part et à plusieurs sauts d'autre part. On constate que chaque architecture est efficace dans un contexte spécifique, mais aussi que les architectures à sauts multiples augmentent dans certains cas la consommation d'énergie et peuvent augmenter les temps d'acheminement. Les architectures en étoile ne consomment pas autant d'énergie mais ne sont pas flexibles. Elles peuvent bien fonctionner dans un environnement fermé mais leurs performances se dégradent totalement dans des environnements ouverts où les nœuds peuvent avoir besoin de coopérer. Il ne s'agit toujours pas ici de proposer une solution d'adaptation au contexte.

Des travaux sur la détection de topologies de phénomènes physiques ont fait l'objet de plusieurs publications, comme dans [FZWN08]. Dans cet article, qui concerne la surveillance de phénomènes répartis sur une certaine zone géographique, comme les feux de forêts ou les marées noires, les capteurs mesurent une valeur. Les auteurs s'intéressent à la topologie des zones constituées de capteurs contigus ayant la même valeur, au-dessus ou en-deçà d'un seuil. Celles-ci donnent une information en soi sur le phénomène mesuré, comme l'étendue d'une catastrophe. Elles permettent également d'optimiser les ressources du réseau. L'objet de [FZWN08] est de détecter dynamiquement les changements de ces topologies. En revanche, la question de la gestion dynamique des protocoles n'est pas vraiment abordée. Par exemple, si un protocole est plus adapté à une topologie qu'un autre, le fait d'en changer dynamiquement n'est pas évoqué.

Nous commençons par introduire le contexte spécifique de la chaîne du froid, ce qui nous permet de formaliser les hypothèses générales qui définissent les limites d'applications du cadre conceptuel proposé, puis de présenter ce cadre et le mécanisme qui le sous-tend. Nous passons ensuite en revue et discutons rapidement les protocoles que nous retenons pour notre cadre puis le mécanisme qui permet de passer de l'un à l'autre. Enfin, nous détaillons le mécanisme conçu pour la chaîne du froid, et évaluons son intérêt à travers une analyse de ses performances.

3.2 De la chaîne du froid et des hypothèses retenues

Une chaîne du froid est une chaîne d'approvisionnement à température contrôlée. C'est un enchaînement ininterrompu d'activités de stockage, de transport et de distribution qui maintient une gamme de produits à une température donnée. La chaîne du froid est un élément

important dans la livraison de marchandises fragiles comme les médicaments, les aliments, les produits chimiques etc. Plusieurs acteurs interviennent dans la chaine de froid, des entrepôts jusqu'aux détaillants, en passant par les transporteurs routiers, ferroviaires ou maritimes. La question de la responsabilité d'une rupture de la chaîne se pose alors lorsqu'un tel événement survient. Il faut alors disposer d'un système qui surveille en permanence la température des denrées pour pouvoir donner l'information de responsabilité le cas échéant. Le scénario que nous considérons est celui d'un tel système.

Il y a plusieurs niveaux dans la chaîne du froid. Nous nous intéressons aux produits frais (entre 0 et 4°C). Comme indiqué dans la thèse de Chérif Diallo au §4.3, les produits frais passent en entrepôt par des phases de réception, de stockage, de préparation des commandes et leurs envois. Les produits arrivent à une température comprise entre 0 et 4°C, le fournisseur ayant l'obligation contractuelle de respecter cette température. La température est mesurée avec des enregistreurs, le système de refroidissement adapté en fonction de la température mesurée, une alarme envoyée en cas de situation critique. Les produits sont ensuite passés en revue, leurs numéros, dates limites de vente, de consommation, etc. relevées avec une douchette reliée à un ordinateur lui-même connecté par liaison sans fil au système de gestion de l'entrepôt. Les palettes sont ensuite stockées sur des racks. En fonction des commandes, les marchandises sont ensuite prélevées et mises sur des palettes ou dans des containers réfrigérés sur le quai pour l'expédition puis transportées en camion.

La température est enregistrée dans l'entrepôt, elle l'est dans le camion, mais il n'y a pas de suivi sur la chaîne d'une part et, d'autre part, ce n'est qu'un point de mesure à un endroit précis. Sans prétendre mesurer la température de chaque produit, l'avoir pour chaque palette permettrait une mesure plus fine qu'une seule à un endroit de l'entrepôt. Nous supposons donc qu'il y a un capteur par palette.

Retrouver l'information pour imputer une responsabilité n'exige pas d'intervenir immédiatement lors d'un problème, ce qui nous permet d'affirmer que l'information n'a pas besoin d'être remontée en temps réel. Les alertes sont par contre stockées dans la mémoire du capteur pour une consultation en différé. Les capteurs communiquent donc entre eux, toutes les vingt minutes pour s'échanger des paquets mais il n'y a pas d'alarme donc pas de paquet de données envoyé en-dehors de ces paquets périodiques.

De plus, pour des raisons de coûts du système, et donc d'acceptabilité de notre solution, nous souhaitons que le système développé ne nécessite aucune infrastructure ni station de base pour collecter les données. Pour faciliter la récupération des données, nous souhaitons aussi que l'information relative à n'importe quel événement soit récupérable de n'importe quel capteur, ce qui impose que les données soient toutes diffusées à tous les capteurs de telle sorte que chaque capteur ait la même base de données d'événements que tout autre capteur du réseau. Ainsi, à tout moment, toutes les données sur le réseau peuvent être récupérées avec un simple PDA à partir de n'importe quel capteur.

Dans un camion, les palettes sont toutes dans le même plan. Comme les palettes sont dans les capteurs et qu'il n'y a pas plus de trente trois palettes par camion on peut considérer que tous les capteurs sont en visibilité totale. En revanche, dans l'entrepôt, tous les capteurs ne se voient pas et, vue leur grand nombre, l'ensemble des palettes constitue un très grand réseau.

Dans ce chapitre on suppose qu'il n'y a pas d'interférence imprévisible causée par d'autres sources que le réseau de capteurs sans fil considéré. Par exemple, il n'y a pas de trafic WiFi. Le cas où d'autres trafics entre en concurrence avec celui du réseau considéré fait l'objet des chapitres suivants. Seules les communications des capteurs eux-mêmes, et leurs déplacements, modifient l'état de l'environnement.

Pour résumer, les hypothèses prises sont :

1. Un capteur par palette ;
2. Envoi de données périodiques, de l'ordre de la dizaine de minutes ;
3. Pas d'infrastructure ;
4. Tous les capteurs ont la même base de données d'événements : les mesures doivent donc être transmises à tous ;
5. Les capteurs alternent entre des séjours prolongés dans des endroits où ils constituent un grand réseau dont tous les nœuds ne sont pas tous en visibilité avec des séjours de quelques heures par groupes de trente-trois tous en visibilité totale ;
6. Ils ont tous la même puissance nominale de transmission et elle est fixe.

Il existe des solutions pour surveiller la chaîne du froid (cf. [NFVCBCCL07] par exemple), mais elles consistent généralement à avoir des enregistreurs de données dans chaque partie de la chaîne du froid, les camions, les trains, entrepôts, etc. sans avoir de réseau pour assurer une surveillance de bout en bout. Dans [R04] une solution basée sur les réseaux de capteurs est proposée, mais elle nécessite une infrastructure, qui a un coût prohibitif dans la pratique. Dans [FCAMO08] une autre solution est proposée, mais les auteurs ne traitent pas la question de passage à l'échelle, en particulier, dans les grands entrepôts. En outre, dans ces solutions, les données ne sont pas diffusées à tous les nœuds pour être récupérées ultérieurement à partir de n'importe quel nœud. Une solution existe qui n'est pas de bout en bout, mais qui satisfait les contraintes sur la redondance de données sur tous les capteurs, sur l'organisation d'un réseau sans infrastructure, sur le nombre limité de capteurs dans un camion, dans le même plan et tous en visibilité : PLACIDE ([KDB09]). Dans ces conditions, on montre que PLACIDE est optimal en termes de consommation d'énergie. Il s'agit d'un mécanisme à la fois sur les couches MAC et routage: il synchronise la mise en sommeil des capteurs, leur réveil, il spécifie les instants de transmission des nœuds et diffuse l'information de nœud en nœud en formant un anneau virtuel entre les capteurs, le nœud n envoyant les données qu'il mesure au nœud n+1 agrégées à celles qu'il reçoit du nœud n-1. Toutefois, le protocole PLACIDE est conçu spécifiquement pour la surveillance de la partie précise de la chaîne qu'est le transport en camion et ne fonctionne pas de bout en bout sur toute la chaîne.

Les cinq hypothèses ci-dessus sont bien plus générales que le simple cas de la chaîne du froid, le cadre conceptuel que nous élaborons dépasse donc cette application spécifique et pourrait s'appliquer à tout autre suivi que la température dans le domaine logistique. Par exemple, le suivi des chocs pour une livraison de parfums ou d'appareils de haute technologie pourrait bénéficier de notre solution.

3.3 Le cadre conceptuel proposé et son mécanisme d'adaptation au contexte (CAM)

3.3.1 Présentation générale

Pour rendre le système adaptable au contexte, il faut un mécanisme qui réalise l'adaptation dynamique et une panoplie de protocoles. Nous proposons dans ce chapitre un cadre conceptuel pour cela. Il utilise la structuration en couches de la norme OSI, et, en particulier, il repose sur le fait que les couches sont indépendantes les unes des autres, ce qui rend les protocoles interchangeables, et le fait qu'elles peuvent communiquer par les interfaces standard. Il doit, pour avoir le comportement optimal de la partie radio, pouvoir gérer les trois premières couches du modèle OSI, couches qui sont impliquées dans les opérations de communication. Nous sélectionnons dans les parties qui suivent des protocoles pour chaque couche qui sont bien adaptées à l'ensemble des hypothèses exposées au §3.2, mais ceux-ci sont des exemples, d'autres étant possibles. En revanche, l'utilisation d'un protocole transverse à plusieurs couches n'est pas possible dans le cadre que nous proposons. Le mécanisme CAM qui sous-tend notre proposition doit pouvoir détecter les contextes rencontrés dans la chaîne du froid et exposé au §3.2. Ils se ramènent à deux contextes précis: le premier, est celui où les nœuds du réseau peuvent se voir tous, le deuxième correspond à celui où ils ne sont pas en visibilité totale.

Principalement, le mécanisme est composé de trois fonctions (cf. Figure 3.1): la détection de changement de contexte elle-même, la détection du nouveau contexte et l'adaptation par l'activation des protocoles les plus efficaces dans le nouveau contexte. Le mécanisme CAM choisit le protocole adapté à chaque condition qu'il détecte, spécifiquement celles présentées au §3.3.3 ainsi que des conditions sur la mobilité des nœuds, la densité du réseau et son étendue. Ces protocoles sont discutés dans les paragraphes qui suivent. Nous en retenons certains, à titre d'exemples qui conviennent bien, pour l'application à notre étude de cas au §3.3.6.

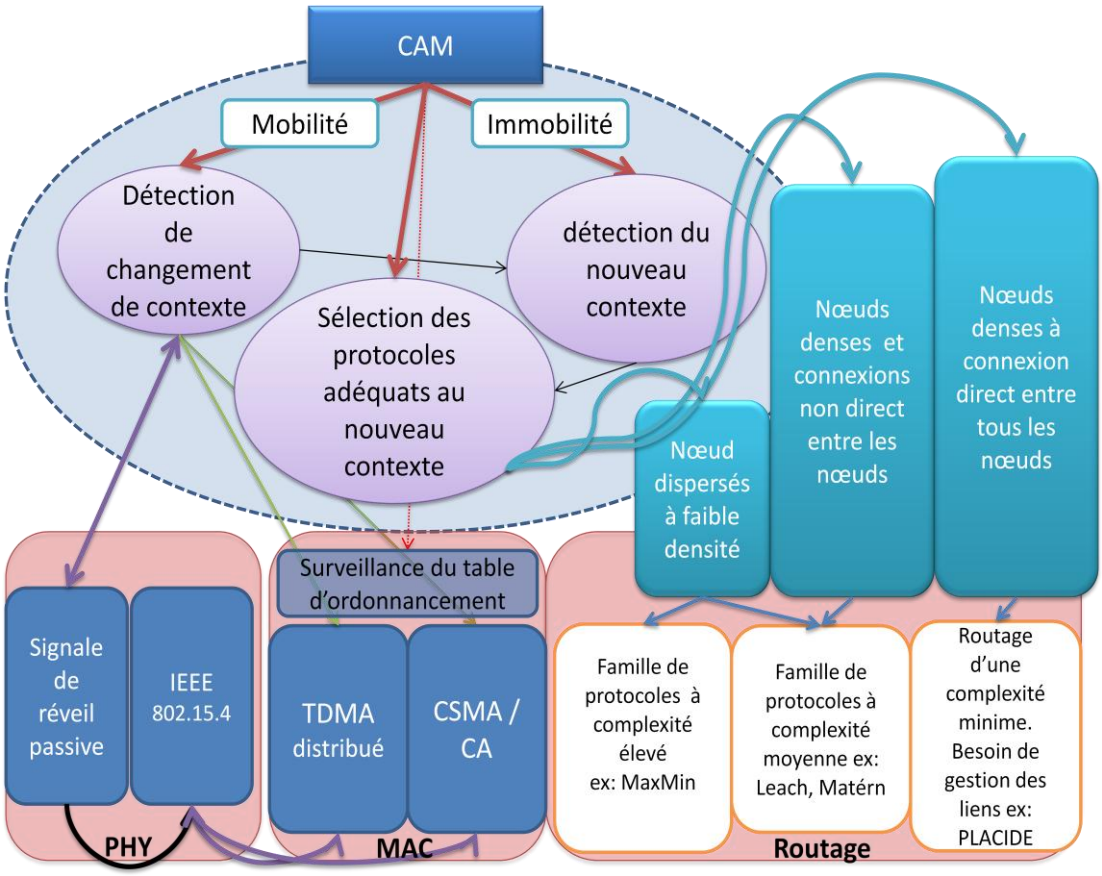


Figure 3.1 : architecture du mécanisme CAM

3.3.2 Détection de changement de contexte

Puisque nous supposons que seule une variation dans la topologie peut causer un changement dans le réseau, un changement de contexte est la détection du fait qu'un nœud ou l'un de ses voisins s'est déplacé. La difficulté à détecter un changement de contexte provient du fait que les nœuds ne peuvent pas réaliser des traitements complexes d'une part et qu'ils sont à l'intérieur d'un environnement fermé d'autre part et donc qu'ils ne peuvent recevoir de signal GPS qui donnerait une information sur leur environnement. La seule information qui permet de détecter un changement de contexte ne peut alors venir que du voisinage. Si un nœud du voisinage s'est déplacé, il est probable que le nœud lui-même s'est déplacé ou encore qu'il va se déplacer dans un future proche. Il faut alors adapter le fonctionnement de ses protocoles et mécanismes de communications en conséquence. La détection du voisinage doit alors être faite au préalable de cette adaptation, ce qui implique de rafraîchir le tableau d'ordonnancement du nœud et de choisir ensuite le protocole adéquat pour cette nouvelle situation.

La détection de changement de contexte repose donc sur la variation du voisinage. Le mécanisme CAM surveille continuellement les apparitions et les disparitions des voisins pour déclencher la procédure de détection de contexte. Il utilise le tableau d'ordonnancement du nœud contenant les informations sur les voisins : leurs identificateurs, leurs dates de transmission, leurs voisins et les dates de transmission de leurs voisins. L'activation de la procédure de détection est déclenchée à partir d'un seuil qui indique à partir de quel taux de modification de voisinage le mécanisme CAM doit rafraîchir son tableau d'ordonnancement. Ce taux est typiquement un pourcentage de voisins qui changent (disparition ou apparition). Ce

seuil est fixé par l'administrateur du réseau. S'il est petit, le nœud s'éveille plus fréquemment pour détecter ses voisins et son nouveau voisinage, ce qui épuise plus rapidement les ressources énergétiques du nœud. S'il est élevé, le nœud prend plus de temps pour détecter les changements dans son voisinage mais cela lui conserve l'énergie restante. Ce mécanisme est très important surtout quand les nœuds sont endormis la plupart du temps et réveillés périodiquement pour communiquer. En effet, dans ce cas les nœuds ne peuvent pas découvrir tout le voisinage les voisins étant endormis. Ils doivent alors rester moins souvent éteints pour pouvoir détecter plus rapidement les voisins, et donc rafraîchir leurs tableaux d'ordonnancement.

3.3.3 Détection de contexte

Dès qu'un changement de contexte est détecté, la procédure de détection de contexte commence. Deux cas sont possibles.

- Le nœud est en visibilité totale avec ceux de la composante fortement connexe auquel il appartient:

Si V est l'ensemble des nœuds du réseau et $Vois(x)$ l'ensemble des voisins de x, tous les nœuds de la composante fortement connexe à laquelle appartient x sont tous en visibilité si et seulement si

$$\forall y \in Vois(x), Vois(x) = Vois(y).$$

Dans ces conditions, tous les nœuds étant en visibilité il n'est pas nécessaire de former un réseau à plusieurs sauts. Dans les cas de densités extrêmes de nœud, le mécanisme CAM peut ordonner, si c'est possible, à la couche physique d'utiliser différentes fréquences ou modulations pour augmenter la capacité du médium partagé. D'autres solutions consistent à diminuer le rapport cyclique de durée des nœuds comme par exemple, si la durée de réveil des nœuds est de 5 minutes l'étendre à 10 minutes.

- La proposition suivante indique s'il n y a pas de visibilité totale :

$$\exists y \in Vois(x), \exists z \in Vois(y), z \notin Vois(x)$$

Lorsque cette proposition est vérifiée, il est obligatoire de faire du routage et de construire un réseau à plusieurs sauts. Un choix est alors fait sur le protocole de routage le plus adapté aux caractéristiques de l'environnement détecté. Par exemple, on doit prendre en compte l'adéquation entre le protocole choisi, la densité des nœuds, leur mobilité et la complexité du protocole. Ce choix a un impact très important au niveau des traitements et de la mémoire des nœuds et donc de la consommation d'énergie.

3.3.4 Mécanisme pour la couche physique

Les capteurs utilisent le standard IEEE802.15.4. Pour optimiser les dépenses d'énergie, on les endort et les réveille périodiquement. Se pose alors le problème de la synchronisation des nœuds. En théorie, la question est assez facile à résoudre, en pratique, lorsque les temps à l'état de veille sont de l'ordre de la dizaine de millisecondes toutes les vingt minutes comme dans la chaîne du froid, c'est plus difficile. On a proposé en quinze ans de recherche sur la question de nombreuses solutions mais aucune n'est optimale. L'idéal serait d'avoir un mécanisme qui

permette de réveiller un capteur à la demande. Des solutions ont été proposées, qui se basent sur une signalisation hors-bande.

1- Le dispositif de réveil radio déclenché (radio triggered wakeup call, [GS04]):

Ces solutions permettent de recevoir un signal sur un circuit passif, de le convertir en signal numérique qui, transmis à un borne de la CPU de la carte radio, permet de rallumer cette dernière. Une balise de synchronisation est envoyée pour réveiller les capteurs pour pouvoir recevoir et transmettre les paquets de données. Comme l'illustre la Figure 3.2, une antenne détecte l'onde électromagnétique et la convertit en courant. Une tension «V_{in}» apparaît alors à l'entrée de la résistance "R". Après démodulation de V_{in}, grâce à R_p et D_{out}, le signal démodulé apparaît comme V_{out}. A la réception du signal V_{out} sur la broche d'interruption externe du microcontrôleur, le microcontrôleur se réveille. Cette approche fonctionne à une distance très faible de l'émetteur.

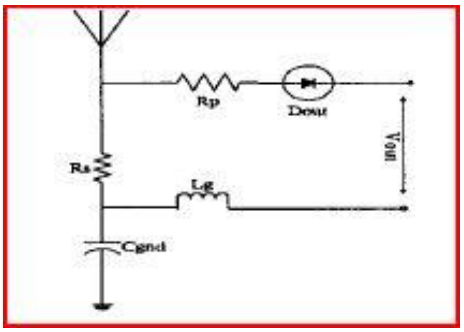


Figure 3.2 : dispositif de réveil déclenché radio ([GS04])

2- Radio triggered ID (RTID, [GS04]):

Le RTID utilise cette technique mais il utilise différentes fréquences pour distinguer certains nœuds à activer tout en en laissant d'autres éteints. (Figure 3.3)

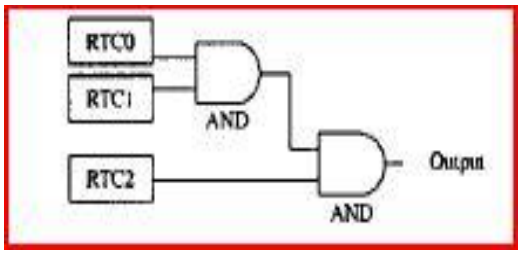


Figure 3.3 schéma du RTID

Quand les capteurs sont mobiles, le problème du choix des fréquences est posé.

3- Système de Jurdak et al. [JRO08], [RJO07] :

C'est la solution la plus intéressante et la plus simple. En outre, elle a été testée avec des capteurs. Le principe est toujours le même mais les auteurs ont conçu, et testé, une carte intégrant une telle partie de réveil à la demande avec le standard IEEE802.15.4. Le mécanisme de réveil utilise la bande ISM 2,4 GHz commune entre l'IEEE 802.15.4 et la technologie de réveil, ce qui permet d'utiliser la radio du capteur de l'expéditeur pour émuler un lecteur RFID et activer le récepteur à distance. Contrairement aux solutions précédentes, ceci élimine la nécessité d'un dispositif spécifique distinct à chaque nœud pour le réveil. Ces solutions étant

analogues au RFID, dans les solutions précédentes il faut un dispositif analogue au lecteur RFID pour pouvoir réveiller à distance un nœud tandis que tout est intégré dans la même carte dans la présente solution. Une comparaison est faite par les concepteurs de cette carte entre BMAC, l'IEEE802.15.4 et cette solution Figure 3.4. Les résultats montrent une meilleure performance en consommation d'énergie pour cette solution. C'est donc elle que nous retenons pour notre proposition : une couche physique IEEE802.15.4 et cette solution de réveil à la demande en mode passif et signalisation hors bande..

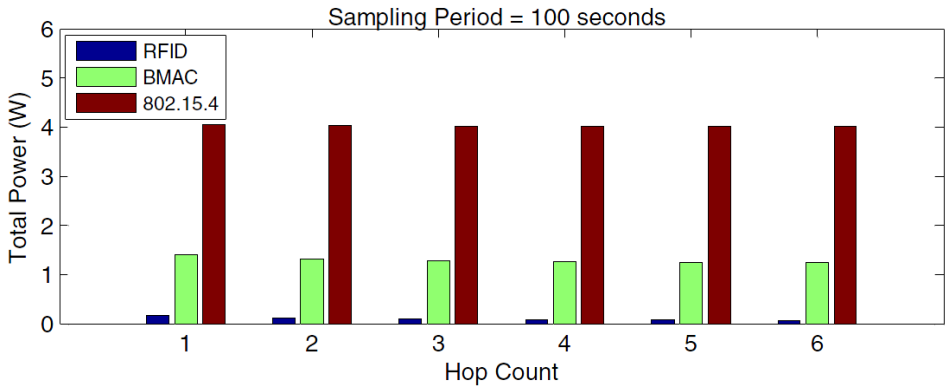


Figure 3.4:comparaison de la consommation de puissance pour une durée de 100 secondes en fonction du nombre de saut pour le système de Jurdak [JRO08]

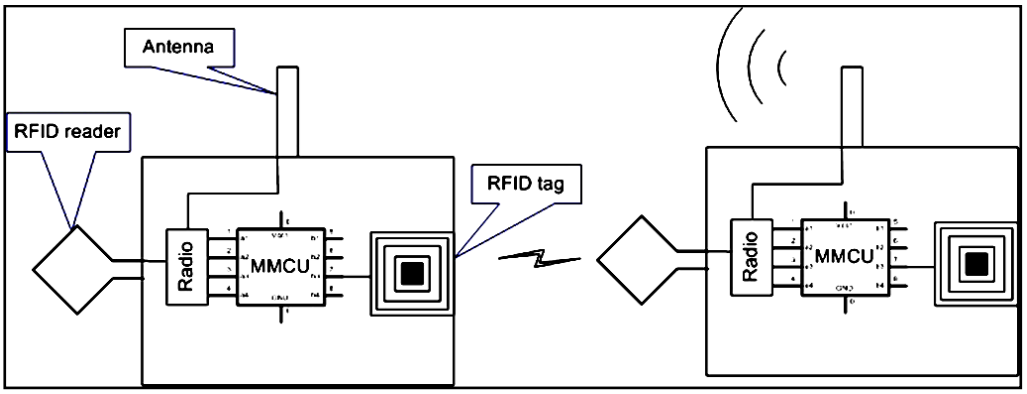


Figure 3.5: schema du système de Jurdak

3.3.5 Protocoles pour la couche MAC

La couche MAC doit pouvoir ordonnancer la communication en gérant la mise en sommeil, le réveil et les dates de transmission d'une manière optimale pour consommer le minimum d'énergie. Le meilleur mécanisme pour optimiser l'énergie est le TDMA [CND08]. Il organise les transmissions et les réceptions pour éviter les collisions et les écoutes inutiles du médium partagé, son inconvénient étant la surcharge de trafic liée à l'initialisation et à la synchronisation. Or, dans un réseau distribué sans infrastructure et mobile, les nœuds doivent s'auto-organiser et reconfigurer les instants réservés de transmission à chaque fois qu'il y a un changement dans la topologie dû à la mobilité des nœuds, ce qui, en plus de contribuer à la dépense énergétique, allonge les temps de transmission et n'est par parfait puisqu'il y a toujours des nœuds non synchronisés qui provoquent des collisions. Le CSMA/CA est adapté à la mobilité mais consommateur d'énergie de par l'écoute qu'il nécessite et n'est pas efficace quand le trafic est important. Les terminaux cachés imposent l'usage de RTS/CTS qui contribuent encore plus à la dépense d'énergie.

Beaucoup de mécanismes ont été développés pour concilier les avantages du TDMA et du CSMA/CA (cf. BMAC [PHC04], ZMAC [RWAP05], MS-MAC [PJ04], S-MAC [YHE02], RMAC [DSJ07], [S04], [DBN01], [ANA07]) mais aucun protocole n'a vraiment réussi à combiner les qualités des deux pour donner un mécanisme optimal. Il leur manque de pouvoir basculer du TDMA au CSMA/CA et inversement d'une manière dynamique selon la variabilité de l'environnement.

Nous souhaitons que les capteurs communiquent autant que possible à des instants réservés, selon un mode TDMA, mais la mise en place de ces réservations requiert un mode CSMA/CA pour la mettre en place. Un mécanisme hybride (TDMA-CSMA/CA) pour la couche MAC est proposé dans [RWAM05]. Il est développé pour optimiser le fonctionnement de la couche MAC en cas de mobilité et haute contention mais il n'est pas aussi optimal que le TDMA pour l'optimisation de la consommation d'énergie puisqu'il n y a pas de réservation permanente des intervalles de temps : à chaque fois qu'il veut émettre un nœud doit tester et écouter le canal pour choisir un intervalle à utiliser. Les inconvénients de ce mécanisme nous conduisent à faire gérer par CAM le passage dynamique d'un mode TDMA au mode CSMA/CA.

Le mécanisme CAM que nous proposons permet de basculer de l'un à l'autre dynamiquement en fonction de l'environnement. Il pourrait même être adapté pour apprendre à la volée au cours de la durée de vie d'un réseau la variation de sa topologie, ce qui permettrait au mécanisme CAM de prédire le taux de déplacement (en s'inspirant par exemple de [SMPKL11] et [ZGSZ11]) et le corréler aux déplacements des voisins pour soit utiliser CSMA/CA s'il y a un taux de mobilité élevé et soit basculer en TDMA sinon. Dans notre approche, le mécanisme CAM ne fait qu'utiliser le CSMA/CA pour la signalisation lorsqu'un changement de topologie est détecté et le TDMA lorsque l'environnement est stable.

3.3.6 La couche routage, discussion générale

Beaucoup de protocoles de routage ou de clusterisation pour les réseaux de capteurs ont été développés (e.g. LEACH [HCB00], PEGASIS [LR02], cf. [VOCA09], [SSS10], [AK12], et [MAR10] pour une étude approfondie). Cette diversité n'indique qu'une chose : jusqu'à maintenant personne n'a pu développer un protocole de routage universel qui puisse être efficace dans toutes les conditions. Pour un réseau suivant les hypothèses données au §.3.23.2 p.53, qui donc peut passer par différentes conditions de topologies et de visibilité des nœuds, nous sélectionnons des protocoles qui peuvent convenir dans chacune des configurations possibles. Ces protocoles sont des exemples bien adaptés, mais le choix que nous faisons ne se prétend pas exhaustif, d'autres pouvant convenir. Néanmoins, les protocoles que nous discutons ici sont des protocoles qui ont été implantés et testés sur plate-forme réelle.

Lorsque nous parlons de « topologie », il ne s'agit pas uniquement du graphe induit par la position géographique des nœuds mais du graphe des connexions logiques, qui dépend de nombreux facteurs comme les anomalies de transmission ou les connexions intermittentes, atténuations, obstacles, problèmes de temporisations, etc. Cette topologie peut aussi être le résultat d'un certain algorithme de routage. Sur l'exemple de la Figure 3.6, les nœuds ont les positions géographiques indiquées à gauche mais résultant en la topologie logique de réseau donnée à droite.

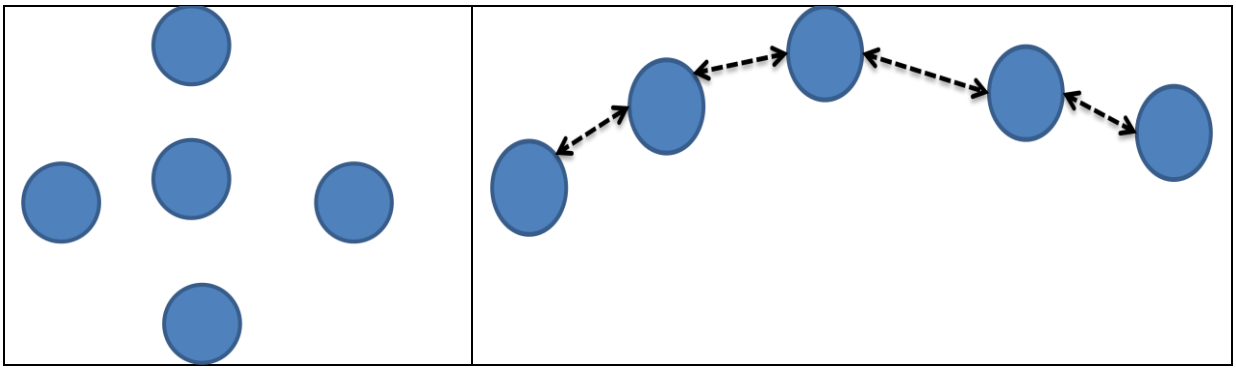
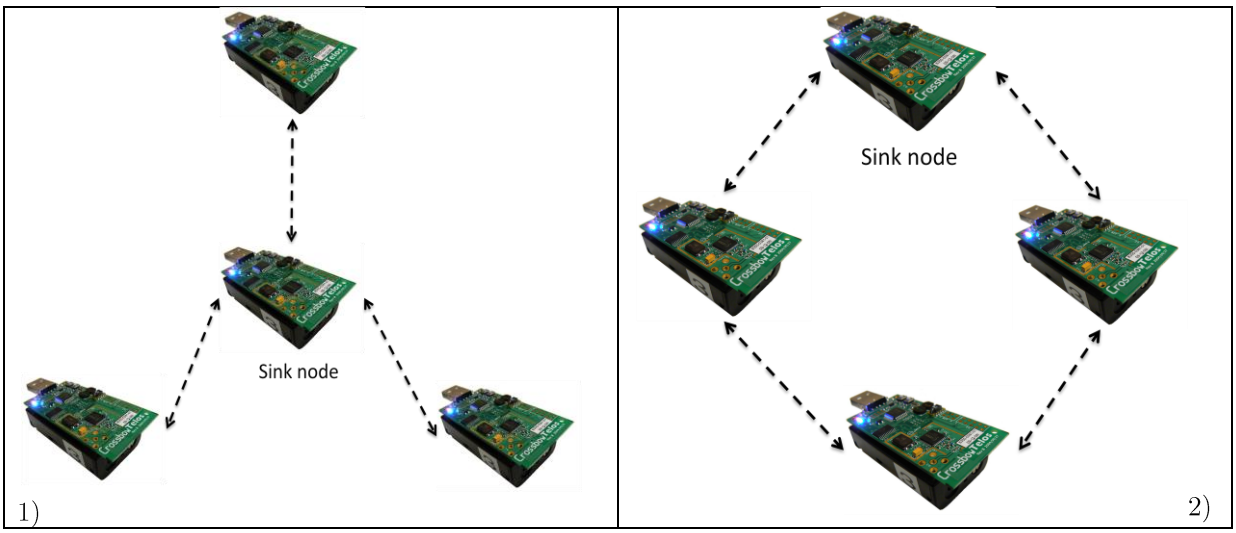


Figure 3.6 à gauche la répartition géographique des noeuds, à droite la topologie des connexions logiques entre les nœuds

La topologie impacte les temps de réponse. Dans [VOCA09], une étude sur le temps de convergence selon différentes structures de topologie formées par un algorithme de routage, et que nous recopions Figure 3.7, montre des résultats très différents : de l'ordre de 9ms pour la topologie 1), 25ms pour la topologie 2), 18,5ms pour la topologie 3) et 29ms pour la topologie 4). De la même manière, la topologie impacte le nombre de transmissions et donc la consommation énergétique des capteurs. Pour chacune de ces topologies, il faut alors une solution adaptée. Nous en sélectionnons trois : l'organisation en anneau virtuel de PLACIDE, l'organisation en clusters de MAXMIN (cf. [APDH00] et [DMB07]) et l'organisation en clusters de MHP ([BGMS10]).



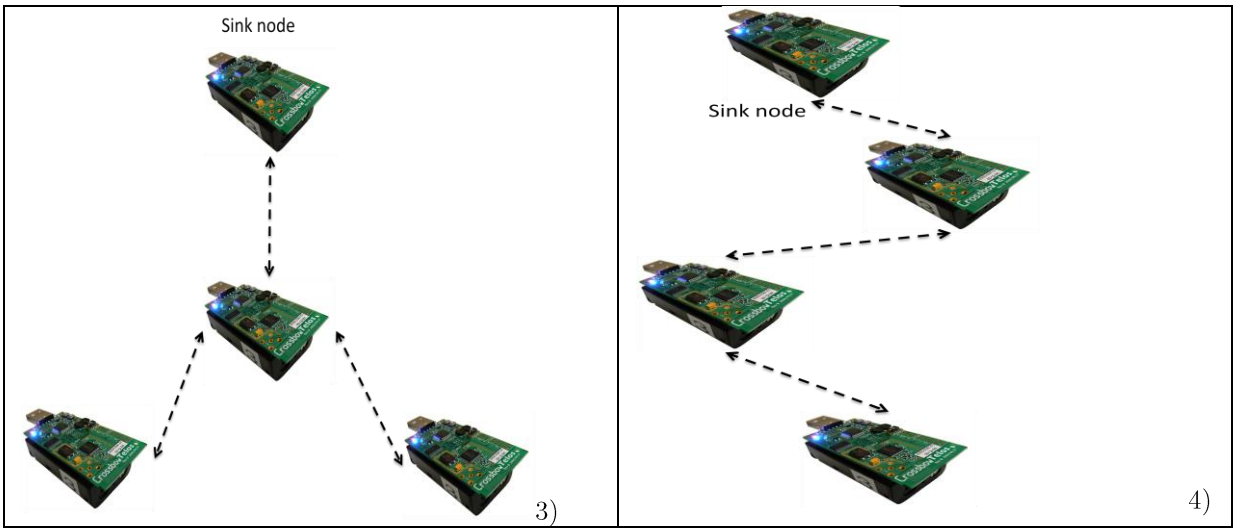


Figure 3.7 : quatre topologies différentes d'un réseau de capteurs

3.3.7 La couche routage, de PLACIDE pour le cas de visibilité totale

Pour le cas où tous les capteurs sont en visibilité totale, PLACIDE est la solution optimale pour économiser de l'énergie. C'est une solution intervenant sur plusieurs couches : elle comporte les fonctionnalités de la couche MAC dans la mesure où PLACIDE organise les instants d'émissions et d'écoutes et d'une certaine façon de la couche routage dans la mesure où PLACIDE diffuse l'information de nœud en nœud selon un anneau virtuel. PLACIDE assure un minimum de signalisation ce qui produit des avantages et des inconvénients. L'avantage est que cela limite la consommation d'énergie. L'inconvénient est que l'insertion et l'extraction des nœuds peut créer des anomalies dans la construction du réseau : le fait par exemple que, lors d'une insertion, seul un nœud de la boucle PLACIDE accuse réception de la demande d'insertion du nouveau nœud, et non l'ensemble des nœuds de la boucle PLACIDE, limite bien la signalisation et donc la dépense énergétique mais peut causer problème si le nouveau nœud n'est visible par exemple que du nœud qui lui répond. Dans une architecture qui est appelée à changer au cours du temps, telle qu'à certains moments des ensembles de nœuds constituent une composante fortement connexe où tous les nœuds sont en complète visibilité mais telle qu'à d'autres ce n'est plus le cas, nous ne pouvons donc retenir une telle signalisation. En revanche, lorsque le nombre de nœuds est raisonnable et qu'ils sont tous en visibilité, nous retenons le routage de PLACIDE c'est-à-dire son organisation en anneau virtuel. Cependant, cette organisation en anneau n'est pas scalable avec le nombre de nœuds car plus il y en a plus les temps d'acheminement des donnée à l'ensemble des nœuds de la boucle sont grands (cf. topologie 4) sur la Figure 3.7).

PLACIDE est composé de 5 phases éventuelles: initialisation et configuration de la chaîne, régime permanent, ajout d'un capteur, suppression planifiée d'un capteur et suppression non planifiée d'un capteur.

Pendant la phase d'initialisation et de configuration de la chaîne, après leur activation et une durée aléatoire d'attente un des capteurs débute la signalisation en transmettant un message SYNC contenant son adresse MAC, et il s'affecte à lui-même la position numéro 1 dans la chaîne. Il indique sa prochaine date de réveil. Dans le meilleur des cas, il n'y a pas de collision ni d'erreur dans la transmission, sinon un mécanisme de retransmissions est mis en

oeuvre. Tous les nœuds voisins sont finalement supposés recevoir le message et tirent alors une durée aléatoire. À la fin de cette durée, un de ces nœuds transmet un acquittement accompagné de son propre message SYNC. Ce message SYNC-ACK transmis contient l'adresse de ce nœud, sa position dans la chaîne qui est 2 et sa prochaine date de réveil. À la réception du message envoyé par le second nœud, le premier nœud s'endort. La construction de la chaine continue alors de la même manière. Quand c'est au tour du dernier nœud, celui-ci transmet son message, ne reçoit pas d'acquittement et s'endort.

La phase de régime permanent commence par l'accomplissement de la phase d'initialisation où le dernier nœud n'a trouvé aucun nœud pour acquitter sa date de réveil. Le dernier nœud transmet alors son premier message MSG contenant sa date de réveil et le transmet au nœud suivant. Le premier cycle commence, dans la direction opposée à celle suivie pour sa formation. Le dernier capteur est le seul nœud à avoir toute l'information sur le réseau, en particulier le nombre de capteurs du réseau. Durant cette phase, chaque nœud transmet un message MSG-ACK à son prédécesseur et transmet le message MSG à son successeur puis s'endort. Les messages MSG contiennent les données reçues du prédécesseur. C'est ainsi que les données sont diffusées, et aussi « routées », dans la boucle.

Pour la phase d'ajout d'un capteur, quand un ou plusieurs nœuds sont ajoutés, ils écoutent le canal pendant une durée suffisamment longue pour recevoir les messages des nœuds appartenant à une chaîne déjà construite, pour ne pas créer une autre chaîne en parallèle et par suite créer des collisions et de l'inconsistance dans le protocole. Quand ils reçoivent un message indiquant la présence d'une autre chaîne, ils attendent la fin du cycle en cours. Pour cela, le PDU doit contenir les informations nécessaires permettant aux nœuds de préparer leur fusion avec la chaîne existante.

Pour la phase de suppression non planifiée d'un capteur, si un nœud S_i est perdu, c'est-à-dire qu'il ne répond pas après un certain nombre de retransmissions, son successeur dans la chaîne et son prédécesseur réagissent. S_{i-1} étend sa durée de réveil durant le cycle et communique directement avec S_{i+1}. Le problème est alors réglé. Durant les cycles suivants les autres nœuds sont informés de la disparition de S_i et mettent à jour leurs bases de données.

Pour la phase de suppression planifiée d'un capteur, un capteur détectant que l'énergie résiduelle de sa batterie passe sous un certain seuil prévient les voisins de son extinction imminente.

