Réseaux de capteurs sans fil linéaires : impact de la connectivité et des interférences sur une méthode d'accès basée sur des jetons circulants

El Hadji Malick Ndoye

▶ **To cite this version:**

El Hadji Malick Ndoye. Réseaux de capteurs sans fil linéaires : impact de la connectivité et des interférences sur une méthode d'accès basée sur des jetons circulants. Autre. Université Blaise Pascal - Clermont-Ferrand II; Université Cheikh Anta Diop (Dakar), 2015. Français. NNT : 2015CLF22661 . tel-01330769

HAL Id: tel-01330769
https://theses.hal.science/tel-01330769

Submitted on 13 Jun 2016

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

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

N° d'ordre : D.U. 2661
EDSPIC : 737

THÈSE EN COTUTELLE
UNIVERSITÉ BLAISE PASCAL
UNIVERSITÉ CHEIKH ANTA DIOP

ÉCOLE DOCTORALE SCIENCES POUR L'INGÉNIEUR
DE CLERMONT-FERRAND

Laboratoire d'informatique, de modélisation et
d'optimisation des systèmes

THÈSE
présentée par
EL Hadji Malick NDOYE
pour obtenir le grade de

DOCTEUR D'UNIVERSITÉ
Discipline : Informatique

Réseaux de capteurs sans fil linéaires

Impact de la connectivité et des interférences sur une méthode d'accès basée sur des jetons circulants

Soutenue publiquement le 21 Décembre 2015 en France devant le jury

Directeur :	M. Michel MISSON	Professeur à l'Université de Clermont
Encadrants :	Mme Frédérique JACQUET	Maitre de conférences à l'Université de Clermont
	M. Ibrahima NIANG	Maitre de conférences et HDR à l'Université Cheikh Anta Diop de Dakar
Rapporteurs :	M. Laurent GEORGE	Professeur à l'université de Paris Est
	M. Nadjib ACHIR	Maitre de Conférence et HDR à l'université de Paris XIII
Examinateur :	M. Olivier FLAUZAC	Professeur des Universités à l'université de Reims

Résumé

Dans cette thèse, il s'agit de proposer un protocole MAC qui prend en compte certaines spécificités des réseaux de capteurs sans fil linéaires. Ce protocole MAC est basé sur des jetons circulants qui donnent aux nœuds le droit d'accès au canal de transmission. Nous évaluons à partir de ce protocole l'impact des interférences et de la connectivité sur un réseau linéaire. Cette évaluation nous permet de proposer des techniques de clustering dans un réseau de capteurs sans fil linéaire. Nous supposons d'abord un clustering basé sur une exploitation logique du voisinage des nœuds capteurs. Nous considérons dans ce cas, un modèle de propagation déterministe qui ne tient pas en compte la complexité du milieu. Ensuite, nous considérons une technique de clustering dans laquelle le modèle de propagation prend en compte les fluctuations qui rendent le milieu complexe.

Mots clés : Réseau de capteurs sans fil linéaire, jeton, navette, cluster, QoS, protocole MAC.

Abstract

In this thesis, we propose a MAC protocol that takes into account the specific characteristics of LSNs. This MAC protocol is based on tokens circulating that give the right to nodes to access to the transmission channel. We evaluate from this protocol the impact of interference and connectivity in the LSN. This evaluation allows us to propose clustering techniques in a LSN. We assume first a clustering based on a logical exploitation of the vicinity of the sensor nodes. In this case, we assume that a deterministic propagation model that does not take into account the complexity of the environment. Next, we consider a clustering technique wherein the propagation model takes into account the fluctuations that make complex the medium.

Keywords: Linear Sensor Network, token, shuttle, cluster, QoS, MAC protocol.

À ma famille…

Remerciements

« La réussite appartient à tout le monde.
C'est au travail d'équipe qu'en revient le mérite.»

Franck Piccard.

À l'issue de ces travaux de recherche, je suis convaincue que la thèse est loin d'être un travail solitaire. En effet, je n'aurai jamais fait tout ce travail sans l'aide incessante de personnes qui m'ont toujours tiré vers le haut. Je tiens à remercier très sincèrement toutes ces personnes de leur gratitude et de leur disponibilité durant tous ces moments de stress et de pression.

Tout d'abord mes remerciements les plus sincères à Monsieur Michel MISSON pour la confiance qu'il m'a accordée en acceptant d'encadrer ce travail. Il a été toujours très disponible tout au long de la thèse avec son sens de l'écoute, ses conseils et son investissement sans faille. Monsieur MISSON est pour moi une source de motivation et d'inspiration.

Mes remerciements vont aussi à l'endroit de Mme Frédérique JACQUET, mon encadrante pour sa disponibilité et son implication incessante dans le bon déroulement de cette thèse. Elle a toujours été présente pour apporter son soutien et ses idées durant toutes ces années de thèse.

Je tiens à remercier Monsieur Ibrahima NIANG, mon encadrant au Sénégal qui a toujours eu confiance en moi. Il a toujours été présent depuis le DEA et m'a initié à la recherche. Il n'a jamais cessé de me soutenir et de m'accompagner durant toute la thèse.

Je remercie Monsieur Laurent GEORGE Professeur à l'université de Paris Est et Monsieur Nadjib ACHIR Maitre de Conférence et HDR à l'université de Paris XIII qui ont accepté de juger mon travail et d'en être les rapporteurs, ainsi que pour lecture très constructive de mon manuscrit. Je remercie Monsieur Olivier FLAUZAC Professeur des Universités à l'université de Reims d'avoir accepté de participer à ce jury de thèse. Je suis très reconnaissant de sa disponibilité.

J'adresse mes remerciements à toute l'équipe Réseaux et Protocoles. C'est grâce vous que je me suis toujours senti bien à l'aise et épanoui ici. Je veux citer en particulier Gérard, Alexandre, François, Nancy pour leur aide et leur soutien sans faille. Mes remerciements vont aussi aux autres membres de l'équipe (Thérèse, Honoré, Déthié, Antonio, Joél, Xavier, Hamadoun, Marie Françoise, Pascal, Rana, etc.) pour cette ambiance cordiale et conviviale qu'ils ont développée avec moi durant cette thèse.

Mes remerciements vont à l'endroit de Nadir Hakem. Vos suggestions et conseils m'ont aidé dans l'avancement de la thèse.

J'adresse mes remerciements au gouvernement du Sénégal d'avoir financé cette thèse par le biais du S.G.E.E (Service de Gestion des Etudiants sénégalais à l'Etranger).

Mes remerciements vont aussi à la coopération franco-sénégalaise qui a aussi financé une partie de la thèse.

Mes remerciements à l'équipe du Dimanche ***« Hell Foot »***. J'ai passé des moments de détente et de loisir avec vous les gars. C'était vraiment formidable de décompresser avec vous.

Finalement, mes remerciements à ma famille. D'abord à mes parents Ousseynou NDOYE et Fatou LY qui n'ont ménagé aucun effort pour ma réussite depuis le début de mes études. Je remercie Awa NDOYE qui m'a aidé, soutenu et réconforté depuis toujours. Comme on dit en Wolof « Amouma sa fay ». Mes remerciements à Marème NDOYE pour toute la peine qu'elle s'est donnée à s'occuper de mes démarches administratives au Sénégal lorsque je suis en France et pour son soutien permanent. À Ndoumbé NDOYE pour son aide, son soutien et sa disponibilité pour traiter mes multiples demandes. C'est vraiment gentil de ta part. Je remercie Ndongo NDOYE et sa femme Fatou NDOYE ainsi que toute la famille pour tout qu'ils ont fait pour moi. C'est vraiment sympa et je n'oublierai jamais. Je tiens à remercier aussi Fally Ndiaye pour son soutien sans faille et ses encouragements. Mes remerciements aux autres frères et sœurs et (Diaga, Maimouna, Absa, Aita, Bougouma, etc.)

Tables des matières

Introduction générale 13

État de l'art sur les réseaux de capteurs sans fil linéaires 17

1. Introduction 18

2. Définition 18

3. Applications des réseaux de capteurs sans fil linéaires 20

3.1. Surveillance de pipelines 20

3.2. Surveillance de lignes électriques 22

3.3. Surveillance de rails 22

3.4. Surveillance d'activités routières 23

3.5. Surveillance de frontières 23

4. Problématique des réseaux de capteurs sans fil linéaires 24

5. Topologie physique des réseaux de capteurs sans fil linéaires 25

5.1. Les réseaux linéaires à une dimension 25

5.2. Les réseaux linéaires multi-dimensionnels 26

6. État de l'art des protocoles MAC pour réseaux de capteurs sans fil linéaires 27

6.1. Le protocole MAC 802.15.4 29

6.2. Les protocoles basés sur la synchronisation temporelle 36

6.3. Les protocoles basés sur la contention 41

6.4. Les protocoles hybrides 49

7. Les protocoles de routage pour réseaux de capteurs linéaires 50

7.1. Le protocole MERR (*Minimum Energy Relay Routing*) 50

7.2. Les protocoles de routage hiérarchiques 51

8. Conclusion 54

Contribution relative aux méthodes d'accès 55

1. Introduction 56

2. Intégration du mécanisme RTS/CTS dans 802.15.4 non slotté 56

2.1. Hypothèses 57

2.2. Le problème du terminal caché 58

2.3. Le mécanisme RTS/CTS 60

2.4. Intégration du mécanisme RTS/CTS dans le CSMA/CA non slotté de 82.15.4 63

2.5. Analyse du comportement des files d'attente des nœuds par un modèle de registres à décalage 68

2.6. Simulations et résultats 70

3. LTB-MAC (Linear Token-Based MAC Protocol): Protocole MAC basé sur un jeton 76

3.1. Hypothèses 76

3.2. Spécifications 78

3.3. L'effet d'écrêtage du trafic 83

3.4. Simulations et résultats 85

4. Conclusion 90

Clustering basé sur une exploitation logique du voisinage des nœuds 92

1. Introduction 93

2. Hypothèses 95

3. Prise en compte d'un facteur de redondance 96

3.1. Définition de la redondance 96

3.2. Quelques exemples de réseaux R-redondant 97

3.3. Impact de la redondance sur la distance au puits 99

4. Estimation de la distance entre jetons 101

4.1. Cas du réseau *1*-redondant 102

4.2. Cas du réseau 2-redondant 103

4.3. Cas du réseau 3-Redondant 104
4.4. Généralisation 105
5. Impact de la distance entre les possesseurs de jeton sur le débit au puits 107
6. Définition d'un cluster logique 110
7. Simulations et résultats 112
7.1. Paramètres de simulation 113
7.2. Résultats 113
8. Conclusion 120
Clustering avec prise en compte de la complexité du milieu 121
1. Introduction 122
2. Modélisation des conditions de propagation 123
3. Modélisation des conditions de réception 124
3.1. *Outage probability* 125
3.2. Calcul de la puissance d'émission 128
3.3. Introduction des modèles de capture 130
4. Méthodes et démarches 134
5. Analyse de l'impact de la distance entre deux nœuds possesseurs jetons 138
5.1. En capture binaire 138
5.2. Cas d'une capture probabiliste 142
6. Calcul de la probabilité de réception en tenant compte des caractéristiques temporelles de l'échange de trames 145
7. Formalisation du compromis permettant la définition d'un cluster physique 151
7.1. Estimation de l'influence de la redondance sur l'impact des interférences 151
7.2. Critères de choix de la taille d'un cluster d'un LSN 155
7.3. Synthèse 159
8. Conclusion 160

Conclusion et Perspectives 162

Liste des publications 166

Annexe A : Présentation de NS2 167

Annexe B : Quelques fonctions importantes de LTB-MAC 170

Glossaire 175

Liste des abréviations 177

Bibliographie 179

Liste des figures

Figure 1. 1 - Un exemple de réseau de capteur sans fil linéaire. 19
Figure 1. 2 - Réseau linéaire à un niveau. 26
Figure 1. 3 - Réseau linéaire multi-dimensionnel à 3 niveaux. 27
Figure 1. 4 - Topologies de réseau proposées par IEEE 802.15.4. 29
Figure 1. 5 - Structure de la supertrame 802.15.4. 31
Figure 1. 6 - Mécanisme CSMA/CA slotté. 33
Figure 1. 7 - Mécanisme CSMA/CA non slotté. 35
Figure 1. 8 - Transmission des trames données dans LC-MAC. 38
Figure 1. 9 – Découpage temporel et acheminement des données dans WiWi. 40
Figure 1. 10 - Activité du nœud X. 41
Figure 1. 11 - Les différentes étapes du processus de transmission dans MFT-MAC. 43
Figure 1. 12 – Négociation pour l'accès au canal entre deux nœuds adjacents. 45
Figure 1. 13 - Découpage d'un réseau linéaire en niveaux. 46
Figure 1. 14 - Processus de communication dans EEDA-MAC. 49
Figure 1. 15 - Illustration de l'adressage hiérarchique. 52

Figure 2. 1 - Problème de stations cachées. 59
Figure 2. 2 - problème du terminal exposé. 59
Figure 2. 3 - Le mécanisme de RTS/CTS. 61
Figure 2. 4 – Exemple d'échec. 62
Figure 2. 5 - Algorithme d'envoi. 65
Figure 2. 6 - Algorithme de réception. 67
Figure 2. 7 - Représentation du modèle de registre à décalage avec fuite. 69
Figure 2. 8 - Les différentes phases de l'évolution de l'activité du nœud. 71
Figure 2. 9 - Comparaison entre le nombre de paquets droppés en mode CSMA/CA avec ou sans RTS/CTS. 73
Figure 2. 10 - Évolution des FIFO dans le temps. 74
Figure 2. 11 - Taux de délivrance pour nœud 1. 75
Figure 2. 12 - Taux de délivrance pour le nœud 5 75

Figure 2. 13 – Présentation des différents types de nœuds nécessaires à un protocole LTB-MAC basé sur le jeton. 77
Figure 2. 14 – Les différents états d'un nœud dans LTB-MAC. 79
Figure 2. 15 - Automate d'un nœud courant. 80
Figure 2. 16 - Token passing appliqué à un réseau sans fil linéaire. 81
Figure 2. 17 - Processus de passage de la navette. 82
Figure 2. 18 - Comportement du contenu des files d'attente. 84
Figure 2. 19 - Critères de comparaison entre LTB-MAC et CSMA/CA. 86
Figure 2. 20 - Comparaison du débit au puits. 88
Figure 2. 21 - Taux de délivrance au puits pour les nœuds 1. 89
Figure 2. 22 - Taux délivrance au puits pour le nœud 5. 89
Figure 2. 23 - Délai de bout-en-bout du nœud 1. 90
Figure 2. 24 - Délai de bout-en-bout du nœud 5. 90