3.3.8 La couche routage, du cas de non visibilité totale, de LEACH, de Mattérn et de MAXMIN

Pour les cas où la visibilité des nœuds n'est pas totale, c'est-à-dire où certains nœuds ne sont pas en visibilité d'autres, ou bien si tous les nœuds sont en visibilité mais où ils excèdent un certain nombre limite, il faut un routage plus élaboré, à base de clusters pour des raisons de passage à l'échelle, car le nombre de nœuds est supposé grand. La formation de ces clusters peut être faite à partir, par exemple, de deux algorithmes : MAXMIN et une méthode basée sur le processus ponctuel de Matérn (MHP pour Matérn Hard-Core Process ou processus à noyau dur de Matérn) détaillée dans [BGMS10]. Toutes les deux sont implantées et comparées sur des capteurs dans [BGMS10]. Les deux sont des algorithmes pour former des clusters et plus précisément pour choisir des chefs de clusters dans un réseau, de capteurs en particulier. On

peut utiliser l'un ou l'autre selon que l'on veut des clusters à plusieurs sauts (MAXMIN) ou à un seul saut (MHP).

Le processus ponctuel de Matérn est un processus qui sélectionne certains nœuds, dans un ensemble de nœuds disposés sur un plan, tels qu'aucun couple de points sélectionnés ne peut avoir une distance les séparant inférieure à un certain seuil. C'est le sens donné à la qualification de « à noyau dur » dans ce type de processus : un nœud et le disque qui l'entoure est un noyau impénétrable par un autre nœud sélectionné. Les chefs de clusters sont alors sélectionnées à partir d'un point donné sous l'unique contrainte de non recouvrement des clusters. LEACH pourrait être utilisé pour construire des clusters à un seul saut mais il y a le risque d'avoir plusieurs chefs de clusters dans un seul cluster, chaque nœud s'autodéclarant tête de cluster avec une certaine probabilité.

MAXMIN est une bonne heuristique pour construire des clusters à plusieurs sauts, les données étant diffusées ensuite entre les clusters. L'intérêt de MAXMIN est qu'il choisit les chefs de clusters en fonction d'un poids affecté à chaque nœud ce qui n'est le cas ni de Matérn ni de Leach par exemple. Cette existence de poids peut présenter de nombreux avantages, du choix des chefs de clusters en fonction de l'énergie restante, à celui basé sur leur position géographique dans l'entrepôt dans le but d'optimiser la forme des clusters, ou tout autre critère. On peut aussi éventuellement forcer des nœuds de qui l'on récupère les données plus souvent que d'autres à devenir chefs de clusters. L'atout de MAXMIN sur les autres est finalement qu'il est paramétrable, d'un paramètre qui peut être fixé de nombreuses façons différentes, soit « à la main », soit dynamiquement.

Les résultats expérimentaux présentés dans [BGMS10] montrent que le MHP est meilleur que MAXMIN en termes de nombre de messages nécessaires pour choisir la tête de cluster, pour la maintenance de l'ensemble des chefs de clusters, qu'il demande moins de mémoire, aussi bien dans les réseaux denses que dans ceux clairsemés. Les auteurs de [BGMS10] montrent que MHP a un comportement qui dans une certaine mesure passe à l'échelle et qu'il est très facile à implanter. MAXMIN a évidemment un coût lié à la possibilité qu'offre son paramétrage qui permet de choisir comme chefs de clusters les nœuds ayant une valeur élevée de poids, tandis que MHP n'a pour seul critère que l'éloignement des chefs des clusters. Chercher le meilleur nœud en fonction d'un certain critère, son poids par exemple, impose nécessairement des échanges et donc un certaine complexité. Enfin, si MAXMIN est plus complexe que le MHP, sa complexité dépend aussi du degré moyen des nœuds et il peut donc être utilisé dans un réseau étendu peu dense. Dans le cas spécifique de la chaîne du froid que nous détaillons dans les paragraphes suivants, c'est MAXMIN que nous utilisons.

MAXMIN est, plus précisément, une heuristique distribuée de sélection d'un arbre d-dominant dans un graphe, c'est-à-dire d'un sous-ensemble du graphe tel que tout nœud est à au plus d sauts d'un élément de cet ensemble d-dominant. L'ensemble d-dominant est, comme nous l'avons dit, déterminé à partir de valeurs de poids affectés aux nœuds. Soit $x \in V$ un nœud du réseau. $N_i(x)$ le voisinage à moins de i sauts de x ; $(N_i(x))_i$ est une suite croissante au sens de l'inclusion d'ensemble. Soit Y un ensemble sur lequel une relation d'ordre total est disposée. Soit v une fonction injective de V dans Y. Soit X l'image de V par v ; v réalise alors une bijection de V sur X dont la fonction inverse est notée v^{-1} : $\forall x \in V$, $v^{-1}(\, v(x)) = x$. L'algorithme de MAXMIN dans [DMB07] généralise celui proposé par Amis et al. [APDH00] Il se déroule en 2d+1 tours.

Le premier est constitué d'éventuels échanges permettant l'initialisation de l'algorithme. Les d suivants constituent la phase Max. Les d derniers forment la phase Min. Tout sommet a deux listes Winner et Sender, de taille 2d + 1. Winner est une liste d'éléments de X. Sender est une liste d'éléments de V. Nous notons W_k (x) et S_k (x) les images en x des fonctions W_k et S_k, que nous définirons par récurrence. Nous notons k le numéro du tour.

Lors de la phase Max, un nœud détermine son nœud dominant dans son voisinage à d sauts. La phase Min permet au nœud de savoir s'il est le nœud dominant pour l'un des nœuds de son voisinage. Si c'est vrai, ce nœud doit alors appartenir à l'ensemble S, ensemble des chefs de clusters.

Phase initiale : k = 0

$$\forall x \in V,\ W_0(x) = v(x)\ et\ S_0(x) = x$$

Phase Max : $k \in [1; d]$

Supposons que les fonctions W_{k-1}et S_{k-1} soient déjà connues à partir des étapes précédentes.

Pour $x \in V$, soit $y_k(x)$ le sommet (unique) de $N_1(x)$tel que :

$$\forall y \in N_1(x)\backslash\{y_k(x)\},\ W_{k-1}(y_k(x)) > W_{k-1}(y)$$

W_k et S_k sont calculés par :

$$\forall x \in V,\ W_k(x) = W_{k-1}(y_k(x))\ et\ S_k(x) = y_k(x)$$

Phase Min: $k \in [d+1; 2d]$

Supposons que les fonctions $W_{k-1}\ et\ S_{k-1}$ soient déjà connues à partir des étapes précédentes.

Pour $x \in V$, soit $y_k(x)$ le sommet (unique) de $N_1(x)$tel que :

$$\forall y \in N_1(x)\backslash\{y_x(x)\},\ W_{k-1}(y_k(x)) < W_{k-1}(y)$$

W_k et S_k sont calculés par :

$$\forall x \in V,\quad W_k(x) = W_{k-1}(y_k(x))\ et\ S_k(x) = y_k(x)$$

Ces étapes se terminent par la construction de l'ensemble S, ensemble des nœuds d-dominants.

Soit S l'ensemble défini par :

$$S = \{x \in V, W_{2d}(x) = v(x)\}.$$

On montre (cf. [DBM07]) que tout sommet du graphe V est effectivement à moins de d sauts d'un élément de S. S est donc bien un ensemble d-dominant, celui qui est retenu comme ensemble des chefs de clusters.

3.3.9 Conclusion de la discussion

Les protocoles que nous retenons, dans l'organisation en couche et la position de notre mécanisme peuvent se résumer dans le schéma suivant :

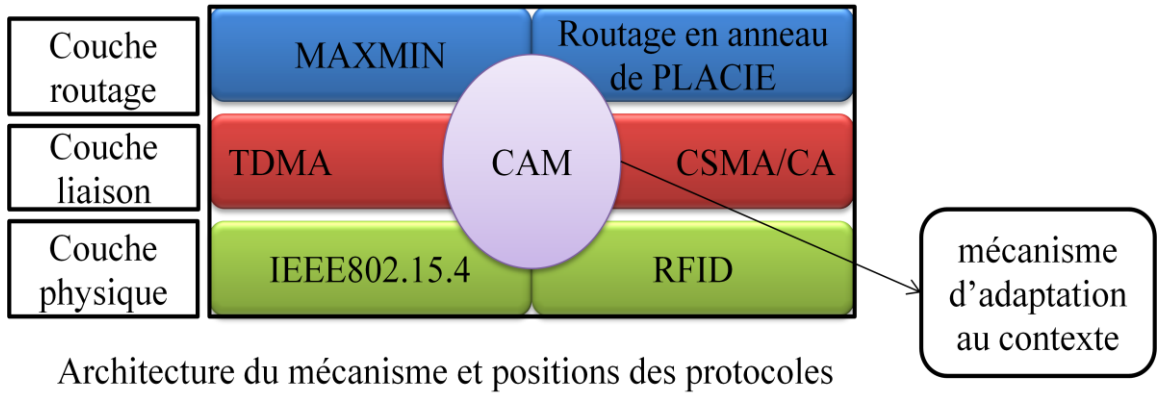


Figure 3.8 : ensemble des protocoles retenus et position du mécanisme CAM dans cette architecture

Le mécanisme CAM, dans le cadre conceptuel des protocoles retenus pour les trois premières couches du modèle O.S.I. et l'organisation retenue, communique avec ces différentes couches et joue le rôle d'un gestionnaire de toutes leurs fonctionnalités d'une manière optimale (cf. Figure 3.8).

3.4 Description du mécanisme CAM appliqué à la surveillance de la chaîne du froid

Le mode CSMA/CA sans RTS/CTS est utilisé pour transmettre la signalisation et aucun accusé de réception après la réception des paquets n'est envoyé, pour minimiser la consommation d'énergie. Pour les paquets de données, on utilise un mode TDMA, chaque nœud ayant une table d'ordonnancement contenant, ses propres dates de transmissions, réceptions et mise en sommeil, celles de chacun de ses voisins et de chaque voisin de ses voisins. En d'autres termes, tout nœud dispose de la connaissance de ses propres dates d'émissions, de celles de ses voisins et de ses voisins à deux sauts. De plus cette table d'ordonnancement contient l'identifiant des nœuds, l'algorithme de routage choisi et la chef du cluster si le nœud appartient à un réseau géré par MAXMIN.

Les informations dans la table d'ordonnancement sont échangées entre voisins. Juste après cet échange, le mécanisme CAM utilise ces informations pour détecter le changement de contexte. Les informations reçues concernant les voisins à deux sauts servent d'abord à détecter s'il y a une visibilité totale entre tous les capteurs et, dans ce cas, à provoquer l'utilisation de PLACIDE et MAXMIN sinon et, ensuite, à communiquer avec un capteur voisin en évitant le phénomène des terminaux cachés, c'est-à-dire à éviter les collisions avec les voisins des voisins. Toutes ces informations échangées sont également utilisées par un nouveau capteur qui vient d'arriver pour calculer ses propres dates d'écoute du trafic envoyé par ses nouveaux voisins, ses propres dates de transmission et sa propre durée de sommeil.

PLACIDE permet aux données d'être diffusées entre les capteurs et optimise le nombre de réveils et les périodes de sommeil. Il met en place une boucle entre les capteurs. Les périodes de réveil sont extrêmement petites et les informations envoyées par le capteur numéro n au capteur numéro n+1 dans la boucle sont envoyées par le capteur n+1 au capteur n+2 avec les

informations détectées par le capteur n+1 de sorte que les informations sont effectivement diffusées sur l'anneau formé. En outre, PLACIDE est conçu pour être utilisé seulement dans les camions où tous les capteurs sont en visibilité totale et leurs nombre limité (au plus 33). PLACIDE organise les communications d'une manière telle que dans une topologie à un seul saut l'échange de données soit efficace, sans collision en une boucle dans laquelle les flux d'informations suivent le sens de la boucle. Cette fonctionnalité lui donne non seulement les caractéristiques d'un protocole MAC, mais aussi celles d'un protocole de routage.

Nous ne pouvons pas utiliser PLACIDE tel quel, c'est pourquoi nous n'utilisons que sa partie « routage » c'est-à-dire son fonctionnement en anneau virtuel mais pas sa méthode de synchronisation qu'il utilise pour mettre en place cet anneau. En effet, PLACIDE est prévu pour fonctionner dans le cas où tous les nœuds sont en visibilité totale, et nous l'utilisons bien uniquement dans ce cas, cependant, beaucoup d'autres cas peuvent survenir qu'il ne peut pas gérer, comme ceux où un nœud arrive et n'est pas en visibilité totale avec ceux déjà présents. On peut aussi imaginer le cas où un nœud qui arrive est en visibilité totale avec les nœuds configurés en PLACIDE déjà présents mais aussi qu'il réalise un pont avec un autre nœud non visible des nœuds de la boucle PLACIDE. Ceci n'est pas géré par le protocole PLACIDE. Ces cas provoquent des comportements non prévus. Par exemple, des terminaux cachés dans PLACIDE peuvent conduire à plusieurs anneaux virtuels établis en parallèle. La synchronisation exige donc une signalisation plus complexe.

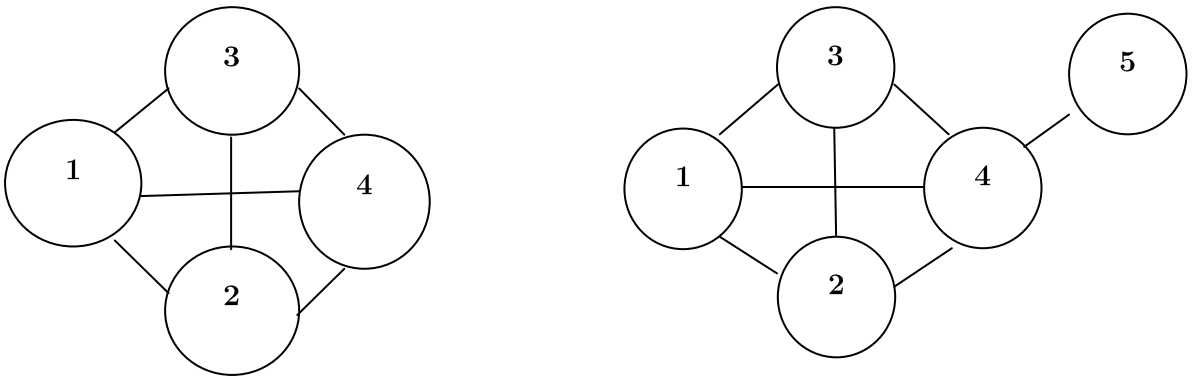


Figure 3.9 : Situation de différents voisinages

Après la synchronisation d'un nœud avec son entourage, il faut qu'il active une méthode de routage. Deux choix sont possibles: la solution de routage de PLACIDE et la configuration en cluster mise en place par MAXMIN. Le mécanisme CAM active l'un plutôt que l'autre à partir de deux critères sur le voisinage du noeud. L'un, le plus important, concerne la visibilité des voisins entre eux. Elle est totale si tous les nœuds peuvent se voir entre eux, partielle sinon. On peut encore dire qu'elle est totale si l'ensemble des voisins d'un nœud est le même que la réunion des ensembles des voisins de tous ses voisins. Le deuxième critère est le nombre de voisins. Dans notre scénario, et en se basant sur l'expérience, un nombre limite de 33 capteurs (palette) peut être transporté par camion. Le mécanisme CAM détecte alors le nombre de voisins pour vérifier s'il est inférieur ou égal à 33 et, si c'est le cas, il compare, pour chaque nœud voisin X, à partir de son tableau d'ordonnancement, l'ensemble des voisins de ce voisin X avec l'ensemble de ses propres voisins, afin de vérifier s'il a le même ensemble de voisins que X. Si c'est le cas, cela implique une visibilité totale entre tous les capteurs voisins. PLACIDE est alors activé, sinon c'est MAXMIN qui est utilisé comme algorithme de routage. Par exemple, sur le réseau du schéma à gauche de la Figure 3.9, le nœud 1 a les mêmes voisins que ses

voisins 2, 3 et 4, et ils sont bien tous en visibilité directe, en revanche, sur la figure de droite, 4 et 1 ont des ensembles différents de voisins.

La Figure 3.10 présente de façon résumée le fonctionnement du mécanisme CAM.

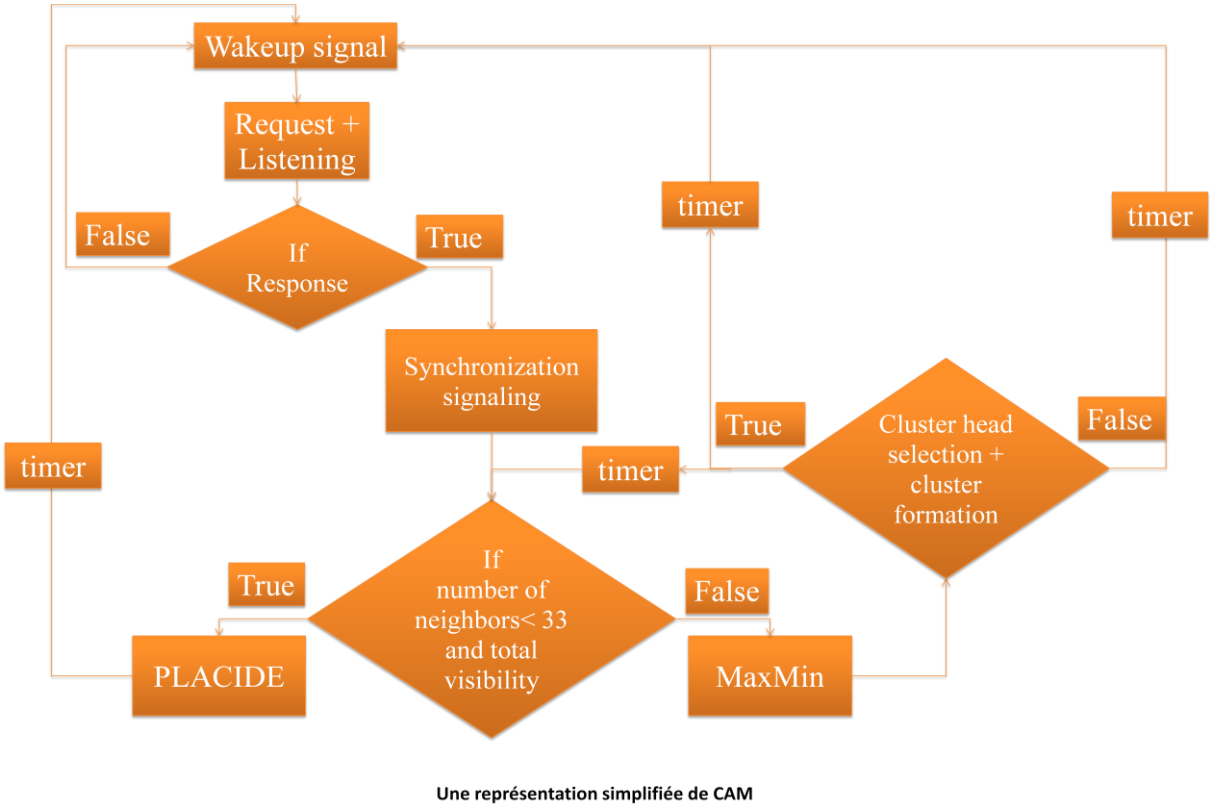


Figure 3.10 : présentation résumée du mécanisme CAM

3.4.1 La synchronisation et la détection de changement de topologie

- ***Initialisation et synchronisation***

Comme nous l'avons déjà exposé au §58, p.58, la couche physique retenue utilise à la fois le standard IEEE802.15.4 et le mécanisme de réveil à la demande et est celle proposée dans [JRO08].

La mobilité et le fait d'éteindre et allumer périodiquement la partie radio des capteurs engendrent une signalisation lourde pour la synchronisation et l'initialisation du système de communication, c'est pourquoi nous avons choisi d'utiliser un mécanisme de réveil hors-bande utilisant un système passif embarqué qui démarre, sur un signal de réveil quand un nouveau capteur change de réseau, la procédure de synchronisation. Par système passif, on entend un système électronique qui n'a pas d'alimentation en propre mais utilise l'énergie de l'onde servant à transmettre le signal et qui sert à envoyer une interruption au microcontrôleur de l'interface radio pour le « réveiller » afin qu'il puisse recevoir des données. À chaque signal de réveil, la radio de tous les capteurs voisins est activée et attend une requête. Après que cette requête est transmise, les nœuds voisins répondent et ensuite un accusé de réception du nœud demandeur termine la période de signalisation (cf. figure 2).

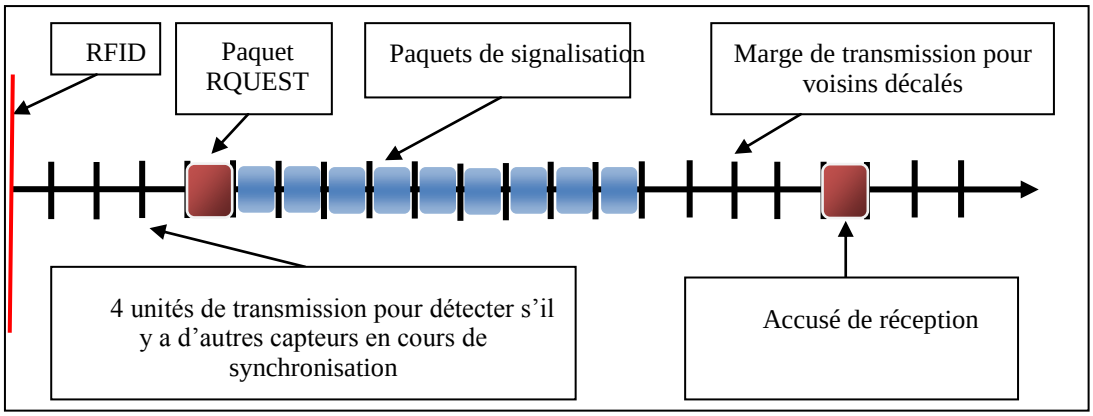


Figure 3.11 : ordre chronologique des événements de synchronisation après déclenchement d'un signal de réveill

Nous appelons synchronisation un accord sur un certain nombre d'intervalles de temps où un capteur transmet et reçoit des données sans provoquer de collision ni perturber le réseau.

Lors de la synchronisation un certain nombre de mesures doivent être prises:

1- Après le signal de réveil, les capteurs voisins entrent dans le mode de signalisation en utilisant CSMA/CA. Ce mode ne se termine pas tant que le nouveau capteur n'a pas calculé et diffusé son propre instant de transmission. Durant ce mode, le nouveau capteur demande à ses voisins leurs tables d'ordonnancement ;
2- À la réception de ces tableaux, le nouveau capteur choisit un intervalle de temps qui n'est pas déjà choisi par les autres et le diffuse aux voisins en tant que sa date de transmission permanente ;
3- Au cours de cet échange de messages, chaque capteur affecté par le signal de réveil écoute les messages envoyés par ses voisins et met à jour ses propres tableaux, sans ajout ou suppression de voisins ;
4- Après ces événements, la signalisation se termine et au cours du prochain cycle, la mise à jour horaire est transmise aux voisins des voisins.

- ***Détection de changement de topologie***

Il y a deux cas provoquant une demande de synchronisation : la détection par un nœud que le nombre de ses voisins a changé (changement de topologie) et la détection d'une collision de paquets de données. Dans ces deux cas, le mécanisme CAM déclenche un signal de réveil pour calculer un nouveau temps de transmission.

1- Cas de changement du voisinage :

Chaque capteur possède un tableau d'ordonnancement comme déjà indiqué auparavant, ce tableau contenant toutes les informations sur les voisins d'un nœud. Les voisins qui se trouvent dans le tableau forment deux ensembles : le premier contient les nœuds avec qui il doit communiquer, le deuxième contient les voisins avec qui il n'a pas besoin de communiquer. En effet, les nœuds ne communiquent pas avec tous leurs voisins, l'algorithme de routage spécifiant avec qui il doit communiquer pour optimiser les transmissions. Typiquement, dans le cas de PLACIDE, on pourrait communiquer avec tous ses voisins mais on ne le fait qu'avec un seul. Après la phase de synchronisation et durant la phase de régime permanent, un nœud écoute ses voisins pour recueillir leurs messages. S'il ne reçoit pas les messages des voisins qui sont censés

l'être, il essaie d'écouter tous ses voisins qui se trouvent dans son tableau d'ordonnancement. Si moins de 50% des réponses des voisins sont reçues, il envoie un signal de réveil et commence une nouvelle phase de synchronisation. S'il n'y a pas de réponse à une demande de synchronisation, un autre signal de réveil est réémis après un certain temps.

2- Cas de détection de collision des paquets de données :

Une collision de paquets qui arrive pour la première fois cause l'activation d'un drapeau, mais aucune mesure n'est prise contre cette collision pour s'assurer qu'elle n'est pas causée par un nouveau voisin pas encore synchronisé. Après une période, si une deuxième collision est observée, un signal de réveil est envoyé suivi d'une demande resynchronisation indiquant que les nœuds qui ont transmis à l'intervalle de temps marqué doivent envoyer le nombre de leurs voisins. Le voisin qui a le plus petit nombre de voisins, pour assurer un coût d'énergie minimale, est alors invité à se resynchroniser. Dans le cas où plus de deux réponses sont reçues à la demande de nombre de voisins, plus de deux voisins sont impliqués dans la collision et, dans ce cas, c'est le voisin qui a le plus petit nombre de voisins, et uniquement lui, qui N'est PAS affecté par la demande de resynchronisation. Si un capteur ne reçoit plus de paquets d'un voisin après deux périodes, il élimine ce voisin de sa table d'ordonnancement et il le considère comme extrait du réseau.

3.4.2 Evénements conduisant au choix de PLACIDE par le mécanisme CAM

Comme nous avons dû supprimer la partie initialisation de PLACIDE, nous avons modifié ce protocole pour qu'il puisse établir un ordonnancement des transmissions à partir du tableau d'ordonnancement construit par le mécanisme CAM. À chaque fois que ce mécanisme détecte une région de faible densité (nombre de nœud de moins de 33 capteurs) dont les nœuds sont tous en visibilités directe (cf. Figure 3.12), il choisit PLACIDE pour construire un réseau en anneau. Il fait cette détection en vérifiant à partir des tableaux d'ordonnancement leur nombre et aussi que chaque capteur a les mêmes voisins que les siens. Si c'est le cas, il choisit PLACIDE sinon il choisi l'autre algorithme qu'est MAXMIN

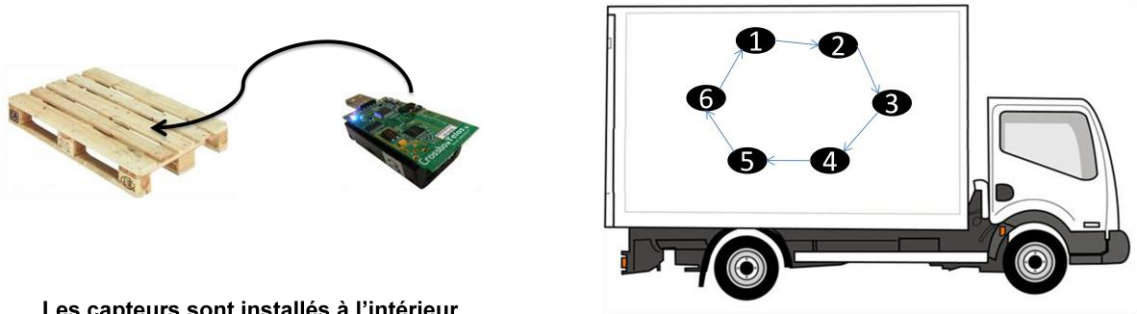


Figure 3.12

L'insertion et l'extraction d'un nœud dans une boucle PLACIDE est simple. Le mécanisme CAM gère ces événements et exécute les tests de validation des conditions de PLACIDE, puis il fait se réorganiser PLACIDE si les conditions d'utilisation de PLACIDE sont encore vérifiées et bascule vers MAXMIN si se n'est pas le cas.

Dans le cas où il détecte qu'il faut changer de protocole de routage (donc de PLACIDE à MAXMIN), le changement est fait par transmission d'un message d'un nœud à un autre dans

le sens du cycle de PLACIDE. Les nœuds qui utilisaient PLACIDE savent quand le dernier nœud du cycle est informé du changement de protocole, ils s'éveillent alors tous ensembles à ce moment pour commencer la signalisation nécessaire pour MAXMIN.

3.4.3 MAXMIN d'une heuristique de construction d'un ensemble d-dominant à un protocole de routage

Ce que nous appelons MAXMIN en tant que protocole de routage utilise l'heuristique MAXMIN pour construire un ensemble d-dominant, celui des têtes de cluster à partir du poids des nœuds. Un cluster est ensuite construit fonction du nombre de sauts spécifié (cf. Figure 3.13). Dès que le mécanisme CAM détecte une topologie qui impose l'utilisation de MAXMIN, les capteurs transmettent leur choix de routage avec leurs poids (le critère sur lequel est basé le choix de la tête de Cluster). Lorsque la confirmation que la demande d'activation de MAXMIN est reçue par tous les nœuds du réseau, ceux-ci restent dans un état de veille au cours duquel ils calculent la table de construction des clusters de MAXMIN. L'échange des poids que MAXMIN requiert impose qu'ils n'utilisent plus le mode TDMA mais CSMA/CA pour la signalisation correspondante. Durant cet état de veille, si, après quatre intervalles de temps pendant lesquels rien n'est reçu, aucun message n'est reçu et aucune collision n'est détectée, tout capteur redemande leurs poids à ses voisins. À la fin, si un capteur découvre qu'il est chef d'un cluster, il diffuse un message qui est rediffusé de nœuds en en nœuds dans la limite de la taille des clusters pour annoncer qu'il est le chef du cluster qui est en cours de construction.

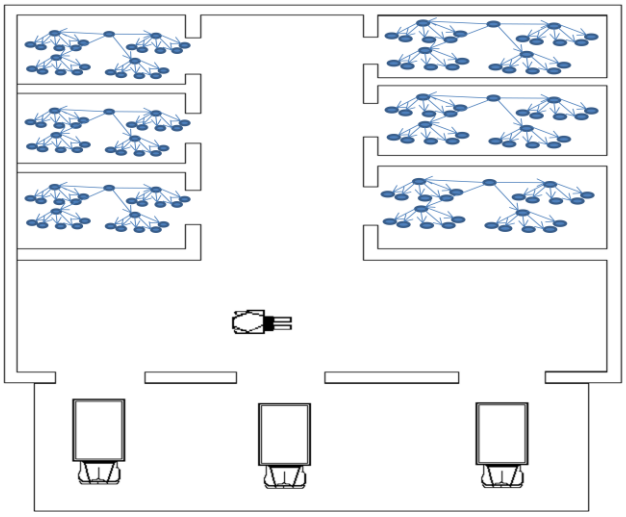


Figure 3.13 : dans un entrepôt, organisation en clusters

Après que chaque capteur a reçu et transmis l'annonce de la tête de cluster élu, MAXMIN donne la main au mécanisme CAM pour remettre le capteur dans son état synchronisé comme prévu dans son tableau d'ordonnancement. Au cours du déroulement de MAXMIN, tous les nœuds sont synchronisés au sens des étapes de l'algorithme MAXMIN : chaque capteur reste bloqué jusqu'à ce que tous ses voisins aient fini l'étape de MAXMIN dans laquelle il est, ainsi l'envoi des poids entre les nœuds est-il synchronisé entre eux.

- ***Insertion et extraction des nœuds et réélection périodique de la tête de cluster dans un réseau géré par MAXMIN :***

Durant l'insertion et l'extraction d'un nœud, c'est le mécanisme CAM qui assure la synchronisation pour les couches MAC et physique. La gestion du réseau reste faite en mode MAXMIN. Si un nouveau nœud est inséré, le réseau reste en MAXMIN parce qu'il y a déjà une contrainte qui n'est pas satisfaite de PLACIDE. Si un réseau est géré par MAXMIN, seul l'enlèvement d'un nœud peut le conduire à basculer en PLACIDE : si les contraintes de celui-ci deviennent satisfaites.

- ***Election de la tête de cluster :***

La tête de cluster est l'élément le plus important dans le protocole MAXMIN. Toute décision de changement de tête de cluster et de reconstruction du cluster est prise seulement par la tête de cluster lui-même. Dans le cas de l'extraction de la tête de cluster, ses voisins détectent sa disparition lorsque la tête de cluster ne transmet plus ses paquets aux instants qui lui sont réservés pendant deux périodes. Dans ce cas, ses voisins se comportent comme s'ils avaient reçu un message de la tête de cluster lui-même demandant de reconstruire le cluster. Chaque message envoyé par la tête de cluster est marqué par lui et transmis du nœud père au nœud fils par tous les nœuds du cluster. Ainsi, si la tête de cluster disparaît tous les membres du cluster connaissent-ils sa disparition. Dès que celle-ci est détectée, une signalisation spécifique pour la réélection d'un nouveau chef et la construction d'un nouveau cluster démarre.

- ***Gestion de l'insertion et de l'extraction d'un nœud régulier par MAXMIN :***

Toute extraction ou insertion d'un capteur n'étant pas tête de cluster provoque une intervention du mécanisme CAM pour décider du choix de l'algorithme de routage. Si PLACIDE doit être appliqué, alors le message est envoyé à la tête de cluster, qui donne l'ordre de basculer vers PLACIDE et l'ordre est aussitôt appliqué.

Nous avons dit que tout nœud a des voisins avec qui l'algorithme de routage autorise la communication et d'autres auxquels il n'envoie jamais de données directement. Même si ces derniers ne communiquent pas directement avec le nœud, ils doivent mettre à jour la liste de leurs voisins contenue dans leurs tables d'ordonnancement (lesquelles contiennent bien la liste des voisins avec qui ils communiquent et les dates d'envois correspondantes dans la période mais aussi les voisins avec qui ils ne communiquent pas directement). Pour cela, quand l'extraction d'un nœud est détectée, l'information correspondante est transmise à la tête de cluster qui, en retour, diffuse vers les noeuds voisins du nœud extrait une demande pour l'enlever de leurs tables d'ordonnancement. C'est ainsi que les voisins qui avaient ce nœud dans leur ensemble « des nœuds à ne pas écouter » sont informés de l'extraction. En effet, ils ne peuvent pas détecter l'extraction par eux-mêmes n'étant pas en communication directe avec lui.

- ***La réélection périodique de la*** tête ***de cluster :***

La structure du réseau géré par MAXMIN est rafraichie périodiquement. Le protocole MAXMIN impose que la tête de cluster initie régulièrement la procédure d'élection d'un

nouveau chef. Dès son élection, celui-ci diffuse un message indiquant la prochaine date de réélection.

3.5 Consommation d'énergie et résultats de simulation

Pour évaluer notre mécanisme, nous nous intéressons à l'énergie consommée par les différentes parties de notre mécanisme (signaux de synchronisation, signalisation de MAXMIN et transmission de données) pour vérifier si elle est compatible avec l'ordre de grandeur de l'énergie stockée dans les batteries classiques mais, comme le temps de synchronisation est également un critère de performance important de notre système à cause de la mobilité inhérente à la chaîne du froid, nous l'évaluons aussi dans les camions. En effet, c'est dans les camions que ce temps doit être le plus élevé.

Nous avons construit notre propre simulateur C à événements discrets pour obtenir une première évaluation des performances de notre mécanisme. Pour modéliser le transport de palettes, 33 palettes sont aléatoirement et uniformément prélevées de l'entrepôt et mises en place dans un camion. En même temps, deux temporisateurs sont utilisés pour tirer des instants exponentiellement distribuées : l'un représente la date où le camion revient à l'entrepôt et l'autre le départ du camion suivant. Lorsque le camion revient, les 33 palettes sont aléatoirement et uniformément distribuées dans l'entrepôt. Après la synchronisation, chaque capteur est configuré par l'administrateur du réseau pour transmettre un paquet toutes les vingt minutes et reçoit un paquet de chacun de ses voisins selon l'algorithme de routage.

Les paramètres utilisés dans la simulation sont les suivants:

1. La capacité du lien est de 250kbps.
2. La taille de chaque paquet est de 132octets.
3. Chaque période est de 20 minutes (chacune décomposée en 282352 slots, temps d'envoi d'un paquet).
4. La moyenne de la distribution exponentielle du temps écoulé entre deux arrivées est de 4 heures et de même pour la moyenne de la distribution du temps séparant deux départs exponentielle de camions.
5. Le rayon de couverture du signal de réveil est le même que la portée de transmission des données: 6m.
6. La surface où les nœuds sont rassemblés dans l'entrepôt est de 6000m^2 et pour le véhicule de 12 m^2.

3.5.1 Evaluation de la consommation d'énergie

Le nombre de paquets échangés est évalué relativement au nombre total de nœuds, puis nous en déduisons une estimation de l'énergie consommée par un nœud. Nous considérons que les coûts énergétique E pour la transmission et la réception d'un paquet sont les mêmes. Pour estimer la borne supérieure de la consommation d'énergie, nous prenons E égal au coût de la réception du plus grand paquet qui peut être reçu par ZigBee.

$$E= 21,8mA*4.25ms*3V \text{ soit } 0,00027795\ J.$$

Le nombre de signaux de réveil déclenchés dépend de la mobilité des nœuds voisins. L'énergie consommée liée à un signal de réveil est égale à:

$$E_{WS} = (N * E_{RFID}) + E_{Trx}.$$

où E_{RFID} est l'énergie consommée pour déclencher un signal de réveil égale à 1.2mJ pour le récepteur et l'émetteur, E_{Trx} est l'énergie consommée lors de l'échange de messages de signalisation entre voisins, égale à la somme des coûts énergétiques de chaque événement de transmissions ou réceptions suivants : requête, acquittement contenant la date de transmission du nouveau nœud et les 8 intervalles de temps de marge ainsi que les paquets des voisins. N est le nombre de voisins affectés.

$$E_{WS} = N*1.2*10e\text{-}03 + (N+10)*E.$$

Sur la Figure 3.14, l'énergie consommée pendant deux ans par le réseau pour la signalisation de synchronisation, pour la transmission des paquets de données et pour la signalisation MAXMIN est représentée. On peut remarquer que le coût de synchronisation est assez faible. En effet, cela dépend de la fréquence des déplacements et la fréquence des arrivées de camions: plus il y a de déplacements et plus la consommation d'énergie est importante. Néanmoins, ce coût devrait rester faible, car le camion ne peut supporter le transport que de peu de palettes à la fois et elles passent la plupart de leur temps dans les entrepôts.

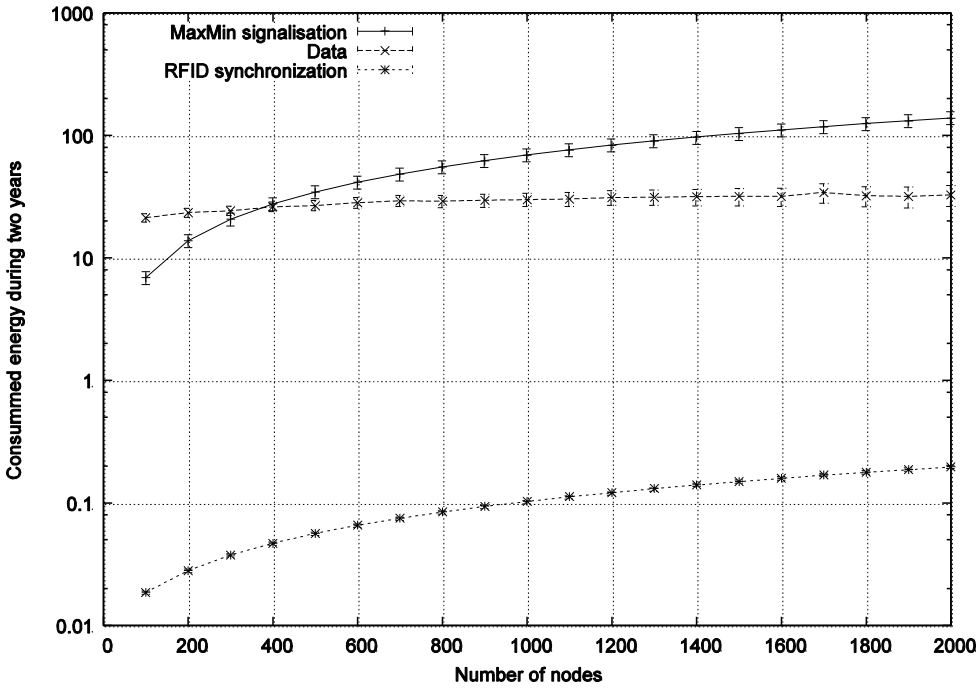


Figure 3.14: consommation d'énergie (en joules) pour les différents types de trafics en fonction du nombre de nœuds dans le réseau

3.5.2 Estimation des retards de synchronisation dans le camion

Il est important d'avoir une idée du temps nécessaire pour que les capteurs se synchronisent. Dans les entrepôts, les retards sont plus petits que dans le camion où la densité de nouveaux capteurs mis en place est plus élevée que dans les entrepôts puisque les palettes sont serrées au maximum dans le camion. Soit $E[T_1]$ le temps moyen d'attente pour que le premier capteur se synchronise quand il arrive dans un camion. $E[Ti]$ est le temps de réponse moyen (temps d'attente et temps de service) pour que *l'i-ème* nœud se synchronise.

$$E[T_1]=C+E[\tau_1]+T_{request}+N_{respons}*T+T_{Ack}+\theta_{margin\ slots}\theta_{marginSlots}$$

$$E[T_i]=E[T_{i-1}]+E[\tau_i]+T_{request}+N_{respons}*T+T_{Ack}+\theta_{margin\ slots}$$

où $i \in [1,\ldots,N_{Truck}]$, N_{Truck} est le nombre total de capteurs dans le camion, C est la durée d'une période, $N_{respons}$ est égal à N_{Truck}, $T_{request}$ et T_{ack} sont pris égaux à T (4.25ms), $\theta_{marginSlots}$ est égal à $8 * T$. τ_i est une variable aléatoire uniformément répartie sur $[0;Tmax]$. τ_i représente la durée d'attente qui indique aux nœuds quand déclencher leur signal de réveil. La moyenne $E[\tau_i]$ est donc T_{max}/N_{Truck} pour tout i, où on fixe la valeur de T_{max} à 20 minutes.

Le délai de synchronisation dans un camion est majoré par 2 cycles. Dans la Figure 3.15, il est intéressant de remarquer que ce retard diminue avec le nombre de nœuds. En fait, $E[\tau_i]$ qui est dominant dans la formule diminue avec le nombre de nœuds, mais le temps de synchronisation globale reste à peu près le même.

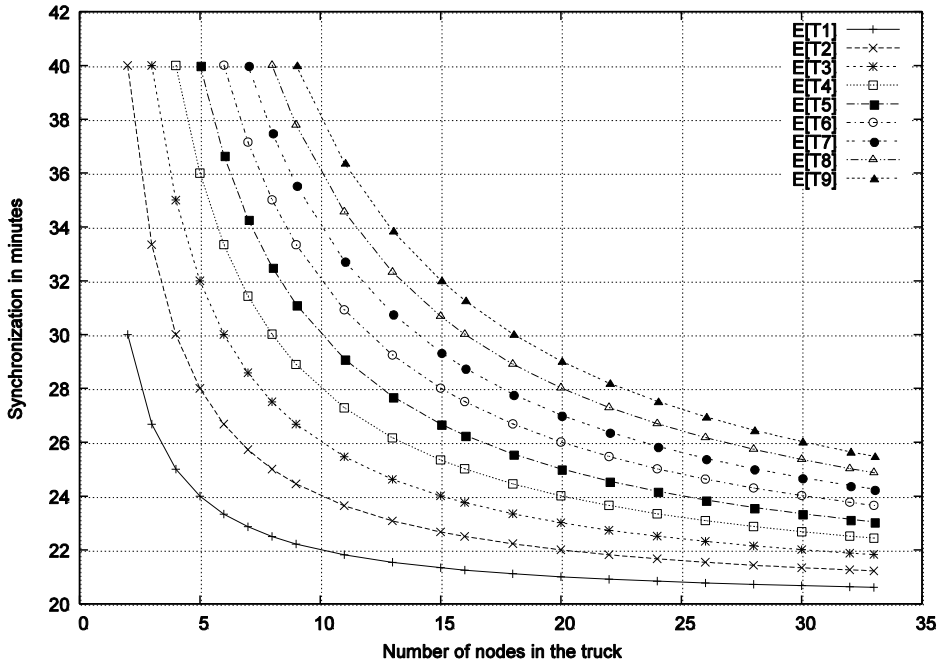


Figure 3.15 : durée de synchronisation en fonction du nombre de nœuds dans le camion

En conséquence, les retards estimés par les modèles proposés sont compatibles avec le temps passé dans l'entrepôt et le temps de transport à l'intérieur du camion.

3.6 Conclusion

Les réseaux de capteurs sont amenés à passer par des environnements très différents et à former des réseaux ayant des structures variées. Les protocoles doivent donc être choisis en conséquence. Comme il n'existe pas de protocole de routage ou d'accès au médium qui soit universel, c'est-à-dire adéquat à toutes les topologies et tous les contextes possibles, il est nécessaire de pouvoir changer de protocoles dynamiquement en fonction du contexte. Ceci pose des problèmes précis comme celui de la détection du changement de contexte, celui de la reconnaissance du contexte et celui du choix du meilleur protocole à utiliser. Nous proposons dans ce chapitre un cadre conceptuel pour permettre une telle adaptation dynamique au contexte au niveau des trois couches basses du modèle O.S.I., nous sélectionnons une panoplie de protocoles adaptés aux différentes situations que peut rencontrer le réseau dans le cadre

d'hypothèses précises et nous présentons le mécanisme CAM qui permet d'orchestrer le tout en détectant le changement de contexte, en reconnaissant le nouveau contexte et en activant les bons protocoles en conséquence.

Cette proposition part d'un besoin identifié dans le cadre de la chaîne du froid mais dépasse cette application spécifique. Nous reconnaissons par exemple les mêmes problématiques qui se posent pour la surveillance du corps humain. Ces réseaux alternent des moments où leurs nœuds sont tous en visibilité directe avec d'autres où ils sont plus étendus, à densité plus faible et nécessitent un routage à plusieurs sauts. Après avoir posé les hypothèses sur lesquelles nous construisons notre proposition, nous passons en revue et discutons les protocoles que nous retenons dans notre cadre. Ceux-ci sont des exemples qui conviennent bien aux situations que le réseau risque de rencontrer, mais nous ne prétendons pas que d'autres protocoles ne peuvent pas faire également l'affaire. C'est ainsi que nous utilisons la solution de Jurdak présentée dans [JRO08] pour la couche physique, qui comprend à la fois le standard IEEE 802.15.4 et un système de réveil à la demande, un passage dynamique entre un mode TDMA et un mode CSMA/CA au niveau MAC et une alternance entre la solution de diffusion de l'information de PLACIDE et une autre basée sur une organisation en clusters, celle de MAXMIN ou le processus ponctuel de Mattérn pour la couche routage. Outre leur adéquation à nos attentes en termes de fonctionnalités, ces trois derniers protocoles présentent l'avantage d'avoir été déjà testés en environnement réel.

Le mécanisme est décrit en détails pour le cas particulier de la chaîne du froid, puis ses performances sont évaluées.

À l'issue de ce travail, plusieurs améliorations sont possibles et des perspectives nouvelles se dessinent. On pourrait coupler la durée des périodes au contexte dans lequel se trouvent les capteurs ou à l'activité de l'homme ou encore à l'activité des voisins. Il est raisonnable de penser que dans l'entrepôt elles peuvent être plus longues que pendant les phases de transport. On pourrait aussi les coupler aux résultats des mesures comme le suggère Frederica Darema dans d'autres contextes (cf. [DAR10]).

Par ailleurs, dans ce chapitre les canaux de communications sont considérés idéaux. Les seules causes de perturbations de l'environnement provoquant une réaction du mécanisme CAM sont les déplacements de nœuds. Nous n'avons pas pris en compte la variation de l'environnement due à d'autres phénomènes comme des trafics concurrents d'autres réseaux, d'autres technologies qui peuvent interférer comme le WiFi ou le BlueTooth par exemple. La détection et l'adaptation à tout phénomène exogène ne sont pas gérées par le mécanisme CAM mais il n'en demeure pas moins que ces phénomènes peuvent perturber grandement le réseau et qu'on peut concevoir des mécanismes réactifs pour s'y adapter. Cette question est justement traitée dans le chapitre suivant. On s'intéresse à la cause des pertes de paquets dans un réseau de capteurs, et plus particulièrement à l'identification de cette cause pour mettre en place les réactions les plus appropriées. En effet, lorsque des paquets sont perdus, des réactions génériques peuvent être appliquées mais connaître précisément la cause de la perte permet d'appliquer une réaction optimale. Cela peut aider aussi à mettre en place des systèmes d'auto-organisation. Par exemple, si la perte est due à un problème de faible rapport signal sur bruit ou à des interférences avec un réseau WiFi, les solutions à apporter sont de natures vraiment différentes.

Chapitre 4. Détection à la volée des empreintes des réseaux concurrents et proposition d'adaptation dynamique de lien

4.1 Introduction

Les réseaux de capteurs et ZigBee se basent sur le standard IEEE802.15.4. Ils constituent l'un des types de réseaux les plus utilisés et déployés dans les environnements industriels et médicaux. Dans ce chapitre, par ZigBee et réseau de capteurs on sous-entend IEEE802.15.4. Les réseaux de capteurs partagent avec d'autres technologies la bande 2.4 GHz du spectre de fréquences connue comme bande dite industrielle, scientifique et médicale (ISM). Les technologies les plus présentes dans cette bande sont celles qui se basent sur Bluetooth et standard IEEE 802.11b/g. En raison de la coexistence dans la même bande ISM, lorsque qu'aucune planification radio n'est faite, les interférences imposées au réseau de capteurs par ces technologies sont inévitables. C'est un problème essentiel puisque les réseaux de capteurs sont très sensibles à l'environnement (cf. [BBDGKM09]) et ils se basent souvent sur les mesures de performance du réseau pour adapter leurs algorithmes de configuration (niveau routage et ordonnancement). Le but de ce chapitre est de présenter un mécanisme de détection et d'adaptation permettant aux nœuds d'un réseau de capteurs de reconnaître dynamiquement la présence de différentes technologies utilisant la même bande de fréquence au même moment et d'adapter leurs modes de transmission en conséquence.

La source de cette vulnérabilité à la coexistence est l'hétérogénéité des mécanismes des couches physiques et MAC. Cette hétérogénéité conduit à un phénomène similaire aux terminaux cachés et est accompagnée de collisions et d'interférences. La coexistence avec le WiFi a un effet important sur la performance des réseaux de capteurs sans fil, surtout sur la prévention des collisions et l'équité entre les deux technologies. Les taux de transmission (Tx) du WiFi et du ZigBee impactent beaucoup cet effet. En revanche, notre travail ainsi que [BGS08] montrent que les interférences avec le Bluetooth, grâce à son mécanisme de saut de fréquences, ont un effet moindre sur le réseau de capteurs. Ceci provient de ce que le Bluetooth n'utilise pas de mécanisme de détection de la puissance du canal pour déterminer si le canal est occupé ou pas, mais emploie à la place le FH/TDD pour l'accès au canal.

En raison de sa faible puissance d'émission et son faible débit nominal, le réseau de capteurs est affecté par les technologies qui ont des puissances de transmission et des seuils de détection plus élevés que les siens. Le protocole de la couche MAC le plus utilisé par ces technologies de communication sans fil est le CSMA/CA. Quand il a été mis au point, la diversité des technologies telles que le IEEE802.11 et le IEEE802.15.4 n'existait pas. En adaptant le CSMA/CA à ces technologies, des modifications ont été introduites sur ses seuils de sensibilité, les taux de transmission, etc. Cela a conduit, dans un environnement de coexistence, à la perte de l'équité et de la prévention des collisions initialement assurées par le CSMA/CA dans un contexte homogène.

Le problème du CSMA/CA est dû aux techniques utilisées pour faire l'évaluation de l'état libre du canal (le "clear channel assessment" ou CCA). Les différents types de CCA existants [RR07] sont: celui reposant sur la détection d'énergie (ED), celui sur la détection de préambule (PD) et enfin celui basé sur la décorrélation (DB).

Les méthodes alternatives de détection de spectre utilisées par les radios cognitives, y compris l'estimation spectrale à fenêtres de pondération multiples, l'utilisation de la transformée en ondelettes, de la transformée de Hough, et l'analyse temps-fréquence ne peuvent pas être appliquées par les technologies se basant sur l'IEEE802.15.4 en raison des limitations en complexité de calcul des capteurs et à cause des contraintes énergétiques. La détection de préambule ne peut pas être utilisée par l'IEEE802.15.4 pour détecter les transmissions des technologies utilisant l'IEEE802.11 en raison du coût énergétique et de la complexité des traitements (nécessité de taux d'échantillonnage élevé, filtrage, etc.). La détection basée sur la décorrélation est une combinaison de celles basées sur l'énergie et sur le préambule et hérite donc des mêmes limitations. La détection basée sur l'énergie n'est pas très efficace dans les cas de signaux large bande avec de l'étalement de spectre car la puissance de transmission étant proche du seuil de bruit [RR07] il est difficile de détecter la transmission (cf. Figure 4.1). En outre, selon les canaux utilisés, le canal ZigBee peut se chevaucher avec l'un des canaux de WiFi. Le canal ZigBee est d'une largeur de 2 MHz et le WiFi est de 20MHz. En raison de la puissance d'émission plus faible utilisé par le ZigBee et la moyenne faible de l'énergie reçue sur la bande passante WiFi 20Mhz, un équipement WiFi ne peut pas toujours détecter une transmission ZigBee.

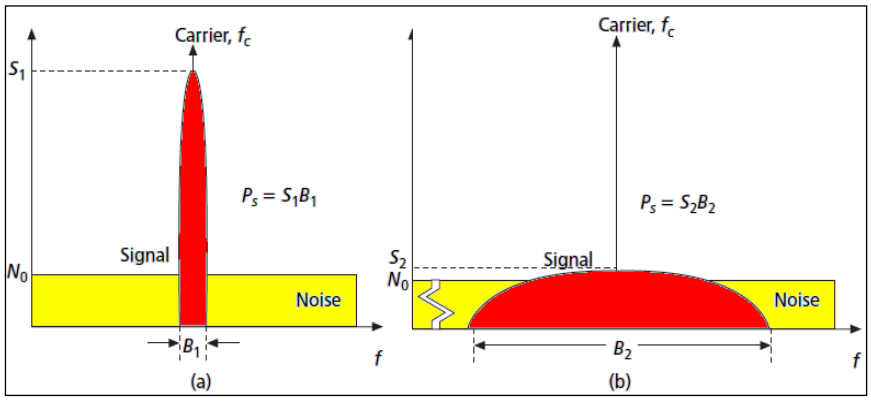


Figure 4.1 : Spectre de puissance (Ps) d'un signal bande étroite (figure a)) et Spectre de puissance d'un signal large bande pour la même puissance (Ps) (figure b)). Les deux parties sont accompagnées de la densité spectrale de bruit qui les entoure.

L'incompatibilité du CSMA/CA avec un environnement hétérogène et l'incapacité de déterminer la cause de la corruption conduisent les protocoles de la couche de liaison conçus pour un réseau de capteurs à réagir aveuglément à un paquet corrompu.

Ignorer la nature du réseau concurrent conduit à l'échantillonnage excessif de la puissance sur le canal. Inversement, connaître la technologie qui occupe le canal de façon concurrente permet, si l'on connaît les caractéristiques de ses temps de silence (moyenne, distribution, etc.) d'optimiser l'échantillonnage et l'utilisation de la bande.

Si la coexistence ne peut être évitée, nécessairement des paquets corrompus sont reçus et le réseau doit alors s'adapter intelligemment, ce qui requiert de reconnaître la cause des interférences. Connaître la cause des interférences permet alors de cibler de manière fine la bonne réaction à entreprendre. L'adaptation du lien peut être faite au niveau de la couche de routage en changeant la structure du réseau ou bien au niveau des couches MAC et physique en changeant la puissance d'émission, le canal, le taux de transmission, en ajoutant des bits redondants, etc. Dans un réseau auto-organisé où l'énergie est une ressource limitée, l'analyse

de la qualité et de la stabilité du canal est une procédure coûteuse en énergie et diminuant donc le rendement. Dans cette thèse, et c'est l'un des buts principaux de ce chapitre, nous affirmons que la cause exacte de l'erreur sur un paquet peut être déduite d'une simple analyse des erreurs sur ses bits. La meilleure contremesure peut ensuite être choisie. Lorsque les erreurs sur les paquets sont inévitables et si un mécanisme de répétition comme ARQ est utilisé, le paquet correct est finalement reçu tôt ou tard. Au lieu d'ignorer les paquets corrompus déjà reçus, nous suggérons de les conserver et de les comparer avec le paquet correct finalement reçu afin de détecter la forme des séquences d'erreur et d'utiliser cette information pour en déduire la cause des erreurs. Chaque cause doit produire une empreinte différente.

Connaître la cause des erreurs des paquets peut aider à prendre des décisions adéquates à la couche liaison (cf. Figure 4.2). En identifiant une empreinte WiFi dans le modèle des octets corrompus des paquets de ZigBee, un changement de canal peut être fait. Si la technologie Bluetooth est détectée, la contre-mesure appliquée pour le WiFi ne peut pas être utilisée puisque Bluetooth utilise le saut de fréquence. En revanche, des longueurs de paquets plus petites peuvent être utilisées. Les erreurs sur des transmissions peuvent aussi être dues au fait que l'émetteur est loin du récepteur, de sorte que le rapport signal sur bruit est petit. Dans ce cas, que nous appelons cas de lien faible, seule une faible quantité des bits des paquets transmis subit des erreurs. Des contremesures comme l'utilisation de codes FEC et de redondance de bits peuvent être appliquées. Les erreurs sur des paquets transmis peuvent aussi provenir de terminaux cachés appartenant au même type de réseau et, si elles sont reconnues, un mécanisme du type RTS/CTS ou une resynchronisation (si le réseau utilise le TDMA) peuvent être appliqués.

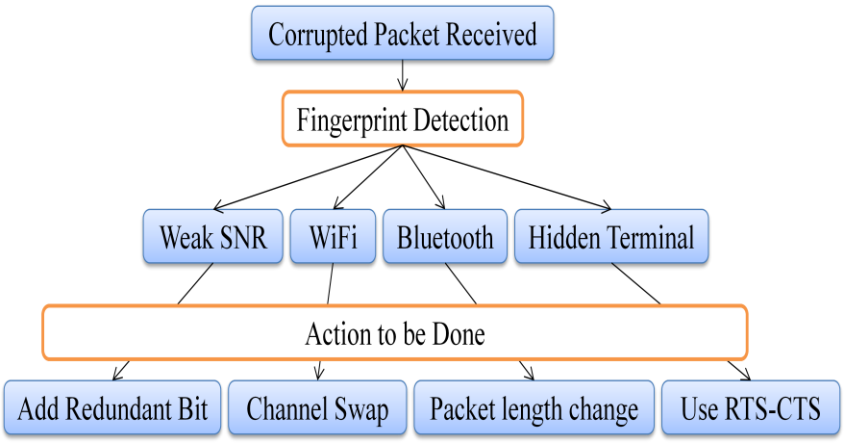


Figure 4.2 Différentes réactions possibles à différentes réseaux concurrents

Une fois les technologies concurrentes détectées et reconnues, des décisions peuvent également être prises au niveau de la couche routage. Pour un réseau utilisant un mécanisme de routage en cluster, la sélection du cluster-head peut dépendre des technologies qui l'entourent et de leurs effets sur sa communication. Par exemple, si du WiFi est détecté au voisinage d'un nœud ZigBee il y a une forte probabilité que ce nœud interfère pendant une longue durée avec le WiFi. Il est alors préférable de construire les feuilles d'une topologie à multiples sauts arborescente de telle sorte que les nœuds interférant avec d'autres technologies soient les feuilles de ces arbres, ou, au moins, ne soient pas les « cluster-heads ». Si des slots de temps périodiques sont réservés pour les émissions de certains nœuds, on peut les modifier en fonction de la technologie concurrente détectée ou les mettre sur une liste noire.

Dans ce chapitre, nous développons cette idée à partir d'expérimentations faites avec des capteurs sans fil. Les principales contributions sont les suivants:

1) Une étude empirique sur les types d'erreurs causés par différentes sources d'interférences pour exhiber des modèles d'erreurs,
2) L'identification de l'empreinte de chaque technologie à partir des modèles d'erreur,
3) La proposition d'un nouveau mécanisme et son application pour faire l'adaptation dynamique de lien. Le mécanisme de l'identification d'empreintes (FIM) nécessite peu de surcharge de trafic, est efficace au niveau de la consommation d'énergie et permet d'identifier à la volée les technologies coexistantes en fonction de leurs empreintes, enfin,
4) L'implémentation et l'évaluation de FIM sur une plate-forme réelle de réseau de capteurs.

Les applications de FIM sont vastes et dépassent certainement tout ce que nous avons suggéré ci-dessus. Bornons-nous à dire qu'il est très efficace dans les applications qui ont besoin d'un taux élevé de transmission de paquets comme dans la détection d'intrusion ou certaines applications médicales ou de surveillance de la santé.

4.2 Etat de l'art

Dans la littérature aucun mécanisme n'a été proposé jusqu'ici pour permettre à des capteurs sans fil de faire la reconnaissance dynamique des technologies qui coexistent dans la même bande de fréquence. En revanche, différents protocoles ou mécanismes ont été développés pour adapter les nœuds utilisant le IEEE802.15.4 aux cas de coexistence avec des réseaux utilisant d'autres technologies sans faire la reconnaissance : on se contentait de détecter que le trafic transmis subissait un grand niveau d'interférences pour détecter qu'il y avait un problème sans chercher à identifier de manière précise s'il était dû à un réseau WiFi, à un réseau ZigBee, ou à une autre cause. D'ailleurs, le plus souvent ces mécanismes ne sont pas mis au point pour détecter la coexistence. Ils la supposent avec une technologie donnée, par exemple avec le WiFi, et ils essayent d'adapter les nœuds Zigbee en conséquence. La plupart de ces protocoles ou mécanismes visant à atténuer les effets d'une quelconque coexistence, cible celle avec le WiFi en raison de son fort impact sur les performances du Zigbee.

A titre d'exemples, dans [YLN10] et [BGS07] le seuil du CCA de ZigBee est ajusté afin de minimiser la perte de paquets mais la technologie concurrente n'est pas explicitement reconnue. D'autres propositions, comme dans [HXZZ10], modifient la taille des paquets en se basant sur un modèle de la longueur des périodes de silence WiFi mais ils supposent que le trafic concurrent vient d'un réseau WiFi et présupposent alors des distributions de longueurs de silences. Dans [PPSG09], les auteurs font une analyse de la distribution de l'énergie reçue dans différents scénarios de coexistence, ils constatent qu'il y a des profils différents selon les scénarios mais ne vont pas plus loin dans leurs analyses. Ils l'utilisent seulement pour proposer un mécanisme qui permet, à partir de la distribution de l'énergie reçue, de déterminer la capacité du canal et éventuellement d'en changer dynamiquement si elle est trop mauvaise. Dans [PTHCB08], les auteurs proposent un mécanisme qui, lorsqu'il y a un niveau d'énergie sur un canal qui dépasse un certain seuil d'une part et, d'autre part, que le nombre de balises ZigBee reçues diminue, nécessairement à cause d'interférences selon eux, déduit qu'il y a un réseau WiFi dans l'environnement et proposent de changer de canal. Dans [HLLK07], un

algorithme est proposé permettant de choisir dynamiquement un canal d'émission en ayant éliminé ceux sur lesquels un niveau d'énergie dépassant un certain seuil est détecté. Dans [ZXX10] une méthode de détection du WiFi est présentée qui repose sur la recherche de motifs périodiques dans l'énergie mesurée sur un canal, ceci permettant de détecter la présence de balises. Celles-ci sont supposées WiFi mais ne peuvent pas être distinguées d'un autre protocole qui enverrait aussi des motifs périodiques d'une part et, d'autre part, cela nécessite une écoute permanente du canal, contrairement à notre méthode qui établit ses déductions uniquement à partir de paquets reçus, corrompus ou pas, et qu'on ne peut pas ne pas écouter ! L'article [YXG11] recense des propositions de ce type.

À notre connaissance, aucun des travaux portant sur la détection et la reconnaissance d'une technologie concurrente n'a été mené et a fortiori aucun utilisant les erreurs sur les paquets reçus.

4.3 Mesures empiriques et identification des modèles d'erreur

4.3.1 Équipements utilisés et topologie des expériences

Le but de ces expériences est de caractériser les modèles statistiques de corruption dans les paquets ZigBee, relativement à chaque technologie. Notre plate-forme se compose de capteurs sans fil "Tmote-Sky" dont l'interface radio se base sur le standard IEEE802.15.4. Ces capteurs sont équipés de l'émetteur-récepteur Chipcon CC2420 [CC2420]. On crée un signal d'interférence grâce aux équipements suivants:

a. Deux cartes WiFi intégrées dans deux pc portables DELL : la carte Intel ® pro/wireless LAN 2100 3A Mini PCI adapter dans le premier et la carte intel ® WiFi link 5100 AGN dans le deuxième.
b. La carte Bluetooth intégrée dans le portable Dell latitude utilisée comme récepteur et celle d'un téléphone NOKIA E51, l'émetteur, permettant d'envoyer un fichier vidéo long avec un débit de 2.1Mbps. L'émetteur-récepteur Bluetooth utilise la technique d'accès TDM et FHSS, avec 79 canaux, chacun étant d'une bande passante de 1MHz. Il y a 1600 sauts par seconde, l'intervalle de temps est donc de durée 625 μ s. Le débit équivalent transmis par Bluetooth sur un canal ZigBee est alors de *2MHz/ (79*1MHz)*2.1Mbps=53kbps.*

Pour surveiller les caractéristiques du canal pendant les essais, pour régler et sélectionner les canaux qui se chevauchent entre le WiFi et le Zigbee, nous avons utilisé l'analyseur de spectre «BK PRECISION by MICRONIX (8.5GHz) 2658». Nous utilisons le canal 1 pour le WiFi et les canaux 11, 13 et 14 pour Zigbee. La puissance de transmission de ZigBee a été fixée à -7dBm (PA_LEVEL = 15).

Comme il fonctionne dans la bande 2.4 GHz, l'IEEE802.15.4 nécessite de choisir les versions de WiFi qui opèrent dans cette même bande pour tester la coexistence : ce sont les versions IEEE802.11b / g. En outre, entre l'IEEE 802.11b et le 802.11g, il est important de prendre en compte le fait que l'IEEE802.11g utilise la modulation OFDM qui utilise un faible seuil de CCA. Ceci permet à l'IEEE802.11g de détecter la présence d'une transmission IEEE802.15.4 et d'appliquer le backoff. En revanche, l'IEEE802.11b utilise l'étalement de spectre DSSS (haute puissance de transmission) et a donc des seuils plus élevés que l'IEEE802.11g. Comme nous avons affaire à la corruption de paquets due à des problèmes de transmission et non à des

phénomènes de congestion, cette étude se concentre sur l'IEEE802.11b. La même idée peut être étendue à d'autres technologies.

Pour accélérer la convergence, nous avons soumis les équipements à des conditions extrêmes et des débits de transmission très élevés. Pour ces expériences, nous avons utilisé TinyOS 1.x pour programmer les capteurs. Des modifications sont apportées à l'application TOSBASE pour recevoir et analyser les paquets reçus. Afin de recevoir des paquets erronés, nous avons désactivé le contrôle du CRC et les accusés de réception de matériel générés par le CC2420 [CC2420]. Pour avoir un taux de collision élevé et par conséquent un taux de convergence rapide, nous avons désactivé le CCA et le backoff (ils sont réactivés plus tard pour la validation de FIM). Les canaux et la puissance sont configurés et adaptés selon le but de chaque expérience. Nous avons utilisé les API développées dans [BDP07] pour générer un trafic de WiFi personnalisé. Pour surveiller le trafic WiFi (paquets de données et de contrôle), nous avons utilisé Wireshark. L'analyse de collisions est effectuée pour une longueur de paquet fixe de ZigBee : 122 octets pour toutes les expériences. La topologie des expériences est présentée dans Figure 4.3 et Figure 4.4. Une distance entre un et deux mètres est utilisée pour séparer les émetteurs et les récepteurs ZigBee ce qui évite les pertes aléatoires causées par la distance et le faible SNR.

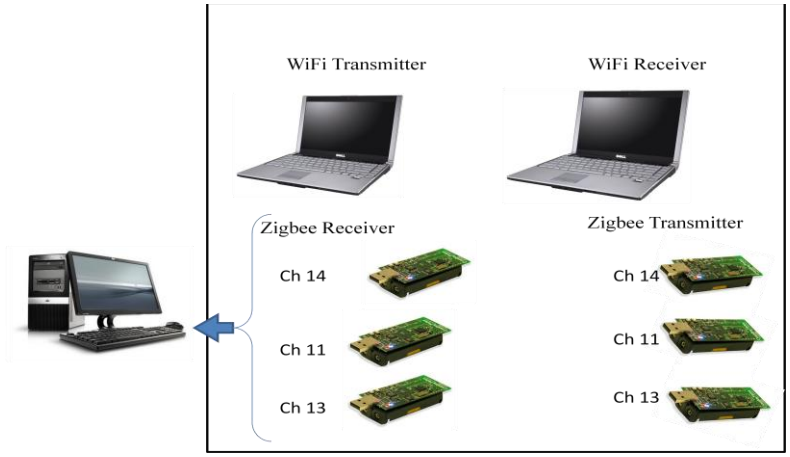


Figure 4.3 : Topologie des expériences pour l'étude de la détection de coexistence et la reconnaissance de WiFi dans l'environnement ZigBee.

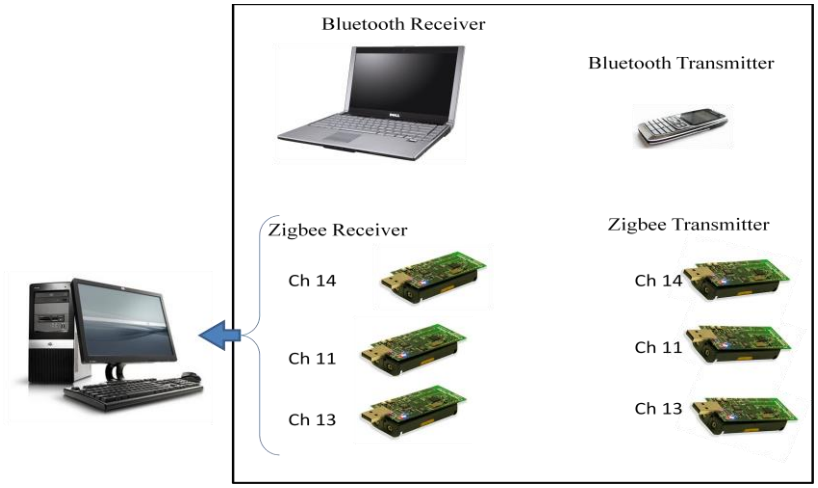


Figure 4.4 : Topologie des expériences pour l'étude de la détection de coexistence et la reconnaissance de BlueTooth dans l'environnement ZigBee.

4.3.2 Résultats des mesures

Dans cette partie, les collisions sont générées afin de déterminer les empreintes digitales des différentes technologies. La grandeur mesurée est la distribution du nombre d'octets erronés dans un paquet reçu. Nous représentons la fréquence empirique de cette distribution dans les graphes ci-dessous. C'est aussi cette fréquence qu'utilise notre mécanisme FIM. Nous définissons cinq scénarios pour les expériences correspondant aux contextes les plus typiques d'erreurs. Dans toutes les expériences, l'influence des taux de paquets transmis, les tailles de paquets et les numéros de canaux sont observés. Lorsque des collisions se produisent, le paquet ZigBee que nous analysons est soit (a) pas reçu, soit (b) reçu avec une erreur soit (c) reçu correctement. Le cas (a) se produit lorsque la collision corrompt l'en-tête de synchronisation (SHR) et la longueur de la trame. Pendant toutes les expériences, nous avons directement rejeté les paquets dont l'en-tête, qui contient la longueur du paquet, est corrompu parce qu'il provoque un dysfonctionnement à l'application. La longueur du paquet indique la durée pour laquelle la radio doit continuer à échantillonner et démoduler la porteuse et par suite très souvent quand une corruption touche l'entête qui contient la longueur du paquet il y en a buffer over flow ou bien des erreurs de parsing ce qui conduit à une halte du capteur.

Les scénarios sont les suivants:

a. Cas où il n'y a que des nœuds ZigBee dans l'environnement mais les erreurs sur les paquets sont dues à des liens à faible signal par rapport au bruit ;
b. Même cas que (a) sauf que les erreurs sont dues à des terminaux cachés ZigBee ;
c. Cas où le trafic concurrent est du BluTooth ;
d. Cas où c'est du WiFi ;

- **Cas des liens ZigBee à faible signal par rapport au bruit**

Les longues distances et la faible puissance de transmission créent des liens que nous appellerons ici par abus de langage liens faibles. Pour analyser les liens faibles, une expérience a été effectuée avec une faible puissance d'émission. Les résultats obtenus sont représentés sur la

Figure 4.6. Ici, 105849 paquets ont été transmis, dont 18% ont subi des erreurs. Les émetteurs et les récepteurs ont été placés dans des salles différentes, séparées d'une distance de cinq mètres (cf. Figure 4.5). Les expériences ont été menées sur tous les canaux. En raison de la similarité des résultats sur différents canaux de communication Zigbee, nous ne montrons que ceux qui sont typiques : ceux des canaux 11, 13 et 14 et qui serviront dans les paragraphes qui suivent. Ces canaux étant théoriquement quasi-orthogonaux, il n'y a pratiquement pas d'interférence entre les nœuds adjacents utilisant des co-canaux et la même puissance pour la transmission de paquets: chaque trafic généré sur ses canaux ne subit aucune inter-collision. Des mesures particulières ont été prises pour veiller à ce qu'aucun interférant ne soit présent, évitant ainsi la possibilité de pertes de paquets dues aux collisions.

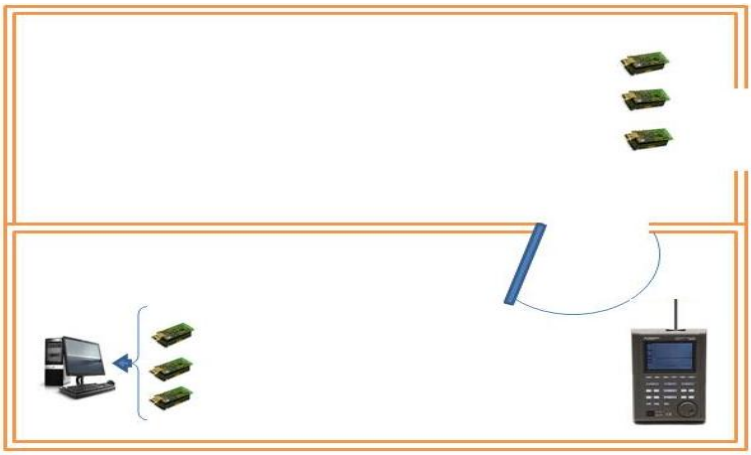


Figure 4.5 : lors de l'expérience la qualité du canal est surveillée à l'aide d'un spectromètre

La Figure 4.6 présente la fréquence empirique du nombre d'octets corrompus dans les paquets ZigBee. La longueur du paquet est de 122 octets. La densité est toujours décroissante avec le nombre d'octets erronés. Elle ne correspond pas à une distribution géométrique, qui était attendue car les erreurs sont censées être indépendantes. En fait, les erreurs dans la séquence des bits transmis sont indépendantes, mais puisque l'étalement de spectre est utilisé, lorsque le flux de bits reçu est « dé-étalé », bien des erreurs sont corrigées, ce qui est du reste la raison pour laquelle l'étalement de spectre est efficace dans les cas de signal faible, ce qui a pour effet de supprimer dans une certaine mesure l'indépendance des erreurs observées et finalement aboutit à une distribution non géométrique des erreurs.

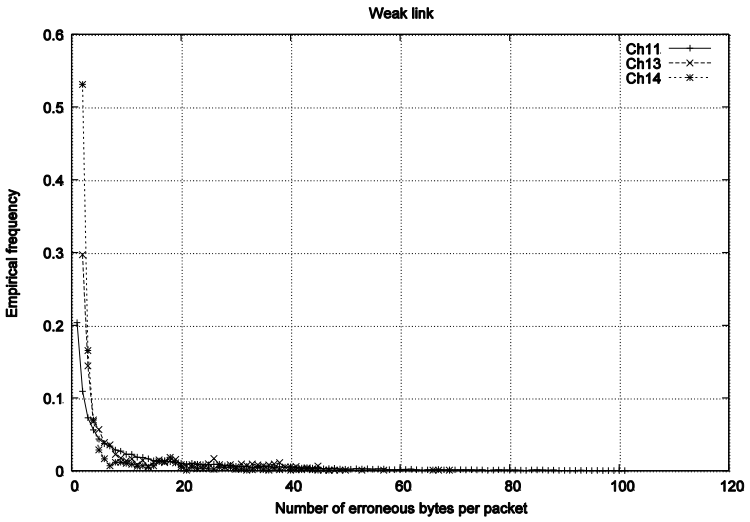


Figure 4.6: Fréquence empirique du nombre d'octets erronés pour les liens faibles

- **Interférence ZigBee (Terminaux cachés)**

Dans ce scénario, un émetteur ZigBee envoie le trafic vers son récepteur, tandis qu'un autre émetteur ZigBee envoie le trafic vers un autre, les deux couples interfèrent. Un émetteur génère des paquets d'une taille de 122 octets. Nous avons fait varier la taille du paquet envoyé par l'émetteur ZigBee concurrent (cf. Figure 4.7, Figure 4.8, Figure 4.9 et Figure 4.10).La Figure 4.7 représente les résultats du cas où un couple communique avec des paquets de longueur 122 octets tandis que l'autre utilise une taille de paquets de 16 octets. Le maximum est atteint à 11 octets avec une densité de 0,3.

La Figure 4.8 représente la collision entre les paquets de 122 d'octets et ceux de 90 octets. Un maximum apparaît à 85 octets avec une densité de 0,22.

Dans le cas de la Figure 4.9 tous les paquets ont une taille égale de longueur 122 octets. Deux maximums apparaissent, à 1 octet et à 106 octets.

La Figure 4.10 représente les collisions entre les paquets de 122 octets et les paquets de longueur 12 octets(le plus petit paquet qui peut être transmit). Un maximum apparaît à 1 octet avec une densité de 0,1.

La différence de cinq octets entre la longueur des paquets interférant avec le trafic principal des paquets de 122 octets et le nombre d'octets du pic signant la présence de ce trafic concurrent sur les fréquences empiriques est une propriété commune et remarquable entre tous ces cas. Elle est due au fait que cinq est la longueur de l'en-tête de la couche physique. Elle est moins évidente dans le cas des collisions entre des paquets de 122 octets et les paquets de 12 octets (cf. Figure 4.10). Sur la Figure 4.9, le maximum est à 106 octets, ce qui est égal à *122-11 (longueur de l'en-tête ZigBee)-(5).* Deux explications sont possibles à la présence d'un autre maximum à un octet, reliées à la différence de l'instantd'émission par rapport à un paquet de grande taille.

En effet, la radio CC2420 exige une écoute par défaut du canal après chaque transmission. A cette écoute, la radio essaye de faire un backoff que nous avons désactivé. A un certain

moment, quand la file est pleine, il y a une transmission et le résultat est qu'il y a une collision avec une grande partie du paquet visible par le pic à une longueur d'erreur égale à 106 octets.

Le deuxième type de collision est causé par la nature du système d'exploitation utilisée par les capteurs. Comme le système est basé sur les événements la cause peut être une désynchronisation entre la file et le transmetteur. Quand un paquet n'est pas prêt à être transmis après l'écoute par défaut et dès qu'il a été reçu, il est transmis sans faire l'écoute par défaut, ce qui cause le pic à un octet.

Dans les corruptions des paquets de taille 122 octets, la taille de l'en-tête doit être soustraite parce que les paquets pour lesquels l'en-tête est corrompu ne sont pas reçus et pris dans l'analyse.

Dans le cas des collisions entre des paquets de 12 octets avec ceux de 122 octets les résultats sont présentés dans la Figure 4.10. Les paquets ont une très petite taille parsuite il y a une difficulté à avoir des collisions. En principe on devrait avoir un pic à une longueur d'erreur de cinq octets, mais l'effet observé dominant est un mélange de l'effet du bruit causé par quelques collisions et de celui du lien faible.