Figure 3. 1 - Connectivité du nœud courant Ni dans un réseau R-redondant. 97
Figure 3. 2 - Formation des branches logiques dans un réseau 2-redondant 99
Figure 3. 3 - Formation des branches logiques dans un réseau 3-redondant 100
Figure 3. 4 – Exemple de zones d'activités dans un réseau linéaire 1-redondant. 102
Figure 3. 5 - Distance entre deux possesseurs d'un jeton dans un réseau 1-redondant 103
Figure 3. 6 - Distance entre possesseurs de jetons dans un réseau 2-redondant 104
Figure 3. 7 - Distance entre jetons dans un réseau 3-redondant 105
Figure 3. 8 - Distance entre deux nœuds possesseurs d'un jeton dans un réseau R-redondant 107
Figure 3. 9 - Courbe représentant l'impact de la redondance sur le débit 109
Figure 3. 10 - Identification des interférences 111
Figure 3. 11 – Représentation du cluster linéaire. 111
Figure 3. 12 - Processus de déplacement du cluster 112
Figure 3. 15 - Débit au puits pour un réseau 3-redondant pour plusieurs navettes 115
Figure 3. 13 - Débit au puits pour un réseau 1-redondant pour plusieurs navettes 115
Figure 3. 14 - Débit au puits pour un réseau 2-redondant pour plusieurs navettes 115
Figure 3. 16 - Taux de délivrance au puits dans un réseau 2-redondant 117
Figure 3. 17 - Taux de délivrance au puits dans un réseau 3-redondant 117

Figure 3. 18 - Taux de délivrance au puits dans un réseau 1-redondant 117
Figure 3. 19 - Délai de bout-en-bout dans un réseau 3-redondant 119
Figure 3. 20 - Délai de bout-en-bout dans réseau 1-redondant 119
Figure 3. 21 - Délai de bout-en-bout dans un réseau 2-redondant 119

Figure 4. 1 - Activités de deux nœuds possesseurs de jetons..... 125
Figure 4. 2 - Distribution de la puissance reçue au récepteur à une distance donnée par le modèle Log Normal Shadowing 126
Figure 4. 3 - Représentation de l'outage probability 127
Figure 4. 4 - Représentation de la capture binaire..... 132
Figure 4. 5 - Représentation de la capture probabiliste..... 133
Figure 4. 6 - Conditions de réception de B quand A et E sont possesseurs d'un jeton..... 135
Figure 4. 7 - Distribution de la puissance reçue en B de A..... 136
Figure 4. 8 - Probabilité de réception en fonction de la distance de l'interférent..... 141
Figure 4. 9 - Impact sur la capture d'une activité à 2 sauts et à 3 sauts 142
Figure 4. 10 - Intervalle de capture probabiliste 143
Figure 4. 11 - Pourcentage des paquets capturées..... 145
Figure 4. 12 - Chronogramme des échanges entre les nœuds 146
Figure 4. 13 - Probabilité de réception en capture probabiliste 149
Figure 4. 14 - Cumul des probabilités..... 150
Figure 4. 15 - Représentation d'un nœud et son interférent 152
Figure 4. 16 - Probabilité de capture pour un réseau R-redondant 154
Figure 4. 17 - Représentation de h en fonction du seuil de réception..... 155

Introduction générale

Depuis quelques années, les réseaux de capteurs se présentent comme une solution au besoin d'observer, d'analyser et de contrôler des phénomènes physiques sur des zones éventuellement étendues et hostiles d'accès. Ils sont utilisés dans une multitude de domaines tels que le domaine militaire (surveillance et sécurité des champs de guerre), environnemental (surveillance de zones sismiques, zones volcaniques, etc. Il peut s'agir par exemple d'un réseau ad hoc comportant un grand nombre de nœuds composés de micro-capteurs capables de récolter et de transmettre des données environnementales d'une manière autonome. La position des nœuds n'est pas obligatoirement prédéterminée et ils peuvent être aléatoirement dispersés dans une zone géographique, appelée « champ de captage », correspondant au point d'intérêt pour le phénomène capté. Ainsi, ils sont essentiels pour de nombreuses applications environnementales et scientifiques et sont de plus en plus utilisés dans l'industrie grâce notamment aux derniers développements réalisés dans le domaine des technologies sans fils. Cette nouvelle manière de surveiller, en détectant des variations de grandeurs physiques à différents points disséminés sur un système ou un site, fait émerger de nouvelles problématiques technologiques, par exemple sur l'autonomie énergétique des capteurs, et de nouveaux types d'applications nous permettant de mieux connaitre notre environnement et d'anticiper les problèmes de sécurité, de pollution, de risques naturels, de défaillances, de maintenance, ou plus généralement de tout phénomène non désiré qui pourrait être anticipé.

Dans certains cas, les infrastructures surveillées font que le déploiement des nœuds capteurs doit être fait de façon linéaire sur une ou plusieurs lignes. On trouve ce type de déploiement dans des applications de surveillance de pipeline par exemple. Les réseaux de capteurs dans ce cas, sont utilisés pour détecter des produits toxiques contenus dans ces pipelines (gaz, produits chimiques, éléments radioactifs, pétrole, etc.) ou des fuites. Une autre application des réseaux de capteurs à topologie linéaire est la surveillance des mines ou des cours d'eau. Dans ce cas, les nœuds capteurs se chargent en particulier de surveiller les changements de température du milieu pour détecter des anomalies dans une mine ou les effets d'éventuelles pollutions. On retrouve aussi de tels types de réseaux de capteurs dans la surveillance des trains, des rails, pour détecter un dysfonctionnement des composants matériels comme les wagons, la qualité des rails, etc. Enfin, ces réseaux sans fil à topologie

linéaire sont utilisés dans des applications de surveillance de ponts ou de routes. Ce type de réseau est appelé réseau de capteurs sans fil linéaire (WLSN pour *Wireless Linear Sensor Network*).

Les réseaux de capteurs linéaires sont caractérisés par un voisinage et des possibilités de routage limités. En effet, dans un réseau linéaire, chaque nœud a peu de nœuds à sa portée que nous désignons par voisins de gauche ou voisins de droite. Le nombre de voisins est défini par la portée du lien radio du capteur et de la distance entre deux nœuds adjacents. Ces caractéristiques spécifiques des réseaux de capteurs linéaires peuvent avoir des effets néfastes sur l'acheminent des données au puits, les délais de bout-en-bout ou encore la durée de vie du réseau si le mécanisme d'accès ne les prend pas en compte. Par exemple, dans le cas d'un réseau linéaire où un nœud a exactement deux voisins (un à gauche et un autre à droite), un défaut sur un lien radio ou d'un nœud peut remettre en cause le fonctionnement du réseau par des pertes de paquets et une consommation énergétique considérables.

Les réseaux de capteurs sans fil linéaires sont utilisés pour des applications basées sur l'agrégation de données vers un ou plusieurs puits localisés dans le réseau. Dans ce type de réseau, le routage de proche en proche est un moyen efficace d'acheminer les données au puits. Cependant, cette technique entraine une concentration progressive de données au niveau des nœuds qui peut entrainer un débordement des files d'attente quand on s'approche du puits. En effet, chaque nœud capteur en plus de sa production locale doit aussi router les données provenant de ses voisins qui sont en amont du puits dans ce réseau. Ces zones d'accumulation appelées aussi zones de congestion peuvent dégrader les performances si elles ne pas bien gérées par la méthode d'accès.

Les protocoles MAC basés sur la contention ou sur une synchronisation stricte ne sont pas adaptés aux réseaux linéaires du fait qu'ils ne prennent pas en compte les caractéristiques spécifiques de la topologie linéaire. Il est important que le protocole MAC implémente des mécanismes d'accès adaptés à ce type de réseau qui prennent en compte le voisinage des nœuds capteurs, la linéarité et une gestion efficace de l'énergie ; ceci dans le but d'augmenter la durée de vie du réseau mais surtout d'améliorer ses performances.

Dans cette thèse, il s'agit de proposer un protocole MAC qui prend en compte certaines spécificités des réseaux de capteurs linéaires. Nous basons notre protocole sur la génération d'un jeton circulant de proche en proche et qui donne à un nœud visité le droit d'accès au canal

de transmission. Le jeton contient des informations temporelles nécessaires au bon fonctionnement du réseau. Il est créé par le nœud se trouvant à l'autre extrémité opposée du puits que nous appelons *Token Allocator* ou générateur de jeton. Il est propagé de proche en proche jusqu'au puits. Cette façon de manager l'accès au canal de transmission de proche en proche peut être comparée à un passage d'une navette dans laquelle chacun dépose les données collectées. Ainsi, le départ de la navette est décidé par le *Token Allocator*. L'avantage de cette méthode d'accès est d'une part d'éviter les accès concurrentiels au canal de transmission et d'autre part de résoudre le problème du terminal caché. L'agrégation de proche en proche et la possibilité de faire circuler plusieurs jetons en même temps permettent d'entrelacer les activités des nœuds et d'offrir des performances intéressantes en termes de délais et de latence.

La circulation de plusieurs jetons en même temps dans une topologie linéaire impose une distance minimale entre deux jetons afin de protéger les activités des nœuds possesseurs de jetons. Ceci revient à définir un motif d'isolement autour des nœuds récepteurs pour éviter que la réception des paquets soit exposée aux interférences radios. Dans cette thèse ce motif d'isolement sera appelé cluster linéaire. La taille d'un cluster linéaire dépend principalement de la portée des nœuds et des conditions de propagation.

Cette thèse est organisée comme suit.

Le chapitre I fait un état de l'art sur les réseaux de capteurs sans fil linéaires. Dans ce chapitre, nous détaillons différentes applications des réseaux linéaires. En fonction des applications et des besoins, il existe plusieurs types de réseaux de capteurs qui se distinguent par leur déploiement et le voisinage de leurs nœuds. Ainsi, les méthodes d'accès ou de routage utilisées peuvent différer d'un réseau à un autre suivant les exigences requises. Dans ce chapitre, nous passons en revue les différents protocoles MAC et de routage de réseaux de capteurs sans fil linéaires en expliquant leur fonctionnement.

Le chapitre II présente deux contributions relatives aux protocoles MAC pour les réseaux de capteurs sans fil linéaires: une proposition basée sur la contention et une proposition basée sur la synchronisation. La première contribution est une intégration du mécanisme RTC/CTS dans une version non slottée du CSMA/CA de 802.15.4. Un problème spécifique aux réseaux sans fil est celui du "nœud caché". Pour apporter une réponse à cette problématique, le standard 802.11 définit sur la couche MAC un mécanisme optionnel de type RTS/CTS

(*Request to Send / Clear to Send*). Dans ce chapitre, il s'agit d'étudier l'impact du mécanisme RTS/CTS sur les performances d'un réseau linéaire de capteurs sans fil linéaire basé sur un mécanisme de CSMA/CA non slotté de 802.15.4.

La deuxième contribution de ce chapitre II est relative à un protocole MAC basé sur la génération d'un jeton. Nous présentons les principes de fonctionnement de la méthode d'accès en expliquant le rôle des informations temporelles liées au jeton. Nous expliquons le processus de propagation du jeton de nœud en nœud et définissons par la suite la notion de navette qui permet aux nœuds d'envoyer leurs données de manière synchronisée.

Dans le chapitre III, nous proposons une méthode de découpage d'un réseau linéaire en plusieurs clusters. Nous supposons des conditions de propagation déterministes basées sur le modèle *Tworayground*. Dans ce modèle, les portées radios sont supposées stables et constantes. Par conséquent, la complexité du milieu considéré n'est pas prise en compte. Nous verrons que dans ce type de *clustering*, la taille d'un cluster donné dépend uniquement du facteur de redondance ***R*** défini à partir du voisinage des nœuds.

Dans le chapitre IV, nous proposons une nouvelle technique de *clustering* qui prend en compte la complexité du milieu. On considère un modèle de propagation de type *Log Normal Shadowing*. Dans ce cas, les interférences engendrées par les activités des nœuds deviennent aléatoires et la manière statique de déduire la taille du cluster en se basant sur la connaissance du voisinage des nœuds devient obsolète. La taille du cluster dépend du facteur de redondance ***R*** mais aussi des paramètres du modèle de propagation censés représenter les conditions réalistes de propagation. Il s'agit alors de proposer une analyse qui nous permet d'optimiser le nombre de paquets capturés par un nœud malgré les interférences créés par les voisins possesseurs d'un jeton ceci en utilisant deux modèles de capture (binaire et probabiliste).

La conclusion de cette thèse sera accompagnée des perspectives sur nos travaux futurs.

État de l’art sur les réseaux de capteurs sans fil linéaires

1. Introduction

Ce chapitre introduit les réseaux de capteurs sans fil linéaires. Il fait une présentation de l'état de l'art des travaux existants dans ce domaine. Ces travaux sont principalement basés sur la recherche de solutions de déploiement des nœuds selon une ou plusieurs lignes et de routage ou d'accès au canal en se basant sur les caractéristiques spécifiques liés à la linéarité du réseau. Les solutions proposées dans la littérature visent essentiellement à faciliter l'acheminement des données, à réduire les délais de bout-en-bout, et/ou à économiser l'énergie des nœuds capteurs. Leur mise en place dépend des besoins des applications qui sont nombreuses et variées. On peut citer entre autres applications la surveillance de pipelines, de trains ou encore de mines. Les méthodes d'accès utilisées dans les réseaux linéaires sont principalement basées sur la contention et sur la synchronisation stricte.

Dans ce chapitre, nous proposons une définition et une présentation détaillées des différentes applications des réseaux de capteurs sans fil linéaires. Ensuite, nous présentons les protocoles MAC utilisés dans ces réseaux. Nous faisons une revue des protocoles MAC basés sur la contention ou la synchronisation stricte. Il s'agit ici d'expliquer leur fonctionnement et la manière dont ils sont implémentés dans de tels réseaux. Enfin, nous terminons ce chapitre par une présentation des protocoles de routage utilisés dans les réseaux de capteurs sans fil linéaires.

2. Définition

Les avancées opérées dans les domaines des technologies sans fil et de l'électronique ont permis de développer des capteurs qui sont des minuscules composants électroniques à faible coût et consommant peu d'énergie (solution *low cost* et *low power*). Le mot capteur (ou nœud capteur) désigne ici une entité ayant principalement trois fonctions :

- capter des données (de type son, vibration, lumière, température, pression,...) ;
- calculer des informations à l'aide de ces valeurs collectées ;
- communiquer à travers un réseau de capteurs qui dans cette étude sera sans fil.

Les capteurs sont donc capables de mesurer des grandeurs physiques, chimiques ou biologiques, de traiter ces informations et de les stocker. Ils sont le plus souvent alimentés électriquement via une batterie individuelle dont la durée de vie est limitée. Un réseau de capteurs est composé d'un nombre important de nœuds capteurs qui sont déployés aléatoirement ou de façon planifiée sur un site bien défini appelé champ de captage. Le rôle du réseau de capteurs est de surveiller les changements dans l'environnement là où les capteurs sont déployés. Chaque capteur peut collecter des données et les transférer à un point de collecte appelé puits ou *sink* par l'intermédiaire d'une architecture multi-sauts. Les réseaux de capteurs ont plusieurs domaines d'application. On peut citer le domaine écologique (Musaloiu-e et al., 2006) (Porter et al., 2005) (Mainwaring et al., 2002) pour la surveillance des polluants, le domaine médical (Baldus et al., 2004) (Malan et al., 2004) (Virone et al., 2006) pour la surveillance des patients et pour la collecte d'informations physiologiques, le domaine militaire (Simon et al., 2004) (Lee et al., 2009) pour la surveillance des troupes, ou encore le domaine industriel (Agha et al., 2009) pour la surveillance de chaînes de production.

Dans certaines applications, le déploiement des nœuds capteurs se fait de façon linéaire sur une ou plusieurs lignes, comme montré dans la figure 1.1. Dans ce cas, on parle de ***réseaux de capteurs sans fil linéaires***.

Dans la suite nous allons donner quelques exemples représentatifs.

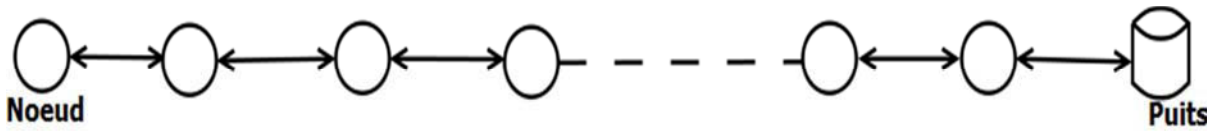


Figure 1. 1 - Un exemple de réseau de capteur sans fil linéaire.

3. Applications des réseaux de capteurs sans fil linéaires

Les applications des réseaux de capteurs sans fil linéaires sont nombreuses et variées. On retrouve les réseaux linéaires dans les applications de surveillance de pipeline d'eau, de gaz, dans la surveillance des routes, des ponts ...

3.1. Surveillance de pipelines

Aujourd'hui les ressources naturelles telles que le pétrole brut ou le gaz naturel sont acheminés sur de longues distances depuis des régions productrices jusqu'aux raffineries et usines de traitement, où ces sources d'énergie sont transformées en carburants utiles tels que l'essence, le diesel et le gaz naturel de qualité commerciale. Ces carburants prêts pour la consommation sont ensuite transportés jusqu'aux grands terminaux situés en périphérie des villes, d'où ils sont distribués aux usagers, aux foyers et aux entreprises. Les pipelines (Kennedy, 1993) sont le moyen le plus sûr et le plus efficace pour transporter de larges quantités de pétrole brut et de gaz naturel par voie terrestre ou par voie maritime. Les réseaux de capteurs sont un moyen de surveiller ces pipelines afin de prévenir tout dommage matériel, fuites, etc.

3.1.1. Pipelines terrestres

Une des applications des réseaux linéaires est la surveillance et la protection de pipelines de gaz et d'eau. Dans de nombreux pays, de longs pipelines sont utilisés pour un certain nombre d'applications telles que le transfert de l'eau des usines de dessalement, généralement situées près de la mer, vers les villes. Au Moyen-Orient, une grande ville comme Riyad avec ses quatre millions d'habitants, est complètement dépendante de l'eau transférée par d'énormes et longs pipelines situés dans la partie orientale de l'Arabie saoudite. En fait, l'Arabie saoudite est aujourd'hui le plus grand producteur mondial d'eau dessalée. L'approvisionnement des zones urbaines et industrielles majeures est réalisé grâce à un réseau de conduites d'eau qui

coure jusqu'à plus de 3800 km. Par ailleurs, les industries pétrolières et gazières dans le golfe Persique sont fortement tributaires des pipelines pour relier les ports maritimes, les raffineries et les puits de pétrole et de gaz. Par exemple, dans les Émirats arabes unis, à partir de 2006, il y'a 2 580 km de pipelines de gazoducs, 300 km de pipelines de gaz, 2 950 km de pipelines de pétrole. Les travaux présentés dans (Jawhar et al., 2011) présentent un réseau de capteurs sans fil linéaire pour la surveillance et le suivi de canalisations pour des pipelines de pétrole et de gaz. D'autres travaux (Stoianov et al., 2007) montrent l'utilisation des réseaux de capteurs linéaires pour les besoins de surveillance et de suivi des pipelines.

3.1.2. Pipelines sous-marins

La surveillance de pipeline sous-marin est aussi une application des réseaux de capteurs sans fil linéaires. Un des plus longs pipelines en usage est le pipeline LAngeled (Fitzsimons, 2005) qui s'étend sur 1 200 km sous la mer du Nord en Angleterre. Il est utilisé pour transférer le gaz naturel. Ce pipeline a commencé à fonctionner en Octobre 2007 et peut transporter jusqu'à 25,5 milliards de mètres cubes de gaz naturel par an et fournit presque 20% de la demande de gaz naturel en Angleterre. Les pipelines sous-marins sont utilisés intensivement dans le golfe du Mexique pour transférer du pétrole. Il y a près de 30 000 *miles* de pipelines sous-marins dans le golfe du Mexique et plusieurs de ces pipelines ont été endommagés par les ouragans en 2005. Le processus d'inspection des pipelines pour trouver les dommages occasionnés par les ouragans est très complexe et prend du temps. Avec l'existence de réseaux de capteurs, les infrastructures de pipelines peuvent être surveillées à distance. Des projets de construction de pipelines sous-marins pour le transfert de pétrole ou de gaz naturel sont en cours en différents endroits du monde. C'est le cas du projet de pipeline de gaz entre Oman et l'Inde via la mer arabique sur une distance de 1 200 Km et une profondeur de 3 500 m. La partie Nord de Chypre envisage également la construction d'un pipeline sous-marin de transfert d'eau à partir de la Turquie. La surveillance fiable et sans système de pilotage de ces infrastructures peut aider de façon significative dans le suivi et l'inspection des pipelines. Les réseaux de capteurs constituent une approche idéale pour la protection de ces pipelines contre les dommages qui peuvent affecter l'environnement et entrainer une perte de production.

3.2. Surveillance de lignes électriques

Un autre domaine d'intérêt des réseaux de capteurs sans fil linéaires est la surveillance des lignes électriques haute tension, à la fois aérien et souterrain. L'information collectée par les capteurs permet à la compagnie d'électricité d'anticiper les pannes qui peuvent survenir en raison d'équipements défectueux et la surcharge des lignes haute tension. Ces pannes entraînent des pertes de service pour un grand nombre de clients, et peuvent causer d'importantes pertes financières aux entreprises en raison des coûts de maintenance élevés. De nouvelles recherches dans ce domaine ont conduit à la mise au point de capteurs spécifiques aux lignes électriques qui détectent des paramètres électriques tels que la puissance, la tension ou encore l'intensité. Dans cette application particulière, les capteurs acquièrent leur énergie à partir de la ligne électrique elle-même. Les capteurs envoient les données collectées via la ligne électrique. En plus, l'installation de ces capteurs se fait rapidement et sans interrompre ou affecter le service pour les clients. Dans de tels réseaux linéaires, on s'intéresse aux questions relatives à la communication des capteurs, sur le placement des nœuds et sur l'architecture pour assurer une fiabilité des données échangées et diminuer les coûts de maintenance (Agrawal and Zeng, 2015).

3.3. Surveillance de rails

On retrouve les réseaux de capteurs linéaires dans la surveillance et le contrôle des chemins de fer et des lignes de métro. La sécurité des infrastructures ferroviaires constitue une grande préoccupation dans de nombreux pays (Hartong et al., 2008). Dans (Lee et al., 1999), les auteurs ont étudié le déploiement de capteurs à fibre optique sur un rail passant sur un pont. Les capteurs peuvent surveiller dans ce cas les anomalies dynamiques provoquées par les passages des trains afin de détecter les fissures qui peuvent être critiques et dangereuses.

Dans ce type de réseau, les lignes téléphoniques sont souvent utilisées comme relais pour acheminer les données à la station de base. Afin de réduire le coût de déploiement, minimiser la maintenance et améliorer l'évolutivité des réseaux de capteurs, les caractéristiques logicielles et physiques des nœuds diffèrent suivant leurs rôles dans l'acheminement des données. Ceci permet de surveiller de plus grandes étendues ferroviaires.

3.4. Surveillance d'activités routières

La surveillance des routes pour contrôler l'activité des piétons et des véhicules dans le but d'éviter les accidents est aussi une application des réseaux de capteurs sans fil linéaires (Karpiriski et al., 2006). Les voitures ont des dispositifs qui communiquent avec des nœuds capteurs déployés le long de la route sous la forme d'un réseau linéaire. Cette communication appelée *car-to-road* est un bon moyen de prévention routière. Les informations échangées concernent généralement des alertes relatives aux accidents ou au trafic routier (Shuai et al., 2008). Il peut aussi s'agir de messages d'avertissement pour un conducteur somnolent dont la voiture s'éloigne de sa trajectoire. En fait, les contrôleurs embarqués dans la voiture peuvent même prendre des décisions dans le cas où le conducteur n'a pas eu le temps de réagir. Il existe aussi la communication *car-to-car* où les données agrégées sur le réseau linéaire sont transférées de voiture en voiture dans le but d'éviter des accidents dans les intersections par exemple ou lors des conditions climatiques défavorables à la conduite.

3.5. Surveillance de frontières

Devant l'émergence de nouveaux risques et de nouvelles menaces plus globales, les gouvernements appellent à plus de sécurité. La surveillance et le contrôle des zones frontalières ainsi que la prévention des activités illégales est une question cruciale pour assurer la sécurité nationale. La surveillance des frontières internationales par des réseaux de capteurs sans fil linéaires suscite de nombreuses recherches ces dernières années (Dudek et al., 2009). Le rôle du réseau linéaire dans ce cas est la détection d'activités illégales telles que la contrebande de marchandises ou des médicaments, les passages frontaliers non autorisés ou tout autre type d'activités (Komar et al., 2012). Différentes stratégies de déploiement peuvent être utilisées pour la mise en place de tels réseaux. Le mode de déploiement le plus utilisé est celui d'une distribution uniforme pour laquelle les nœuds sont déployés de façon fixe et à égale distance. C'est cette distribution qui sera privilégiée dans cette thèse.

4. Problématique des réseaux de capteurs sans fil linéaires

Depuis plusieurs années, les solutions retenues dans le domaine des réseaux de capteurs étaient principalement pour des réseaux sans fil classiques où les nœuds sont dispersés sur une surface délimitée et une connectivité qui offre des solutions de routage diverses et variées. L'émergence d'applications utilisant les réseaux linéaires a orienté la recherche vers des solutions adaptées à la linéarité de ces types de réseau. Il est devenu nécessaire voire primordial de reconsidérer les solutions classiques proposées jusqu'à présent pour les réseaux de capteurs. Les caractéristiques principales des réseaux linéaires sont donc un voisinage limité, une zone de couverture longue mais plutôt étroite, des possibilités de routage limitées, etc.

- Contrairement aux réseaux sans fil classiques où les voisins d'un nœud sont dispersés dans son entourage, dans un réseau linéaire, un nœud a un nombre limité de voisins qui sont répartis dans deux directions privilégiées uniquement. Un nœud a des voisins à sa gauche appelés "voisins de gauche" et à sa droite appelés "voisins de droite". Le nombre de voisins de chaque côté dépend principalement de la portée radio et de la distance entre deux nœuds adjacents. La portée des capteurs sans fil est très variable car dépendante de l'environnement et de la technologie utilisées. La distance entre deux nœuds adjacents quant à elle dépend du modèle de déploiement qui est souvent lié à l'application.
- De même, contrairement aux réseaux sans fil classiques où les nœuds sont généralement dispersés sur une surface géographique délimitée, dans les réseaux linéaires, les zones de couverture des réseaux de capteurs linéaires peuvent s'entendre sur des distances très longues exprimées en kilomètres voire des milliers de kilomètres. L'application présentée dans (Jawhar et al., 2011) décrit un réseau linéaire de longueur 3 800 Km. Par ailleurs, la densité au mètre carré définie dans les réseaux de capteurs classiques pour évaluer les possibilités d'interférences est obsolète dans les réseaux linéaires. Par conséquent, dans ces réseaux, les temps de transit des données en direction du puits sont souvent longs et les données exposées aux risques d'une transmission multi-sauts dû à une faible connectivité.

- Enfin, du fait du voisinage limité et de la linéarité du réseau, les possibilités de routes pour acheminer les données au puits sont peu nombreuses. Donc, dans ce type de réseau, le choix du prochain saut s'effectue toujours sur le même petit nombre de nœuds voisins et le défaut d'un nœud ou d'un lien radio est préjudiciable au fonctionnement global du réseau.

Ces caractéristiques particulières font apparaitre de nouvelles méthodes d'organisation de la topologie, de nouvelles méthodes d'accès et d'acheminement des données au puits. Dans ce qui suit, nous ferons un état de l'art sur la topologie, les protocoles MAC et de routage utilisés dans les réseaux de capteurs sans fil linéaires.