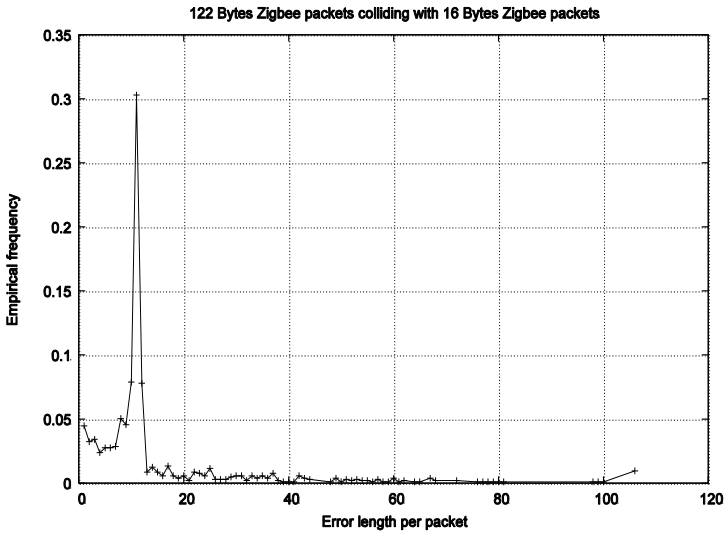


Figure 4.7 : fréquence empirique du nombre d'octets erronés dans des paquets ZigBee de 122 octets confrontés à du trafic concurrent ZigBee dont les paquets sont de taille 16 octets (scénario d'étude de l'effet des terminaux cachés)

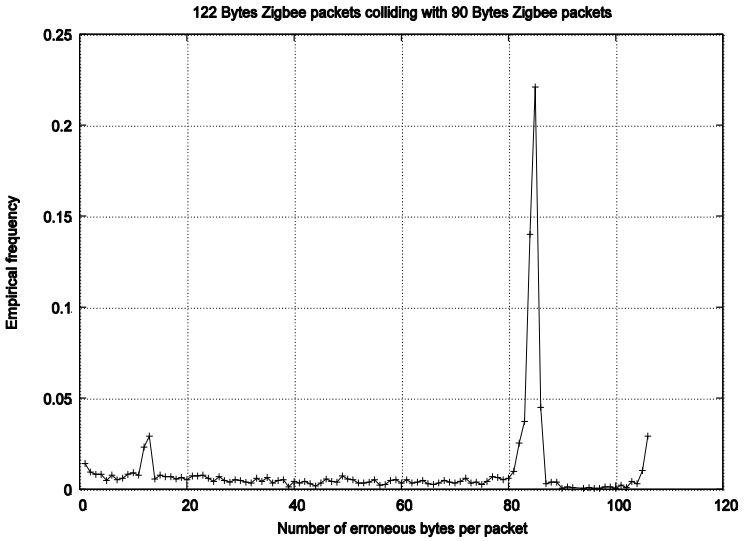


Figure 4.8 : fréquence empirique du nombre d'octets erronés dans des paquets ZigBee de 122 octets confrontés à du trafic concurrent ZigBee dont les paquets sont de taille 90 octets (scénario d'étude de l'effet des terminaux cachés)

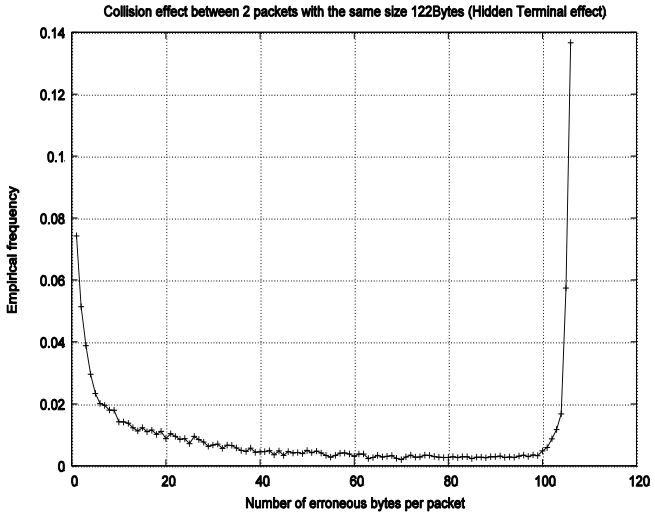


Figure 4.9 : fréquence empirique du nombre d'octets erronés dans des paquets ZigBee de 122 octets confrontés à du trafic concurrent ZigBee dont les paquets sont de taille 122 octets (scénario d'étude de l'effet des terminaux cachés

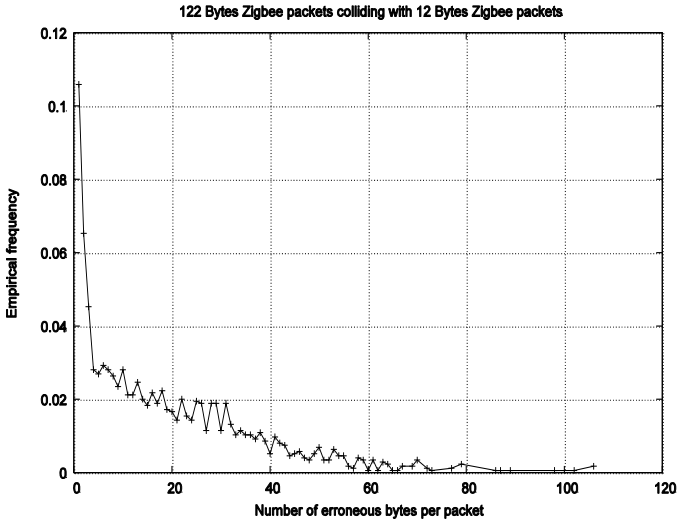


Figure 4.10 : fréquence empirique du nombre d'octets erronés dans des paquets ZigBee de 122 octets confrontés à du trafic concurrent ZigBee dont les paquets sont de taille 12 octets (scénario d'étude de l'effet des terminaux cachés

- **ZigBee avec Bluetooth**

Le scénario suivant (cf. Figure 4.11 et Figure 4.12) est destiné à observer l'empreinte Bluetooth. Lors de l'essai, 68006 paquets ont été transmis, dont 2531 paquets ont été perdus. Le taux de transmission des paquets ZigBee et les canaux utilisés ont des paramètres qui varient. Seuls les taux de transmission les plus élevés et les plus faibles de Zigbee sont présentés : 12,5 et 166 paquets par secondes (PPS). Comme on s'y attendait, la coexistence avec la technologie Bluetooth a un faible effet sur le trafic Zigbee. Moins de 4% des paquets sont perdus à cause de collisions avec les paquets du Bluetooth. Plus précisément les paquets perdus ont été perdus durant l'établissement de la connexion entre les périphériques Bluetooth (dans ce cas le taux de sauts de fréquences devient 3200 sauts par seconde).

Bluetooth a le même effet sur les trois canaux et quel que soit le taux de transmission utilisé par Zigbee. La cause de la ressemblance entre les trois canaux est due aux sauts de fréquence effectués par Bluetooth.

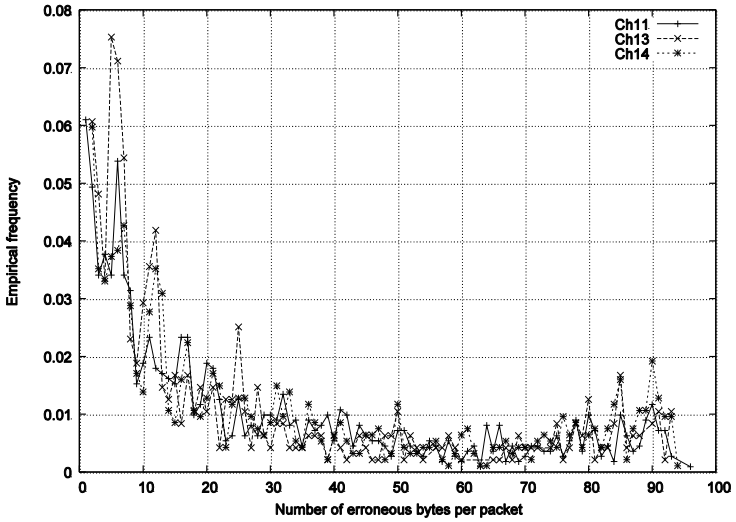


Figure 4.11 : fréquence empirique du nombre d'octets corrompus pour le scénario des collisions entre ZigBee et Bluetooth pour un taux de transmission utilisé par ZigBee de 12,5pps

L'effet des collisions des paquets ZigBee avec les paquets Bluetooth est comparé au cas des liens faibles sur la Figure 4.13. Pour la courbe qui représente les résultats de la collision entre les paquets Bluetooth et les paquets ZigBee, la plupart des corruptions ont des densités inférieures à 0,08, ce qui représente le même ordre de grandeur que les densités de corruption plus grandes que 4 octets dans le cas de la liaison faible. Les principales différences sont d'abord la densité élevée de la "corruption d'un seul octet" par rapport aux autres tailles de corruptions pour la courbe du scénario des liens faibles , l'autre différence étant le fait qu'à la queue de la courbe de densité de la collision avec Bluetooth, il y a des densités plus élevées qui apparaissent, entre 80 octets et 90 octets.

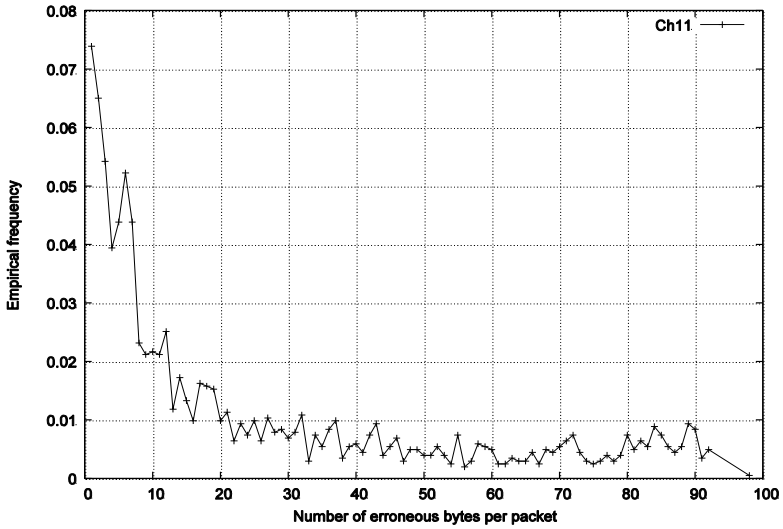


Figure 4.12 : fréquence empirique du nombre d'octets corrompus pour le scénario des collisions entre ZigBee et Bluetooth pour un taux de transmission utilisé par ZigBee de 166pps

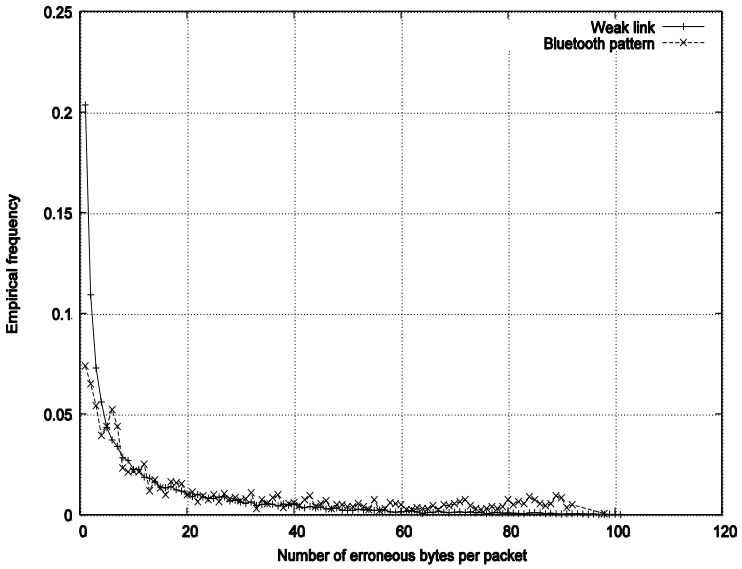


Figure 4.13 : comparaison de la fréquence empirique des erreurs causées par Bluetooth avec celles causées par un lien faible

- **Expérimentation sur les collisions de paquet entre ZigBee et WiFi**

Il convient de souligner que les taux de transmission utilisés dans les expériences de coexistence WiFi sont basés sur des scénarios réels.

Ces scenarios reposent sur le principe que l'interférence causée par les liaisons descendantes dans une surface de couverture d'un point d'accès WiFi est beaucoup plus élevées que l'interférence causée par les liaisons montantes des nœuds WiFi mobiles. La cause de cette faible interférence causée par une liaison montante est que les nœuds WiFi mobiles utilisent cette liaison pour envoyer des requêtes au point d'accès. Les requêtes sont de petites tailles, en revanche la liaison descendante supporte un trafic agrégé de différents types de trafics et pour différents nœuds mobiles ce qui cause un débit élevé. La somme de tous les trafics générés par ce point d'accès à chacun des nœuds mobiles appartenant à son domaine entre en collision avec le trafic généré par un capteur.

Tout d'abord, nous avons désactivé le trafic de données et nous avons observé l'effet du trafic de contrôle sur les différents canaux. Les résultats sont présentés sur la Figure 4.14, la Figure 4.15 et la Figure 4.16. Le chevauchement d'un canal WiFi avec les canaux Zigbee (cf. Figure 4.20) a des effets différents sur les canaux ZigBee selon leur écart à la fréquence centrale du canal WiFi. Nous avons fait varier les canaux utilisés mais nous ne montrons que les résultats du chevauchement du canal 1 du WiFi avec les canaux Zigbee 11, 13 et 14. Les résultats peuvent être étendus aux autres canaux où il y a un chevauchement similaire, par exemple celui entre le canal 1 du WiFi et le canal 11 du Zigbee a un effet similaire à l'effet du canal 7 du WiFi sur le canal Zigbee 17. Sur la Figure 4.14 et la Figure 4.16, il y a des pics à 26 et 27 octets respectivement. Ces sommets sont dus aux collisions entre ZigBee et les paquets de contrôle WiFi (balises, requêtes, etc.).

L'effet du chevauchement du canal 1 du WiFi avec le canal 14 du ZigBee présenté sur la Figure 4.15 est plus ressemblant au modèle de corruption dû à l'effet du lien faible. Cela est dû à la distribution d'énergie du trafic WiFi qui n'est pas uniforme sur son spectre, mais plus

importante sur la gauche du spectre que sur la droite (cf. [STDW99]). Le taux de transmission utilisé par le Zigbee est de 33 pps. Pendant toutes les expériences effectuées ni le taux de transmission, ni la taille des messages de contrôle n'ont été modifiés. Pour le canal 11 du ZigBee, 51182 paquets sont transmis, 7% sont perdus. Pour le canal 13, 26444 paquets sont transmis dont 18% sont perdus. Pour le canal 14, 26167 paquets sont transmis dont 6% sont perdus.

Ensuite, au trafic de contrôle du WiFi nous avons ajouté le trafic de données (cf. Figure 4.17, Figure 4.18 et Figure 4.19). Le taux de transmission de données pour le WiFi est de 916 pps avec une taille de paquets de 1500 octets, le taux de transmission de Zigbee est de 166pps avec une taille de 122 octets par paquets. Sur le canal 11, 51200 paquets ont été transmis dont 6% ont été perdus. Sur le canal 13, 51049 paquets ont été envoyés dont 18% ont été perdus. Sur le canal 14, 51182 paquets ont été transmis dont 0,7% ont été perdus. L'effet des transmissions à partir du canal 1 du WiFi sur le canal 11 du ZigBee est moindre que sur le canal 13 en raison de sa plus grande déviation de la fréquence centrale de WiFi. Sur le canal 13, il y a deux pics principaux à 27 et 4 octets. Sur le canal 11, on remarque des pics semblables, mais le premier pic est à une valeur plus petite.

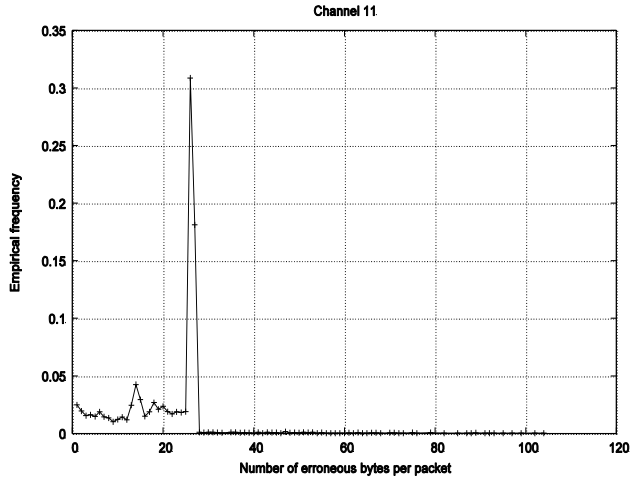


Figure 4.14 : Fréquence empirique du nombre d'octets corrompus pour les paquets du ZigBee en présence d'interférences causées par les paquets de contrôle du WiFi sur le canal 11

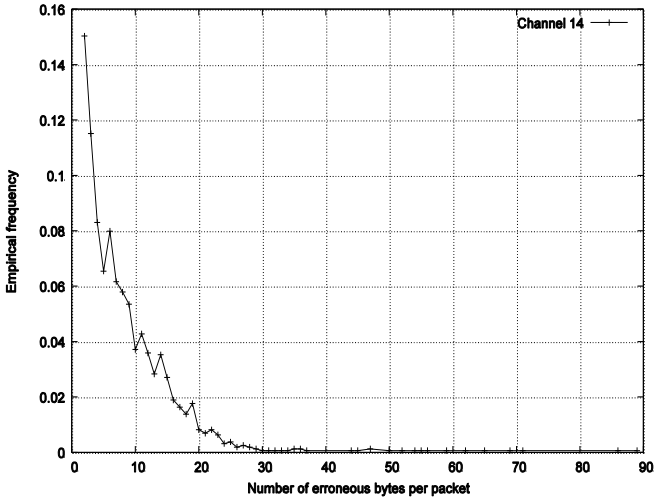


Figure 4.15 : Fréquence empirique du nombre d'octets corrompus pour les paquets du ZigBee en présence d'interférences causées par les paquets de contrôle du WiFi sur le canal 14

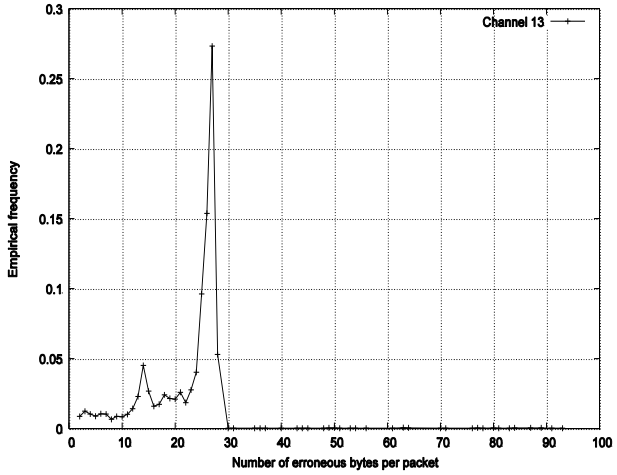


Figure 4.16 : Fréquence empirique du nombre d'octets corrompus pour les paquets du ZigBee en présence d'interférences causées par les paquets de contrôle du WiFi sur le canal 13

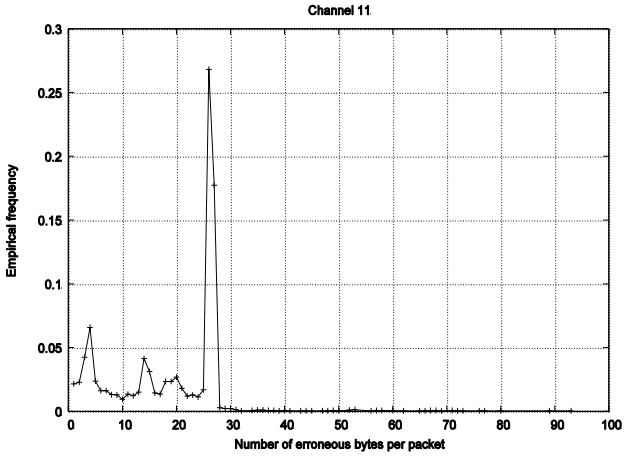


Figure 4.17 : Fréquence empirique du nombre d'octets corrompus pour les paquets du ZigBee en présence d'interférences causées par les paquets de données et de contrôle du WiFi sur le canal 11

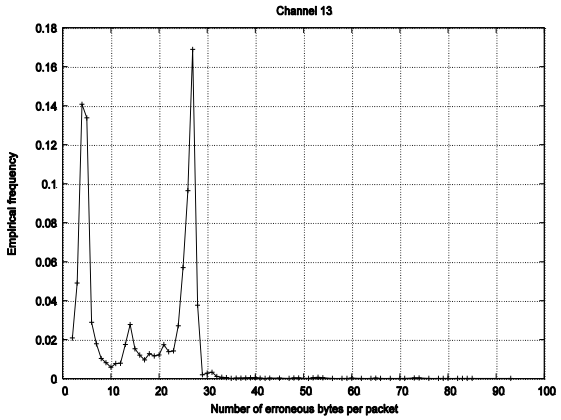


Figure 4.18 : Fréquence empirique du nombre d'octets corrompus pour les paquets du ZigBee en présence d'interférences causées par les paquets de contrôle et de données du WiFi sur le canal 13

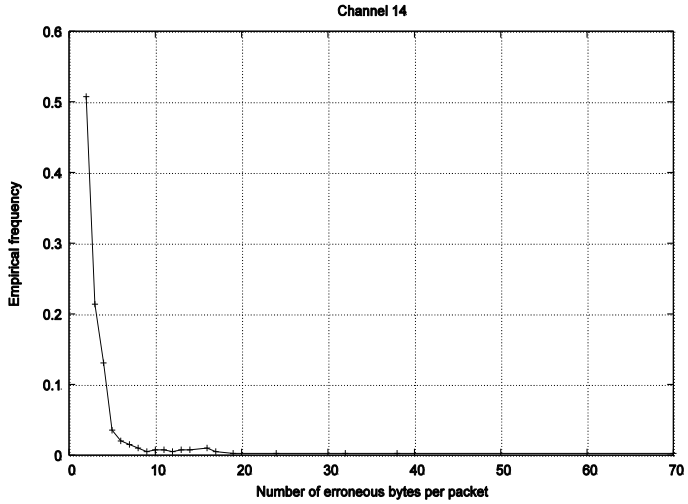


Figure 4.19 : Fréquence empirique du nombre d'octets corrompus pour les paquets du ZigBee en présence d'interférences causées par les paquets de contrôle et de données du WiFi sur le canal14

Le cas du canal 14, celui de la Figure 4.19, pour la même raison que celui de la Figure 4.15, a la même forme que la courbe du scénario de lien faible. La cause du pourcentage faible de pertes de paquets du ZigBee est que les paquets de contrôle utilisent une modulation différente de celle des paquets de données, ce qui crée plus d'interférences sur la plupart de la bande du canal du WiFi, et plus précisément sur le bord supérieur de la bande où le canal 14 du Zigbee est situé. En même temps les paquets de contrôle utilisent le débit de base ce qui implique que l'occupation du canal de ces paquets prend plus de temps que les paquets de données, provoquant ainsi une probabilité élevée d'avoir plus de collisions avec les paquets de Zigbee. Quand on ajoute le trafic de données aux paquets de contrôle, cela fait que l'émetteur WiFi envoie plus de trafic de données à la place des paquets de contrôle. Avec moins de paquets de contrôle envoyés il y a moins de collisions qui se produisent. Par conséquent l'effet dominant devient plus ou moins l'effet de lien faible.

Enfin, le WiFi a une empreinte en une forme de selle de cheval. Le premier sommet est lié aux corruptions provoquées par les paquets de données de l'émetteur WiFi. Les paquets de données provoquent des corruptions de petites tailles en raison du débit de transmission élevé des données WiFi et du fait que seulement une petite partie des canaux du ZigBee se superpose avec ceux du WiFi. Le second pic est lié aux paquets de contrôle qui utilisent un débit de base

qui est différent (2Mbps, cf. [STDW99]) du débit binaire utilisé par les paquets de données. Il y a une faible probabilité d'avoir un recouvrement entre les surfaces de couvertures des points d'accès WiFi qui utilisent les mêmes canaux. Par conséquent, l'effet de ce recouvrement est minime sur l'empreinte du WiFi. Généralement, s'il y a des points d'accès adjacents, ils utilisent des canaux différents pour éviter les interférences intercellulaires. Le résultat que Zigbee interfère seulement avec un seul point d'accès.

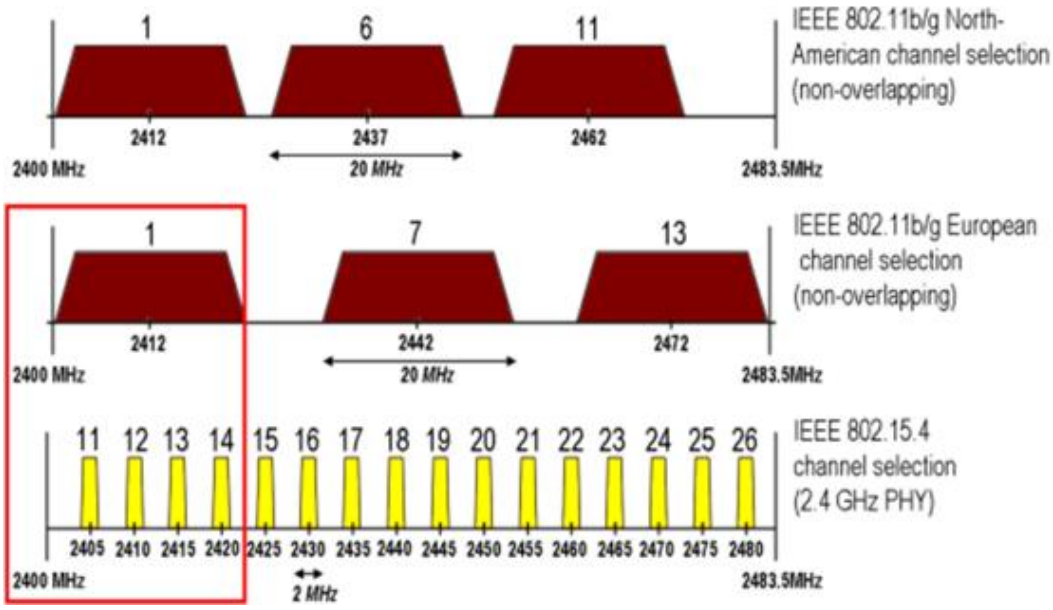


Figure 4.20 : Les canaux WiFi et ZigBee. La zone rectangulaire rouge représente les canaux utilisés dans l'expérience

Selon le taux de trafic de données, le poids de chaque pic est différent (cf. Figure 4.21), mais le modèle ne change pas. L'effet des paquets de contrôle (le pic en 26-27 octets) est observé sur les canaux 11 et 13, mais n'est pas clair sur le canal 14.

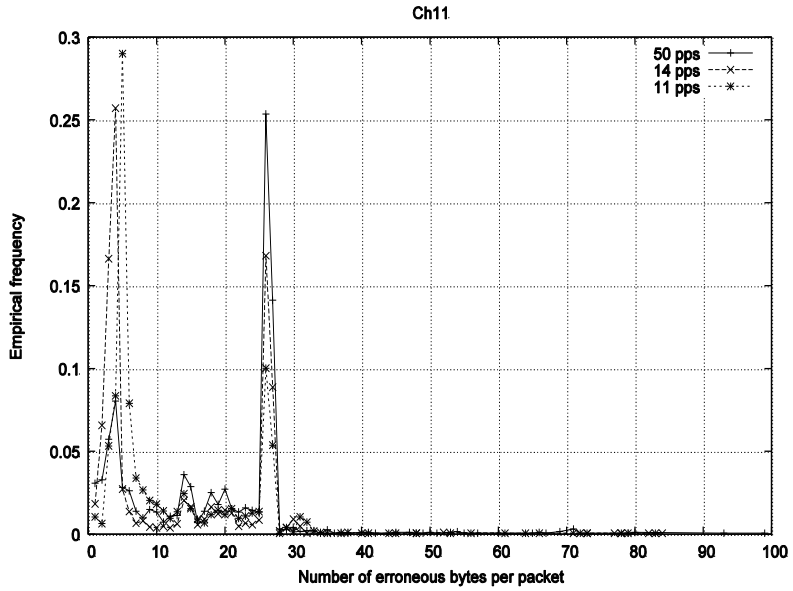


Figure 4.21: trafic WiFi qui contient des paquets de contrôle et de données, effet de la variation du taux de trafic des nœuds ZigBee

Les expérimentations avec différentes tailles de paquets WiFi montrent qu'au-dessous d'une certaine taille seuil de paquet, égale à L = 1100 octets, le pic signalant les paquets de données disparait. Dans une expérience où une transmission des paquets WiFi avec un taux de 1250 pps est effectuée, l'effet des paquets de données WiFi de taille 1100 octets est encore détectable (cf. Figure 4.22). En revanche, avec une taille de paquet de 1000 octets, par exemple, seul le pic correspondant aux paquets de contrôle apparaît (cf. Figure 4.23). Nous ne représentons pas le canal 14 sur la Figure 4.23, car nous avons eu seulement 0,2% des paquets perdus à partir de 39634 paquets transmis. Pour le canal 11, 1,5% des paquets sont corrompus sur 38488 paquets envoyés. Pour le canal 13, 19% des paquets sont corrompus sur un total de 38672 paquets transmis.

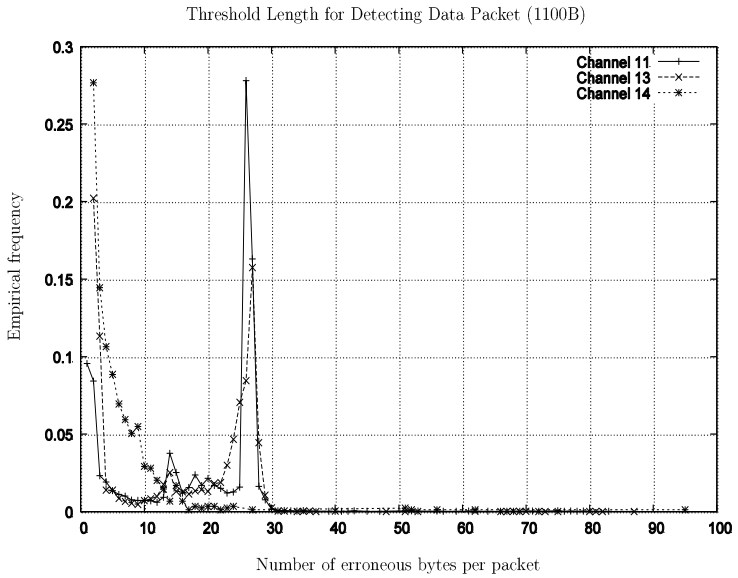


Figure 4.22 : trafic WiFi avec des paquets de contrôle et de données, effet des grands paquets WiFi

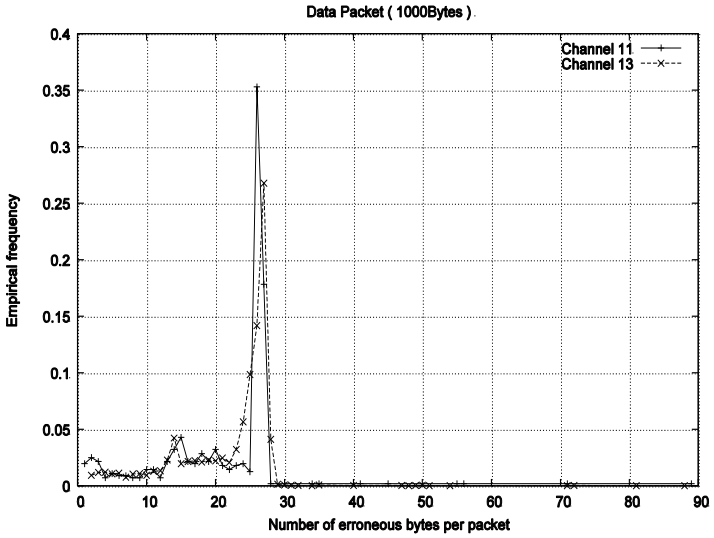


Figure 4.23 : trafic WiFi avec des paquets de contrôle et de données, effet des petits paquets WiFi

- **ZigBee avec un mélange de réseaux concurrents**

Dans une dernière expérience, nous avons mélangé les différents types de technologies concurrentes en même temps. Nous avons utilisé un émetteur WiFi transmettant des paquets de données de taille 1400 octets à la vitesse de 1250 pps à un récepteur, avec sur le canal 11 du ZigBee, deux émetteurs ZigBee qui transmettent des paquets vers un récepteur écoutant le même canal. A ces nœuds on a ajouté un émetteur ZigBee qui transmet des paquets vers un récepteur, les deux nœuds occupant le canal 13, et un autre émetteur ZigBee transmettant sur le canal 14 des paquets vers un récepteur qui écoute ce canal.

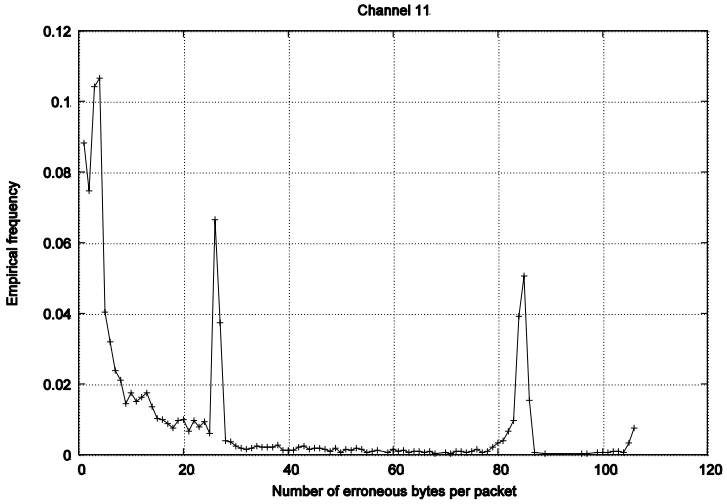


Figure 4.24 : Un mélange de réseaux concurrents observés sur le canal 11

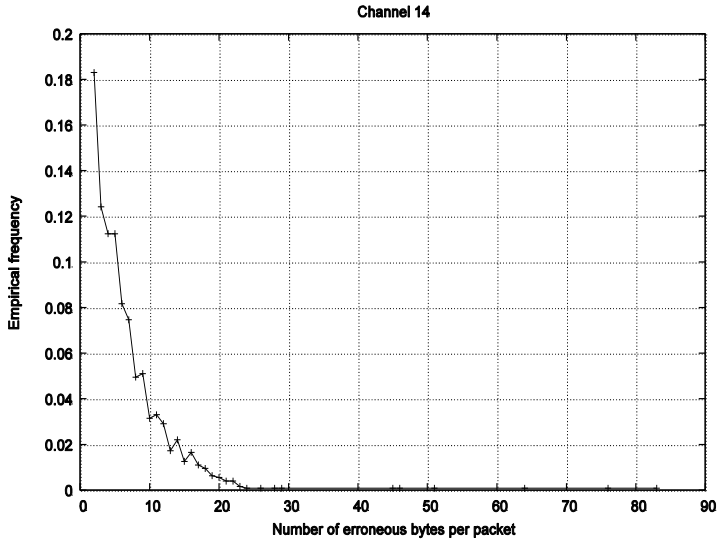


Figure 4.25 : ZigBee avec un mélange de réseaux concurrents, observé du canal 14

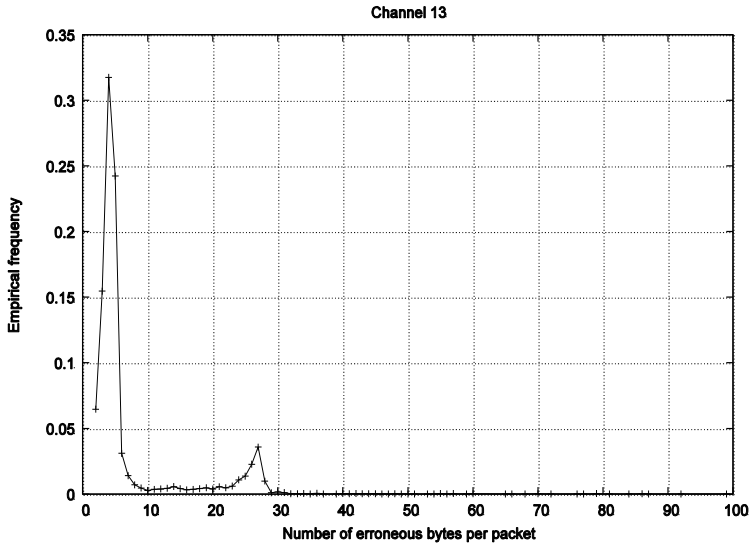


Figure 4.26 : ZigBee avec un mélange de réseaux concurrents, observé du canal 13

Sur le canal 11, un nœud ZigBee transmet des paquets d'une taille de 122 octets et l'autre transmet des paquets de 90 octets. Les résultats sont présentés sur la Figure 4.24, Figure 4.25 et la Figure 4.26. La distinction entre ces technologies est claire. Sur la Figure 4.24 qui représente les erreurs des paquets transmis sur le canal 11, les trois pics apparaissent. Le premier pic, entre 2 et 6 octets, est dû aux paquets de données WiFi. Le deuxième pic est dû à des paquets de contrôle WiFi et le dernier, à 85 octets, correspond à des collisions avec des paquets ZigBee coexistant sur le même canal. Les canaux ZigBee étant quasi-orthogonaux, aucun effet des transmissions ZigBee sur le canal 11 n'est observé sur les canaux 13 et 14 (Figure 4.26, Figure 4.25 respectivement). L'effet WiFi apparaît clairement sur les canaux 11 et 13.

Les zones de chevauchement entre les points d'accès peuvent exister, ce qui suggère que les modèles d'erreur peuvent être affectées. En réalité, ces zones ne sont pas souhaitables et sont destinées à être petites puisqu'elles causent des interférences sur les nœuds WiFi eux-mêmes. Dans un environnement industriel ces interférences sont évitées en affectant un canal différent pour chaque point d'accès adjacent. L'impact sur les capteurs est qu'ils ne sont perturbés que par un seul point d'accès la plupart du temps. Par conséquent, l'empreinte du WiFi devrait rester applicable la plupart du temps dans la zone couverte par le point d'accès, même s'il y a plusieurs nœuds WiFi mobiles. En outre, s'il y a différents types de trafics, le capteur est affecté principalement par la plus longue rafale de données et par la taille des paquets transmis, comme cela a été démontré par les expériences.

4.4 Discussion

En raison de la nature qu'on imagine chaotique des interférences on peut s'attendre à un grand nombre de modèles d'erreurs. Nous visons à détecter des technologies spécifiques dignes d'intérêt, ce qui signifie des types spécifiques d'interférences. Le fait est que chaque technologie utilise des composants spécifiques pour communiquer : type de modulation, la puissance d'émission et de mécanisme d'ordonnancement. Il est démontré dans la littérature que chaque équipement produit un taux d'erreur binaire spécifique. Cela suggère que la combinaison de ces équipements avec une technologie spécifique engendre une combinaison unique de taux d'erreur binaire. Cela est illustré dans les résultats des expériences que nous avons menées et identifiés

comme modèle des erreurs de paquet reçu. En outre, les expériences ont montré que grâce à l'utilisation d'un certain nombre de paquets reçus et pas seulement un seul échantillon, les modèles convergent vers l'empreinte du brouilleur dominant.

Le point remarquable est que le cas de la coexistence est toujours détectable, même si la technologie concurrente a une faible partie qui chevauche le spectre du ZigBee, ou une petite durée d'occupation du spectre ou encore une faible puissance de transmission. Cette remarque est déduite des résultats des expériences (cf. Figure 4.10, Figure 4.11, Figure 4.12, Figure 4.15, Figure 4.19 et Figure 4.25). Sur la Figure 4.27 on a combiné trois courbes différentes représentant les cas de collision où une technologie précise n'est pas détectable mais l'effet de la collision est distinguable de l'effet du lien faible et l'accent est mis sur les différences. Sur la zone 1 de la Figure 4.27 un pic dominant pour une taille d'erreur de deux octets est présent dans tous les courbes, mais pour les collisions la différence est que des densités d'erreur élevées sont visibles pour des longueurs d'erreur élevées (qui atteignent 20 octets). C'est ce que représente une distinction de l'effet de lien faible. En outre, dans la « Zone 2 » de la Figure 4.27 on peut voir l'existence des erreurs de grandes tailles spécifiquement pour les collisions causées par le Bluetooth. Bien que dans ce cas nous ne puissions pas identifier une technologie spécifique, nous pouvons être sûrs que le nœud est dans un cas de coexistence et non pas dans le cas de lien faible et le nœud doit réagir en conséquence.

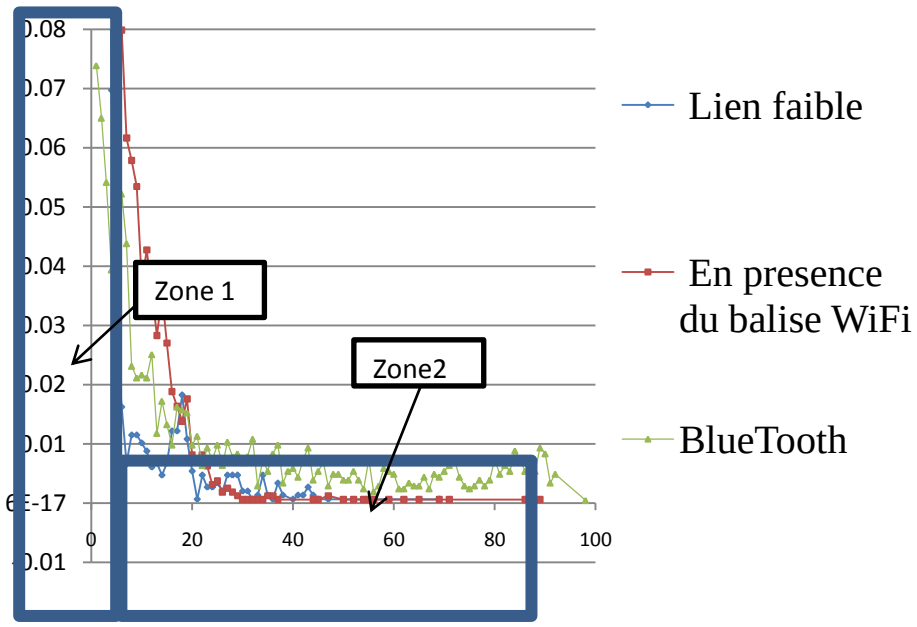


Figure 4.27 différences entre collision et corruption due au lien faible sur le canal 14

4.5 Application de FIM à l'adaptation dynamique de lien

Nous avons conçu un mécanisme d'identification des empreintes, FIM, qui permet de reconnaître à la volée les technologies utilisées dans les réseaux concurrents. Nos observations ont montré que pouvoir déterminer la cause des corruptions des paquets à partir du nombre d'octets erronés est fiable et simple. Il n'est pas nécessaire d'utiliser des méthodes sophistiquées et coûteuses pour faire la détection. Chaque paquet corrompu est stocké dans une file d'attente (en mode "push out" à cause de la mémoire limitée) puis un accusé de réception négatif est

envoyé. Chaque fois qu'un paquet correct (CRC correct) est reçu, les paquets ayant le même ID et le même numéro de séquence sont recherchés dans la file d'attente. Le nombre d'octets erronés dans les paquets corrompus est calculé et une fréquence empirique du nombre d'octets erronés est mise à jour. Une comparaison est ensuite déclenchée afin de détecter des sommets pour longueurs d'erreurs. Le seuil utilisé dans la détection d'un sommet dans la courbe de fréquence empirique est de 0,05. La variable booléenne WiFiC dans l'algorithme FIM est activée dès détection de la présence du WiFi. En se basant sur cette variable, l'adaptation de lien à partir de FIM (Algorithme 3-4) permet d'éviter la coexistence avec le WiFi en changeant le canal de communication pour un autre. S'il y a une ambiguïté dans le modèle de l'empreinte, FIM ne réagit pas (*Algorithme 1,2*).