5. Topologie physique des réseaux de capteurs sans fil linéaires

Du point de vue topologique, les réseaux de capteurs sans fil linéaires peuvent se diviser en deux grandes catégories en fonction du nombre de lignes et des niveaux de hiérarchisation des nœuds. Nous avons les réseaux linéaires à une dimension et ceux à plusieurs dimensions. Dans chaque type de réseau on peut définir des types des nœuds suivant leur rôle et la façon dont ils communiquent entre eux.

5.1. Les réseaux linéaires à une dimension

C'est le type de réseau linéaire le plus basique car dans ce cas les nœuds du réseau sont déployés sur une seule ligne. Ce type de réseau convient aux applications de surveillance de pipeline ou de canalisation d'eau précédemment cités. Et en fonction du rôle de chaque nœud, on peut associer des niveaux à un réseau linéaire. Un réseau linéaire est dit de niveau ***N*** s'il existe ***N*** types de capteurs différents du point de vue fonction. On trouve trois niveaux principalement.

Les réseaux linéaires à un niveau: dans ce type réseau tous les nœuds ont le même rôle comme le montre la figure 1.2.a. Chaque nœud joue le rôle de capteur et de relayeur. Les données recueillies par chaque capteur doivent être propagées par les autres capteurs jusqu'au puits.

Les réseaux linéaires à deux niveaux: dans ce réseau linéaire, il existe deux types de nœuds. Les nœuds basiques qui se chargent de recueillir les données de l'environnement et les nœuds relais qui ont pour rôle de collecter les données des nœuds basiques et de les transférer au puits via des protocoles de routage. Ce type est réseau est illustré par la figure 1.2.b.

Les réseaux linéaires à trois niveaux: en plus des nœuds relais et basiques, nous avons des nœuds appelés DDN (Data Dessimination Node) qui se chargent d'envoyer les données collectées au puits. La technologie utilisée pour transférer les données peut être variable dans ce cas (lignes téléphonique, satellite, etc.). La figure 1.2.c illustre un réseau linéaire à une dimension à trois niveaux.

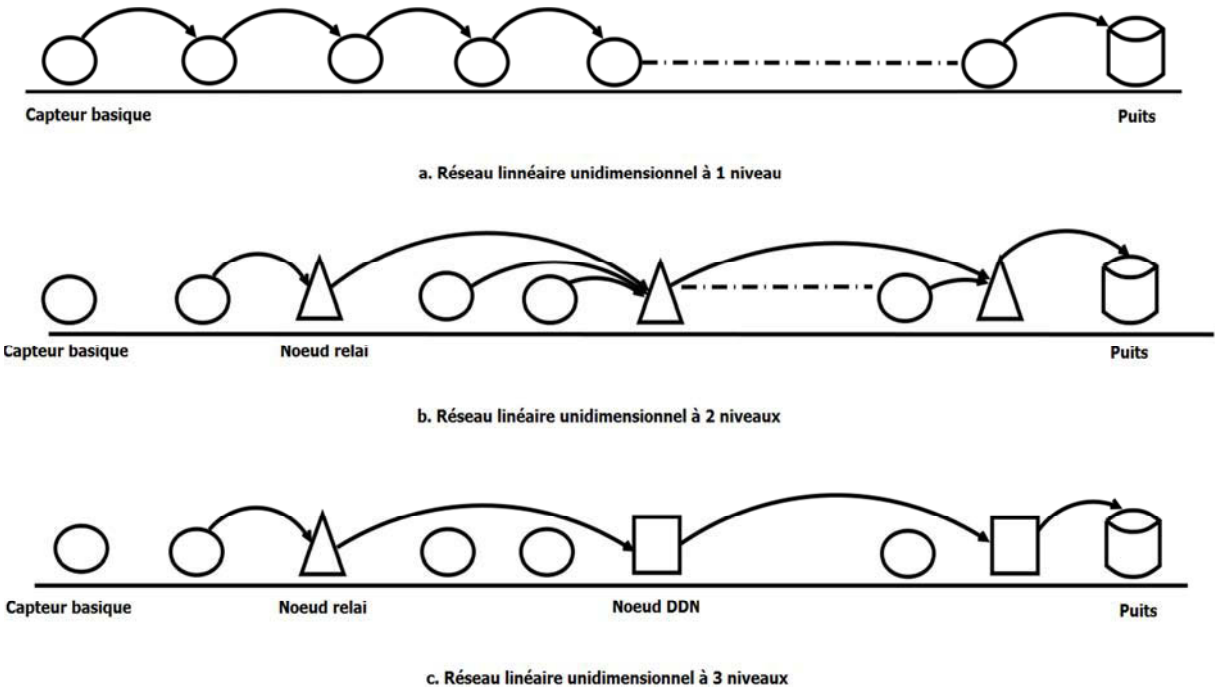


Figure 1. 2 - Réseau linéaire à un niveau.

5.2. Les réseaux linéaires multi-dimensionnels

Dans cette topologie linéaire, les nœuds sont déployés sur plusieurs lignes. Le nombre de lignes dépend souvent de la nature de l'application, de la zone de couverture et aussi du rôle des nœuds.

Comme dans le cas précédent, on peut définir plusieurs niveaux dans les réseaux linéaires multi-dimensionnels. Ainsi, dans le cas d'un seul niveau les nœuds sont disposés sur plusieurs lignes et jouent tous le même rôle de collecte et de relai des données vers le même puits. Dans le cas de plusieurs niveaux, la linéarité n'existe pas forcément à tous les niveaux. Généralement, seuls les nœuds relais et les DDNs suivent la topologie linéaire tandis que les nœuds capteurs ne sont pas forcément disposés en ligne. La figure 1.3 est une illustration d'un réseau linéaire multi-dimensionnel.

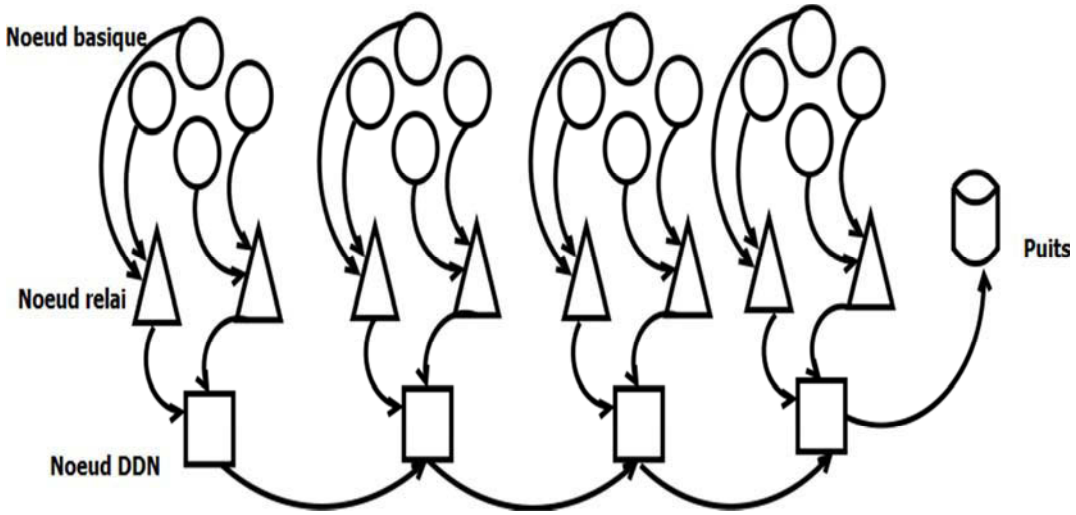


Figure 1. 3 - Réseau linéaire multi-dimensionnel à 3 niveaux.

Cette topologie convient bien à des applications de surveillance couvrant des longues zones de couverture mais pas très étroites. Dans (Felemban, 2013), les auteurs décrivent une application utilisant un réseau de capteurs linéaire multi-dimensionnel pour surveiller l'activité à la frontière.

6. État de l'art des protocoles MAC pour réseaux de capteurs sans fil linéaires

La méthode d'accès au canal de transmission est une problématique très présente dans les réseaux de capteurs sans fil. En effet, la méthode d'accès doit gérer efficacement les ressources des nœuds capteurs et optimiser les paramètres de performance du réseau comme

le délai de bout-en-bout, le taux de délivrance de paquets au puits, le débit, etc. L'utilisation abusive provient essentiellement cinq (5): la sur-écoute, les collisions, l'écoute passive, le surcoût protocolaire, les envois infructueux.

- La sur-écoute (*overhearing*) est le temps d'écoute du canal des nœuds voisins pendant le préambule, même si tout le monde n'est pas forcément le récepteur. Il est clair que la sur-écoute consomme inutilement l'énergie et donc elle est à minimiser.
- La collision (*collision*) constatée au niveau d'un nœud récepteur correspond à la réception d'un signal porteur d'une trame altérée par une activité radio concurrente. Quand cette altération ne permet pas la bonne compréhension de la trame on parle de collision. Si le nœud en était le destinataire cela conduit à des transmissions inutiles et à la nécessité de retransmissions. Elle est donc à éviter et/ou à minimiser.
- L'écoute passive (*Idle listening*) est une autre source du gaspillage de l'énergie que l'on doit minimiser. Elle a lieu quand un nœud doit maintenir son écoute du canal alors qu'il n'a pas de trames à émettre ou à recevoir.
- Le surcoût protocolaire ou *Overhead* (e.g. utilisation de RTS/CTS et autres paquets de contrôle supplémentaires, ajout des informations dans l'entête) doit être minimisé car il diminue le débit utile et augmente la consommation de l'énergie.
- Les envois infructueux se produisent quand un nœud essaie de communiquer avec un autre nœud qui n'est plus accessible parce qu'il est en mode sommeil par exemple (ou hors de portée). Le nœud émetteur est en attente d'un acquittement, et il retransmet donc la même trame plusieurs fois. Il consomme alors de l'énergie en le faisant du fait qu'il doit rester en mode transmission et en mode réception pour l'éventuel acquittement.

Il existe plusieurs protocoles MAC spécifiquement implémentés pour les réseaux de capteurs linéaires. Ces protocoles tentent de résoudre les problèmes cités ci-dessus en tenant compte des spécificités de ces réseaux. Ils sont principalement basés sur la contention et la synchronisation. Il existe d'autres protocoles utilisant des approches hybrides combinant contention et synchronisation temporelle. Dans ce chapitre, nous présentons les principaux protocoles MAC utilisés dans les réseaux sans fil linéaires. Nous commençons notre étude par le protocole MAC 802.15.4 qui est essentiellement utilisé dans les réseaux de capteur sans fil.

6.1. Le protocole MAC 802.15.4

La norme 802.15.4 (IEEE, 2003) est un protocole de communication défini par IEEE. Il est destiné aux réseaux sans fil de la famille des LR WPAN (*Low Rate Wireless Personal Area Network*) du fait de leur faible consommation, de leur faible portée et du faible débit des dispositifs utilisant ce protocole. La norme IEEE 802.15.4 prévoit deux types de topologie.

- Étoile : tous les nœuds communiquent avec un nœud central appelé coordinateur du PAN (*Personal Area Network*). Les nœuds appelés aussi feuilles communiquent entre eux en passant systématiquement par le coordinateur. Celui-ci gère les associations des feuilles au réseau.
- Point à point: tous les nœuds à portée radio peuvent communiquer ensemble sans hiérarchie. Dans cette topologie, les nœuds peuvent être divisés en trois catégories. En plus du coordinateur du PAN, nous avons des nœuds coordinateurs et des nœuds feuilles. Les coordinateurs peuvent aussi gérer les associations d'autres coordinateurs et feuilles.

La figure 1.4 montre les deux topologies de réseau utilisées dans 802.15.4.

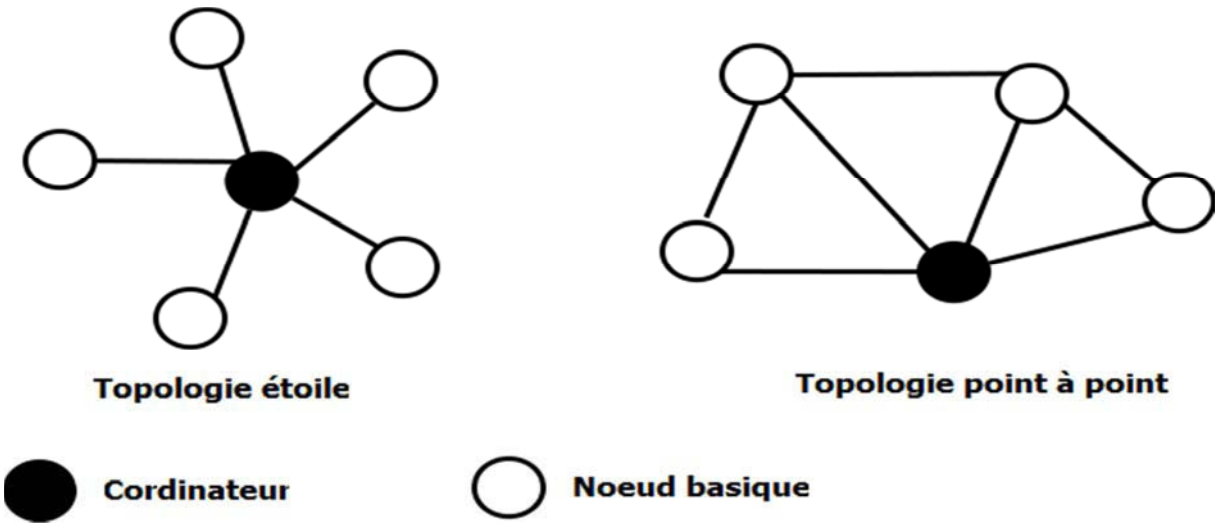


Figure 1. 4 - Topologies de réseau proposées par IEEE 802.15.4.

802.15.4 propose une couche physique et une couche liaison de données adaptées aux applications à faible débit dont l'autonomie énergétique est une contrainte forte. Beaucoup d'applications de surveillance basées sur les réseaux de capteurs sans fil utilisent la norme 802.15.4 pour les couches physique et liaison de données. On retrouve cette norme dans les réseaux de capteurs sans fil linéaires comme ceux présentés dans (Jawhar et al., 2011) .

La couche MAC 802.15.4 supporte deux modes de fonctionnement selon les besoins applicatifs : le mode « suivi de balise (*beacon*) » et le mode « non suivi de balise ». Une balise est une trame diffusée par un coordonnateur, porteuse d'informations de service et de synchronisation principalement.

En mode « non suivi de balise », il n'y a pas de synchronisation. Les balises ne servent qu'à l'association des nœuds au réseau. Les nœuds coordinateurs sont toujours actifs alors que les nœuds feuilles ne le sont que lorsqu'elles souhaitent communiquer. L'accès au medium n'est pas garanti : les entités sont toujours en concurrence pour émettre.

En mode suivi balise, l'activité des nœuds est synchronisée par un coordonnateur qui envoie périodiquement les informations de synchronisation à travers la balise. Le coordinateur peut modifier l'intervalle entre deux balises consécutives pour que les nœuds travaillent plus ou dorment plus selon le type d'application. La balise contient des informations décrivant la structure d'un cycle. L'information de synchronisation définit les périodes de sommeil et de réveil des nœuds. Ce cycle, nommé supertrame, est découpé en deux périodes principales : une période d'activité suivie d'une période d'inactivité.

6.1.1. La structure de la supertrame

La structure de la supertrame est définie par les deux paramètres BI (*Beacon Interval*) qui définit l'intervalle qui sépare deux balises consécutives et SD (*Superframe Duration*) qui définit la durée de la supertrame. Les durées de l'intervalle inter-balise BI et de la supertrame SD sont déterminées respectivement par l'ordre de balise BO (*Beacon Order*) (Equation.1) et le paramètre SO (*Superframe Order*) (Equation.2).

$$\mathrm{BI} = \mathrm{aBaseSuperframeDuration} * 2^{\mathrm{BO}} \ [\mathrm{Symbols}] \quad (1)$$

$$SD = aBaseSuperframeDuration * 2^{SO} \text{ [Symbols]} \quad (2)$$

Avec 0 ≤ SO ≤ BO ≤ 14. aBaseSuperframeDuration est un attribut de la sous-couche MAC qui est égal par défaut à 15,36 ms. La supertrame est composée d'une section active et d'une section inactive. Dans la section inactive, les nœuds sont dans un mode de fonctionnement basse consommation afin d'économiser leur énergie. La section active de la supertrame est divisée en 16 slots de durées identiques durant lesquelles les nœuds envoient leurs données au coordonnateur. Elle se compose de trois sous-parties: (i) la balise, (ii) une CAP (*Contention Access Period*) ou période avec contention, (iii) une CFP (*Contention Free Period*) ou période sans contention. Durant la CAP les nœuds communiquent avec leur coordinateur et durant le CFP le nœud demande l'attribution exclusive d'un slot appelé GTS (*Guaranted Time Slot*). Notons que quand SO est égal à BO, la supertrame ne dispose pas d'une période d'inactivité et les nœuds sont toujours actifs. La structure de la supertrame est représentée dans la figure 1.5.

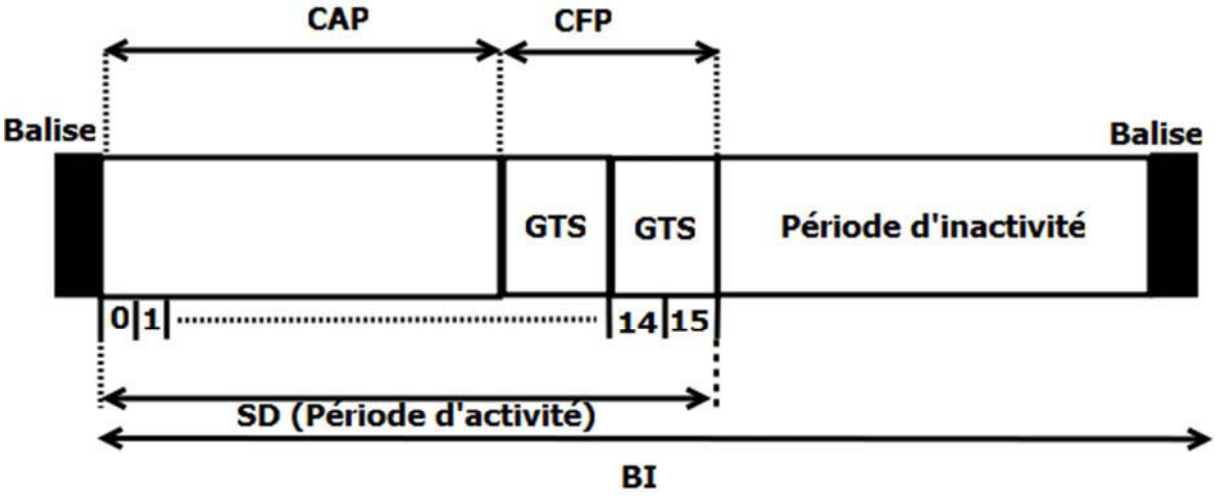


Figure 1. 5 - Structure de la supertrame 802.15.4.

L'accès au médium durant la CAP est géré selon l'algorithme de CSMA/CA slotté pour toute trame, sauf les acquittements et les balises. Avant tout envoi, l'entité doit s'assurer de pouvoir finir la transaction (incluant la réception d'un acquittement s'il est demandé) et de pouvoir attendre un IFS (*InterFrame Space*) avant la fin de la CAP. Si ce n'est pas le cas, l'envoi est

reporté à la CAP de la supertrame suivante. L'envoi de trames durant les slots réservés aux GTS s'effectue sur la base de TDMA.

6.1.2. Algorithme de CSMA/CA slotté

Le CSMA/CA slotté est une variante de CSMA/CA à la base de IEEE 802.11, (IEEE, 2005). Son mécanisme est cadencé par une unité de temps appelée période de backoff et égale au temps d'envoi effectif de 20 symboles (équivalent à 10 octets) par le module radio, soit 320 µs. Les entités sont synchronisées sur cette échelle de temps grâce à la réception de la balise. Les backoffs servent à discrétiser le temps afin de réduire le temps de surveillance du médium et de garantir une économie d'énergie, point critique dans les réseaux de capteurs sans fil. Ce mécanisme implique trois paramètres :

- NB qui représente le nombre de tentatives pour accéder au médium. Il est initialisé à 0 avant chaque nouvelle transmission. Si NB dépasse la valeur de la constante macMaxCSMABackoffs (dont la valeur initiale est fixée à 4), l'accès au médium est considéré comme un échec.
- CW qui représente la durée en nombre de périodes de backoff du test du canal. Il est initialisé à 2, et réinitialisé à cette valeur à chaque fois que le médium est trouvé occupé.
- BE qui représente l'exposant de la fenêtre de tirage du backoff. Ce paramètre permet de déterminer le nombre de backoff qu'un nœud doit attendre avant de tenter d'accéder au médium.

La figure 1.6 représente les différentes étapes du mécanisme CSMA/CA slotté.

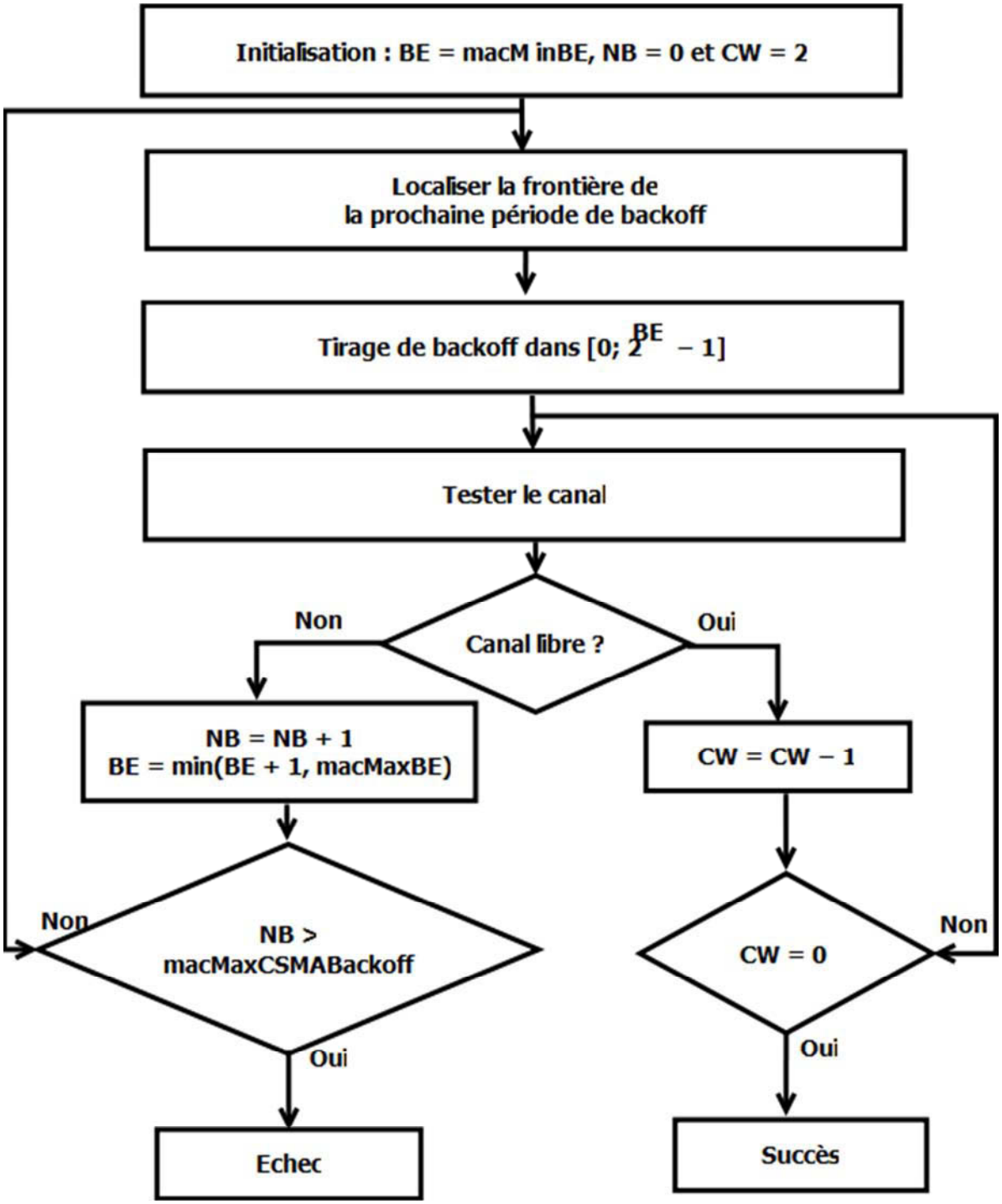


Figure 1. 6 - Mécanisme CSMA/CA slotté.

La première étape est la phase d'initialisation. L'algorithme commence avec BE = macMinBE, NB = 0 et CW = 2. Une fois les paramètres initialisés, l'etape 2 consiste à

localiser la frontière de la prochaine période de backoff et à attendre un nombre entier de périodes de backoff tiré aléatoirement dans l'intervalle [0; $2^{BE}-1$]. Si la durée du backoff tiré est plus longue que le nombre restant de périodes de backoff dans la CAP, l'algorithme consomme le backoff jusqu'à la fin de la CAP et reporte ce qui lui reste pour la CAP de la supertrame suivante. Après la consommation de ce backoff, la couche MAC vérifie que le nombre restant de périodes de backoff dans la CAP est suffisant pour effectuer 2 CCA (*Clear Channel Assessment*), transmettre la trame physique et recevoir un éventuel acquittement. Si c'est le cas, l'étape 3 est appliquée. Dans cette étape, la couche MAC demande à la couche PHY d'effectuer un CCA à la frontière de la prochaine période de backoff. Si le temps restant dans cette supertrame est insuffisant, la couche MAC reporte le CCA au début de la CAP de la prochaine supertrame, en commençant avec un tirage de backoff pour éviter les collisions systématiques dues à plusieurs reports de CCA effectués par différentes entités (Koubaa et al., 2006). Si la couche PHY détecte que le canal est libre, la couche MAC décrémente CW, puis teste si CW est nul. Si c'est le cas, la couche MAC demande à la couche PHY de commencer la transmission à la frontière de la prochaine période de backoff. Si CW n'est pas nul, la couche MAC demande à la couche PHY de faire un autre CCA. Le médium n'est donc pas scruté en permanence, mais ce sont deux CCA consécutifs positifs qui permettent de conclure que le médium est libre. Si la couche PHY détecte que le canal est occupé, la couche MAC incrémente NB et BE de 1 (à condition que BE reste inférieur ou égal à macMaxBE) et remet CW à 2. Si NB = macMaxCSMABackoffs, l'algorithme renvoie un échec d'accès. C'est alors à la couche MAC de demander une retransmission de la même trame tant que le nombre de tentatives est plus petit que macMaxFrameRetries (macMaxFrameRetries = 3 par défaut). Si NB < macMaxCSMABackoffs, l'algorithme retourne à l'étape 2.

6.1.3. Algorithme de CSMA/CA non slotté

L'algorithme de CSMA/CA non-slotté est appliqué pour les envois de trames dans un réseau en mode non suivi de beacon. Pour autant, il ne s'agit pas de CSMA/CA de la norme IEEE 802.11. Le paramètre CW n'existe pas dans l'algorithme de CSMA/CA non-slotté : il suffit de détecter une seule fois que le canal est libre pour commencer une transmission. L'unité du

temps reste la période de backoff, mais l'activité des entités n'est pas synchronisée sur ces périodes de backoff. La figure 1.7 présente les différentes étapes du CSMA/CA non-slotté.