Algorithm 1- Au niveau du récepteur:

```
1. If Msg.length=L then
2.   If Msg.crc = False then
3.     StoreCorruptedPacket()
4.     SendNegativeAcknowledgment()
5.   Else
6.     For i in 1… Number_Corrupted_Packets do
7.       If Msg.SrcAddress=CorruptedPacket[i].SrcAddress  then
8.           NberErroneousBytes<-DetectErrors(i,Msg)
9.           EDF[NberErroneousBytes]<-EDF[NberErroneousBytes]+1
10.        RemoveCorruptedPcket(i)
11.      End if
12.   Next i
13.   End if
14.   WiFiC←WiFiCheck()
15.   WLC←WeakLinkCheck()
16.   HTC←HiddenTerminalCheck()
17.   BC← BluetoothCheck()
18. Else
19.    Reject(Msg)
20. End if
```

Algorithm 2- Au niveau du transmetteur:

```
1.If NegativeAckReceived() then
2.RetransmitPacketOf(NegativeAck)
3.End if
```

Pour démontrer, par expérimentations sur plate-forme réelle de capteurs, l'efficacité de notre proposition, nous avons implémenté FIM avec un simple CSMA/CA, nous avons réactivé les fonctionnalités désactivées précédemment comme le CCA, le backoff, etc., dans un environnement de coexistence avec WiFi. Deux scénarios ont été étudiés: le premier scenario utilise un simple CSMA/CA sans FIM, le deuxième scénario CSMA/CA avec FIM pour détecter le WiFi. Dans ce dernier, une détection WiFi déclenche un changement de canal du canal 11 au canal 15 afin d'éviter le réseau concurrent trouvé (cf. *Algorithme 3,4*). Cette

approche est uniquement destinée à servir d'exemple d'application de FIM et n'est en aucun cas un algorithme optimal.

Algorithm 3- Côté récepteur: changement de canal

```
1. If  WiFiC = True then
2.    If ConfirmChannelSwapMsg = Received then
3.          WiFiC ←False
4.         ChannelSwap()
5.    Else
6.        SendChannelSwapMsg()
7.    End if
8. End if
9. //if no acknowledgment is received in the swapped
10.// channel Fall back to the old channel
11.If  ChannelSwapAck!= received then
12.     UndoChannelSwap()
13.Else
14.    SendChannelSwapFinal()
15.End if
```

Algorithm 4- Côté transmetteur:

```
1.      If ChannelSwapMsg=received then
2.          SendConfirmChannelSwapMsg ()
3.          ChannelSwap()
4.      End if
5.      //if channel swap is done, send an acknowledgment
6.      //Using the new channel
7.      SendChannelSwapedACk()
8.      If  ChannelSwapFinal!=received then
9.              UndoChannelSwap()
10.     End if
```

Le but de ce scénario est de démontrer comment FIM peut être efficace dans la prise de décisions intelligentes afin d'optimiser la qualité de lien d'une manière auto-organisée. Nous avons mené deux expériences : l'une avec un taux de transmission de données de WiFi égale à 458 pps et l'autre avec un taux de 916 pps, la longueur des paquets étant toujours égale à 1500 octets. Le taux de transmission des paquets ZigBee est de 33pps. Au cours de ces expériences, nous avons utilisé un taux de trafic typique à des scénarios comme la détection d'intrusion, la surveillance de la chaîne du froid ou bien la surveillance de la santé, tout au long d'un scénario dans lequel un nœud est un nœud critique (bottleneck): Cluster-Head ou nœud relai. La présence de ces nœuds est essentielle pour créer des ponts entre les clusters et les parties d'un réseau. Les liens reliant ces nœuds critiques engendrent un fort trafic qui contient l'agrégat de différents trafics passant par les différentes parties du réseau. Si ces nœuds sont perdus la

connectivité entre les nœuds du réseau est perdue. Les taux dans ces circonstances peuvent dépasser 50 pps dans le cas d'une activation d'alerte ou d'une surveillance continue.

Après 105 collisions pour 458 pps et 20 collisions pour 916 pps le WiFi est détecté, La présence d'un pic à 5 ∈ [2, 6] octets corrompus et d'un pic à 26-27 ∈ [26, 28] sur la Figure 4.28 et la Figure 4.29 indiquant la présence de WiFi et provoquant le déclenchement de la contremesure. La Figure 4.31 représente le changement de débit à travers le temps pour le cas 458 pps. A l'activation de l'adaptation du lien, c'est-à-dire à 173s, le changement peut être observé à travers le passage de 18 pps à 28 pps. Sur la Figure 4.30, l'amélioration globale moyenne du débit est représentée. Pour un taux de transmission WiFi de 458 pps le gain est égal à 87%, et pour un taux de transmission de 916 pps, il est de 100,9%. FIM est conçu pour la détection d'empreintes. Il forme aussi mais indirectement un indicateur de l'efficacité des contre-mesures utilisées contre les technologies concurrentes. Plus la contre-mesure est efficace, moins il doit y avoir d'octets erronés et donc la technologie concurrente doit devenir moins détectable. En outre, l'efficacité de FIM augmente avec les collisions. S'il y a peu de collisions, il converge lentement mais dans ce cas le problème des collisions est moins crucial: si l'effet des technologies coexistantes est minime ou bien s'il n'y a aucun effet, il n'est pas nécessaire de s'adapter.

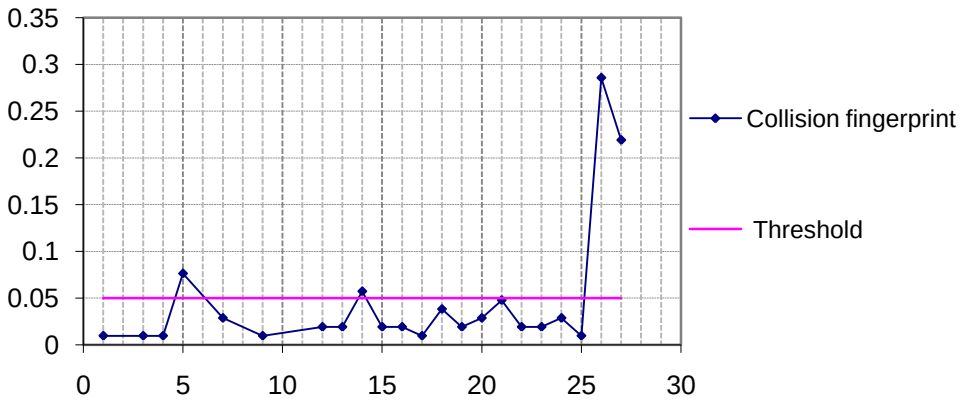


Figure 4.28 : Cliché instantané du graphe de détection de l'empreinte de WiFi sur le canal 11 de ZigBee où le taux de transmission de WiFi est 458pps

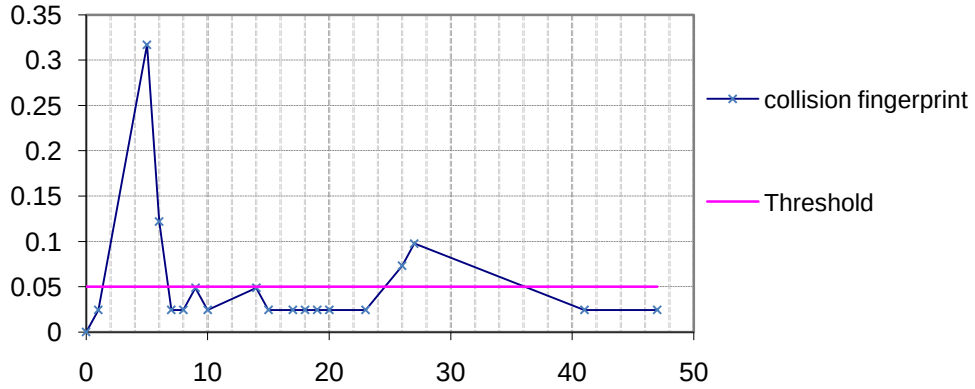


Figure 4.29 : Cliché instantané du graphe de détection de l'empreinte de WiFi sur le canal 11 de ZigBee où le taux de transmission de WiFi est 916pps

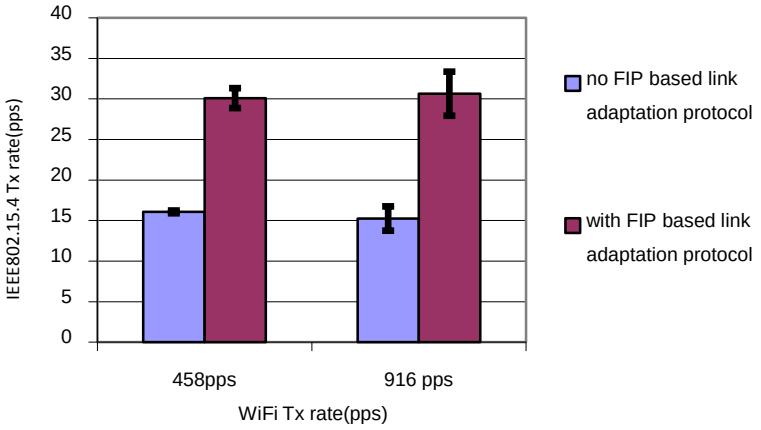


Figure 4.30 : débit avec et sans adaptation de lien en utilisant FIM

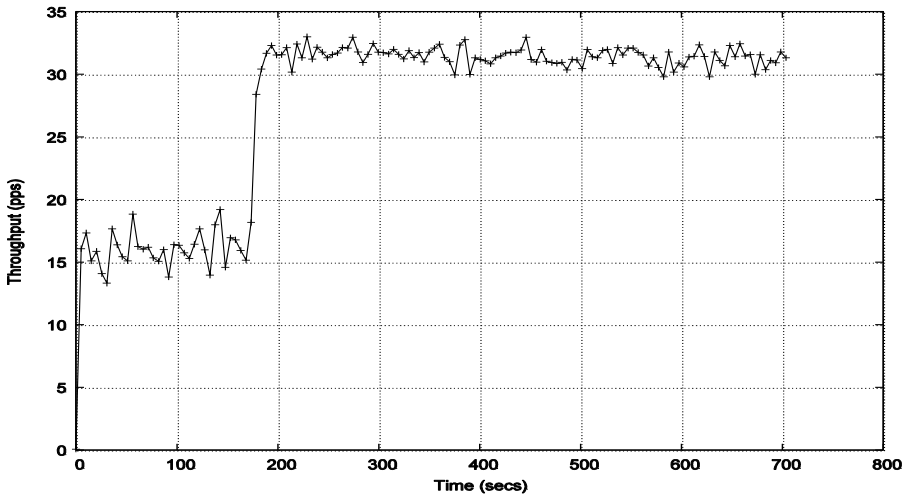


Figure 4.31 : débit du trafic ZigBee à l'instant de la détection de WiFi pour un taux de transmission WiFi de 458pps et un taux de transmission ZigBee de 33.3pps

Nous avons testé le taux de non détections par rapport au nombre de collisions. C'est la proportion des cas où FIM ne détecte pas la présence de WiFi, bien que, à ce moment même, la corruption de paquet ZigBee soit causée par le trafic WiFi. Dans la fonction WiFiCheck () nous avons spécifié un seuil pour déterminer s'il y a un pic ou non à un certain intervalle de nombre d'octets erronés. Le choix du seuil est empirique, basé sur les résultats expérimentaux. Durant les expériences pour déterminer le taux de non détections, le seuil utilisé est de 0,035. La Figure 4.32 et la Figure 4.33 représentent le taux de non détection des paquets WiFi (contrôle et données). Ces graphes montrent une baisse du taux de non détection quand il y a un nombre élevé de collisions. Les taux typiques de l'IEEE802.15.4 utilisés varient entre 11 et 50 pps. La taille des paquets IEEE802.11 est de 1428 octets et le taux de transmission est de 962 pps. Ces deux figures représentent les taux de non détections des deux trafics de contrôle et de données qui sont dépendants. Le taux de non détection pour la détection des données dans la Figure 4.33 est à son minimum 5% lorsque le taux du trafic Zigbee est de 11pps et le nombre de collisions est de 100. Dans ce cas, l'effet du trafic de données est dominant mais le trafic de contrôle est moins clair (Figure 4.32).

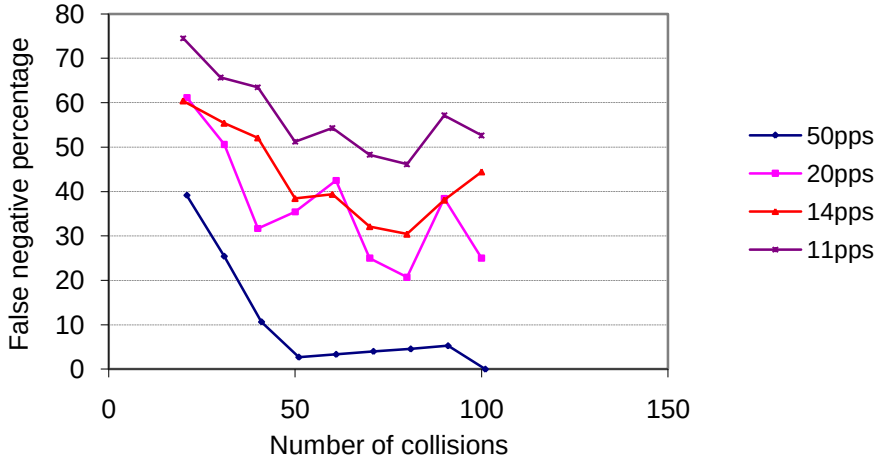


Figure 4.32 : détection des paquets contrôle vs. Le taux de transmission des paquets ZigBee

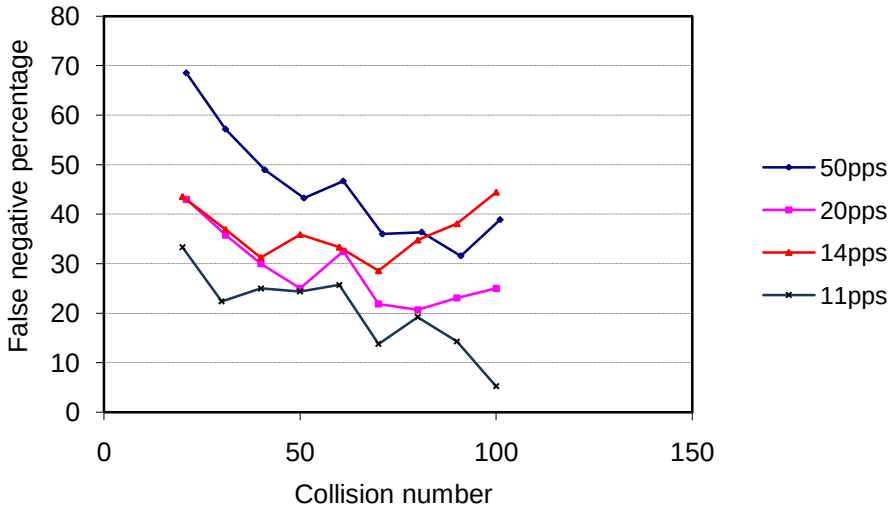


Figure 4.33 : détection de paquets données vs. Le taux de transmission des paquets ZigBee

4.6 FIM distribué pour la détection de WiFi dans le cas de la mobilité

4.6.1 Le mécanisme

Dans le cas de l'influence d'un nœud WiFi sur un grand nombre de nœuds du réseau ZigBee (cf. Figure 4.34), le fait d'avoir une collaboration entre les nœuds ZigBee voisins conduit à un fonctionnement amélioré au niveau décisionnel. On peut donc poursuivre la réflexion menée sur la détection automatique de l'environnement en rendant notre proposition distribuée. Cependant, dans un environnement comme celui des réseaux de capteurs, l'échange des informations a un coût, d'une part, et, d'autre part, le choix des nœuds de qui proviennent une information est déterminant pour les performances du réseau car certains nœuds ont une information plus fiable que d'autres ou plus appropriée selon l'environnement. C'est l'idée même des réseaux docitifs (cf. [GGBD10]) dont il est question ici. Nous avons donc décidé d'introduire ce concept de docition dans une version de FIM distribuée. Le concept de docition

vient du domaine de la radio cognitive qui proposait des méthodes permettant à des nœuds sans licence d'écouter une bande de fréquence et de l'utiliser de manière autonome si des nœuds licenciés ne l'utilisent pas mais qui propose maintenant d'introduire de la coordination entre les nœuds non licenciés à travers ce nouveau concept, lequel sera traité en détail dans le chapitre V. Disons rapidement qu'il définit deux types de nœuds : un nœud professeur et un nœud élève qui tient ses informations du premier.

La présence d'une communication WiFi dans une région implique qu'il y a une grande probabilité qu'il existe plusieurs nœuds WiFi dans le voisinage. De plus, l'influence d'un nœud WiFi est envahissante dans son environnement, à cause de sa puissance de transmission élevée donnant un grand rayon de couverture. La détection d'un nœud WiFi au voisinage d'un nœud ZigBee et la propagation de cette information peut donc donner un grand avantage à un réseau de capteurs mobiles en train de se former. L'intérêt de prendre des contremesures de façon collaborative pour éviter l'interférence est donc évident.

Dans le cas de la mobilité, les paramètres d'un nœud mobile prennent beaucoup de temps pour converger à un état adapté à l'état actuel de l'environnement. Cela cause une perte d'énergie élevée à cause du nombre de collisions dont FIM a besoin pour faire une détection. En outre, FIM nécessite un taux de traitement élevé à chaque réception de paquets. Nous proposons donc dans cette partie que, si un capteur (enseignant) détecte la présence de WiFi, il donne cette information à un nouveau voisin (mobile) qui vient d'arriver. Cette action n'est pas aussi simple puisqu'au début il faut s'assurer que l'enseignant est fiable.

Pour déterminer la fiabilité de l'enseignant, un nouveau nœud doit chercher si l'enseignant a un environnement semblable au sien et si cet enseignant est expert, c'est-à-dire qu'il dispose d'une bonne information. Dans le cas de FIM un nœud expert est un nœud qui a fait sa détection en se basant sur un nombre suffisant de paquets corrompus.

Le niveau de ressemblance entre l'environnement du nouveau nœud et son voisinage est supposé corrélé à la distance entre un nœud et chacun de ses voisins [XL06]. Plus les nœuds ZigBee sont proches l'un de l'autre, plus ils sont affectés par les mêmes sources d'interférences. Le RSSI, indicateur de niveau de signal reçu lu à partir d'un champ de l'en-tête des paquets IEEE 802.15.4, peut être considéré pour déterminer la distance [HAH06]. Pour qu'un nœud choisisse un enseignant parmi ses voisins, il estime la distance qui le sépare de ses voisins en utilisant le RSSI, il choisit un ensemble de candidats enseignants parmi eux. Puis de ces candidats il choisit comme enseignant celui qui est le plus fiable.

Dans le cas ou le nœud mobile ne trouve aucun enseignant candidat il utilise la version initiale de FIM.

Remarque : *dans ce chapitre, pour appliquer la docition, l'on suppose que les nœuds les plus proches sont corrélés et l'on utilise le RSSI pour déterminer cela. Dans le chapitre suivant, sur la* ***Docition Dynamique****, le critère de corrélation et la vérification de la corrélation entre les nœuds sont discutés plus en détails.*

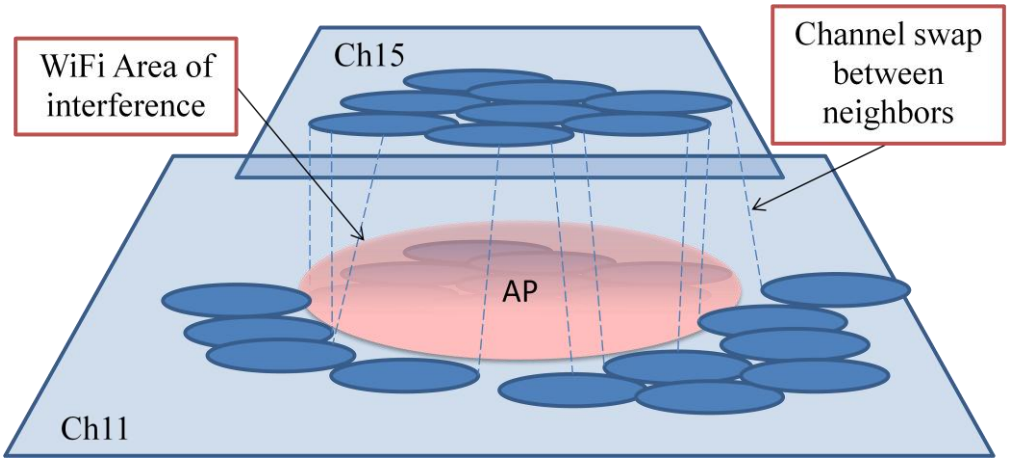


Figure 4.34 : représente l'adaptation des nœuds voisins à la présence de WiFi

Dès qu'un enseignant ZigBee indique la présence de WiFi à un nœud ZigBee mobile, le nouveau nœud équipé de FIM distribué diminue le seuil de détection d'un pic. Ensuite, il modifie la condition de déclaration de la présence de WiFi. Cette condition qui indique que pour déclarer la présence de WiFi, il faut détecter le pic des paquets de contrôle et celui des paquets de données devient : le nœud déclare la présence de WiFi s'il y a une détection du pic des paquets de contrôle ou bien de celui des paquets de données. Cela rend le mécanisme plus rapide au niveau de sa convergence et moins coûteux en énergie (cf. Algorithme 5).

Algorithme 5 : Composantes ajoutées sur l'algorithme FIM distribué

IF theNumberOfNeighbors>1 and detectWiFi (Max (RSSI (neighbor))) = true and old (neighbor) =true ***THEN***
ActivateDociTionParametersModification ()
ELSE
DefaultParameters()
END IF

ActivateDociTionParametersModification () {
1. Threshold<- minimumThresholdValue
2. ***IF*** detectWiFiData() ***OR*** detectWiFiBeacon() ***THEN***
3. WiFidetection <- true
4. ***ELSE***
5. WiFidetection<- false
6. ***END IF***
7. **Return** WiFidetection

}

DefaultParameters(){
1. Threshold<-maximumThreshold
2. ***IF*** detectWiFiData() ***AND*** detectWiFiBeacon() ***THEN***
3. WiFidetection <- true
4. ***ELSE***
5. WiFidetection<- false
6. ***END IF***

7. **Return** WiFidetection

}

DetectWiFi (nodeWithMaximumRSSI) {

1. ***IF*** nodeWithMaximumRSSI.WiFiDetect=true ***THEN***
2. **Return** true
3. ***ELSE***
4. ***Return*** false
5. ***END IF***

}

Old (neighbor) {

1. ***IF*** CorruptedPacketsNumber(neighbor)>=75 ***THEN*** // the 75 is taken from the false negative rate as most suitable value
2. ***RETURN*** true
3. ***ELSE***
4. ***RETURN*** False
5. ***END IF***

}

4.6.2 Résultats des expériences

FIM distribué utilise le RSSI comme critère principal pour le choix d'un nœud comme enseignant : le voisin qui a le RSSI le plus élevé est choisi comme enseignant. Pour montrer que le RSSI peut être mesuré d'une manière fiable en présence d'interférences et donc l'utiliser pour estimer la distance entre les nœuds, on a fait l'expérience suivante. On a collecté les valeurs de RSSI reçues à la réception des paquets en filtrant les RSSI des paquets dont l'en-tête est corrompu. On compare les valeurs de RSSI reçues dans des paquets corrompus avec les mêmes valeurs pour des paquets intègres sur la Figure 4.35. La même distribution des mesures de RSSI est obtenue dans les deux cas, ce qui signifie que le RSSI continue à être un bon estimateur de distance même en cas de coexistence.

Ce qu'on présente sur le RSSI n'est qu'une illustration pour montrer que le RSSI ne sera pas influencé par les interférences en cas de coexistence. Beaucoup des travaux ont présenté des approches pour utiliser le RSSI pour la localisation on cite quelques uns [CYCC09], [LOJ10], [SLNL11].

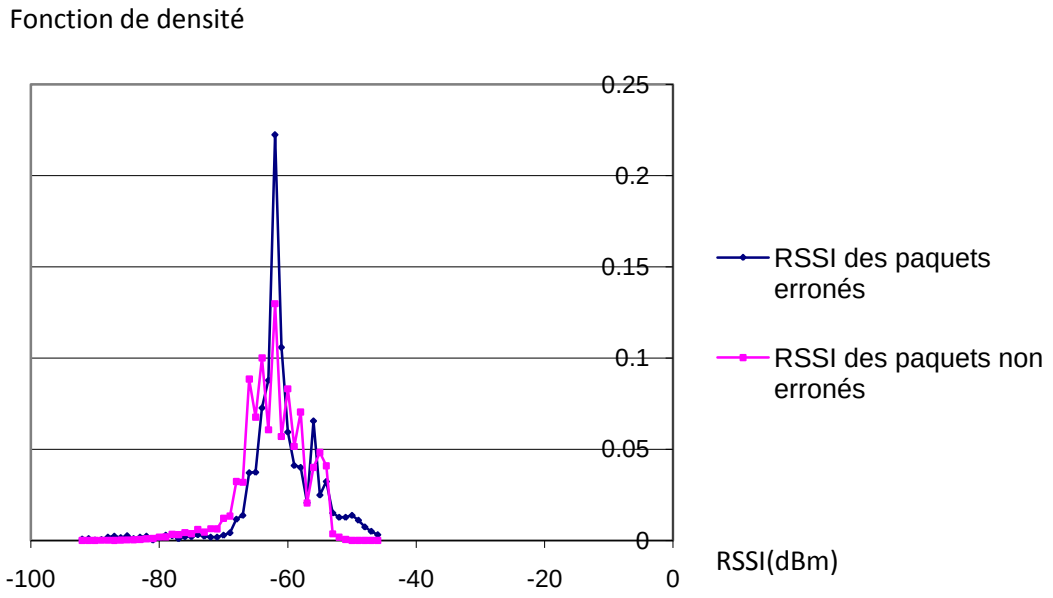


Figure 4.35 : fréquence empirique des paquets erronés et non erronés pour un taux de transmission WiFi de 687 pps et ZigBee de 33 pps

La vitesse de convergence entre FIM et FIM distribué est comparée Figure 4.36. Un trafic WiFi est généré avec un taux de transmission de 687pps et un autre l'est par les nœuds ZigBee à un taux de 33pps. Les résultats sont représentés sur la Figure 4.36. Le nœud ZigBee qui utilise FIM simple a pris six minutes de plus pour détecter le WiFi, tandis que le nœud qui utilise FIM distribué a pris moins de temps pour détecter la présence de WiFi.

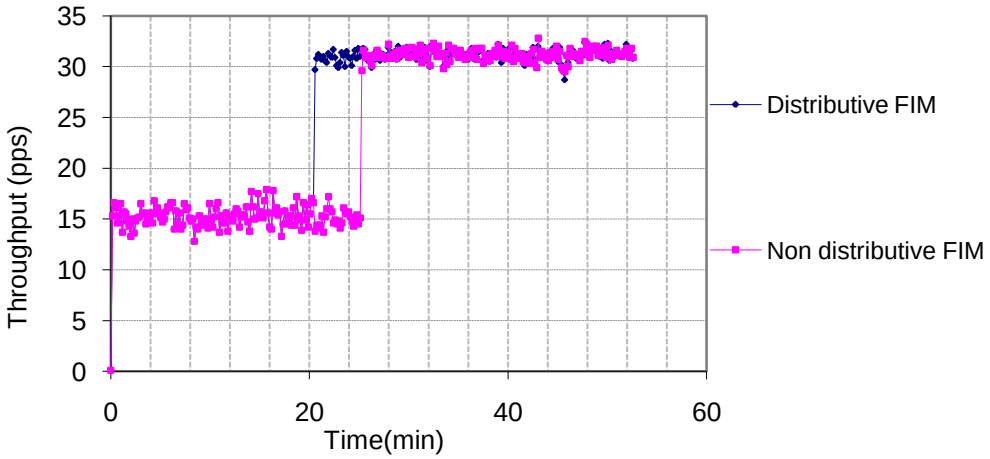


Figure 4.36 : comparaison de la série temporelle du débit d'émission des capteurs dans les cas FIM et FIM distribué pour un taux de transmission de WiFi de 687pps et de ZigBee 33pps

Pour s'assurer de l'efficacité de FIM distribué, le taux de non détection est étudié avec des taux de transmissions pour ZigBee qui varient de *11.1pps* jusqu'à *166.6pps* et un taux de transmission pour WiFi de *916pps*. Les résultats sont présentés sur la Figure 4.37. La diminution rapide du taux de non détection est claire relativement au nombre de paquets : après 20 collisions la probabilité d'avoir une non détection diminue de 40% à moins que 20%.

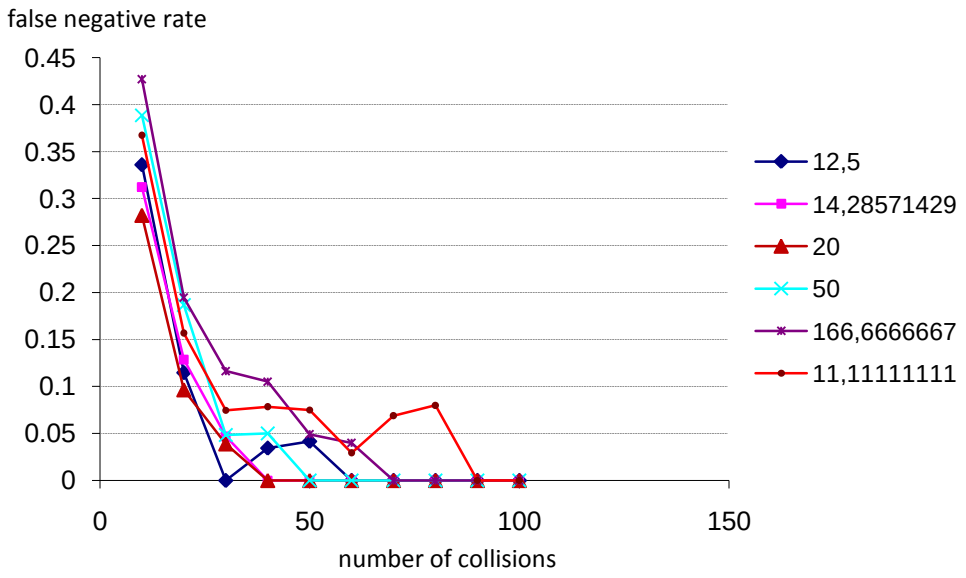


Figure 4.37: taux de non détection relativement au nombre de paquets reçus

Comme il a besoin de moins de temps de convergence (cf. Figure 4.36) que FIM non distribué et un nombre de collisions faibles pour avoir une détection correcte de coexistence (cf. Figure 4.37), FIM distribué présente une amélioration par rapport au comportement de FIM simple. Un temps de convergence plus petit permet une contremesure plus rapide. L'ordre de grandeur de la complexité $O(n)$ de FIM étant relié au nombre de paquets à traiter pour avoir une détection, le fait d'avoir besoin de moins de collisions pour FIM distribué implique une complexité plus faible.

4.7 Contraintes sur l'utilisation de FIM

Deux contraintes fortes régissent le comportement des deux versions de FIM, la première étant que FIM ne fonctionne que si le paquet à analyser a un temps de transmission plus long que celui du paquet avec qui il entre en collision et la deuxième étant que les deux versions de FIM sont développées pour détecter des empreintes fixes. Si le nœud qui cause l'interférence met en œuvre des algorithmes d'adaptation qui peuvent changer l'empreinte, les propositions que nous avons faites doivent être adaptées. Cette deuxième contrainte peut être contournée si l'algorithme d'adaptation est connu et par suite l'empreinte peut être estimée. Dans tous les cas, nous avons mené un premier travail d'identification d'empreintes comme preuve de concept qu'il faudrait étendre par des analyses systématiques et exhaustives pour une application opérationnelle.

4.8 Conclusion

La diversité des technologies qui coexistent dans la même bande ISM, telles que les réseaux de capteurs, varie de technologies qui n'appliquent pas l'écoute du canal avant leur transmission comme le Bluetooth, à d'autres qui, en raison des propriétés de leur CCA, ne détectent pas d'autres technologies comme le WiFi. A cause du manque de coordination entre ces technologies, les réseaux de capteurs ont besoin de détecter la présence de chacun d'eux. Ainsi, une contre-mesure spécifique à chaque technologie peut-elle être appliquée par un capteur pour éviter les collisions avec eux.

Dans ce chapitre nous avons identifié les empreintes de diverses technologies qui coexistent sur la même bande de fréquence sous forme de modèles de corruption des paquets des capteurs sans fil (IEEE802.15.4). Nous avons considéré des trafics concurrents générés par les technologies ZigBee, Bluetooth et WiFi, chacun engendrant un modèle spécifique de corruption. De plus, le cas de corruption due à un lien faible est également considéré. A partir de l'identification de ces empreintes, nous avons conçu FIM, un mécanisme réactif pour détecter à la volée chaque technologie concurrente. On a testé FIM sur notre plate-forme "Tmote Sky". Dans certains cas, FIM fournit jusqu'à 100% de précision dans la détection de l'empreinte digitale correcte. Au cours de quelques-unes des expériences, son application pour l'adaptation de lien a amélioré le débit par 100,9%.

Une version de FIM qui fonctionne en mode distribué est développée. Comme attendu, cette deuxième version présente une meilleure performance que FIM simple. Les résultats montrent une amélioration dans la vitesse de convergence et dans l'ordre de complexité.

Ce travail préliminaire est une preuve de concept. Nous avons effectué des expériences initiales qui doivent être étendues à d'autres technologies et d'autres configurations, comme des points d'accès WiFi plutôt que du WiFi en mode ad hoc, en utilisant OFDM au lieu de l'étalement de spectre DSSS, etc. L'impact de la mobilité des nœuds sur les formes d'erreur est également un sujet intéressant. Dans ce chapitre nous ne donnons qu'un exemple d'implémentation du mécanisme d'adaptation après la détection WiFi pour illustrer l'efficacité et l'utilité de notre mécanisme d'adaptation de lien. De nombreux mécanismes d'adaptation peuvent être conçus et optimisés et pour diverses autres technologies.

Chapitre 5. Radio docitive pour les réseaux ad-hoc mobiles et les réseaux de capteurs

5.1 Introduction

Un nouveau paradigme du domaine des réseaux coopératifs et distribués a émergé récemment : les réseaux docitifs [GGBD10]. Un réseau docitif est l'aboutissement naturel auquel devait arriver la recherche sur la radio cognitive [H05] : tandis que celle-ci utilise l'intelligence artificielle et des algorithmes d'apprentissage automatiques pour traiter les observations locales des canaux de communication, la radio docitive inclut aussi des informations collectées à partir des nœuds voisins. Le but de cet échange d'informations est d'accélérer et d'améliorer le processus de prise de décision. Le terme de docition dérive du mot latin « *docere* » signifiant enseigner, les radios « enseignant » les informations qu'elles considèrent importantes à d'autres radios [GGBD10]. La docition est donc un paradigme concernant le rapport entre enseignant et élève. L'intelligence est en effet impactée par le degré d'observation ou, plus précisément, de connaissance.

Tandis que par le passé la cognition et l'apprentissage à partir d'informations obtenues directement de son environnement par un nœud ont reçu beaucoup d'attention de la part des différentes communautés scientifiques, le processus de transfert de connaissances, l'apprentissage, au moyen d'un support sans fil a fait l'objet de peu de travaux à ce jour. De même que pour la radio cognitive distribuée la radio docitive a besoin de coopérer avec les radios voisines pour réaliser la docition, cependant dans le principe de docition l'utilisation des informations échangées n'est pas systématique: l'enseignant n'enseigne pas les résultats finaux intéressant directement l'élève, mais propose les éléments des méthodes pour y parvenir. En d'autres termes, les problématiques de docition concernent la façon dont l'information est sélectionnée et transmise d'un nœud à un autre.

Le principe de docition peut être appliqué à des degrés divers, de l'absence totale de docition, c'est-à-dire du transfert systématique à tous les voisins de toute l'information dont disposent les nœuds, ce qu'on appelle encore radio distribuée, jusqu'à la docition parfaite où toute information est filtrée. Les auteurs de [GGBD10] évoquent ces différents degrés possibles mais supposent qu'ils sont statiques : un nœud docitif n'a pas la possibilité de choisir dynamiquement son propre degré de docition.

Pendant la docition, l'échange du tableau de « Q-learning » [HH00] est essentiel, car il contient les informations de docition. Ce tableau contient les informations relatives à l'état de l'enseignant or il est crucial que le nœud étudiant ait un état de l'environnement similaire à celui de l'enseignant. Or, pour que la docition permette au nœud apprenti une convergence rapide vers une prise de décision spécifique, une hypothèse forte est supposée par le paradigme : la cohérence entre les états de l'enseignant et ceux de l'élève. En effet, il n'existe pas de mesure prise dans le paradigme docitif pour s'assurer que l'enseignant et les nœuds étudiants ont des états cohérents. Les auteurs de [GGBD10] supposent que, par construction, puisque la docition est appliquée aux réseaux fixes, avec ou sans infrastructure, il n'y a pas de problème de cohérence d'information entre les nœuds voisins.

En revanche, dans le contexte de cette thèse, nous nous intéressons aux réseaux mobiles sans infrastructure tels que les MANETs et surtout les WSNs. Dans ce type de réseaux, les

nœuds peuvent ne pas avoir de bases d'états cohérentes, du fait de la mobilité, de l'occupation de la bande ISM par des technologies et applications concurrentes variées ou tout autre raison. Dans la suite de ce chapitre, nous appelons docition classique (CD) le principe de docition présenté jusqu'ici dans la littérature et utilisant un degré de docition statique pour les nœuds tout au long de la vie du réseau.

L'objet de ce chapitre est par contre d'étendre ce concept classique en une docition dynamique (DD) qui permet aux nœuds enseignants et apprentis, dans tous les cas possibles de mobilité ou de causes diverses d'incohérences d'état entre voisins, de spécifier le niveau de docition dynamiquement en fonction du niveau de prévisibilité de l'environnement. Nous proposons alors d'ajouter une sonde de prévisibilité de l'environnement (SPE) comme nouvel élément à la docition classique. En fonction du résultat obtenu par l'SPE, si l'état de l'environnement est assez stable et un certain niveau de cohérence entre enseignants et apprentis est observé, des méthodes de docition sont appliquées sinon aucune docition n'est utilisée.

Pour évaluer la pertinence et les performances de la docition dynamique, nous l'appliquons au cas d'une situation de coexistence entre les technologies IEEE802.15.4 (capteurs sans fil) et IEEE802.11b/g (WiFi), où les nœuds capteurs sont mobiles. Pour échapper aux interférences avec le WiFi, les capteurs exploitent l'existence des périodes de silences dans le trafic WiFi, silences modélisés par une loi de Pareto. Cette modélisation est proposée et validée dans [HXZZ10]. Nous la prenons comme hypothèse, qui pourrait être affinée au demeurant mais cela ne devrait pas modifier grandement notre étude. Le scenario qui nous intéresse est semblable à celui d'une radio cognitive qui s'adapte en tant qu'utilisateur sans licence (connu sous le nom d'utilisateur secondaire) pour coexister avec un usager ayant une licence (connu sous le nom d'utilisateur principal) [M98]. Plus précisément, nous cherchons à donner aux technologies « faibles » (alimentation électrique limitée, faibles capacité de traitements, puissances et taux de transmission) comme celles utilisant le standard IEEE802.15.4 les moyens d'adaptation pour coexister avec les technologies « fortes » comme l'IEEE802.11 (alimentation électrique suffisante, taux et puissance de transmission élevés). L'application de notre proposition de docition dynamique dans ce scénario améliore l'efficacité de la consommation d'énergie et assure un temps de convergence des nœuds plus rapide vers la meilleure prise de décision.

Intuitivement, nous nous attendons à ce que dans le cas où l'environnement devient de plus en plus dynamique et de mois en moins autocorrélé, l'utilisation de la docition classique devienne désavantageuse. En effet, le principe de docition reposant sur le fait qu'un enseignant envoie à son élève les informations qu'il a apprises, si l'environnement change de façon totalement décorrélée de ses états précédents, aucune prédiction n'est plus possible. Dans ce qui suit, nous quantifions cette affirmation avec des simulations. Nous proposons ensuite le concept de docition dynamique et nous choisissons de l'appliquer lors de toute initialisation d'un nœud du WSN lorsqu'il vient de détecter un changement de position, ce degré de docition consommant le moins d'énergie relativement à d'autres cités dans [GGBD10]. Enfin, les performances de la docition dynamique sont analysées par simulation.

5.2 Vue générale du fonctionnement de la docition classique

La docition classique est inspirée du concept de l'apprentissage par problèmes utilisé actuellement dans les écoles et les centres d'éducations. Les enseignants sont encouragés à être

des entraîneurs plus que des « fournisseurs » d'information, dans le but d'obtenir des élèves un travail en équipe et un développement de l'esprit critique. La docition peut être vue comme la transposition de ce concept aux réseaux sans fil. Les nœuds partagent potentiellement des quantités différentes d'intelligence acquises pendant la durée de leur activation. Cela doit aiguiser et accélérer le processus d'apprentissage. Tous les gains obtenus, cependant, ont besoin d'être évalués par rapport à la quantité de trafic ajoutée par l'échange d'informations de docition. Se posent alors les questions de savoir comment faire l'apprentissage et l'enseignement.