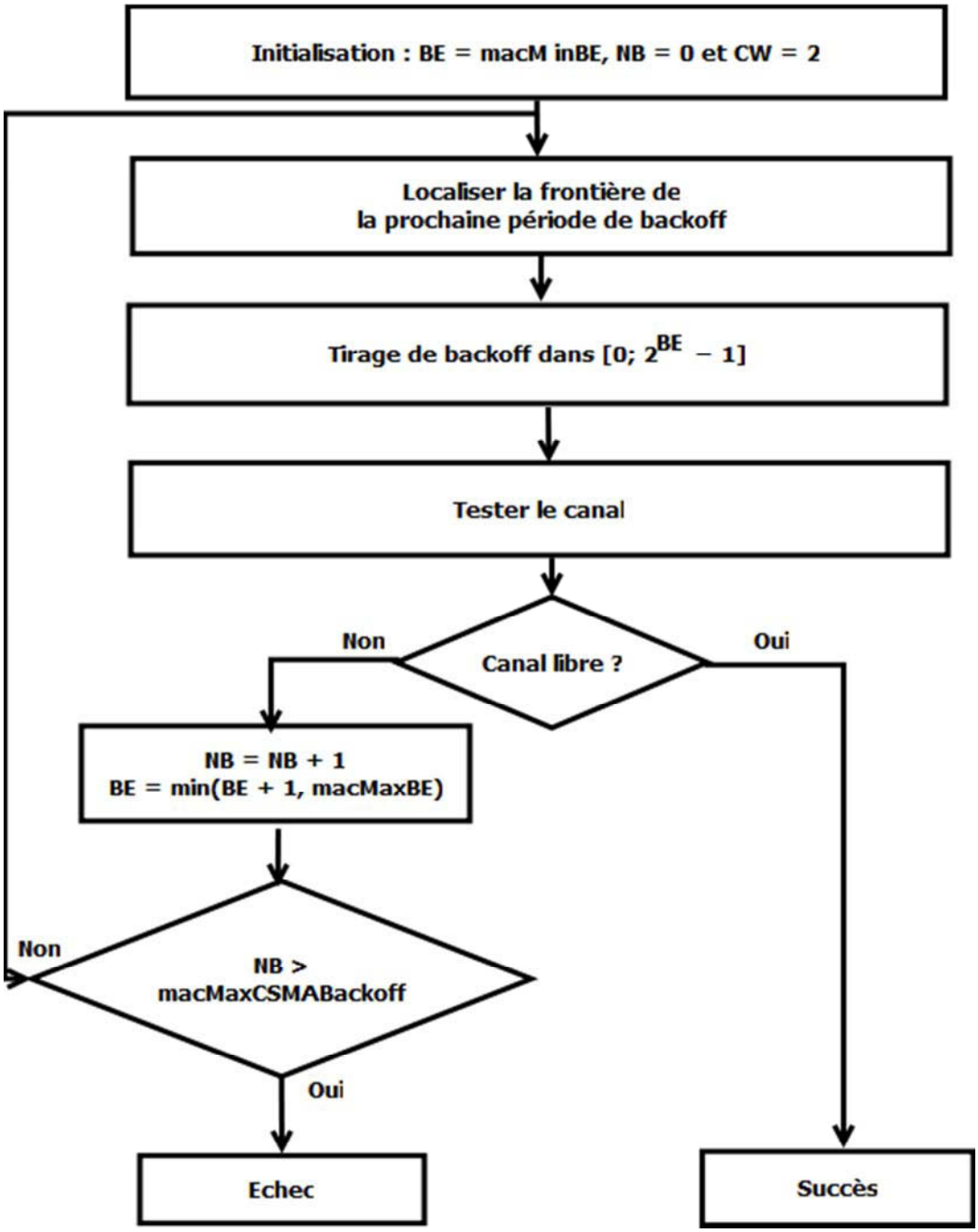


Figure 1. 7 - Mécanisme CSMA/CA non slotté.

L'algorithme commence par la phase d'initialisation en mettant BE = macMinBE et NB = 0. Puis, un nombre entier de période de backoff est tiré aléatoirement. Après la consommation du backoff, la couche MAC demande à la couche PHY d'effectuer un CCA. Si la couche PHY détecte le canal libre, la couche MAC commence la transmission. Si ce n'est pas le cas, la couche MAC incrémente NB et BE (à condition que BE reste inférieur ou égal à macMaxBE). Si NB < macMaxCSMABackoffs, l'algorithme revient au tirage de backoff. Si NB = macMaxCSMABackoffs, l'algorithme renvoie un diagnostic d'échec d'accès. C'est alors à la couche MAC de demander une retransmission de la même trame tant que le nombre de tentatives est plus petit que macMaxFrameRetries (macMaxFrameRetries vaut 3 par défaut).

6.2. Les protocoles basés sur la synchronisation temporelle

Les protocoles MAC appliquant un séquencement temporel découpent le temps en slots, chaque slot de temps est alloué (localement) à un seul nœud pour lui garantir l'accès au canal afin qu'il puisse transmettre ses données. La méthode TDMA est un exemple de méthode de séquencement temporel dans les réseaux sans fil. Ces protocoles sont généralement économes en énergie car ils évitent les collisions, ils limitent le *idle listening* et le *overhearing*, et peuvent mettre les nœuds en mode sommeil durant les slots de temps réservés aux autres nœuds. De plus, ils garantissent un délai borné de bout-en-bout si un algorithme d'allocation prend en compte les caractéristiques du trafic. En revanche, l'aspect centralisé et le besoin d'une synchronisation forte rendent ce type de protocoles rigide et non-adapté pour les topologies dynamiques et mobiles. Dans la suite nous présentons les protocoles utilisés dans les réseaux de capteurs sans fil linéaires.

6.2.1. Le protocole DiS-MAC (*Directional Scheduled MAC*)

DiS-MAC (Karveli et al., 2009) est un protocole MAC basé sur une synchronisation temporelle des nœuds capteurs déployés linéairement dans le cas de la surveillance d'une autoroute. La topologie est caractérisée par deux lignes de nœuds de part et d'autre de l'autoroute. Dans DiS-MAC, chaque nœud utilise des antennes directionnelles orientées afin

de réduire sa portée à un voisin direct dans la ligne. Ceci minimise les interférences entre les nœuds d'une même ligne mais aussi avec les nœuds de la ligne de l'autre côté de l'autoroute. L'accès au canal dans DiS-MAC est divisé en deux phases appelées phase I et phase II de durée respective T_1 et T_2. Il est possible que les durées T_1 et T_2 soient égales. Dans la phase I, seuls les nœuds de position impaire sur le réseau linéaire accèdent au canal de transmission. Les nœuds de position paire sont récepteurs durant cette phase. De même, durant la phase II, les nœuds de position impaire sont émetteurs durant T2 et ceux de position impaire sont récepteurs.

Avec cette méthode d'accès, l'accès au canal de transmission est garanti sans avoir recours à la contention. L'utilisation d'accusés de réception dans DiS-MAC permet d'avoir la confirmation d'une forme de réception ou non d'un paquet comme dans les protocoles classiques mais de plus, elle permet de détecter les nœuds défectueux. En effet, dans DiS-MAC on considère que la réception d'un paquet envoyé est « quasi-garantie » grâce à l'utilisation d'antennes directionnelles qui minimisent les zones d'interférences dans le réseau.

Le protocole DiS-MAC est simple et conçu pour un réseau linéaire où les nœuds ont une portée très limitée. Ceci diminue fortement les interférences et les possibilités de routage multi-saut. Ces propriétés font de DiS-MAC un protocole non adapté aux réseaux linéaires à antennes omnidirectionnelles et/ou les antennes permettent à un nœud d'avoir une portée qui lui assure un voisinage de plus d'un nœud. En effet, dans ce cas, il existe des risques de collisions entre les nœuds d'une même zone.

6.2.2. Le protocole LC-MAC (*Long-Chain MAC*)

LC-MAC (Fang et al., 2011) est un protocole MAC à *duty cycle* basé sur une synchronisation temporelle des nœuds pour l'accès au canal de transmission. Le *duty-cycle* ou cycle actif est défini comme la proportion de la période active sur la durée totale d'un cycle. Un cycle, d'une période fixe ou variable, est composé d'une période active durant laquelle un nœud peut transmettre et recevoir, et une période de sommeil où la partie radio est éteinte. LC-MAC protocole est conçu pour les réseaux linéaires s'étendant sur de longues distances afin de réduire les délais de bout-en-bout tout en économisant l'énergie des capteurs. Le

fonctionnement de LC-MAC s'effectue en trois phases : une phase d'initialisation, une phase de synchronisation et une phase d'émission de trames.

La phase d'initialisation consiste en une découverte de voisinage. Dans cette phase le nœud plus à gauche de la topologie linéaire appelé $\boldsymbol{R_n}$ (*Relay node n*) crée et génère une trame de détection de voisin appelée LDP (*Location Detect Package*). Cette trame contient les informations sur les différents nœuds du réseau linaire et leurs adresses. Elle est diffusée de proche en proche entre les nœuds jusqu'au puits supposé à l'extrémité droite du réseau. Chaque nœud qui reçoit le LDP y ajoute son adresse avant de le relayer à son voisin à un saut en direction du puits. Arrivé au puits, celui-ci ajoute son adresse et le fait circuler en direction du nœud relai afin que chaque nœud ait connaissance de tous les autres nœuds du réseau.

Dans la phase de synchronisation, chaque nœud planifie sa période de prochain réveil pour relayer la trame de synchronisation appelée SSYNC (*Super SYNC*), qui est créé par le nœud $\boldsymbol{R_n}$. Le prochain réveil est calculé en fonction de la position du nœud dans le réseau linéaire et de la connaissance des nœuds du réseau grâce au processus d'initialisation et de détection. La trame SSYNC contient les informations relatives à l'adresse, au nombre de paquets à envoyer et aux périodes d'activité et d'inactivité pour chaque nœud. Chaque nœud qui reçoit le SSYNC le met à jour avec ses informations de synchronisation.

Dans la phase d'émission des trames, chaque nœud envoie ses données en mode rafale à son voisin direct à un saut durant sa période d'émission comme indiqué dans la figure 1.8. Le temps de transmission est calculé en fonction des informations contenues dans le SSYNC.

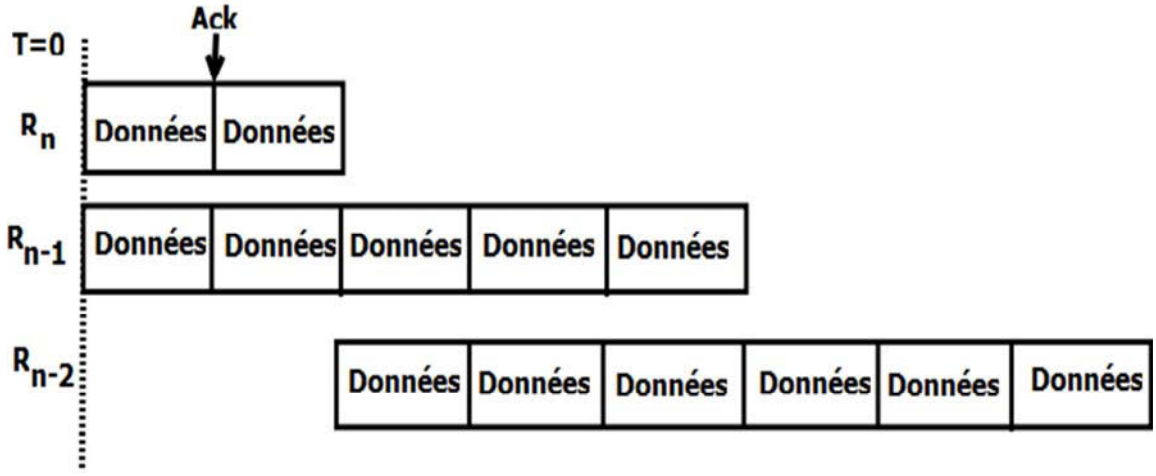


Figure 1. 8 - Transmission des trames données dans LC-MAC.

Cette façon d'acheminer les données de proche en proche entre voisin à un saut jusqu'au puits peut engendrer des délais de bout-en-bout longs si la longueur de la ligne est longue. Ce qui a pour conséquence une perte de débit dans la chaine linéaire. De plus, dans LC-MAC plus le nœud est proche du puits, plus il agrège de données et par conséquent plus son module radio reste longtemps actif. Ceci signifie que les nœuds proches du puits consomment plus d'énergie donc sont très exposés à l'épuisement de leurs batteries et peuvent provoquer la fin de la durée de vie du réseau. En plus, la longueur des trames imposées par les couches basses du réseau sans filest un obstacle au passage à l'échelle de cette solution.

6.2.3. Le protocole CMAC-T (*Chain-type MAC Protocol based on Token*)

CMAC-T (Sun et al., 2013a) est un protocole MAC pour un réseau linéaire basé sur la synchronisation des nœuds à l'aide de jeton. Il est conçu pour la surveillance de cultures en milieu forestier. L'accès au canal de transmission se fait à la demande dans des slot de temps définis. Dans CMAC-T deux types de trames sont utilisés : une trame *beacon* et une trame de données. La trame *beacon* joue le rôle de jeton et est chargée de la synchronisation entre les nœuds adjacents et l'accès au canal. Elle contient deux octets. Un octet qui contient les informations relatives au jeton et permet aux nœuds adjacents de se synchroniser, un autre qui stocke le nombre de nœuds dans le réseau linéaire. La trame de données contient entre autres, des informations sur l'adresse IP du nœud source, les informations d'alerte sur l'état de batterie.

La création et la génération de la trame *beacon* sont gérées par le puits. Ainsi, périodiquement il la diffuse en direction des nœuds pour désigner celui qui a l'accès au canal durant cette période. Le nœud destinataire du *beacon* se synchronise avec son voisin à un saut pour la transmission des données alors que les autres nœuds se remettent en mode sommeil en attendant le prochain *beacon* afin d'économiser de l'énergie. Donc, pour un réseau de N nœud, la transmission complète d'une donnée jusqu'au puits nécessite ***N*** beacons pour la synchronisation et à la transmission de proche en proche. Le calcul des temps de sommeil, d'attente et d'émission de trames dépend du numéro du *beacon*, de la position du nœud et du temps nécessaire pour l'envoie d'une trame.

6.2.4. Le protocole WiWi (*Wireless Wire*)

WiWi (De Caneva et al., 2010) est aussi un protocole MAC conçu pour les réseaux de capteurs sans fillinéaires. Dans ce protocole, le déploiement des nœuds capteurs est organisé de façon à ce que la distance entre deux nœuds adjacents soit très proche de la distance caractéristique. Cette dernière est définie comme étant la distance optimale entre un transmetteur et un récepteur qui minimise la consommation d'énergie dans une communication multi-hop. Elle est strictement déduite des caractéristiques physiques des nœuds. Deux trafics peuvent circuler en même temps et en sens inverse dans le réseau. Un trafic du nœud le plus proche du puits appelé nœud maitre vers les nœuds appelé *downstream* et un trafic qui va des nœuds vers le puits appelé *upstream*. Le premier type de trafic contient des informations de synchronisation principalement alors que le second type est constitué des informations collectées par les nœuds. Le découpage temporel de WiWi est montré dans la figure 1.9.