On est dans un cas d'apprentissage où plusieurs nœuds doivent apprendre d'une manière distribuée une politique optimale pour atteindre un objectif commun. Connu comme le problème d'apprentissage multi-agent, il peut être résolu par l'approche d'apprentissage par renforcement distribué dont le « Q-learning distribué » est un exemple. Le Q-Learning est une technique informatique capable de contrôler de façon optimale un certain système. Il s'agit d'une suite d'expérimentations plus ou moins aléatoires, engendrant une récompense et qui est mémorisée. L'enjeu est de découvrir, parmi toutes les tentatives effectuées, lesquelles sont les plus gratifiantes. Toutefois, dans ce domaine, de nombreux problèmes restent en suspens, même pour les experts en apprentissage automatique. Le principal problème est de savoir comment faire en sorte que les décisions individuelles des nœuds aboutissent à des décisions conjointement optimales pour le groupe. En principe, il est possible de traiter le réseau de radio cognitive distribuée comme un système centralisé où chaque nœud a des informations complètes sur les autres nœuds et apprend la politique optimale conjointe en utilisant des techniques standard d'apprentissage par renforcement. Cependant, la taille des espaces d'états et celle des espaces d'actions augmentent exponentiellement avec le nombre de nœuds, ce qui rend cette approche impossible pour la plupart des problèmes. Une alternative possible est de laisser chaque nœud apprendre sa politique indépendamment des autres, mais alors le modèle de transition dépend de la politique des autres nœuds apprentis, ce qui peut produire des comportements oscillatoires et diminuer la vitesse de convergence ([GG10b]).

En ce qui concerne l'enseignement, certaines des premières contributions à la littérature [T93, AA02] suggèrent que les performances d'un système d'apprentissage décentralisé peuvent être améliorées en utilisant différentes méthodes de coopération entre les apprentis. Par exemple, un nœud peut profiter de l'échange d'informations et de la connaissance provenant des nœuds experts ([T93], [AA02]), nœuds connus par les nœuds docitifs. À cet égard, on peut considérer qu'il y a plusieurs degrés de docition entre les nœuds.Le premier est celui où il n'y a pas de docition. Les nœuds ne coopèrent pas, ignorent les actions et les récompenses des autres nœuds dans le système, et apprennent leurs stratégies de manière indépendante. En particulier, l'adaptation de chaque agent à l'environnement peut modifier l'environnement lui-même d'une manière qui peut rendre les adaptations des nœuds voisins invalides. Malgré cela, cette méthode a été appliquée avec succès dans plusieurs cas, par exemple GG10a] et [GG10b]. Le deuxième degré est celui où la docition n'est utilisée qu'au démarrage. Les radios docitives enseignent leurs politiques à tous les nouveaux arrivants rejoignant le réseau. Dans ce cas, encore une fois, chaque nœud apprend de manière indépendante. Cependant, quand un nouveau nœud rejoint le réseau, au lieu d'apprendre à partir de rien la manière d'agir dans le milieu environnant, il apprend les politiques déjà acquises par les voisins les plus experts. Des gains sont attendus en raison d'une forte corrélation entre les environnements des nœuds adjacents experts (enseignants) et des nouveaux arrivants. Le troisième degré est celui de la

docition adaptative. Les radios docitives partagent ici des politiques fondées sur la performance. Les nœuds coopèrent en échangeant des informations sur la performance de leurs processus d'apprentissage : la variance de l'oscillation par rapport à une cible, la vitesse de convergence, etc.. Sur la base de ces informations, chaque nœud peut apprendre de ses voisins experts (plus intelligents) qui ont une meilleure performance.

Remarquons qu'il ne faut pas confondre docition adaptative et docition dynamique (que nous proposons dans ce chapitre). En effet, cette dernière a pour but d'adapter la docition dans les cas de réseaux mobiles pour en sélectionner dynamiquement le niveau, c'est-à-dire son degré (qui impacte la quantité d'informations à échanger) et choisir le bon enseignant à partir des voisins qui ont potentiellement des informations reçues de nœuds mobiles non actualisés par rapport à l'état actuel de l'environnement.

Le quatrième degré est celui de la docition parfaite. Le système multiutilisateur peut être considéré comme un système intelligent dans lequel chaque action commune est représentée comme une seule action. Les « Q-valeurs » optimales pour les actions conjointes peuvent être apprises en utilisant le « Q-learning » standard centralisé. Afin d'appliquer cette approche, un contrôleur central doit formaliser le processus de décision markovien et communiquer à chaque nœud ses actions individuelles. Sinon, tous les nœuds doivent modéliser le processus de décision markovien complet séparément et choisir leurs actions individuelles et, dans ce cas, aucun échange de décisions n'est nécessaire entre les nœuds mais ils ont tous besoin d'observer l'action de l'ensemble et toutes les récompenses individuelles. Bien que cette approche mène à la solution optimale, elle n'est pas applicable pour les réseaux très denses puisque l'espace des actions commun, qui est exponentiel par rapport au nombre de nœuds, devient impossible à traiter. Le degré de coopération, et donc les échanges de trafic nécessaires pour cela, augmente avec le degré croissant de docition. Un résumé de la taxonomie introduite dans ce paragraphe est donné Figure 5.1.

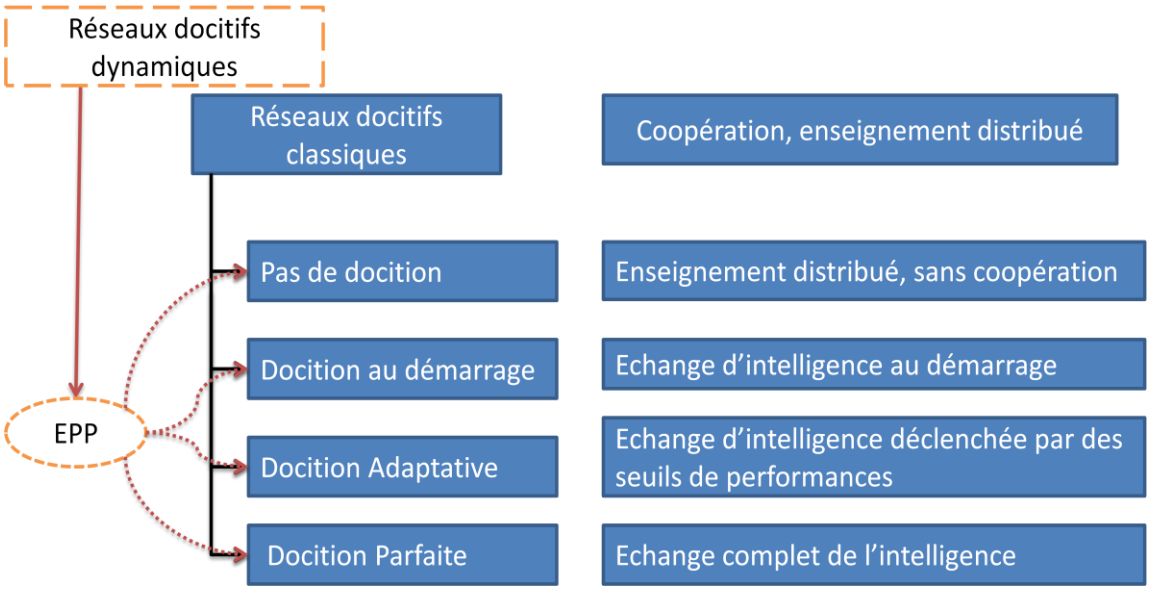


Figure 5.1:Taxonomie des différents degrés de docition

5.3 Vue générale du fonctionnement de la docition dynamique

La docition classique utilise quatre fonctions: l'acquisition, la décision intelligente, l'action et la docition. La contribution principale de la docition dynamique aux réseaux mobiles est de savoir quand utiliser ou pas la docition et de donner à l'étudiant une manière efficace pour sélectionner un enseignant. Dans les réseaux mobiles, l'enseignant est l'acteur le plus important car il doit donner des enseignements à jour. Dans le principe de docition dynamique, il faut déterminer l'enseignant comme dans la docition classique mais la docition dynamique ajoute un nouvel élément par rapport à la docition classique : la sonde de prédictabilité de l'environnement SPE appelée avant les fonctions de docition (cf. Figure 5.2:). En effet, c'est la SPE qui détermine si l'élément de docition peut être invoqué ou pas.

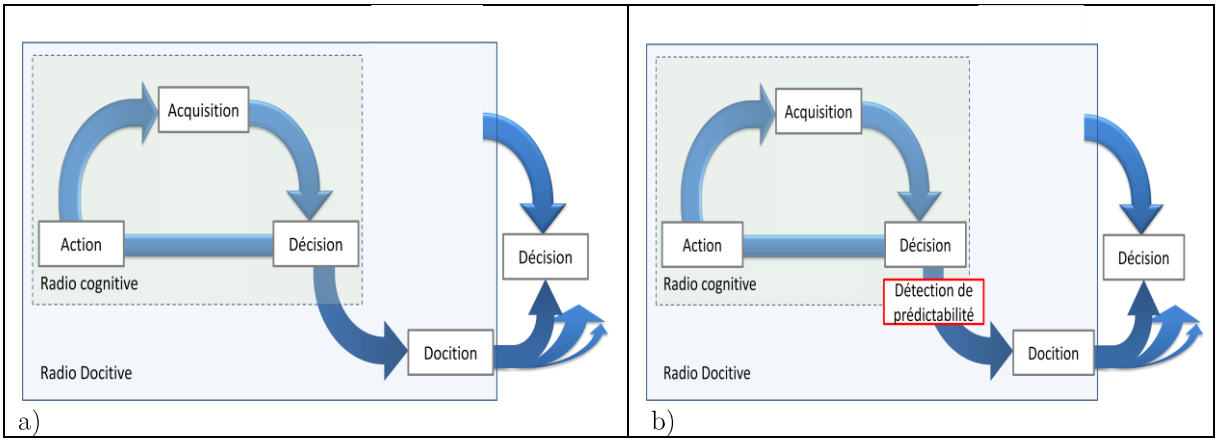


Figure 5.2: a) représente la docition classique b) représente la docition dynamique

Nous attribuons à la SPE deux responsabilités: spécifier le niveau de docition et choisir l'enseignant.

Niveau de docition

Utiliser la docition n'a de sens que si l'on peut espérer obtenir d'un nœud voisin choisi comme professeur une information valide, ce qui n'est possible que s'il y a une certaine dépendance dans les informations considérées. Cette dépendance peut être structurelle et s'exprimer à travers des lois de probabilité (par exemple, des temps entre arrivées dont la distribution est gaussienne) ou bien simplement dans la dépendance des occurrences d'une variable aléatoire exprimée à travers son autocorrélation. Une forte corrélation permet un degré de docition élevé, puisque des informations observées on peut donner une prédiction assez sûre de l'état futur. Il existe toujours des modèles qui caractérisent l'activité du spectre (cf. [XL06], [GS08]). Ces modèles prédisent l'occupation du spectre, et la durée de chaque événement récurrent. La SPE peut donc se baser sur ces conclusions pour déterminer un modèle du canal local. Sous l'hypothèse que l'environnement peut être modélisé, ou, plus précisément, qu'il présente une certaine autocorrélation donc qu'il est prédictible, et qu'un certain niveau de docition peut être appliqué, la SPE doit encore, en raison de la mobilité dans les réseaux ad hoc, assurer et vérifier l'intégrité du modèle. La SPE estime la capacité du modèle à représenter l'état de l'environnement. Dès que le modèle est validé et appliqué, pour qu'un nœud soit sélectionné par la SPE pour être candidat à l'enseignement, il faut qu'il soit considéré comme stable au sens de sa géolocalisation, autrement la SPE l'élimine d'emblée comme professeur potentiel. La SPE utilise le GPS ou bien des méthodes de détection de changement d'environnement comme dans [NMB11] pour identifier le déplacement d'un nœud. À chaque

fois qu'un modèle est validé et utilisé, on enregistre la date du début de son utilisation. L'ancienneté d'un modèle indique son efficacité et la stabilité de l'environnement et peut donc devenir un critère de sélection. Cela rend donc le modèle plus privilégié pour être utilisé et, par suite, la SPE marque le nœud qui l'a adopté après un certain temps comme candidat potentiel à l'enseignement.

Choisir l'enseignant

Bien que les auteurs de [JS06] affirment que si deux nœuds sont capables de communiquer cela implique un niveau minimum de corrélation croisée entre leurs environnements, la SPE doit vérifier elle-même l'existence d'un niveau minimum de corrélation entre les environnements de l'enseignant et des étudiants. Pour déterminer si un nœud candidat à l'enseignement est adapté à un nœud élève en particulier, il doit y avoir un certain degré de similitude entre les environnements des deux nœuds. Il n'est pas toujours facile de trouver la meilleure façon d'estimer cette corrélation croisée sous contrainte de minimisation de dépense énergétique (donc de trafic et d'échantillonnage). La plus simple est par l'échantillonnage de N mesures de l'état de l'environnement du nœud étudiants et le calcul de la corrélation croisée avec les échantillons des voisins mais cela requiert trop d'échanges. Dans certaines conditions on peut y être obligé. Des méthodes basées sur la coopération avec les voisins peuvent être utilisées pour construire une estimation distribuée. Ces méthodes sont moins coûteuses en énergie mais elles sont moins robustes.

5.4 Application à l'adaptation dynamique des tailles de paquets à partir de l'obtention par docition dynamique des paramètres de la loi de Pareto modélisant les silences de trafic WiFi environnant

Pour illustrer l'intérêt de la docition dynamique, nous considérons le scénario où un réseau de capteurs, que nous voulons rendre docitif, coexiste avec un ou plusieurs réseaux WiFi. Les scénarios de coexistence de réseaux de capteurs avec des points d'accès WiFi posent le problème que les nœuds WiFi ne détectent pas les transmissions des capteurs et, par conséquent, n'entendent pas les émissions des capteurs et ne se retiennent donc pas d'émettre lors de leurs transmissions. Notre objectif est alors que chaque nœud de capteur ait un modèle des durées des silences WiFi pour déterminer la taille des paquets qu'ils envoient ou leur nombre. Un silence est le temps qui s'écoule entre deux salves consécutives de transmissions WiFi. Notre proposition de docition dynamique, implantée dans les nœuds du réseau de capteurs, vise à estimer au mieux les paramètres de la loi modélisant les périodes pendant lesquelles l'ensemble des nœuds WiFi sous la couverture desquels un nœud de capteurs se trouve sont silencieux.

L'apport de la docition dynamique est d'accélérer le temps de convergence des paramètres de ce modèle pour un capteur nouvellement arrivé à un endroit du réseau. Accélérer ce temps permet de fixer au mieux la taille des paquets à envoyer et leur nombre et donc de limiter la dépense énergétique. Lorsqu'un nœud arrive, chacun des nouveaux voisins envoie les paramètres du modèle de silence au nouveau avec une mesure de gain de ces paramètres exprimée à travers leur durée d'utilisation : plus les paramètres sont utilisés depuis longtemps, plus ils sont considérés fiables. Le nouveau nœud choisit de tous les candidats à l'enseignement voisins le meilleur en ce sens. Comme modèle des durées des silences, nous utilisons celui proposé dans [HXZZ10]. Selon [HXZZ10], les distributions des silences du trafic WiFi sont bien

modélisées par le modèle de Pareto $P(\alpha, \beta)$. Nous l'adoptons donc et chaque nœud cherche à en déterminer ses paramètres pour ajuster sa communication avec les autres du réseau de capteurs.

La docition dynamique a surtout un intérêt dans les réseaux mobiles sans infrastructure. Dans ce type de réseaux, elle permet de choisir entre docition « au démarrage » seulement, c'est-à-dire à l'arrivée d'un nœud dans un nouveau lieu, et aucune docition. Nous adoptons la docition au démarrage (deuxième degré de docition) pour la détection des paramètres du modèle de silences. Dans le concept initial de docition au démarrage, les radios docitives enseignent leurs politiques à tous les nouveaux arrivants, au début, lorsque les nœuds démarrent. Nous devons souligner que le concept initial de docition fut proposé pour les réseaux à infrastructures, et un nouvel arrivant est une station de base qui passait de l'état "ARRÊT" à l'état "EN MARCHE". Des gains sont alors prévisibles avec la docition au démarrage en raison du fait que l'environnement est fortement corrélé et que les nœuds enseignants ont un modèle mis à jour de l'environnement alimenté par leurs processus cognitifs. Dans le cas de réseaux ad-hoc aucune de ces hypothèses n'étant vérifiée, il n'est par conséquent pas toujours opportun de récupérer des informations d'un professeur voisin, il faut donc se poser la question de l'opportunité de la docition et c'est l'idée même de docition dynamique.

Nous supposons que les nœuds, qu'ils deviennent enseignants ou élèves, ont un mécanisme qui leur permet de détecter instantanément un changement de contexte, par exemple lorsqu'un certain pourcentage du nombre de leurs voisins a disparu ou vient d'apparaître ou grâce à des techniques de géolocalisation comme l'utilisation d'un GPS.

5.4.1 Fonctionnement du nœud enseignant

Le nœud enseignant détermine et maintient une estimation des paramètres de la loi de Pareto modélisant les temps de silence du WiFi. Il les estime à nouveau et retient les nouvelles valeurs si elles changent beaucoup par rapport aux dernières. À chaque changement, il enregistre la date du changement pour que l'on puisse déterminer la durée écoulée depuis le dernier changement, c'est-à-dire « l'âge » des paramètres du modèle. Pour ce faire, il exécute les traitements suivants:

1. Échantillonnage de la puissance du canal et calcul des durées des temps de silence (x_i).
2. Estimation des paramètres de la loi de Pareto $P(\alpha,\beta)$ par maximum de vraisemblance pour β : $\beta = n/\sum_{i=1}^{n} \log(\frac{x_i}{\alpha})$, α étant pris égal au minimum des mesures x_i]; et n étant la taille de l'échantillon des silences.
3. Mise à jour de la durée écoulée depuis le dernier changement des paramètres de la loi de Pareto $P(\alpha,\beta)$.
4. L'exposant de Pareto β' nouvellement calculé est adopté seulement s'il n'appartient pas à l'intervalle $[\beta(1-k);\beta(1+k)]$ où β est la dernière valeur retenue pour l'exposant de Pareto et k est le pourcentage acceptable de l'écart entre β' & β. Si β' est retenu, la durée écoulée depuis le dernier changement est remise à zéro, puis on exécute à nouveau l'étape 2. .
5. Si le nœud n'a pas détecté de changement de position géographique (par GPS ou par un seuil sur le nombre de ses voisins qui changent) depuis la dernière modification retenue des paramètres de la loi de Pareto et si le temps qui s'est écoulé depuis cette

date est au-delà d'un certain seuil, c'est-à-dire sur un critère d'ancienneté validée des paramètres de la loi de Pareto, le nœud se déclare enseignant.

6. Dès qu'il détecte l'arrivée d'un nouveau nœud, s'il s'est déclaré enseignant, le nœud diffuse un message précisant sa fonction de professeur ainsi que la valeur des paramètres de la loi de Pareto et la durée du temps qui s'est écoulé depuis leur mise à jour.
7. Un nœud enseignant qui détecte un changement de contexte (position géographique) cesse immédiatement de devenir enseignant.

Le critère que nous avons retenu pour décider si l'on devient enseignant ou pas est le temps qui s'est écoulé depuis le dernier changement de la valeur des paramètres de la loi de Pareto. D'autres critères auraient pu être retenus comme une estimation du débit transmis, qui doit être élevé si l'estimation est bonne et faible sinon. Cependant, notre critère nous semble préférable car il ne nécessite pas de coopération entre le nœud et ses destinataires.

5.4.2 Traitements au niveau du nœud étudiant

Les nœuds étudiants doivent récupérer les paramètres de la loi de Pareto modélisant les temps de silence du trafic WiFi local. Ils le font lorsqu'ils arrivent dans un nouveau lieu, et uniquement à ce moment-là, c'est pourquoi l'on parle de docition « au démarrage », et ils ne le font que si des nœuds s'étant reconnus comme enseignants potentiels sont présents dans le nouvel environnement d'une part et, d'autre part, si les nœuds enseignants potentiels envoient des valeurs de paramètre de la loi de Pareto qui sont assez regroupées autour de leur valeur moyenne. Sinon, si ces valeurs sont très dispersées, cela n'a pas beaucoup de sens d'en retenir une plutôt qu'une autre et, dans ce cas, aucune docition n'est effectuée. Un noeud étudiant effectue les traitements suivants.

1- Si le nœud détecte un changement d'emplacement, il envoie une balise.
2- Le nœud reçoit les qualifications des voisins s'étant auto-déclarés comme enseignants.
3- Un niveau minimal de consensus entre les candidats à l'enseignement doit exister. Si la corrélation entre eux est faible aucune docition n'est faite. La moyenne des β_i reçus est calculée par le noeud et la dispersion des valeurs reçues par rapport à cette moyenne mesurée. Si celle-ci est supérieure à K (par exemple K = 10%), on considère qu'il n'y a pas de corrélation entre les valeurs mesurées des noeuds. Sinon, le nouveau nœud doit choisir un enseignant et les candidats acceptables sont ceux qui ont une valeur $\beta_i$dans l'intervalle $[E(\beta) - y; E(\beta) + y]$ où $y = \frac{K \times E(\beta)}{2}$; où K est un taux qui exprime la limite acceptable de corrélation entre les voisins candidats à l'enseignement.
4- Le nœud sélectionne en tant qu'enseignant le voisin ayant le gain le plus élevé, c'est-à-dire la plus grande durée écoulée depuis le dernier changement de valeur de β et dont cette valeur tombe dans l'écart indiqué au point 3. S'il n'y a pas de candidat acceptable, aucune docition n'est faite par défaut.
5- Après une période de stabilité, le nœud change d'état de nœud élève à nœud enseignant.

5.5 Evaluation des performances

Nous avons utilisé MalLab pour l'étude des performances par simulation de notre proposition de docition dynamique. Tous les intervalles de confiance sont indiqués sur les figures. Sur une surface, nous avons installé une grille de points d'accès WiFi dont les couvertures se chevauchent. Chacun a une zone de couverture (πR^2) et une zone de chevauchement autorisée $\pi(R^2\text{-}R1^2)$. La zone de chevauchement est prévue pour permettre le hand over de terminaux WiFi mobiles entre plusieurs points d'accès et est accompagnée d'un certain niveau d'interférences. Les capteurs sont distribués selon un processus de Poisson dans le plan Figure 5.3.

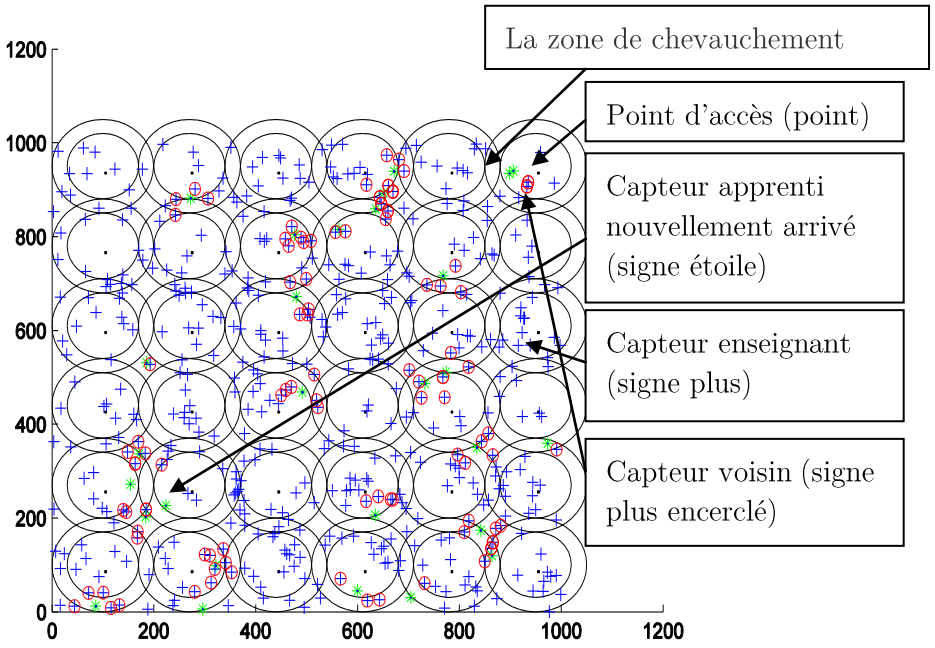


Figure 5.3: topologie simulée

À chaque point d'accès est attribué un générateur de trafic qui envoie des rafales de paquets alternant avec des périodes de silences suivant un modèle de Pareto. Les capteurs échantillonnent le canal pour estimer les paramètres de la loi de Pareto. Remarquons que l'estimation des paramètres par un capteur peut donner un résultat différent des paramètres des générateurs de trafic car la durée des silences en un point du plan dépend du nombre de points d'accès WiFi couvrant ce point.

Comme nous utilisons la modélisation du trafic WiFi par des silences suivant une loi de Pareto proposée par les auteurs de [HXZZ10], nous reprenons également les valeurs des paramètres qu'ils ont obtenues de leurs mesures. Le modèle de Pareto a deux paramètres, α et β. α est défini comme longueur minimale acceptable, choisie dans [HXZZ10] de 1 ms et β est estimé en utilisant le maximum de vraisemblance de la longueur des silences, comme déjà expliquée précédemment. Pour échantillonner les silences, ou, plus précisément l'occupation du canal, nous avons utilisé une fenêtre de 100ms. En conséquence, la durée maximale d'un silence ne peut dépasser 100ms. Le taux d'échantillonnage utilisé sur la fenêtre est de 200Hz. Autrement dit, dans une fenêtre de 100ms on écoute périodiquement le canal et non pas continûment, à cette fréquence. Pour le nœud enseignant, nous avons fixé à 10% l'écart acceptable de l'ancienne version de β (i.e. lorsqu'un nouvel échantillonnage est fait suivi d'une

nouvelle estimation de β par maximum de vraisemblance, la nouvelle valeur n'est retenue que si elle est différente de plus de 10% de l'ancienne).

L'étude des performances comporte deux parties. La première traite du coût énergétique de la signalisation de docition. En effet, la docition requiert d'échanger de l'information (comme les valeurs des β) et ajoute des données aux en-têtes. Le coût correspondant est évalué dans la première partie des simulations et comparé au coût d'un échantillonnage direct et au coût des en-têtes sans information de docition, les coûts étant exprimés en énergie. La seconde partie concerne les performances du mécanisme en termes de pourcentage d'obtention d'informations correctes, le mécanisme n'étant pas fiable à 100% car une mauvaise information peut toujours être apprise d'un voisin, et aussi en termes de taux de perte et d'overhead ajouté. En effet, le mécanisme de docition dynamique que nous proposons a pour but, sur l'exemple qui nous sert à illustrer son intérêt, d'adapter dynamiquement la taille des paquets en fonction des tailles des silences du trafic WiFi concurrent. On doit donc minimiser le taux de perte et ne pas ajouter dans le réseau trop de trafic nécessaire à l'implantation du mécanisme.

5.5.1 Coût énergétique de la signalisation de docition

Pour estimer les paramètres du modèle de Pareto des silences, un capteur a deux méthodes: l'une directe, basée sur l'échantillonnage du canal, et l'autre indirecte à partir de l'information de docition reçue des nœuds enseignants eux-mêmes. Les coûts énergétiques des deux méthodes sont présentés Figure 5.4. D'abord, nous avons calculé le coût de l'échantillonnage direct, puis celui lié à la signalisation de docition. Dans ce dernier cas, le coût dépend du temps passé à transmettre et donc de la quantité d'informations transmises, et, bien sûr du nombre d'occurrences de transmissions. L'information nécessaire à la signalisation de docition est au total de 16 bits:

- 2 bits pour indiquer la durée écoulée depuis le dernier changement de valeur des paramètres de la loi de Pareto (le « gain ») (cf. tableau 1), discrétisé selon le tableau suivant:

Tableau 1 : codage des valeurs du « gain »

00	01	10	11
t(ms)< 100	t>=100 & t<200	t>=200 & t<500	t>= 500

- 14 Bits pour la valeur décimale de β:
  - ✓ 4 bits pour la partie entière (valeur maximum de 15)
  - ✓ 10 bits pour la partie décimale (valeur maximum de 1024)

Le champ longueur du paquet indique indirectement si des informations de docition sont ajoutées au paquet ou pas : celles-ci ne sont transmises que lorsque c'est nécessaire.

Sur la Figure 5.4 nous représentons le coût énergétique de la signalisation de docition en fonction de sa taille dans l'en-tête et en considérant que l'information de docition dans l'en-tête peut varier entre 1 et 16 octets. En effet, dans les faits elle est de 16 octets mais on pourrait envisager de la mettre sur moins ou plus d'octets en joint sur le niveau de discrétisation de l'information de docition par exemple (i.e. au lieu de mettre le gain sur deux octets seulement

on pourrait mettre un codage plus précis sur trois octets ou inversement). Le coût énergétique dépend de la durée et est de E= U*I*t.

T: durée(Secondes)	U: tension (Volts)	I: intensité (A)

L'écoute du canal est faite par échantillonnage d'une fenêtre de 100ms, chaque mesure étant de 8 symboles soit une durée totale de 128µs. La durée pour émettre ou recevoir un bit est de 64 µs, avec un cout de transmission de 0.0174A et de réception 0,0197A, la tension est de 3 V.

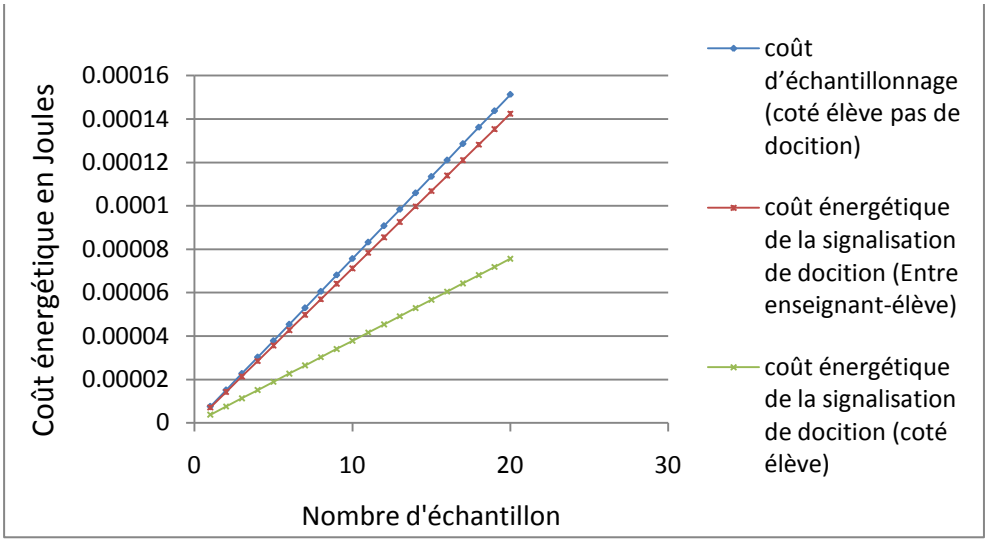


Figure 5.4: coût énergétique en fonction du nombre d'octets ajoutés par la docition dans l'en-tête du paquet pour les courbes bleue et rouge et en fonction du nombre de mesures dans l'échantillon dans le cas de la courbe verte

On peut constater que la signalisation de docition (courbe du milieu) est moins coûteuse que l'échantillonnage direct du canal (courbe la plus élevée). Le coût de la docition au niveau du nœud élève seul est représenté par la courbe la plus basse et représente la quantité d'énergie dont ce nœud a besoin pour découvrir l'environnement (puisque la charge devient partagée entre lui, pour la réception, et son enseignant, pour l'émission).

5.5.2 Etude du taux de perte et du taux d'information correcte de docition

Une grille de 36 points d'accès WiFi avec un rayon de 100m recouvre une surface de $10^6 m^2$. Les capteurs coexistent avec ces points d'accès sur la même surface et ils ont un rayon de couverture de 50m. La distribution des capteurs suit une loi de Poisson, comme nous l'avons déjà dit.

Nous commençons, au A), par observer le taux de sélection de bonne information, puisque la méthode de docition a justement pour but d'obtenir des informations sur l'environnement plus rapidement qu'en les cherchant soi-même. Nous comparons trois méthodes pour sélectionner l'enseignant pour le processus de docition. La première méthode consiste à choisir un enseignant au hasard dans le voisinage, la deuxième choisit la valeur β envoyée par ses voisins qui revient le plus souvent et la troisième méthode est notre proposition de docition dynamique. Dans la partie suivante, au B), nous examinons deux autres critères : le taux de perte de paquets et l'overhead introduit par la docition. Utiliser le mécanisme de docition dynamique pour obtenir des informations a justement pour but de les utiliser pour adapter les

mécanismes réseaux afin d'améliorer leurs performances. Nous nous intéressons donc aux critères de performances réseaux que sont le taux de perte et l'overhead.

Comme nous nous intéressons à la docition « au démarrage » (deuxième degré de docition), la simulation consiste à faire venir des nœuds de l'extérieur et à les placer uniformément dans le plan où sont déjà répartis les capteurs et les points d'accès WiFi. Cette simulation est répétée suffisamment pour obtenir de bons intervalles de confiance. Comme nous étudions la docition au démarrage, nous nous plaçons dans le pire cas où les nœuds viennent de l'extérieur du réseau, dans un environnement où il y a très peu de trafic WiFi, donc des silences WiFi grands c'est-à-dire encore des valeurs de β petites par rapport à celles des nœuds qui sont dans le réseau. Puisque la mobilité se traduit par des nœuds voisins ayant des valeurs de β qui ne sont pas à jour, nous la modélisons en faisant aussi venir de l'extérieur de nouveaux nœuds et en les répartissant aléatoirement et uniformément dans le plan. Ces nœuds ont aussi une valeur de β petite.

Nous avons exécuté quatre types de simulations. Les deux premières ont pour but d'observer l'effet de K, pourcentage des valeurs de β acceptables autour de la moyenne des β reçus des professeurs, ce pourcentage servant à l'étudiant à éliminer les autres valeurs de β reçues. Pour ces deux simulations, le nombre de nœuds venant de l'extérieur est fixé à 30 et l'on observe les résultats en fonction du nombre de nœuds présents dans le réseau. Dans la troisième simulation, on augmente à la fois le nombre de nœuds venant de l'extérieur et celui déjà présent dans le réseau mais en gardant le pourcentage de nœuds venant de l'extérieur par rapport à celui déjà présents dans le réseau constant. La densité des nœuds augmente donc mais la proportion de voisins nouveaux reste pour un nœud venant de l'extérieur (étudiant docitif) inchangée. Enfin, dans la quatrième simulation, le nombre total de nœuds dans le réseau, soit déjà présents avant l'arrivée des nouveaux soit nouveaux, reste constant tandis que le pourcentage de nouveaux voisins augmente. En d'autres termes, le nombre de nœuds venant de l'extérieur augmente tandis que celui anciennement présents sur le réseau diminue.

Tandis que les deux premiers scénarios correspondent au cas où les nœuds de capteurs sont fixes et le seul mouvement est l'arrivée de nouveaux nœuds, les deux derniers permettent d'observer le comportement du réseau en situation de mobilité des capteurs. En effet, pour la docition dynamique, leur mobilité a pour effet que de nouveaux nœuds arrivant de l'extérieur trouvent dans leur nouveau voisinage des nœuds qui ont une bonne estimation de beta car ils ont eu le temps de l'obtenir et d'autres qui viennent d'arriver d'un autre endroit du réseau, qui détectent aussitôt leur changement de contexte mais qui ne peuvent être professeurs à cause de leur changement récent de position. Donc, en situation de mobilité et dans le cas de la docition dynamique, tout se passe pour les nouveaux nœuds qui arrivent comme si les capteurs mobiles dans le réseau et qui se retrouvent sous leur voisinage venaient de l'extérieur. Pour la docition classique, les anciens nœuds du réseau qui sont mobiles et qui se trouvent dans le voisinage des nouveaux arrivés de l'extérieur sont toujours professeurs. Cependant, dans le pire cas, et le plus probable, ils ont une valeur de β qui n'est plus bonne. Tout se passe donc alors en ce qui les concerne comme s'ils arrivaient aussi de l'extérieur pour le calcul du pourcentage de sélection correcte d'information par la docition. C'est pourquoi, dans les deux cas, en augmentant le nombre de nœuds venant de l'extérieur on peut observer l'effet de la mobilité des capteurs déjà présents dans le réseau sur le pourcentage de sélection correcte d'information par la docition. Nous appelons alors les deux premiers scénarios « scénario quasi-statique » et les deux derniers « scénario mobile ».

La valeur de β est affectée aux points d'accès WiFi selon une loi uniformément distribuée. À chaque capteur déjà présent dans le réseau on attribue d'emblée la bonne valeur de β de la distribution des temps de silences des nœuds WiFi qui le recouvrent. En effet, les capteurs présents avant l'arrivée des nouveaux ont eu le temps de faire leur estimation, ce qui n'est pas le cas des autres. La probabilité pour un nouveau nœud étudiant de choisir la bonne valeur de β à partir des voisins est estimée.

- ***Qualité de l'information obtenue par la docition, scénario quasi statique:***

Les nœuds déjà présents avant l'arrivée des nouveaux sont sensés avoir une bonne estimation de β mais celle-ci n'est pas forcément la bonne pour un nouveau nœud arrivant lequel n'est pas à la même position que ses voisins. Le pourcentage de déviation acceptable K de β est fixé à 20% et R1 à 75% de R pour la première simulation. On passe ensuite K à 10% pour la deuxième. Sur la Figure 5.5, les résultats montrent que pour la docition classique, la probabilité de sélection du bon voisin est relativement fixe (environ 67%) par rapport au nombre de nœuds couvrant la région. Dans le cas où la sélection des β est faite à partir du nombre maximal de voisins ayant cette valeur de β, le pourcentage de sélections correctes augmente en fonction du nombre de nœuds existants. Il présente une meilleure estimation que la docition classique. Bien que ce soit meilleur que la docition classique, il reste une marge d'amélioration puisque la docition dynamique, qui se base sur le pourcentage de déviation par rapport à la moyenne (colonne du milieu de la Figure 5.5 et de la Figure 5.6) présente les meilleures performances des trois méthodes.

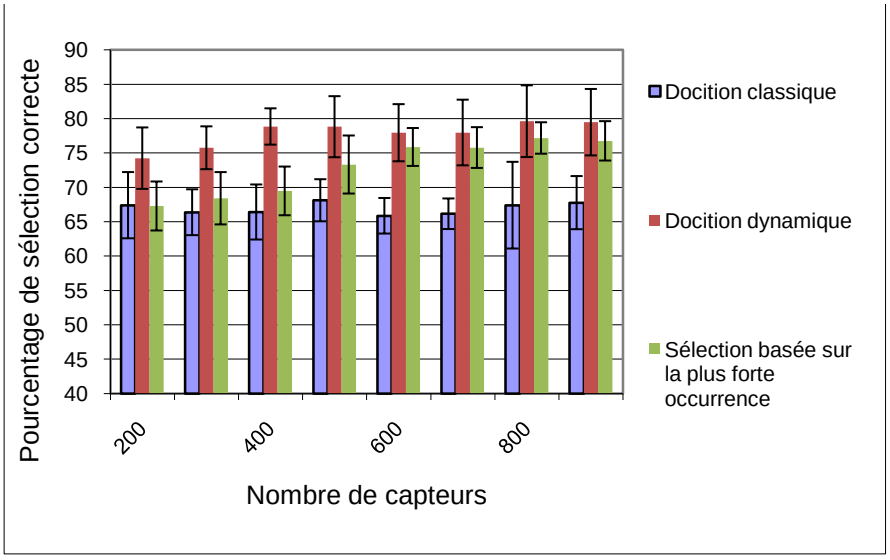


Figure 5.5: pourcentage de sélection correcte de la bonne valeur de β *en fonction du nombre de nœuds qui existant avant l'arrivée d'un nœud étudiant, K=20%*

Nous limitons maintenant à 10% le pourcentage K d'écart acceptable de β pour la docition dynamique. De meilleures performances apparaissent sur la Figure 5.6. Une restriction plus forte sur la sélection de la valeur de β affinerait sa qualité mais entraînerait une plus grande restriction de l'utilisation de la docition : les nœuds seraient alors contraints d'estimer par eux-mêmes la valeur de β.

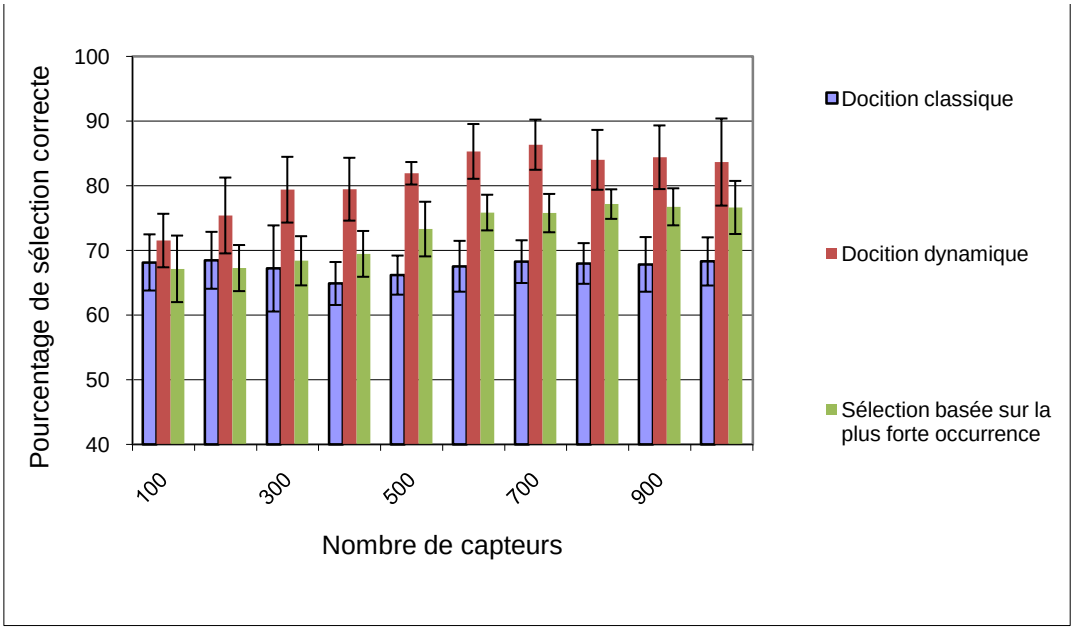


Figure 5.6: pourcentage de sélection correcte de la bonne valeur de bêta en fonction du nombre de nœuds existant avant l'arrivée des nœuds étudiants, K=10%

- ***Scénario Mobile:***

Pour les deux autres simulations, le nombre de nœuds venant de l'extérieur augmente, ce qui permet d'observer l'effet de la mobilité sur notre proposition : de plus en plus de voisins de nouveaux nœuds n'ont pas d'informations à jour et ne peuvent donc les enseigner. En d'autres termes, les voisins d'un nouveau noeud ne sont plus nécessairement candidats à devenir nœuds enseignants dans le cas de la docition dynamique. Pour la docition classique, il n'y a en revanche pas de distinction entre bon et mauvais candidat pour devenir nœud enseignant. La Figure 5.7 présente la dégradation des performances de la docition classique en fonction du nombre de nœuds. En effet, les nœuds mobiles qui ne seraient pas candidats à l'enseignement dans le cas de la docition dynamique peuvent l'être dans le cas de la docition classique, ce qui conduit à la transmission d'informations incorrectes. En revanche, celles de la docition dynamique s'améliorent. Sur la Figure 5.7 la densité du réseau est augmentée mais en gardant toujours 70% des nœuds qui ont des informations périmées.

Pour l'expérience de la Figure 5.8, 300 capteurs sont distribués sur la surface. Le pourcentage de sélection d'une valeur correcte de β est observé. On constate que les nœuds non experts n'influent pas les performances des nœuds qui utilisent la docition dynamique, mais qu'ils affectent les performances de la docition classique, ce qui est normal puisque la docition classique n'établit pas de distinction entre nœuds enseignants experts et nœuds non experts.

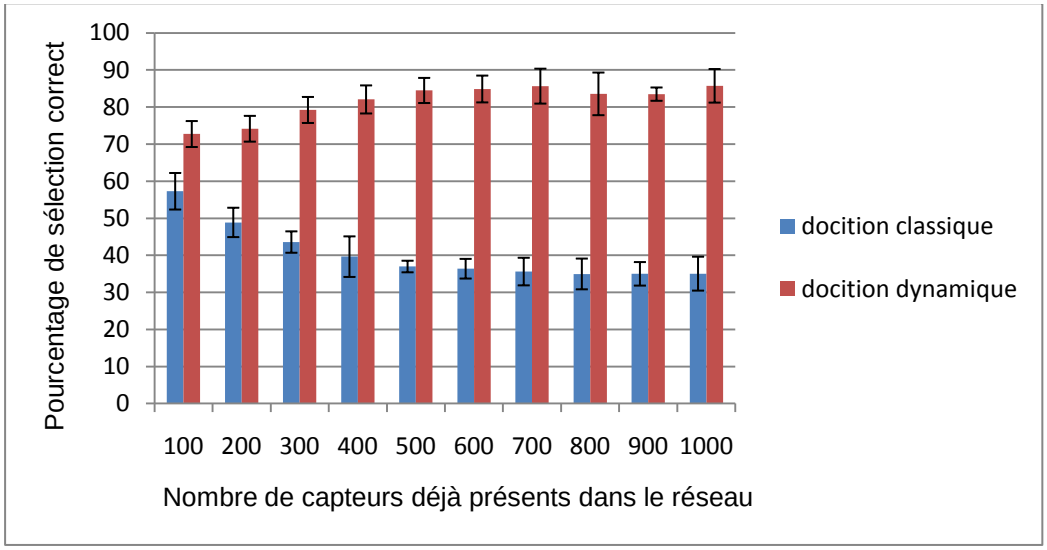


Figure 5.7: pourcentage de sélection correcte de la bonne valeur de bêta en fonction du nombre de capteurs présents dans le réseau

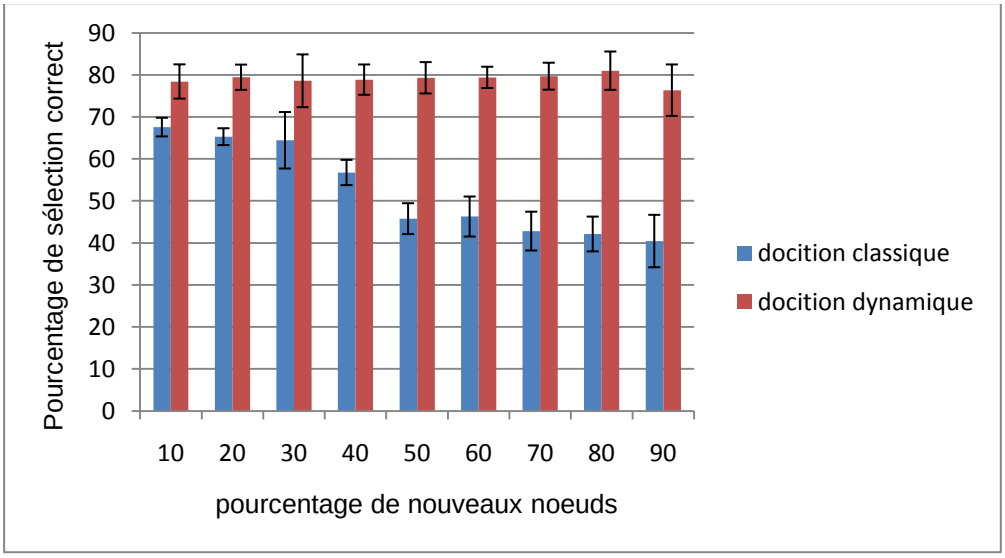


Figure 5.8: pourcentage de sélection correcte de la valeur de bêta en fonction du pourcentage de voisins inexpérimentés

Globalement, on constate que la docition dynamique permet bien d'éviter la réception de fausses informations d'autres nœuds. Ceci peut alors permettre d'accélérer la convergence de mécanismes réseaux en fonction du contexte. Dans la partie suivante, on observe justement l'effet d'un tel mécanisme dont le paramètre est adapté en fonction du contexte avec la docition dynamique.

A. Utilisation de la docition pour l'adaptation dynamique de la taille de paquets des capteurs

Dans la partie précédente, les valeurs de β étaient affectées directement aux nœuds de capteurs en fonction de celles des nœuds WiFi qui les recouvraient, sauf pour les nœuds provenant de l'extérieur qui avaient de petites valeurs de β. Maintenant, le processus de l'échantillonnage des silences et de l'estimation de β par maximum de vraisemblance est aussi simulé. On compare ici le mécanisme de docition dynamique que nous proposons avec la

docition classique et l'estimation directe et systématique de β. L'effet d'une plus ou moins bonne connaissance de β sur les performances du réseau, le taux de perte et l'overhead ajouté par le mécanisme d'estimation, est examiné.

Désormais, les nœuds du réseau de capteurs transmettent des paquets dont la longueur est adaptée dynamiquement en fonction du temps ρ écoulé depuis le début du silence courant, comme les auteurs de [HXZZ10] le proposent:

$$l = \begin{cases} \rho(1-C)^{\frac{-1}{\beta}} - \rho, & si\ \rho > 0 et\ l \geq longueur\ de\ l'en - tête \\ 2\ ms, & \rho = 0\ ou\ l < longueur\ de\ l'en - tête \end{cases}$$

(formule (13) de [HXZZ10])

où l est la durée de transmission d'une paquet en millisecondes et C est la probabilité d'avoir une collision avec une transmission WiFi. Cette probabilité est fixée par l'ingénieur du réseau selon le taux acceptable de collisions (pour toute les simulations le taux acceptable est fixé à 20%). β est l'indice de Pareto et obtenu soit par le mécanisme de docition statique, soit par celui de docition dynamique soit par échantillonnage et estimation directs. En effet, tous le nœuds dans toutes les méthodes estiment le canal régulièrement mais nous nous focalisons ici sur l'initialisation quand un nœud arrive dans le réseau. Pour récupérer la valeur de β, ils peuvent soit l'estimer directement soit la récupérer via la docition dynamique ou classique. C'est en ce sens que nous disons que β est obtenu par estimation directe. Pour le reste des expériences, nous avons fixé le pourcentage acceptable d'écart des nœuds étudiants pour la docition dynamique à 10%.

- ***Scénario quasi-statique:***

Le taux de perte de paquets et le pourcentage d'overhead sur un lien sont observés sur la Figure 5.9. La docition dynamique et la docition classique doivent avoir des performances similaires dans ce scénario quasi-statique puisqu'un nouveau nœud qui arrive trouve des voisins qui ont eu le temps d'avoir une bonne estimation du paramètre de Pareto. R1 est mis à 50% de R. Dans le cas de la docition classique, tous ses nouveaux voisins déjà sur place lui communiquent leurs valeurs et il peut y avoir une faible dégradation des performances car l'étudiant ne filtre pas les valeurs reçues et ne prend donc pas une valeur plutôt proche de leur moyenne empirique, ce qui est fait avec la docition dynamique, mais comme tous les nœuds déjà sur place ont eu le temps d'obtenir une bonne valeur de β, l'écart entre docition dynamique et classique est faible. Dans le scénario mobile, la différence est plus marquée, de même qu'elle était plus marquée dans l'étude précédente du pourcentage de sélection correcte de valeur de β dans le cas mobile que dans celui quasi-statique. Le pourcentage d'overhead atteint 38% et la perte de paquets est de 22% comme le montre la Figure 5.9. Bien que, les résultats de performances sont quasiment similaires pour les trois méthodes, la docition dynamique est légèrement meilleure que la docition classique.

Sur la Figure 5.10, la même simulation est exécutée, mais R1 est pris égal à 70% de R. Les intersections de couvertures WiFi sont donc plus grandes, ce qui introduit plus de diversité pour les valeurs de β reçues des voisins. Cela doit conduire à une probabilité plus élevée de sélectionner une mauvaise valeur de β.

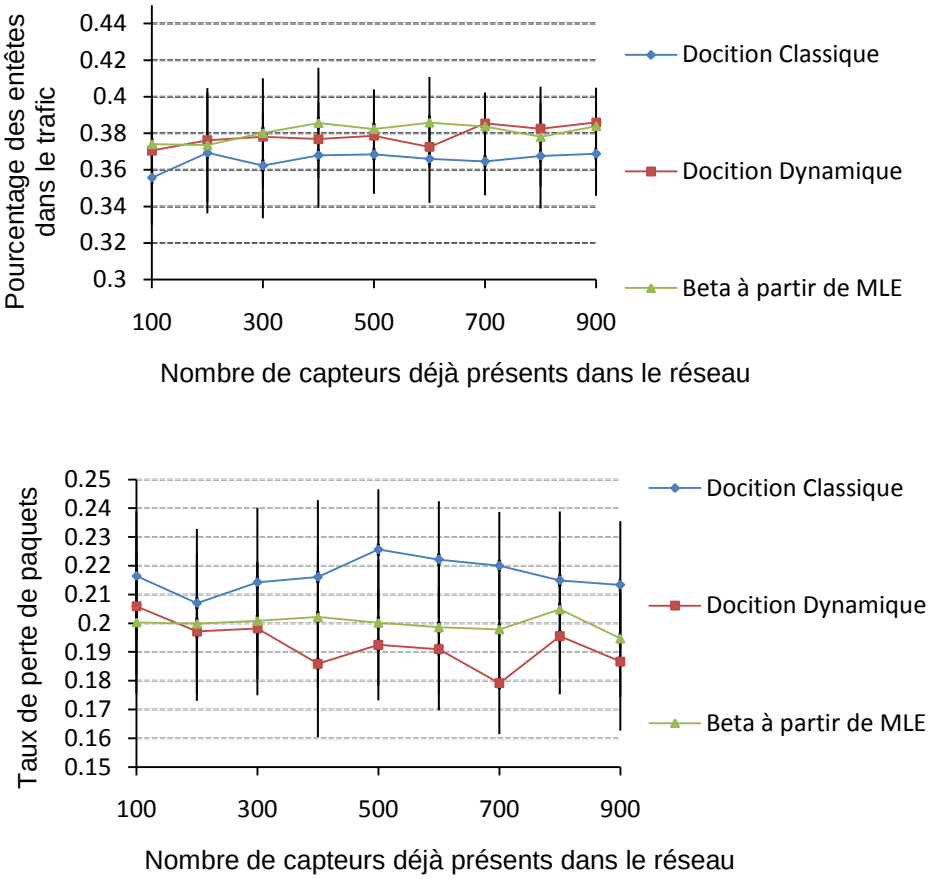


Figure 5.9: Pourcentage d'overhead sur le lien (graphe du haut) et taux de perte (PLR, graphe du bas), en fonction du nombre de nœuds présents dans le réseau avant l'arrivée des nœuds étudiants

Le taux de perte de paquets sur la Figure 5.10 est relativement supérieur à celui de la Figure 5.9 à cause des recouvrements de couvertures WiFi conduisant à des silences moyens plus petits, et donc des tailles de paquets plus petites ce qui diminue le taux de collision, la probabilité de collisions diminuant avec la taille du paquet. Toutes les méthodes de docition utilisées ont les mêmes performances, qui sont assez bonnes. Ceci est encore dû à l'environnement qui est fixe. Comme pour le cas précédent, dans ce scénario quasi-statique les pertes sont dues au fait que l'étudiant n'est pas nécessairement sous la même couverture exactement que ses voisins et peut donc être « arrosé » par du trafic WiFi dont les silences sont de tailles différentes que ses voisins ou bien encore à la volatilité des résultats de reçus, les voisins étant dans des environnements un peu différents. Bien que cette situation ait une faible probabilité, son effet est observé par le rendement plus faible de la docition classique par rapport à la docition dynamique.

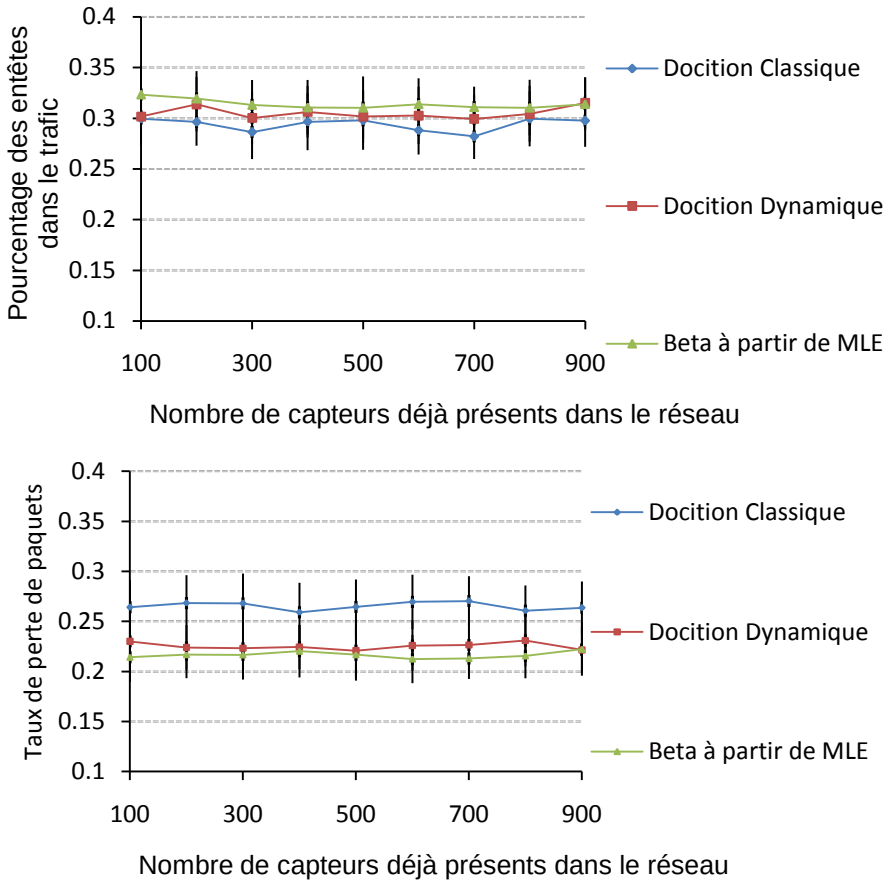


Figure 5.10: Pourcentage d'overhead par rapport trafic total (graphe du haut) et taux de perte de paquets (graphe du bas), en fonction du nombre de nœuds existant avant l'arrivée des nœuds étudiants

- ***Scénario Mobile:***

Dans ce qui suit, R1 est mis à 70% de R. Au début (Figure 5.11 et Figure 5.12), 50% des voisins sont des nœuds mobiles, les performances étant donc tracées en fonction du nombre de nœuds mais le pourcentage de nœuds mobiles étant fixe tandis qu'à la Figure 5.13 le nombre de nœuds est fixe mais le pourcentage de nœuds mobiles augmente. Avec la mobilité, le taux de perte sur la Figure 5.11 subit comme attendu une détérioration forte dans le cas de la docition classique. On constate que la docition dynamique introduit le même overhead que la docition classique mais que le taux de perte est bien meilleur. En prenant comme référence l'estimation directe par maximum de vraisemblance sans docition, qui nous sert ici de référence pour évaluer les performances des deux types de docitions, classique et dynamique, on constate que la docition dynamique maintient un faible taux de perte tout en gardant un pourcentage d'overhead minimal relativement à la courbe d'estimation directe. Son taux de perte est de 20% de même que l'estimation directe. Rappelons que 20% est le taux de perte cible de la formule qui permet de fixer la taille des paquets. En revanche, le taux de perte pour la docition classique atteint 45%. Le pourcentage d'overhead ne dépend pas du nombre de nœuds et vaut 20% pour la doction classique et 30% pour la docition dynamique. Cela montre que ce n'est pas le nombre des nœuds déjà présents dans le réseau qui a une influence sur les performances mais le pourcentage des nœuds mobile (non candidat à être enseignants). Du reste, c'est bien ce qu'on observe sur la Figure 5.13.

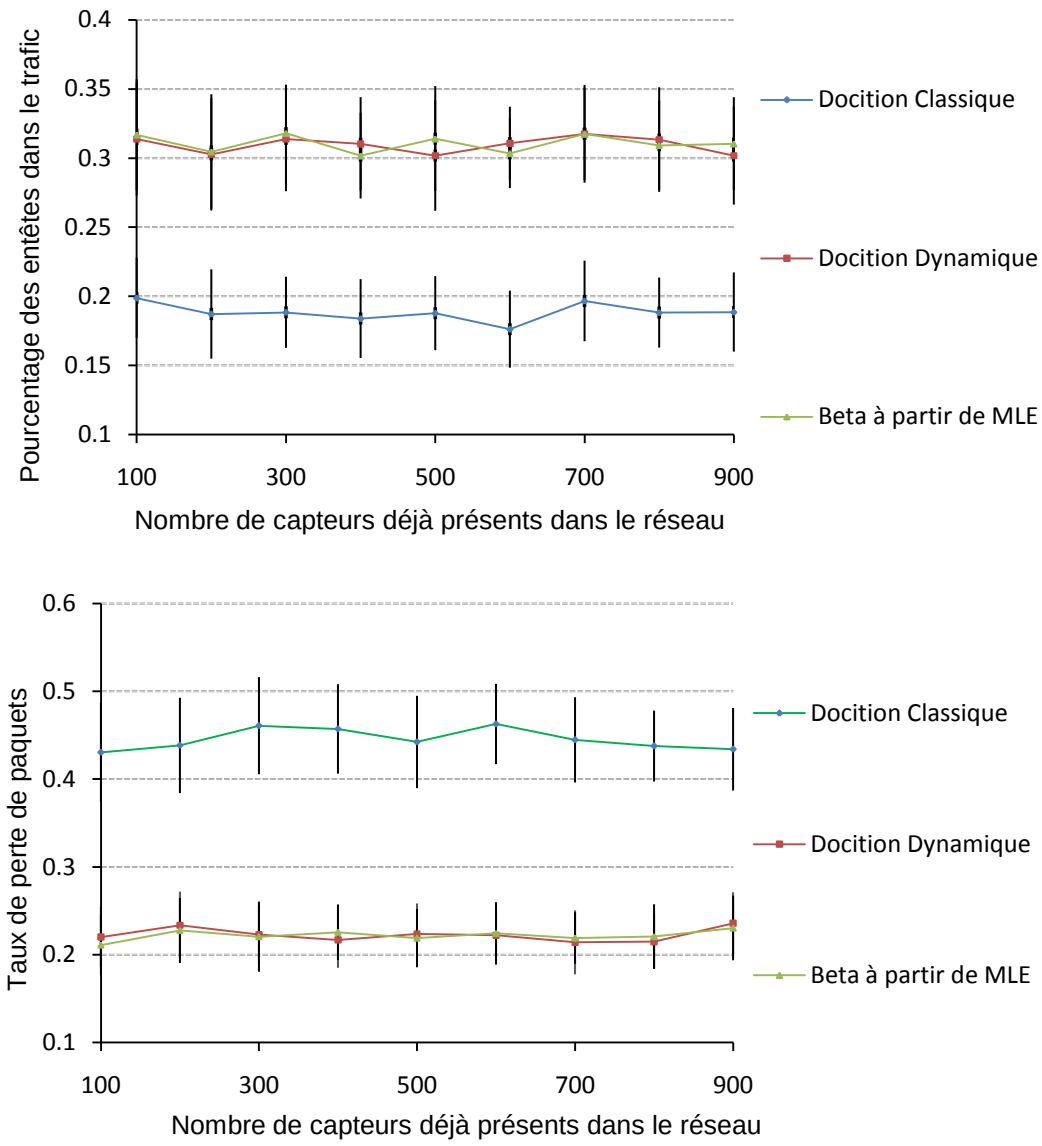


Figure 5.11: pourcentage d'overhead (graphe du haut) taux de perte (graphe inférieur), en fonction du nombre des nœuds existant déjà avant l'arrivée des nœuds étudiants

Comme pour la Figure 5.11, sur la Figure 5.12 le pourcentage d'overhead se stabilise à 17% pour la docition classique et 30% pour la docition dynamique. Sur cette figureFigure 5.12, le pourcentage des voisins mobiles est porté à 70%. Les performances de la docition classique sont encore dégradées. Le taux de perte a faiblement augmenté en fonction du nombre de nœuds existants pour se stabiliser autour de 50%. En revanche, la docition dynamique n'est pas affectée par les voisins inexpérimentés ajoutés.

Nous faisons ensuite varier le pourcentage de nouveaux nœuds tandis que le nombre total de nœuds est fixé à 500. Les résultats de simulation sont donnés Figure 5.13. L'overhead passe de 14% à 28%. La docition classique souffre d'une augmentation du taux de perte à cause de l'augmentation du pourcentage des nœuds inexpérimentés tandis que la docition dynamique s'avère mieux adaptée à la mobilité car elle empêche les nœuds inexpérimentés d'infecter les nœuds élèves de fausses informations.

Ceci met en relief l'importance du discernement dans l'utilisation dynamique de la docition. La sélectivité dans le choix d'un enseignant est importante aussi pour l'amélioration du processus de décision, même si elle est le fruit d'une méthode simple. Des méthodes plus intelligentes peuvent être proposées. Nous avons surtout voulu montrer l'importance de ne pas appliquer d'une façon systématique la docition dans le cas d'un réseau mobile. Les résultats montrent qu'aussi bien la docition dynamique que la docition classique ont plus ou moins les mêmes performances en environnement statique. En revanche, on voit clairement l'effet destructeur de la mobilité sur la docition classique quand le nombre de nœuds mobiles inexpérimentés augmente. Il n'y a pratiquement aucun impact de l'augmentation des nœuds inexpérimentés sur la docition dynamique car elle filtre les nœuds mobiles inexpérimentés.

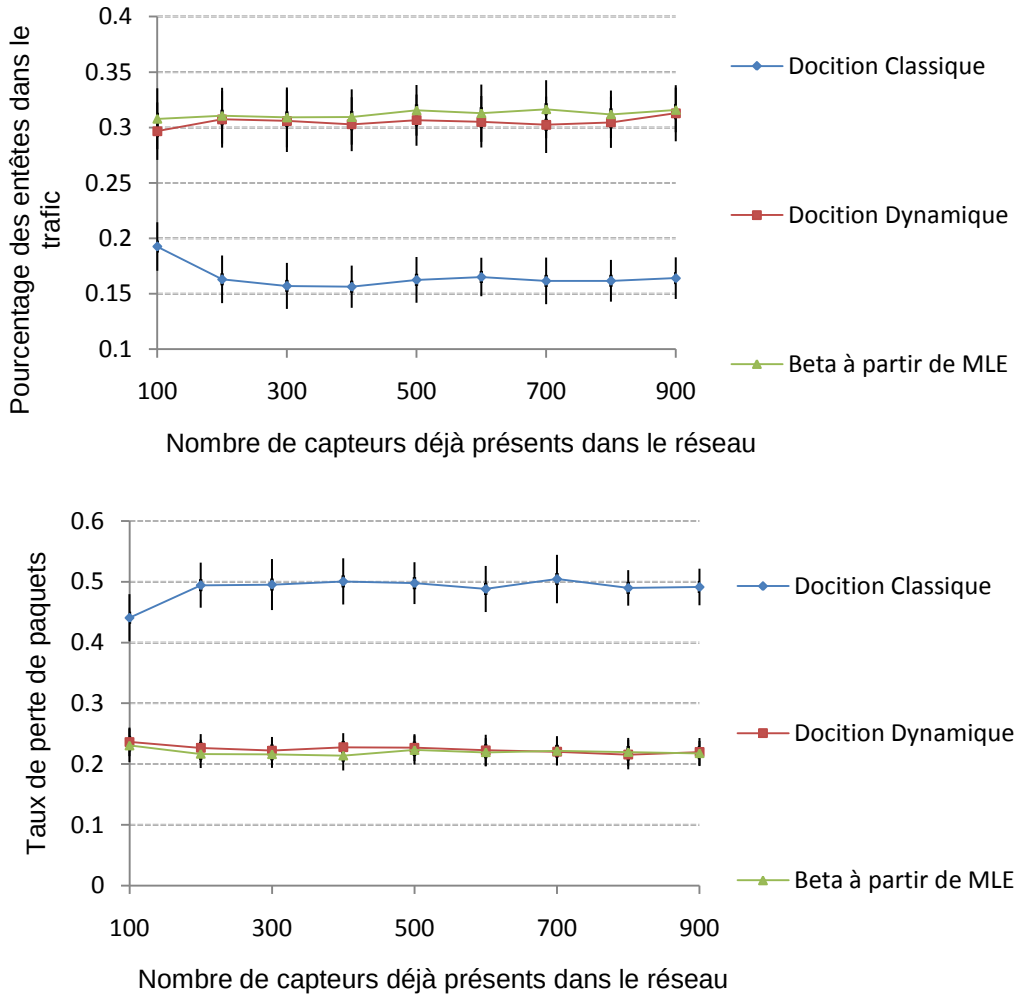


Figure 5.12: pourcentage d'overhead (graphe du haut)et taux de perte (graphe inférieur), en fonction du nombre des nœuds existant avant l'arrivée des nœuds étudiants

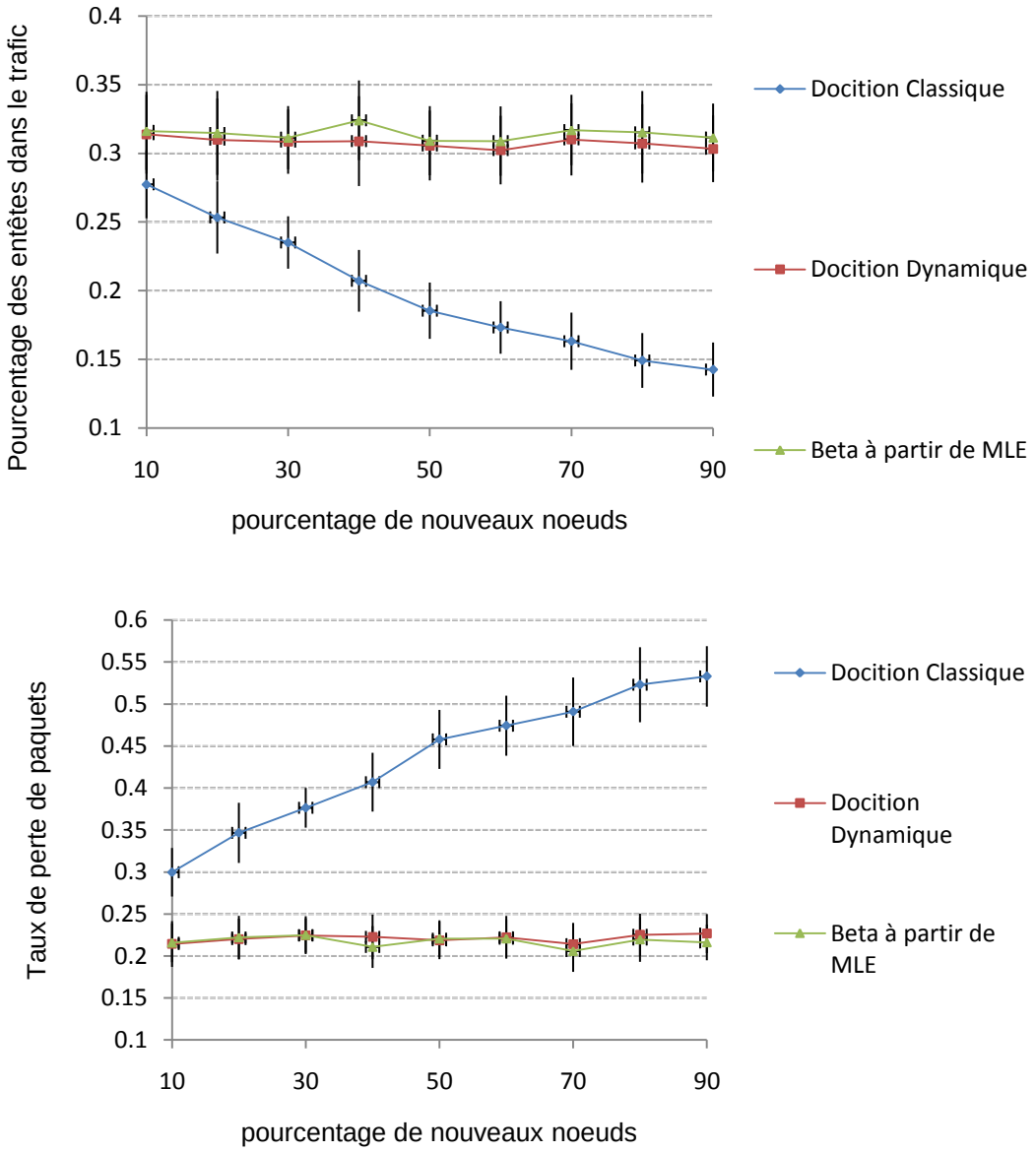


Figure 5.13: pourcentage d'overhead (graphe du haut)et taux de perte (graphe inférieur), en fonction du pourcentage de nœuds inexpérimentés

5.6 Conclusion

La docition est une méthode qui permet d'améliorer la prise de décision dans les réseaux sans fil distribués. Elle permet d'accélérer les processus d'estimation nécessaires à la mise en œuvre de mécanismes réseaux. C'est un nouveau concept qui a été proposé dans un contexte cellulaire, où la cohérence des états des nœuds qui enseignent aux nœuds étudiants est assurée car les stations de base sont immobiles et ont le temps d'apprendre les informations sur l'environnement avec certitude. En revanche, dans le cas d'un réseau de capteurs sans fil, sans infrastructure et mobiles, celle-ci n'est plus certaine et il faut la vérifier. Dans ce nouveau contexte, il est des cas où la docition peut être utile car les nœuds voisins ont une information correcte sur l'état du réseau et dont d'autres nœuds nouvellement arrivés peuvent bénéficier et il en est d'autres pour lesquels les nœuds n'ont pas d'information à jour et, s'ils la

communiquent à des étudiants, peuvent être la cause de dégradations de performances majeures.

Se pose alors la question de savoir, dans le contexte d'un réseau mobile sans infrastructure, quand avoir un comportement docitif et quand s'en abstenir, autrement dit de savoir si le concept de docition lui-même peut être rendu dynamique en fonction du contexte. Dans le concept de docition au démarrage, les radios docitives enseignent leurs politiques à tous les nouveaux arrivants. En d'autres termes, c'est à l'initialisation des nœuds uniquement qu'il y a docition. La méthode que nous proposons, de docition dynamique, tente d'évaluer le degré de cohérence des informations des nœuds à la fois dans le temps et dans l'espace. On s'efforce de mesurer la qualité des informations possédées par les nœuds d'un voisinage en en observant sa cohérence ainsi que son évolution dans le temps.

La docition dynamique ajoute à la docition classique une sonde de prévisibilité de l'environnement qui jauge la stabilité de l'environnement et détermine pour un étudiant le meilleur enseignant. Elle a surtout un intérêt dans les réseaux mobiles sans infrastructure. Dans ce type de réseaux, elle permet de choisir entre docition « au démarrage » seulement, c'est-à-dire à l'arrivée d'un nœud dans un nouveau lieu, et aucune docition. Nous illustrons le concept de docition dynamique au démarrage pour la détection des paramètres d'une loi de Pareto du modèle des silences de trafics WiFi concurrents en vue de l'adaptation dynamique de la taille de paquets envoyés par des capteurs. En effet, il peut arriver que les réseaux de capteurs soient déployés dans un environnement où du trafic WiFi est transmis. Or les points d'accès WiFi, bien qu'ils écoutent le canal avant de transmettre, peuvent ne pas détecter les nœuds de capteurs lorsqu'ils transmettent tout en provoquant chez ces derniers des collisions à cause de la différence de puissance nominale de ces deux types d'émetteurs. Les bornes WiFi ont une puissance de transmission généralement plus élevée que celle des capteurs et un seuil d'écoute moins sensible, ce qui fait que le WiFi « écrase » le trafic des capteurs. Il leur est alors utile de pouvoir profiter des instants de silence observés dans le trafic WiFi pour émettre.

Les simulations montrent que la docition dynamique s'adapte bien à l'évolution du pourcentage de voisins mobiles dans un réseau, contrairement à la docition classique qui entraîne des dégradations de performances lorsque ce pourcentage augmente. Aussi bien le taux de sélection d'informations correctes que les performances des mécanismes réseaux qui les utilisent ensuite sont améliorées avec la docition dynamique par rapport à la docition classique dans le cas d'un réseau de capteurs mobiles sans infrastructure. L'overhead correspondant est à peu près le même pour la docition dynamique que pour la docition classique.

Par rapport à la docition classique, nos simulations ont montré dans certains cas pour la docition dynamique une amélioration de plus de 50% de la sélection correcte de la valeur du paramètre de Pareto par rapport à la docition classique. Une amélioration figure également sur le taux de perte qui présente un gain de plus de 30%. En outre, l'overhead ajouté est estimé et reste moindre qu'une estimation directe du canal en termes de coût énergétique.

Chapitre 6. Conclusion générale

Après une présentation des capteurs sans fil, de leur structure, des principaux types et de leurs limitations, nous avons passé en revue les grandes problématiques actuelles sur le sujet. Les recherches actuelles visent à mettre en place des systèmes s'auto-organisant en fonction du contexte. Les réseaux de capteurs sont déployés dans des environnements qui peuvent changer radicalement, et sont bien souvent sans infrastructure. Nous avons passé en revue les principaux topologies, protocoles MAC ou architectures de routage concernant les réseaux de capteurs. Il est apparu que ce qui a été développé l'a été dans des contextes spécifiques, pour répondre à des besoins particuliers, que, par exemple, dans certains contextes les réseaux ont plutôt une topologie complètement maillée mais que dans d'autres ce n'est plus le cas, et qu'il faut alors qu'ils soient capables de changer dynamiquement d'un protocole à un autre en fonction du contexte mais les résultats répertoriés dans la littérature ne franchissent pas ce pas-là. En effet, les réseaux de capteurs sont amenés à passer par des environnements très différents et à former des réseaux ayant des structures variées. Les protocoles doivent donc être choisis en conséquence. Comme il n'existe pas de protocole de routage ou d'accès au médium qui soit universel, c'est-à-dire adéquat à toutes les topologies et tous les contextes possibles, il est nécessaire de pouvoir changer de protocoles dynamiquement en fonction du contexte.

Par ailleurs, ceci pose des problèmes précis comme celui de la détection du changement de contexte, celui de la reconnaissance du contexte et celui du choix du meilleur protocole à utiliser. Mais détecter le contexte dans lequel se trouve un capteur peut être difficile si tout le voisinage est endormi or, depuis une dizaine d'année, de nouveaux systèmes de réveil à la demande ont été conçus. C'est pourquoi dans la première partie de cette thèse nous nous sommes intéressés justement à un mécanisme permettant de changer dynamiquement de protocoles, mécanisme rendu possible par ces nouveaux moyens de réveil à la demande. Nous avons proposé dans cette première partie un cadre conceptuel pour permettre une telle adaptation dynamique au contexte au niveau des trois couches basses du modèle O.S.I., nous avons sélectionné une panoplie de protocoles adaptés aux différentes situations que peut rencontrer le réseau dans le cadre d'hypothèses précises et nous avons présenté le mécanisme CAM qui permet d'orchestrer le tout en détectant le changement de contexte, en reconnaissant le nouveau contexte et en activant les bons protocoles en conséquence.

Cette proposition est partie d'un besoin identifié initialement dans le cadre de la chaîne du froid mais dépasse cette application spécifique. Nous reconnaissons par exemple les mêmes problématiques qui se posent pour la surveillance du corps humain. Ces réseaux alternent des moments où leurs nœuds sont tous en visibilité directe avec d'autres où ils sont plus étendus, à densité plus faible et nécessitent un routage à plusieurs sauts. Après avoir posé les hypothèses sur lesquelles nous avons construit notre proposition, nous avons passé en revue et discuté les protocoles que nous avons retenu dans notre cadre. Ceux-ci sont des exemples qui conviennent bien aux situations que le réseau risque de rencontrer, mais nous ne prétendons pas que d'autres protocoles ne peuvent pas faire également l'affaire. C'est ainsi que nous avons utilisé la solution de Jurdak présentée dans [JRO08] pour la couche physique, qui comprend à la fois le standard IEEE 802.15.4 et un système de réveil à la demande, un passage dynamique entre un mode TDMA et un mode CSMA/CA au niveau MAC et une alternance entre la solution de diffusion de l'information de PLACIDE et une autre basée sur une organisation en clusters,

celle de MAXMIN ou le processus ponctuel de Mattérn pour la couche routage. Outre leur adéquation à nos attentes en termes de fonctionnalités, ces trois derniers protocoles présentent l'avantage d'avoir été déjà testés en environnement réel. Le mécanisme est décrit en détails pour le cas particulier de la chaîne du froid, puis ses performances évaluées.

Toujours sur l'adaptation au contexte, un sujet actif de recherche concerne l'adaptation à l'environnement et plus particulièrement à la coexistence avec d'autres réseaux concurrents d'autres technologies. C'est d'ailleurs une question qui se pose naturellement dès que l'on est confronté au problème du changement de contexte. Après tout, être plongé au milieu d'un autre réseau ou bien être déjà déployé mais subir l'arrivée d'un autre réseau, de quelque technologie qu'il soit, est bien un changement de contexte auquel il faut pouvoir s'adapter. La diversité des technologies qui coexistent dans la même bande ISM, telles que les réseaux de capteurs, varie de technologies qui n'appliquent pas l'écoute du canal avant leur transmission comme le Bluetooth, à d'autres comme le WiFi qui, en raison des propriétés de leur CCA, ne détectent pas d'autres technologies. Après avoir examiné l'impact de différentes sources d'interférences, nous avons listé les travaux récents pour aider les réseaux à y faire face. Nous avons constaté que les approches proposées conjuguent plusieurs limitations, en particulier celle de nécessiter des écoutes régulières du canal, ce qui est coûteux en termes de consommation énergétique et aussi celle de ne pas permettre d'identifier explicitement la cause de l'interférence. Or, la connaître doit permettre de déclencher la réaction la plus adaptée.

C'est pourquoi nous avons consacré la deuxième partie de cette thèse à la détection et l'identification des réseaux concurrents à celui de capteurs déployé, à partir non pas d'écoutes fréquentes du canal mais des paquets que l'on reçoit. Au lieu de les ignorer, puisqu'on les a reçus, nous avons proposé de les analyser pour déterminer la source des erreurs qui peuvent s'y trouver. C'est un moyen de repérer des signatures de réseaux concurrents, de capteurs ou d'autres technologies. Nous nous sommes donc intéressés à la cause des pertes de paquets dans un réseau de capteurs, et plus particulièrement à l'identification de cette cause pour mettre en place les réactions les plus appropriées car, lorsque des paquets sont perdus, des réactions génériques peuvent être appliquées mais connaître précisément la cause de la perte permet d'appliquer une réaction optimale. Cela peut aider aussi à mettre en place des systèmes d'auto-organisation. Par exemple, si la perte est due à un problème de faible rapport signal sur bruit ou à des interférences avec un réseau WiFi, les solutions à apporter sont de natures vraiment différentes.