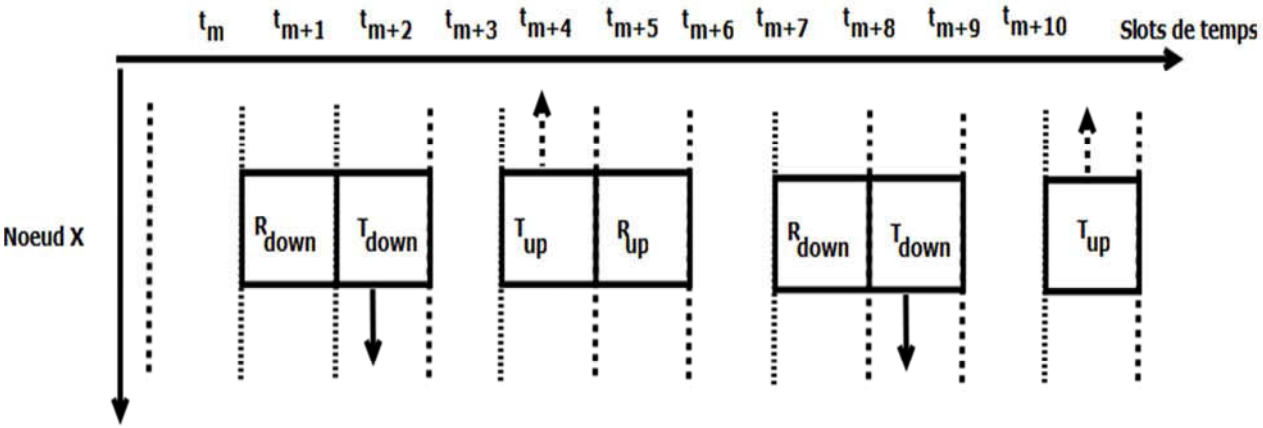


Figure 1. 9 – Découpage temporel et acheminement des données dans WiWi.

Quand un nœud reçoit un trafic *downstream* en provenance du nœud maître, il le relaie immédiatement à son voisin à un saut et se synchronise sur la période de la prochaine réception de ce type de trafic. Le trafic *upstream* suit le même principe de circulation de

proche en proche jusqu'au puits. Cependant, entre la réception et l'envoi de trafic *usptream*, un nœud doit attendre une période de temps équivalent à quatre slots de temps pour recevoir pour recevoir et envoyer du trafic downstream à ses voisins et rester inactif pour éviter toute collision de paquets. Ainsi, une fois synchronisé, le nœud suit le motif de fonctionnement suivant: *(Réception, Transmission, Idle, Transmission, Réception, Idle)* comme montré dans la figure 1.10. (i) Il reçoit le trafic downstream durant un slot de temps $t_{m+1.}$ Durant t_{m+2}, il relaie le trafic *downstream* à son voisin direct et reste inactif durant un slot équivalent à t_{m+3} dans le but d'éviter toute collision avec le trafic *downstream* du voisin X+1. Durant les périodes t_{m+5}, t_{m+6} et t_{m+7} le nœud se met successivement en mode réception de trafic *upstream*, attente et réception de trafic *downstream*.

La figure 1.10 montre l'activité du nœud X.

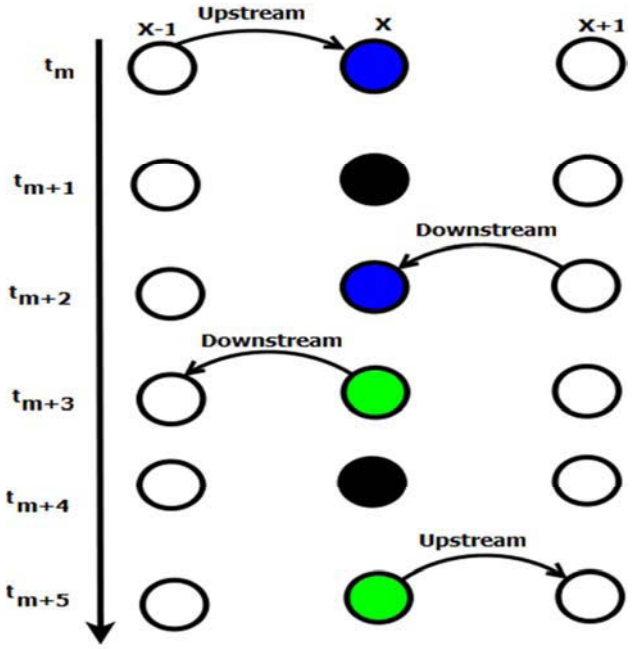


Figure 1. 10 - Activité du nœud X.

6.3. Les protocoles basés sur la contention

Dans ce type de protocoles MAC, les nœuds accèdent au médium durant le même intervalle de temps en utilisant un algorithme de la famille CSMA avec contention ou de ses variantes pour essayer d'éviter les collisions. Le point fort de ce type de protocoles est sans doute l'extensibilité et le passage à l'échelle. En revanche, ces protocoles n'offrent pas de délai borné du fait qu'ils ne garantissent pas l'accès au médium dès que la charge du réseau augmente. Dans la suite, nous allons décrire quelques protocoles MAC basés sur la contention utilisés dans les réseaux de capteurs sans fil linéaires.

6.3.1. Le protocole MTF-MAC (*Multi Frame Transmission MAC*)

MFT-MAC (Lee et al., 2013) est un protocole MAC basé sur la contention des nœuds. On considère un réseau où les nœuds sont distribués sur un espace géographique très limité et sont organisés en chaine linéaire pour la collecte et l'acheminement des données. Ce protocole est basé sur des périodes de synchronisation, de contention et de sommeil. La synchronisation se fait par groupe de 5 nœuds suivant les exigences requises sur la précision des horloges des nœuds. La période de contention est caractérisée par une génération d'une trame de contrôle appelée PION (pionnier). En fait, cette période sert de réservation du canal de transmission pour les nœuds ayant des données à envoyer au puits. L'envoi des trames de données se fait dans la période SLEEP qui suit la période de contention. L'utilisation de la trame PION est identique au fonctionnement du mécanisme RTS/CTS de 802.11 pour la réservation du canal de transmission. Il permet de résoudre le problème du terminal caché pendant une durée définie dans la trame. La particularité de la trame PION est qu'il joue à la fois le rôle de RTS et de CTS. Une autre particularité est la présence du champ *multiframe* qui correspond au nombre de trames de données qu'un nœud doit envoyer à son voisin direct à destination du puits. Le fonctionnement du protocole MFT-MAC avec les différentes périodes d'activités est représenté dans la figure 1.11. Ce fonctionnement peut être composé en trois étapes.

- Une période de synchronisation dans laquelle les nœuds sont tous réveillés et attendent de recevoir la trame PION.
- Un période appelée *DATA period* où le nœud PION est relayé du nœud de l'autre extrémité du réseau jusqu'au puits. Cette étape permet à chaque nœud d'avoir

connaissance du nombre de trames qu'il doit recevoir de son voisin grâce au champ *multiframe.*

- La période *SLEEP* dans laquelle chaque nœud reçoit le trafic de son voisin à un saut puis transmet ses données à son voisin à un saut en direction du puits. À la fin de la transmission de ses données, le nœud se met en mode sommeil jusqu'à à la prochaine période de synchronisation.

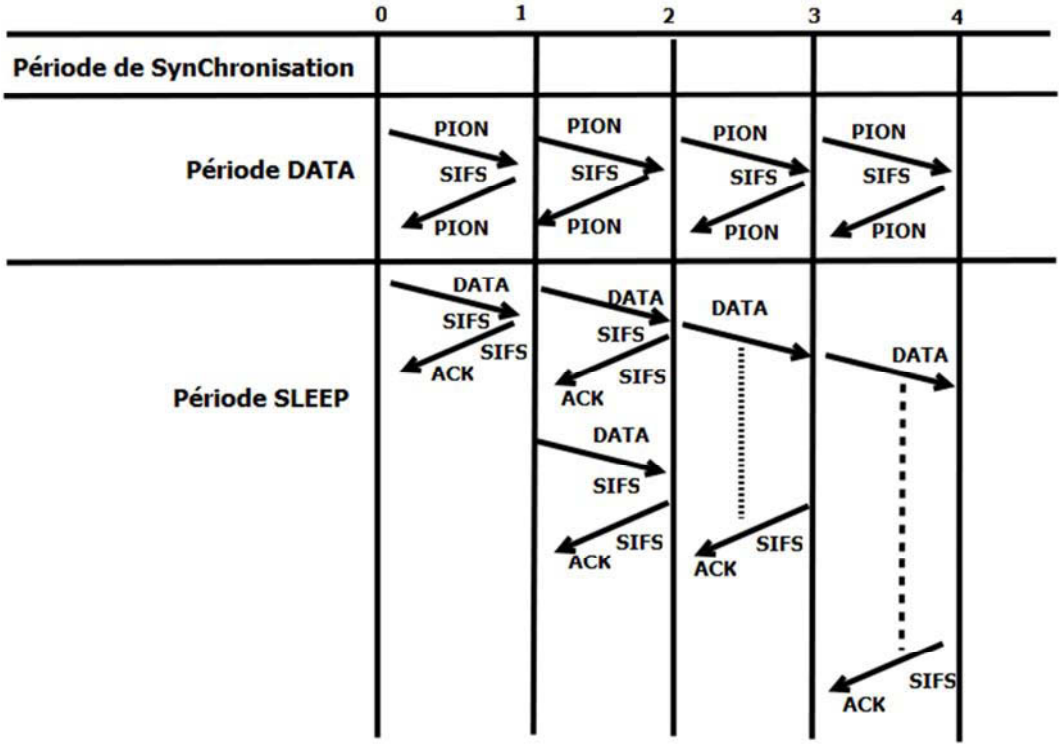


Figure 1. 11 - Les différentes étapes du processus de transmission dans MFT-MAC.

MFT-MAC est un protocole MAC qui convient pour des réseaux de capteurs à zone de couverture limitée. La technique de découpage du réseau linéaire en de petits groupes de nœuds ne convient pas quand la chaine linéaire s'étend sur une longue distance. En effet, dans ce cas, la création de la trame PION à tour de rôle par groupe pourrait augmenter les temps d'acheminement des données vers le puits.

6.3.2. Le protocole L-CSMA (*Linear CSMA*)

L-CSMA (Buratti and Verdone, 2015) est un protocole MAC basé sur CSMA de 802.15.4 et est conçu pour réseaux de capteurs sans fil linéaires pour gérer les pertes de paquets causés par le phénomène du terminal caché et les longs délais engendrés par la contention de CSMA. Il part de l'hypothèse selon laquelle, dans CSMA, la probabilité qu'un paquet entre en collision durant son acheminement est assez élevée dans le cas d'une topologie linéaire. Pour éviter les pertes de paquets dues au terminal caché ou exposé, L-CSMA se base sur des priorités assignées aux différents nœuds du réseau suivant leur position sur la ligne. Ainsi, les nœuds les plus proches du puits sont plus prioritaires du fait qu'ils agrègent plus de données. La priorité du nœud est basée sur la période d'écoute du canal pour tester s'il est libre ou occupé. L'activité d'un nœud dans L-CSMA se fait dans des slots de temps calculés en fonction de la position du nœud dans la chaine linéaire. Ainsi, plus un nœud est prioritaire plus sa période d'écoute du canal est petite ce qui lui permet d'utiliser son slot de temps pour l'envoi de données à son voisin direct. Un slot est composé principalement de trois périodes.

- Dans la première période le nœud se met en mode écoute du canal pour vérifier s'il est libre ou occupé. Soit *n* le nombre de nœuds dans le réseau linéaire, et *i* la position du nœud considéré dans le réseau. Alors le temps $T_{ecoute}(i)$ d'écoute du canal est donnée par $T_{ecoute}(i) = (n - i + 1) * T$ où $\boldsymbol{T}$ est le temps minimal d'écoute du canal égale au temps d'écoute du nœud *n*.
- Dans la période suivante si le canal est libre alors le nœud envoie les données à son voisin direct sinon il se met en mode sommeil. La durée de transmission des données durant cette phase dépend du nombre de paquets que le nœud à agréger de son précédent voisin de la topologie linéaire.
- Enfin, dans la dernière période, le nœud se met en mode sommeil jusqu'à la prochaine période d'écoute du canal de transmission. Ce temps est donné par la formule $T_{attente}(i) = i * T$.

La figure 1.12 montre le fonctionnement de L-CSMA pour deux nœuds relais adjacents R_1 et R_2 dans la topologie linéaire. Dans ce schéma, le nœud R_2 accède au canal de transmission

avant la fin de la période d'écoute du nœud R_1. De ce fait, le nœud R_1 à la fin de sa période d'écoute trouvera le canal occupé et différera ainsi sa transmission.

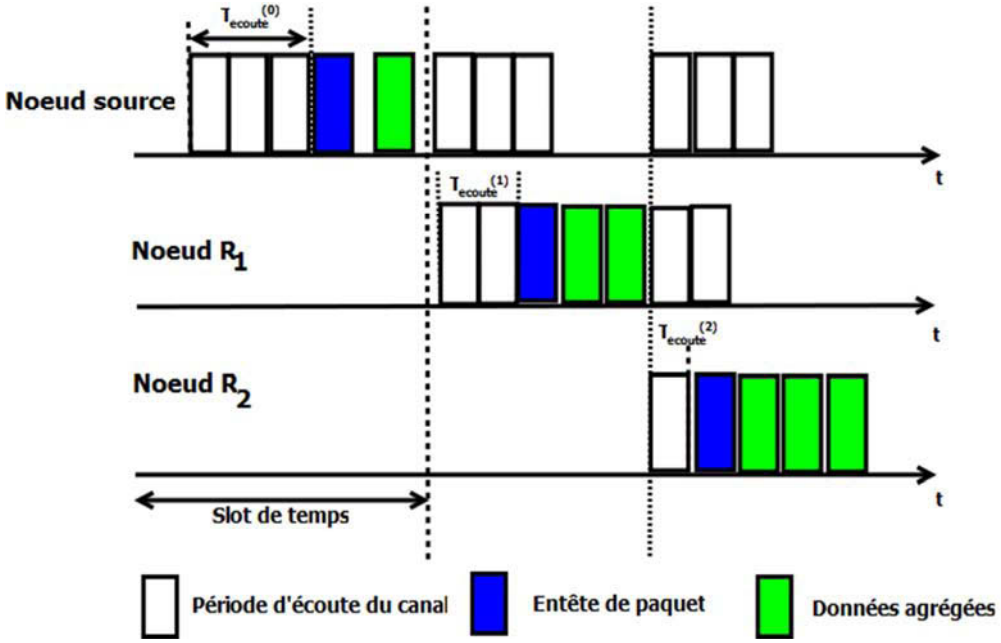


Figure 1. 12 – Négociation pour l'accès au canal entre deux nœuds adjacents.