Dans cette deuxième partie, nous avons identifié les empreintes de diverses technologies qui coexistent sur la même bande de fréquence sous forme de modèles de corruption des paquets des capteurs sans fil (IEEE802.15.4). Nous avons considéré des trafics concurrents générés par les technologies ZigBee, Bluetooth et WiFi, chacun engendrant un modèle spécifique de corruption. De plus, le cas de corruption due à un lien faible est également considéré. A partir de l'identification de ces empreintes, nous avons conçu FIM, un mécanisme réactif pour détecter à la volée chaque technologie concurrente. Nous avons testé FIM sur notre plate-forme "Tmote Sky". Dans certains cas, FIM fournit jusqu'à 100% de précision dans la détection de l'empreinte digitale correcte. Au cours de quelques-unes des expériences, son application pour l'adaptation de lien a amélioré le débit par 100,9%. Une version de FIM qui fonctionne en mode distribué a aussi été développée. Comme attendu, cette deuxième version présente de meilleures performances que FIM simple. Les résultats montrent une amélioration dans la vitesse de convergence et dans l'ordre de complexité.

L'auto-organisation pose la question de la mise en commun d'informations possédées par les capteurs et de la manière de la récupérer. Par exemple, la détection d'un réseau concurrent gagnerait à être transmise à des capteurs « amis » du même réseau. Les techniques de la radio cognitive peuvent être utiles dans ce but. Les réseaux docitifs se situent dans le prolongement naturel de la radio cognitive en explorant les meilleures façons d'échanger les données et aussi de sélectionner celles qui sont utiles et fiables. Dans la dernière partie de cette thèse, nous avons abordé cette question et proposé un mécanisme de docition pour la détection des paramètres de la loi de Pareto modélisant les temps de silence du trafic de réseaux WiFi sous la couverture desquels se trouvent des nœuds de capteurs. Nous illustrons ainsi le concept de docition dynamique au démarrage en vue de l'adaptation dynamique de la taille de paquets envoyés par des capteurs. En effet, il peut arriver que les réseaux de capteurs soient déployés dans un environnement où du trafic WiFi est transmis. Or les points d'accès WiFi, bien qu'ils écoutent le canal avant de transmettre, peuvent ne pas détecter les nœuds de capteurs lorsqu'ils transmettent tout en provoquant chez ces derniers des collisions à cause de la différence de puissance nominale de ces deux types d'émetteurs. Les bornes WiFi ont une puissance de transmission généralement plus élevée que celle des capteurs et un seuil d'écoute moins sensible, ce qui fait que le WiFi « écrase » le trafic des capteurs. Il leur est alors utile de pouvoir profiter des instants de silence observés dans le trafic WiFi pour émettre. La difficulté vient du fait que les capteurs, étant mobiles, peuvent se trouver dans des endroits couverts par peu de points d'accès WiFi et donc de grands silences puis, quelques instants plus tard, dans d'autres très chargés en trafic WiFi. Se pose alors la question de la fraîcheur de l'information, et de l'opportunité de transmettre ou recevoir cette information d'autres nœuds lorsqu'on bouge.

Nous avons montré dans la présentation de l'état de l'art que les travaux sur les réseaux docitifs ont été menés dans le contexte de réseaux cellulaires avec infrastructure, mais que, dans un réseau de capteurs mobiles sans infrastructure concevoir des mécanismes de docition efficaces est beaucoup plus complexe puisque dans un contexte cellulaire, la cohérence des états des nœuds qui enseignent aux nœuds étudiants est assurée car les stations de base sont immobiles et ont le temps d'apprendre les informations sur l'environnement avec certitude tandis qu'en revanche dans le cas d'un réseau de capteurs sans fil, sans infrastructure et mobiles, celle-ci n'est plus certaine et il faut la vérifier. Dans ce nouveau contexte, il est des cas où la docition peut être utile car les nœuds voisins ont une information correcte sur l'état du réseau et dont d'autres nœuds nouvellement arrivés peuvent bénéficier et il en est d'autres pour lesquels les nœuds n'ont pas d'information à jour et, s'ils la communiquent à des étudiants, peuvent être la cause de dégradations de performances majeures.

Ceci amène à la question de savoir, dans le contexte d'un réseau mobile sans infrastructure, quand avoir un comportement docitif et quand s'en abstenir, autrement dit de savoir si le concept de docition lui-même peut être rendu dynamique en fonction du contexte. Dans le concept de docition au démarrage, les radios docitives enseignent leurs politiques à tous les nouveaux arrivants. En d'autres termes, c'est à l'initialisation des nœuds uniquement qu'il y a docition. La méthode de docition dynamique, que nous proposons dans la troisième partie de cette thèse, tente d'évaluer le degré de cohérence des informations des nœuds à la fois dans le temps et dans l'espace. On s'est efforcé de mesurer la qualité des informations possédées par les nœuds d'un voisinage en en observant sa cohérence ainsi que son évolution dans le temps. Notre proposition de docition dynamique ajoute à la docition classique une sonde de

prévisibilité de l'environnement qui jauge la stabilité de l'environnement et détermine pour un étudiant le meilleur enseignant. Dans les réseaux mobiles sans infrastructure, elle permet de choisir entre docition « au démarrage » seulement, c'est-à-dire à l'arrivée d'un nœud dans un nouveau lieu, et aucune docition.

Les simulations ont montré que la docition dynamique s'adapte bien à l'évolution du pourcentage de voisins mobiles dans un réseau, contrairement à la docition classique qui entraîne des dégradations de performances lorsque ce pourcentage augmente. Aussi bien le taux de sélection d'informations correctes que les performances des mécanismes réseaux qui les utilisent ensuite sont améliorées avec la docition dynamique par rapport à la docition classique dans le cas d'un réseau de capteurs mobiles sans infrastructure. L'overhead correspondant est à peu près le même pour la docition dynamique que pour la docition classique. Par rapport à la docition classique, nos simulations ont montré dans certains cas pour la docition dynamique une amélioration de plus de 50% de la sélection correcte de la valeur du paramètre de Pareto par rapport à la docition classique. Une amélioration figure également sur le taux de perte qui présente un gain de plus de 30%. En outre, l'overhead ajouté est estimé et reste moindre qu'une estimation directe du canal en termes de coût énergétique.

À l'issue de ce travail, plusieurs améliorations sont possibles et des perspectives nouvelles se dessinent.

Pour le mécanisme proposé dans la première partie, on pourrait coupler la durée des périodes d'endormissement et de réveil des capteurs au contexte dans lequel ils se trouvent ou à l'activité de l'homme ou encore à l'activité des nœuds voisins. Il est raisonnable de penser que dans l'entrepôt elles peuvent être plus longues que pendant les phases de transport. On pourrait aussi les coupler aux résultats des mesures comme le suggère Frederica Darema dans d'autres contextes (cf. [DAR10]). C'est en effet dans ce genre de systèmes dynamiques conduits par des données qu'un mécanisme d'adaptation au contexte trouve tout son sens.

Nos travaux sur l'identification des empreintes de réseaux concurrents est un travail préliminaire. C'est une preuve de concept. Nous avons effectué des expériences initiales qui doivent être étendues à d'autres technologies et d'autres configurations, comme des points d'accès WiFi plutôt que du WiFi en mode ad hoc, en utilisant OFDM au lieu de l'étalement de spectre DSSS, etc. L'impact de la mobilité des nœuds sur les formes d'erreur est également un sujet intéressant. Dans cette partie, nous n'avons donné qu'un exemple d'implémentation du mécanisme d'adaptation après la détection WiFi pour illustrer l'efficacité et l'utilité de notre mécanisme d'adaptation de lien. Un grand nombre de mécanismes d'adaptation peuvent être conçus et optimisés et pour diverses autres technologies. Des modèles mathématiques de nos résultats pourraient aussi être proposés.

Enfin, la docition est un concept relativement nouveau. Il repose sur une estimation de donnée, choisir, enseignée, filtrée. Parfois celle-ci peut être incomplète mais être complémentaire d'une autre reçue d'autres nœuds. Les techniques de l'estimation distribuée pourraient alors être exploitées avantageusement. Par exemple, l'estimation de corrélation, d'un processus avec lui-même dans le temps ou bien de plusieurs processus correspondants à des mesures de capteurs voisins ou pas pourrait être optimisée et exploitée dans ce contexte. Peut-être pourrait-on aussi indirectement chercher à optimiser une fonction globale, comme l'énergie totale restante du réseau, de manière distribuée, fonction dont les paramètres seraient

justement les paramètres de configuration des nœuds. Ce genre de problème, maximisation globale à partir de décisions locales dans un réseau, est un des problèmes typiques du domaine de l'estimation distribuée. Enfin, le concept de docition peut certainement être exploité avec profit dans les réseaux véhiculaires dont les topologies sont hautement volatiles et où tout gain de temps sur la connaissance du réseau ne peut qu'améliorer les performances.

Chapitre 7. Table des acronymes

ACK	Acknowledgement
AES	Advanced Encryption Standard
ANR	Agence National de Recherche
API	Application Programming Interface
ARQ	Automatic Repeat Request
ASK	Amplitude Shift Keying
BPSK	Binary Phase Shift Keying
BSS	Base Station System
CA	Collision Avoidance
CAM	Context Aware Mechanism
CCA	Clear Channel Assessment
CCK	Complementary Code Keying
COFDM	Coded Orthogonal Frequency Division Multiplexing
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CSMA	Carrier Sense Multiple Access
CTR	CounTeR
CTS	Clear To Send
CW	Congestion Window
DB	Decorrelation Based
DIFS	Distributed Inter-Frame Space
DSSS	Direct Sequence Spread Spectrum
ED	Energy Detection
ESS	Extended Service Set
FEC	Forward Error Correction
FH	Frequency Hop
FHSS	Frequency-Hopping Spread Spectrum
FIM	Fingerprint Identification Mechanism
GFSK	Gaussian Frequency-Shift Keying
GPS	Global Positioning System
ID	Identifier
ISM	Industrial, Scientific and Medical
LAN	Local area Network
LPL	Low Power Listening
MAC	Medium Access Network
MANET	Mobile Ad-hoc NETwork
MSG	MeSsaGe

OFDM	Orthogonal Frequency Division Multiplexing
OS	Operating System
OSI	Open Systems Interconnection
PA_LEVEL	A register in CC2420 ship
PD	Preamble Detection
PDA	Personal Digital Assistant
PDU	Packet Data Unit
PLR	Packets Loss Rate
PPM	Pulse-Position Modulation
PPS	Packet Per Second
PWM	Pulse-Width Modulation
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase Shift Keying
RAM	Random Access Memory
RC	Rivest Cipher
RFID	Radio Frequency IDentification
ROM	Read Only Memory
RSSI	Received Signal Strength Identifier
RTS	Request To Send
SHR	Synchronisation HeadeR
SIFS	Short Inter-Frame Space
SNR	Signal to Noise Ratio
SYNC	SYNChronization
TDD	Time Division Duplex
TDMA	Time Division Multiple Access
TX	Transmission
USB	Universal Serial Bus
WSN	Wireless Sensor Network

Chapitre 8. Liste des publications

- Charbel. Nicolas, Michel. Marot et Monique. Becker, "A Self-Organization Mechanism for a Cold Chain Monitoring System", VTC-Spring 2011. (publié)
- Charbel. Nicolas et Michel. Marot 'Dynamic Link Adaptation Based on Coexistence-Fingerprint Detection for WSN', med-hoc-net 2012. (publié)
- Charbel Nicolas, Michel Marot et Monique Becker, "Dynamic Docition for a Distributed Mobile Wireless Sensor Networks". (soumis)

Chapitre 9. Références

[SB06] S. Mishra, A. Sahai and R.W. Brodersen, "Cooperative Sensing among Cognitive Radios" icc 2006.

[AARA06] A. Ahmed, J. Ali, A. Raza, G. Abbas, "Wired Vs Wireless Deployment Support For Wireless Sensor Networks", TENCON 2006.2006 IEEE Region 10 Conference, pp. 1-3, 2006.

[AFS12] A. Azarfar, J. Frigon, and B. Sanso, "Improving the Reliability of Wireless Networks Using Cognitive Radios", Journal of Communications Surveys & Tutorials, IEEE 2012.

[AK12] R.U.Anitha , P.Kamalakkannan, "A Survey on Energy Efficient Routing Protocols in Wireless Sensor Networks", ICICES-2012-SAEC, Chennai, Tamilnadu.

[ANA07] J. H. Abawajy, S. Nahavandi and F. Al-Neyadi, "Sensor Node Activity Scheduling Approach," in IEEE, 2007 International Conference on Multimedia and Ubiquitous Engineering (MUE'07).

[APDH00] A. Amis, R. Prakash, Thai. P, V. Dung, T. Huynh, "Max-Min D-Cluster Formation in Wireless Ad Hoc Networks", in (2000) IEEE INFOCOM.

[ASL+06] B. Azimi-Sadjadi, D. Sexton, P. Liu, M. Mahony, "Interference Effect on IEEE 802.15.4 Performance ", INSS 2006.

[ATMEL12] Atmel, AVR low power 700/800/900MHz Tranceiver for IEEE 802.15.4-2006, IEEE 802.15.4c-2009, Zigbee, 6LoWPAN, and ISM Applications AT86RF212, (2010). http://www.atmel.com/dyn/resources/prod_documents/doc8168.pdf. Accessed 7 june 2012.

[BBDGKM09] M. Becker, A. Beylot, R. Dhaou, A. Gupta, R. Kacimi, M. Marot, "Experimental Study: Link Quality and Deployment Issues in Wireless Sensor Networks", IFIP Networking 2009.

[BDP07] A.Botta, A.Dainotti, A.Pescapè, "Multi-protocol and multi-platform traffic generation and measurement", INFOCOM 2007.

[BE81] D. J. Baker and A. Ephremides, "The Architectural Organization of a Mobile Radio Network via a Distributed Algorithm", IEEE Transactions on Communications, Vol. 29, No. 11, pp. 1694-1701, 1981.

[BGMS10] M. Becker, A. Gupta, M. Marot, H. Singh, “Improving Clustering Techniques in Wireless sensor Networks Using Thinning Process”, PERFORM'10 Proceedings of the 2010 IFIP.

[BGS07] M. Bertocco, G. Gamba, A. Sona , “ Experimental optimization of cca thresholds in wireless sensor networks in the presence of interference”. Proc. of IEEE EMC Europe 2007 Workshop on Electromagnetic Compatibility. June 14-15, 2007.

[BGS08] M. Bertocco, G. Gamba, A. Sona, “Is CSMA/CA really efficient against interference in a Wireless Control System? An experimental answer” in Proc ETFA 2008, pp. 885–892.

[BHR04] R. Barr, Z. J. Haas, R. van Renesse, “JiST: Embedding Simulation Time into a Virtual Machine.” In Proc. 5th EUROSIM Congress on Modeling and Simulation, Paris, France, September 2004.

[BKM12] N.Baccour, A. Kouba a, L. Mottola, M. Zuniga, H. Youssef, C. Boano, M. Alves, “Radio Link Quality Estimation in Wireless Sensor Networks: a Survey”, In ACM Transactions on Sensor Networks. Volume 8, Issue 4. November 2012.

[BRS05] A. Barroso, U. Roedig, and C. Sreenan, “µ-MAC an energy efficient medium access control for wireless sensor networks”, Proc. of the Second European Workshop on Wireless Sensor Networks, Istanbul, 2005 p70 – 80.

[BTTM11] M. Bykowski, D. Tracey, N. F. Timmons, J. Morrison, "A Schema for the Selection of Network Topology for Wireless Body Area Networks", IEEE Topical Conference on Biomedical Wireless Technologies, Networks, and Sensing Systems, January 2011.

[CC2420] CC2420 datasheet SmartRF CC2420 2.4 GHz IEEE 802.15.4 / ZigBee-ready RF Transceive.

[CCC07] L. Campelli, A. Capone, M. Cesana. “A Receiver Oriented MAC Protocol for Wireless Sensor Networks”, Mobile Ad-hoc and Sensor Systems, Pisa. IEEE International Conference on 8-11 Oct. 2007 p 1–10.

[CCSM12] F. Cadger, K. Curran, J. Santos and S. Moffett “MANET Location Prediction Using Machine Learning Algorithms”, Lecture Notes in Computer Science, 2012.

[CK10] L. CHAARI and L. KAMOUN, "Wireless sensors networks MAC protocols analysis", Journal of telecommunications, volume 2, issue 1, april 2010.

[CLY+12] J. Choi, K. Lee, S. Yun, S. Lee, J. Ko, "An interference-aware 5.8GHz wake-up radio for ETCS", ISSCC 2012 p 446-448.

[CND08] V. Cionca, T. Newe, and V. Dadarlat, “TDMA protocol requirements for wireless sensor networks,” in Proc. 2nd Int. Conf., Sensorcomm. 2008, pp. 30–35.

[COS12] Contiki operating system http://www.contiki-os.org/ July 3, 2012.

[Cross] Crossbow. http://www.xbow.com/ July 3, 2012.

[CYCC09] Yu-Tso Chen, Chi-Lu Yang, Yeim-Kuan Chang and Chih-Ping Chu, "A RSSI-based Algorithm for Indoor Localization Using ZigBee in Wireless

Sensor Network," in Proceedings of the 15th International Conference on Distributed Multimedia Systems (DMS 2009) , San Francisco, USA, Sep. 2009, pp. 70-75.

[CYD06] S. Changsu, K. Young-Bae, S. Dong-Min, “An Energy Efficient Cross-Layer MAC Protocol for Wireless Sensor Networks”, Proc. of the eighth Asia Pacific Web conference, Harbin, 2006 p 410-419.

[D10] C. Diallo, « Techniques d’amélioration du routage et de la formation des clusters multi-sauts dans les réseaux de capteurs sans fil », thèse de doctorat(2010).http://tel.archives-ouvertes.fr/docs/00/59/47/33/PDF/TheseDIALLO.pdf

[D11] R. Dhaou, "Projet CAPTEURS : Une infrastructure pour la surveillance de la chaîne du froid fondée sur un réseau de capteurs mobiles", Journées thématiques Rescom : Réseaux de Capteurs et leurs applications etat de l'art et transfert technologique 19-20 Oct. 2011, Université Pierre et Marie Curie. http://aresa2.imag.fr/colloque/Diapositives/Rescom_2011_part1ANR_Capteur.pdf

[DA10] F. Dressler and O. Akan, “A Survey on Bio-inspired Networking”, Computer Networks Journal 2010.

[DAR10] DoD/AFOSR-NSF, “Dynamic Data-Driven Applications Systems (DDDAS)” - InfoSymbiotic Systems Workshop Arlington, VA, August 30-31, 2010.

[DBN01] B. Deb, S. Bhatnagar, and B. Nath, “A Topology Discovery Algorithm for Sensor Networks with Applications to Network Management” Technical Report Technical Report DCS-TR-441, Department of Computer Science, Rutgers University, May 2001.

[DF09] L. Deliang, P. Fei , “Energy-efficient MAC protocols for Wireless Sensor Networks”, INFORMATION AND COMMUNICATIONS TECHNOLOGIES , Beihang University, Beijing,100083 , Mar 2009.

[DL03] T. Dam, K. Langendoen,” An Adaptive Energy-Efficient MAC Protocol for Wireless Sensor Networks”, SenSys 2003: 171-180.

[DMB07] A. Delye, M. Marot, M. Becker, “Correction, Generalization and Validation of the Max-Min d-cluster formation heuristic”, TC6/LNCS NETWORKING 2007

[DSB+09] S Drago, F Sebastiano, LJ Breems, DMW Leenaerts, KAA Makinwa, B Nauta, “Impulse based scheme for crystal-less ULP radios”, IEEE Trans Circuits Syst (2009) p. 1041–1052.

[DSB12] A. Domenico, E. Strinati, and M. Benedetto, "A Survey on MAC Strategies for Cognitive Radio Networks", Communications Surveys & Tutorials, IEEE Volume: 14 , Issue: 1 2012.

[DSJ07] S. Du, A. K. Saha, D. B. Johnson, “RMAC: A Routing-Enhanced Duty-Cycle MAC Protocol for Wireless Sensor Networks” in INFOCOM 2007.

[DSSF12] Dartmouth SSF (SSF). http://www.crhc.uiuc.edu/ jasonliu/projects/ssf/ July 3, 2012.

[DT12] T. Duong and D. Tran, "An Effective Approach for Mobility Prediction in Wireless Network based on Temporal Weighted Mobility Rule", IJCST Volume 3, Issue 2, February 2012.

[EE12] ERIKA Enterprise http://erika.tuxfamily.org/ July 3, 2012.

[EMS04] L. Girod, J. Elson, A. Cerpa, T. Stathopoulos, N. Ramanathan, D. Estrin, "EmStar: A software Environment for Developing and Deploying Wireless Sensor Networks." In Proc. USENIX 2004, Boston, MA, pp. 283–296, 2004.

[EVMPG05] E. Egea-López, J. Vales-Alonso, A. S. Martínez-Sala, P. Pavón-Mariño, J. García-Haro, "Simulation Tools for Wireless Sensor Networks", SPECTS 2005.

[EWSB09] EasySen WiEye Sensor Board. http://www.easysen.com/WiEye.htm. Last modified: 08/01/09.

[FCAMO08] W. Fu, Y. S. Chang, M. M. Aung, C. Makatsoris, C. H. Oh, "WSN based intelligent cold chain management", The 6th International Conference on Manufacturing research, ICMR'08, Brunel University, UK, 9-11th September, 2008.

[FGM11] S. Feizi-Khankandi, V. K. Goyal, M. Médard, "Time-Stampless Adaptive Nonuniform Sampling for Stochastic Signals", CoRR abs/1110.3774: 2011.

[FZWN08] C. Farah , C. Zhong, M. Worboys, S. Nittel "Detecting Topological Change Using a Wireless Sensor Network" , GIScience, pp. 55–69, 2008

[GG10a] A. Galindo-Serrano and L. Giupponi, "Decentralized QLearning for Aggregated Interference Control in Completely and Partially Observable Cognitive Radio Networks," Proc. IEEE CCNC '10, Las Vegas, NV, Jan. 9–12, 2010.

[GG10b] A. Galindo-Serrano and L. Giupponi, "Distributed QLearning for Aggregated Interference Control in Cognitive Radio Networks," IEEE Trans. Vehic. Tech., vol. 59, no. 4, May 2010, pp. 1823–34.

[GGBD10] L. Giupponi, A. G-Serrano, P. Blasco, M.Dohler, "Docitive Networks – An Emerging Paradigm for Dynamic Spectrum Management", IEEE Wireless Communications, 2010.

[GHF05] S. Guru, S. Halgamuge and S. Fernando "Particle swarm optimizers for cluster formation in wireless sensor networks", IEEE International Conference on sensor, 2005 319–324.

[GMI12] Global Mobile Information Systems Simulation Library (GloMoSim). http://pcl.cs.ucla.edu/projects/glomosim/ July 3, 2012.

[GS04] L. Gu and J.A. Stankovic, "Radio-triggered Wake-up Capability for sensor Networks", Proceedings of the 10th IEEE Real-Time and Embedded Technology and Applications Symposium (2004).

[GS08] R. K. Guha, S. Sarka, "Characterizing Temporal SNR Variation in 802.11 Networks" in IEEE transaction on vehicular technology 2008.

[GSMB10] A. Gupta, M. Sharma, M. Marot, M. Becker, "HybridLQI: Hybrid MultihopLQI for Improving Asymmetric Links in Wireless Sensor Networks", AICT 2010.

[H05] S. Haykin "Cognitive Radio: Brain-Empowered Wireless Communications"in IEEE J. Select. Areas Commun, 2005.

[HAH06] M. Holland, R. Aures, W. Heinzelman, “Experimental investigation of radio performance in wireless sensor networks”, WiMesh 2006.

[HCB00] W.R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, “Energy-efficient communication protocol for wireless microsensor networks,” Proceedings of the 33rd Hawaii International Conference on System Sciences, 2000, 1-10.

[HH00] M. E. Harmon and S. S. Harmon, “Reinforcement Learning: A Tutorial,” 2000.

[HH04] L.F.W. van Hoesel and P.J.M. Havinga, “A Lightweight Medium Access Protocol (LMAC) for Wireless Sensor Networks: Reducing Preamble Transmissions and Transceiver State Switches”, INSS 2004.

[HLL+07] S. Han, Sa. Lee and Su. Lee, Y. Kim, "Coexistence Performance Evaluation of IEEE 802.15.4 under IEEE 802.11B Interference in Fading Channels", PIMRC 2007.

[HLLK07] S. Han, S. Lee, S. Lee, and Y. Kim, “Coexistence performance evaluation of IEEE 802.15.4 under IEEE 802.11B interference in fading channels,” in Proceedings of the IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (IEEE PIMRC '07), Athene, Greece, September 2007.

[HT04] P. Hoen and K. Tuyls, “Analyzing Multi-Agent Reinforcement Learning Using Evolutionary Dynamics,” Proc. 15th Euro. Conf. Machine Learning, 2004.

[HXB+09] H. Huo, Y. Xu, C. Bilen, H. Zhang "Coexistence Issues of 2.4GHz Sensor Networks with other RF devices at Home", Third International Conference on Sensor Technologies and Applications 2009.

[HXZZ10] J.Huang, G.Xing, G. Zhou, R. Zhou, “Beyond Co-existence: Exploiting WiFi white space for zigbee performance assurance”, 18th IEEE International on Network Protocols ICNP, 2010.

[Intelleflex10] Intelleflex (2010), The Intelleflex XC3 Technology™ Platform. An Implementation of the New ISO Class C Standard. http://www.intelleflex.com/downloads/white-papers/Intelleflex-XC3-ISO-C3-White-Paper.pdf. Accessed 7 june 2012.

[J12] J. Torkestani “Mobility prediction in mobile wireless networks”, Journal of Network and Computer Applications 11 April 2012.

[JRO08] R. Jurdak, A.G. Ruzzelli, and G.M.P. O'Hare. "Multi-hop RFID Wake-up Radio: Design, Evaluation and Energy Tradeoffs ICCCN, August, 2008.

[JS06] S.A. Jafar, S. Srinivasa, “Capacity Limits of Cognitive Radio With Distributed and Dynamic Spectral Activity” ICC 2006.

[JSH07] C. Jaejoon, K. Sungho, N. Heungwoo, et al., “An Energy-Efficient Mechanism using CLMAC Protocol for Wireless Sensor Networks”, ICNS 2007, Athens, p 3-3.

[JWM] Jennic Wireless Microcontrollers. http://www.jennic.com/

[KCX+10] H Kim, H Cho, Y Xi, M Kim, S Kwon, J Lim, Y Yang, “CMOS passive wake-up circuit for sensor network applications”, Microw Opt Technol Lett (2010). p 597–600.

[KDB09] R. Kacimi, R. Dhaou, A. Beylot, “Using Energy-Efficient Wireless Sensor Network for Cold Chain Monitoring”, in IEEE CCNC 2009 USA.

[KJT11] V. Kumar, S. Jain and S. Tiwari, "Energy Efficient Clustering Algorithms in Wireless Sensor Networks: A Survey", IJCSI Vol 8 ISSN:1694-0814 journal 2011.

[KL07] P Kolinko, LE Larson, “Passive RF receiver design for wireless sensor networks”, Microwave Symposium, 2007p 567–570.

[KP06] H. Karvonen, C. Pomalaza-Raez, “A Cross Layer Design of Coding and Awake/Sleep Periods in WSNS”, IEEE 17th International Symposium on Personal, Indoor and Mobile Radio Communications, Helsinki, 2006 p1 – 5.

[KV10] P Koskela, M Valta, “Simple wake-up radio prototype”, in ACM HotEMNETS 2010.

[LN07] Y. Liu, L. Ni, “A New MAC Protocol Design for Long-term Applications in Wireless Sensor Networks“, Proc. of Parallel and Distributed Systems, Hsinchu, 5-7 Dec 2007p 1-8.

[LOJ10] Xiaowei Luo,William J.O’Brien and Christine L.Julien, “Comparative evaluation of Received Signal-Strength Index(RSSI) based indoor localization techniques for construction jobsites” International Journal on Information mining and retrieval in design.,Vol.25,2010,pp. 355-363.

[LPL+10] C. Liang, N. Priyantha, J. Liu , A. Terzis "Surviving wi-fi interference in low power ZigBee networks", SenSys 2010.

[LR02] S. Lindsey and C. S. Raghavendra, "PEGASIS: Power Efficient GAthering in Sensor Information Systems," in the Proceedings of the IEEE Aerospace Conference, Big Sky, Montana, March 2002.

[LR10] P Le-Huy, S Roy, “Low-power wake-up radio for wireless sensor networks”, Mob Netw Appl. 15(2), 226–236 (2010).

[M98] J. Mitola, “Cognitive Radio,” Licentiate proposal, KTH, Stockholm,Sweden, December 1998.

[MAR10] Michel Marot, Alexandre Delye, Monique Becker, "On Clustering in Sensor Networks", in "Sustainable Wireless Sensor Networks" edited by Winston Seah and Yen Kheng Tan, Intech, december 2010.

[MAT12] MATLAB – The language of technical computing. http://www.mathworks.com/products/matlab/ July 3, 2012.

[MO12] MantisOS http://mantisos.org/index/tiki-index.php.html July 3, 2012.

[NCT12] NCTUns 2.0 Network Simulator and Emulator. http://nsl.csie.nctu.edu.tw/nctuns.html July 3, 2012.

[NFVCBCCL07] C. Nelson, P. Froes, A. M. Van Dyck, J. Chavarria, E. Boda, A. Coca, G. Crespo, H. Lima, "Monitoring temperatures in the vaccine cold chain in Bolivia", Vaccine, Volume 25, Issue 3, 5 January 2007, Pages 433-437.

[NMB11] C. Nicolas, M. Marot, M. Becker, "A Self-Organization Mechanism for a Cold Chain Monitoring System", VTC-Spring 2011.

[NMSYC07] A. Natarajan, M. Motani, B. de Silva, K.-K. Yap, and K.-C. Chua, “Investigating network architectures for body sensor networks,” , HealthNet, June 2007.

[NRK12] Nano-RK http://www.nanork.org/projects/nanork/wiki July 3, 2012.

[NS212] The Network Simulator, NS–2. http://www.isi.edu/nsnam/ns July 3, 2012.

[NS312] The Network Simulator, NS-3 http://www.nsnam.org/ July 3, 2012.

[NSYM09] A. Natarajan, B. Silva, K. Yap and M. Motani, “To Hop or Not to Hop: Network Architecture for Body Sensor Networks”, IEEE Secon 2009

[OM12] OMNET++ discrete event simulator. http://www.omnetpp.org July 3, 2012.

[P] J. L. Petersen, “Estimating the Parameters of a Pareto Distribution Introducing a Quantile Regression Method”.

[PBM+04] J. Polley, D. Blazakis, J. McGee, D. Rusk, J. S. Baras, M. Karir, “ATEMU: A Fine-grained Sensor Network Simulator.” In Proc. 1st IEEE Int. Conf. Sensor and Adhoc Communication Networks (SECON’04), Santa Clara, CA, October 2004.

[PGR09] NM Pletcher, S Gambini, J Rabaey, “A 52 µW wake-up receiver with -72 dBm sensitivity using an uncertain-IF architecture”, IEEE J Solid-State Circuits (2009). 44(1), 269–280.

[PHC04] J. Polstre, J. Hill, and D. Culler, “Versatile low power media access for wireless sensor networks”, ACM SENSYS 2004.

[PJ04] H. Pham and S. Jha, “An adaptive mobility-aware MAC protocol for sensor Networks (MS-MAC)", The 1st IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS-2004), October 24-27, 2004, Fort Lauderdale, Florida, USA

[PMP+05] P. Levis, S. Madden, J. Polastre, R. Szewczyk, K. Whitehouse, A. Woo, D. Gay, J. Hill, M. Welsh, E. Brewer, and D. Culler, "TinyOS: An Operating System for Wireless Sensor Networks". In book Ambient Intelligence edited by W Weber, J Rabaey, and E Aarts. 2005.

[PPSG09] F.Penna, C.Pastrone, M.A.Spirito, R.Garello, “Measurement-based Analysis of Spectrum Sensing in Adaptive WSNs under Wi-Fi and Bluetooth Interference”, IEEE 69th, VTC Spring 2009.

[PTHCB08] S. Pollin, M. Ergen, M. Timmers, A. Dejonghe, L. V. der Perre, F. Catthoor, I. Moerman, and A. Bahai, “Distributed cognitive coexistence of 802.15.4 with 802.11,” in Proc. of the International Conference on Cognitive Radio Oriented Wireless Networks and Communications, vol. 1, Mar. 2006, pp. 1–5.

[PTO12] Ptolemy II. Heterogeneous model and design. http://ptolemy.eecs.berkeley.edu/ptolemyII July 3, 2012.

[R04] R. Riem-Vis, “Cold chain management using an ultra low power wireless sensor network”, Workshop on Applications of Mobile Embedded Systems. Boston, 2004.

[RJO07] A.G. Ruzzelli, R. Jurdak, and G.M.P. O'Hare. "On the RFID Wake-up Impulse for Multi-hop Sensor Networks," , ACM SenSys 2007.

[RR07] I. Ramachandran, S. Roy, “Clear Channel Assessment In Energy-Constrained Wideband Wireless Networks” IEEE wireless communications June 2007.

[RS12] K. Ramesh and K. Somasundaram, “Improved Fair-Zone technique using Mobility Prediction in WSN”, IJASSN, Vol 2, No.2, April 2012.

[RWAM05] I. Rhee, A. Warrier , M. Aia , J. Min, “Z-MAC: a hybrid MAC for wireless sensor networks”, Proceedings of the 3rd international conference on Embedded networked sensor systems,2005 USA .

[RWAP05] I. Rhee, A.C. Warrier, M. Aia, J. Min, and P. Patel, “Z-MAC: A Hybrid MAC for Wireless Sensor Networks,” Proc. ACM SenSys 2005.

[S04] ML Sichitiu, “Cross-layer scheduling for power efficiency in wireless sensor networks,” in INFOCOM, 2004, pp. 1740–. 1750.

[S11b] E. Sheybani "Dimensionality Reduction and Noise Removal in Wireless Sensor Networks", NTMS 2011.

[SAB04] P. Skraba, H. Aghajan, A. Bahai, “RFID Wake-up in Event Driven Sensor Networks”, SIGCOMM 2004.

[SCH+05] A. Sobeih, W. Chen, J. C. Hou, L. Kung, N. Li, H. Lim, H. Tyan, H. Zhang, “J-Sim: A simulation and emulation environment for wireless sensor networks.” In Proc. Annual Simulation Symposium (ANSS 2005), San Diego, CA, pp. 175–187, April 2005.

[SH07] L. Song, D. Hatzinakos, “A Cross-Layer Architecture of Wireless Sensor Networks for Target Tracking”, IEEE/ACM Transactions on Networking, 2007,15 p145-158.

[SHCWW04] V. Shnayder, M. Hempstead, B. Chen, G. Werner Allen, and M. Welsh, "Simulating the Power Consumption of LargeScale Sensor Network Applications", SenSys’04, Baltimore, Maryland, USA, November 3–5, 2004.

[SHE05] Y. Shih-Hsien, T. Hung-Wei, W. Eric Hsiao-Kuang, et al. “Utilization based duty cycle tuning MAC protocol for wireless sensor networks”, GlobalCom 2005 p 3258-3262.

[SJL+11] W. Shih, R. Jurdak, B. Lee and D. Abbott, "High sensitivity wake-up radio using spreading codes: design, evaluation, and applications", EURASIP journal 2011.

[SKJ05] C. Sungrae,K. Kanuri, C. Jin-Woong, et al. “Dynamic Energy Efficient TDMA-based MAC Protocol for Wireless Sensor Networks” Autonomic and Autonomous Systems and International Conference on Networking and Services, Papeete, Tahiti, ICASICNS 2005, Joint International Conference on 23-28 Oct. 2005 p 48-48.

[SLNL11] M. Soleimanifar, M. Lu, I.Nikolaidis. S. Lee "A robust positioning architecture for construction resources localization using wireless sensor networks", (WSC), Proceedings of the 2011 Winter

[SMPKL11] P.J. Shin, H. Medeiros, J. Park, A. Kak, W. Lafayette, “Predictive duty cycle adaptation for wireless camera networks”, ICDSC 2011

[SSF12] Scalable Simulation Framework (SSF). http://www.ssfnet.org July 3, 2012.

[SSS07] S. Selvakennedya, S. Sinnappan, Yi Shang, "A biologically-inspired clustering protocol for wireless sensor networks" computer communication journal 2007.

[SSS10] S. Singh , M. P. Singh , and D. K. Singh, “Routing Protocols in Wireless Sensor Networks – A Survey”, (IJCSES) Vol.1, No.2, November 2010

[SSW12] Sun SPOT World. http://www.sunspotworld.com/ May 29, 2012.

[STDS03] IEEE Standard for Information Technology-Part 15.4: Wireless Medium Access Control (MAC) and Physical layer (PHY) specifications for Low Rate Wireless Personal Area Networks (LR-WPANS), IEEE 802.15.4-2003, October 2003.

[STDW99] IEEE Std 802.11 2007 (Revision of IEEE Std 802.11-1999).

[SYQ07] L Shan, T Yunjian, Z Qin, “Passive wake-up scheme for wireless sensor networks”, ICICIC 2007,p 507–507.

[T93] M. Tan, “Multi-Agent Reinforcement Learning: Independent vs. Cooperative Agents,” in Readings inAgents, M. N. Huhns and M. P. Singh, Eds., Morgan Kaufmann, 1993, pp. 487–94.

[TOS03] P. Levis, N. Lee, M. Welsg, D. Culler, “TOSSIM: Accurate and Scalable Simulation of Entire TinyOS Applications.” In Proc. 1st ACM Int. Conf. Embedded Networked Sensor Systems (SenSys), pp. 126–137, 2003.

[TS09] G.M.Tamilselvan and Dr.A.Shanmugam, "Probability Analysis of channel collision between IEEE 802.15.4 and IEEE 802.11b using Qualnet Simulation for various Topologies", International Journal of Computer Theory and Engineering, Vol. 1, No. 1, April 2009 1793-8201.

[TSM07] Tmote Sky Datasheet http://www.snm.ethz.ch/Projects/TmoteSky . In “the Sensor Network Museum”, last modified 2/07/2007.

[UV08] J. Unnikrishnan and V.V. Veeravalli, “Cooperative Sensing for Primary Detection in Cognitive Radio” IEEE Journal of Selected Topics in Signal Processing, Vol. 2, No. 1, pp. 18-27, February 2008.

[VA12] R. Viswanathan and B. Ahsant, "A Review of Sensing and Distributed Detection Algorithms for Cognitive Radio Systems", International Journal on Smart Sensing and Intelligent Systems, VOL. 5, NO. 1, MARCH 2012.

[VBI11] G. Vijay, E. Ben-Ali-Bdira and M. Ibnkahla, "Cognition in Wireless Sensor Networks: A Perspective", IEEE SENSORS JOURNAL, VOL. 11, NO. 3, MARCH 2011.

[VOCA09] L. Villalba, A. Orozco, A. Cabrera and C. Abbas, “Routing Protocols in Wireless Sensor Networks”, Sensors 2009, vol. 9, pp. 8399-8421.

[VX06] N. Vlajic and D. Xia, "Wireless Sensor Networks: To Cluster or Not To Cluster?", WoWMoM 2006.

[WR11] B. Wang and K. J. Ray-Liu, "Advances in cognitive radio networks: A survey" Selected Topics in Signal Processing, IEEE Journal Volume: 5 , Issue: 1 , Publication Year: 2011 , Page(s): 5 – 23.

[XL06] Y. Xu, W-C.Lee “Exploring special correlation for link quality estimation in wireless sensor networks”, IEEE PerCom 2006.

[YHE02] W. Ye, J. Heidemann, and D. Estrin, “An Energy-Efficient MAC Protocol for Wireless sensor Networks,” in Proc. IEEE. INFOCOM, Jun. 2002

[YLN10] W.Yaun, J.P.M.G.Linnartz, I.G.M.M.Niemegeers ,”adaptive CCA for IEEE 802.15.4 wireless sensor networks to mitigate interference”. WCNC 2010.

[YLSL08] X Yu, J-S Lee, C Shu, S-G Lee, “A 53 µW super-regenerative receiver for 2.4 GHz wake-up application”, APMC 2008 , pp. 1–4.

[YXG11] Dong Yang, Youzhi Xu, and Mikael Gidlund, “Wireless Coexistence between IEEE 802.11- and IEEE 802.15.4-Based Networks: A Survey,” International Journal of Distributed Sensor Networks, vol. 2011, Article ID 912152, 17 pages, 2011. doi:10.1155/2011/912152.

[ZGSZ11] M.H. Zayani, V. Gauthier, I. Slama, D. Zeghlache, “Tensor-Based Link Prediction in Intermittently Connected Wireless Networks”, CoRR abs/1108.2606: (2011).

[ZXX10] R.Zhou, Y.Xiong, G.Xing, “Zifi : wireless lan discovery via zigbee interference signatures”, In MobiCom 2010: Proceedings of the 16th annual international conference.