Avec cette méthode, un nœud donné a toujours la priorité sur les nœuds en amont sur la ligne pour l'accès au canal ce qui diminue la zone de contention des nœuds. Cette technique diminue donc les collisions de trames entre nœuds concurrents et par conséquent diminue les délais de bout-en-bout.

6.3.3. Le protocole PRI-MAC (pipelined-forwarding, Routing-integrated, and effectively-Identify MAC)

PRI-MAC (Tong et al., 2013) est un protocole MAC pour les réseaux linéaires de surveillance de pipeline. Ce protocole intègre des fonctions de routage pour minimiser les échanges dans le réseau et supporte plusieurs stations de collecte le long du pipeline pour la gestion du

passage à l'échelle. Il se base principalement sur deux notions pour la gestion de l'accès et des ressources des nœuds capteurs.

- Le niveau d'un nœud qui permet de subdiviser le réseau en groupes de nœuds pour gérer l'aspect dynamique du réseau comme la déconnexion des nœuds et le relai des données collectées.
- Un cycle réveil-sommeil permettant de relayer les données le long du pipeline tout en diminuant les délais de bout-en-bout.

La création des niveaux se fait durant la phase d'initialisation du réseau et est initiée par le puits qui est au niveau 0. Un niveau est calculé en fonction du nombre de sauts du nœud au puits et l'acheminement des données se fait du niveau le plus élevé jusqu'au puits. À l'initialisation du réseau, le puits diffuse une trame appelée "GRADE Message" qui contient toutes les informations de création de niveaux, de synchronisation des nœuds au sein des niveaux et entre les niveaux adjacents. Un nœud donné, il peut changer de niveau au cours du cycle de vie du réseau. La figure 1.13 est un exemple de découpage du réseau en plusieurs niveaux.

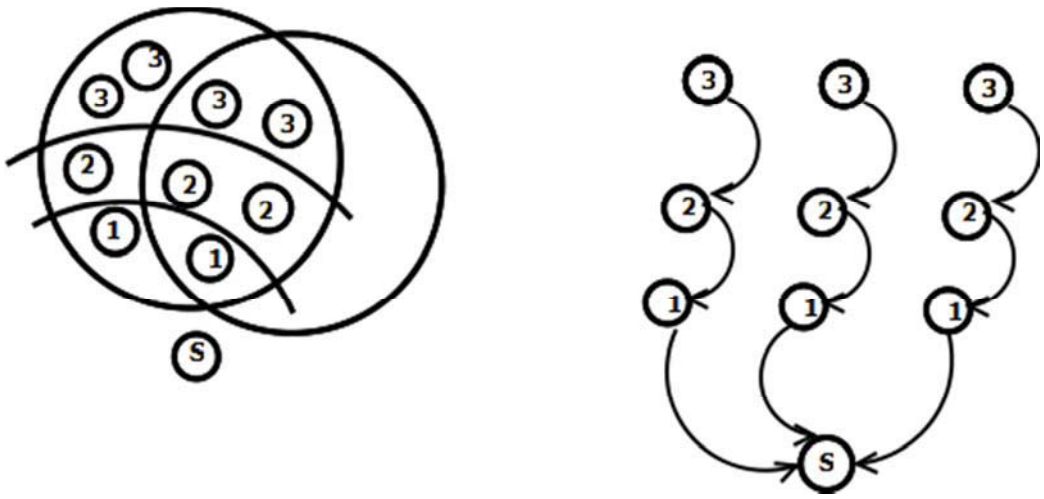


Figure 1. 13 - Découpage d'un réseau linéaire en niveaux.

Les niveaux sont représentés par les numéros sur les nœuds et les cercles représentent les différents niveaux. Quand un nœud prend connaissance de son niveau, il établit ainsi un cycle réveil-sommeil pour la transmission et la réception des données. Les nœuds du même niveau

maintiennent le même cycle et les cycles sont décalés d'un niveau à l'autre. Un cycle se divise en trois périodes principalement : (i) une période de réception durant laquelle le nœud reçoit les données de ses voisins du niveau supérieur ; (ii) une période de transmission durant laquelle le nœud transmet des données à ses voisins du niveau inférieur ; (iii) une période de sommeil où le nœud éteint son module radio. Pour minimiser les délais de bout-en-bout et augmenter les débits au puits, dans PRI-MAC si un niveau est en mode émission alors le niveau adjacent inférieur est en mode réception.

L'accès au canal de transmission entre des nœuds du même niveau se fait par contention en utilisant une variante du mécanisme du RTS/CTS défini dans 802.11. En effet, dans PRI-MAC le paquet RTS contient un champ qui stocke le numéro de niveau du nœud qui souhaite accéder au canal. En outre, dans PRI-MAC les adresses MAC des nœuds sont dynamiques et changent à chaque cycle.

6.3.4. Le protocole ADC-SMAC (*Adaptive Duty Cycle SMAC*)

Le protocole ADC-SMAC (Lin et al., 2004) est une variante du protocole S-MAC à *duty cycle* dynamique conçu et testé pour une topologie linéaire. S-MAC (Van Dam and Langendoen, 2003) est l'un des premiers protocoles MAC à « *duty-cycle* » conçu pour des réseaux multi-sauts. Chaque nœud commute périodiquement entre une période active et une période inactive pour économiser l'énergie. Au début, chaque nœud est libre de choisir son propre « *duty-cycle* ». Afin qu'un nœud émetteur puisse trouver un nœud routeur voisin pendant sa période active, S-MAC adopte la synchronisation suivante. Chaque nœud diffuse périodiquement vers ses nœuds voisins son ordonnancement des périodes actives et inactives. Ainsi, chaque nœud mémorise les ordonnancements de tous ses voisins afin de savoir quand un voisin particulier entrera dans sa période active pour lui transmettre ses trames de donnée. Si plusieurs nœuds doivent transmettre leurs trames à un même nœud routeur ou récepteur, ils utilisent le CSMA/CA de IEEE802.11, y compris RTS/CTS. Le nœud qui diffuse en premier son ordonnancement est un nœud synchroniseur et les nœuds voisins sont des nœuds suiveurs. Néanmoins S-MAC présente deux limites majeures.

- La première est qu'il s'agit d'un protocole à « *duty cycle* » fixe et qui ne s'adapte pas automatiquement à la variation du trafic, seul un nœud le modifie explicitement en devenant un nouveau synchroniseur (mécanisme non prévu dans S-MAC).
- La deuxième limite est que le délai de bout en bout dépend de la période de chaque nœud du chemin, ce qui peut être très long.

ADC-SMAC propose de corriger ces problèmes de S-MAC en proposant un *duty-cycle* dynamique. Il se base principalement sur deux paramètres réseaux: le taux d'utilisation du nœud durant le dernier cycle et la durée moyenne de sommeil. Suivant les valeurs de ces deux paramètres alors il va décider d'ajuster ou non son *duty-cycle* et le diffuser à ses voisins via la trame de synchronisation. Le taux d'utilisation du nœud est donné par la formule:

$$U = \frac{T_{rx} + T_{tx}}{T_{rx} + T_{tx} + T_{idle}}$$

où $\boldsymbol{T_{rx}}$, $\boldsymbol{T_{tx}}$ et $\boldsymbol{T_{idle}}$ signifient respectivement le temps de réception, le temps d'émission et le temps *d'idle listening*.

La durée moyenne de sommeil du nœud est donnée par la formule:

$$\overline{D} = \frac{D}{packet\ count}$$

où $\boldsymbol{D}$ et *packet count* représentent respectivement la durée totale de sommeil durant un cycle et le nombre total de paquets reçus pendant ce cycle.

L'algorithme d'ajustement du duty-cycle procède comme suit. Si $\boldsymbol{U}$ est supérieur à la valeur du seuil maximal de taux d'utilisation $\boldsymbol{U_{seuilmax}}$ fixé et le *duty-cycle* actuel supérieur au seuil maximal de *duty-cycle* $\boldsymbol{DC_{max}}$ alors on augmente de *duty-cycle* d'une valeur *n%* choisi (*n* dépend des besoins de l'application). Si le *duty-cycle* est inférieur au seuil minimal de *duty-cycle* fixé et la durée moyenne de sommeil inférieure à la durée de sommeil maximale fixée, alors on diminue le duty-cycle de *n%.*

Avec cet algorithme, ACD-MAC réajuste le *duty-cycle* d'un nœud donné en fonction de la charge offerte par le réseau. Donc à forte charge, il est plus opportun d'augmenter le *duty-cycle* du nœud afin d'augmenter le débit au puits et diminuer les délais de bout-en-bout. En faible charge, diminuer le *duty-cycle* permet d'économiser l'énergie en évitant l'écoute passive du nœud.

6.4. Les protocoles hybrides

Une troisième famille de protocoles propose de combiner les deux méthodes : TDMA et CSMA/CA. Ainsi, ces protocoles essaient d'avoir les avantages des deux méthodes en alternant les deux dans le temps ou en les combinant d'une manière intelligente.

Le protocole EEDA-MAC (Yu and Guo, 2015) (*Energy-Efficient and Delay-Aware MAC*) est un protocole MAC hybride utilisé dans les réseaux de capteurs sans fil linéaires pour la surveillance de pipeline de gaz. EEDA-MAC divise le réseau linéaire en clusters. Les nœuds basiques envoient leurs données aux *clusterheads* qui se chargent de l'acheminement des informations au puits. L'accès au canal entre les nœuds d'un même cluster se fait en utilisant CSMA/CA. Pour l'acheminement des données agrégées par les *clusterheads*, l'accès au canal se fait en utilisant CSMA/TDMA.

Les slots de temps sont divisés en trois parties : un slot pour la réception, un slot pour la transmission et un slot pour le sommeil. Durant la réception, les autres nœuds *clusterheads* utilisent le CSMA/CA pour lui envoyer les données. La figure 1.14 montre le principe de fonctionnement des communications dans EEDA-MAC.

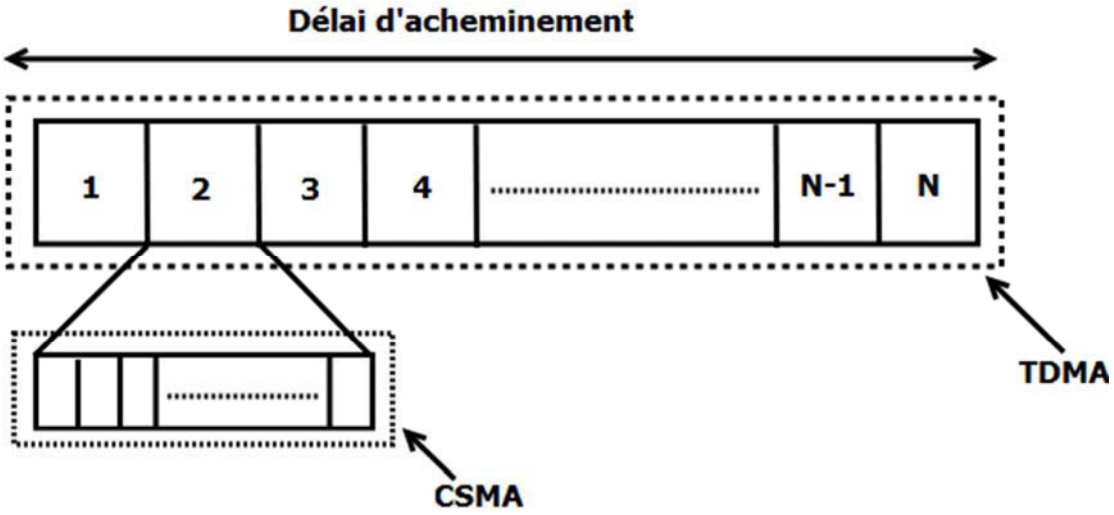


Figure 1. 14 - Processus de communication dans EEDA-MAC.

7. Les protocoles de routage pour réseaux de capteurs linéaires

La gestion de l'acheminement des données ou le routage consiste à trouver une méthode qui garantit la connectivité entre les nœuds du réseau. Dans les réseaux de capteurs sans fillinéaires, la stratégie doit prendre en considération les caractéristiques spécifiques du réseau comme la linéarité, le voisinage. En outre, la méthode adoptée dans le routage, doit offrir le meilleur acheminement des données en respect des métriques de performances considérées. Dans la suite, nous allons présenter quelques protocoles réseaux utilisés dans les réseaux de capteurs sans fillinéaires.

7.1. Le protocole MERR (*Minimum Energy Relay Routing*)

MERR (Zimmerling et al., 2008) est un protocole de routage économe en énergie pour réseaux de capteurs sans fil linéaires. C'est un protocole non hiérarchique basé sur le plus court chemin. Il est conçu pour un environnement où le déploiement des nœuds est aléatoire sur la ligne. Les nœuds capteurs ont les mêmes caractéristiques matérielles et plus précisément les mêmes modules radio. Le protocole se base fondamentalement sur la distance caractéristique qui est définie comme la distance émetteur-récepteur à laquelle un émetteur consomme une énergie optimale. Elle est calculée en fonction des caractéristiques du capteur telles que la perte en chemin, l'énergie perdue par l'amplificateur du module radio ou encore l'énergie consommée par bit par l'émetteur.

Soit ***S*** un nœud source et ***BS*** la station de base, le calcul du nœud prochain saut A s'effectue de la manière suivante :

Si S et BS sont à portée et distant de ***D***. Alors si ***D*** est inférieur à la portée exprimée en mètre, il envoie directement les données à ***BS***. Sinon il choisit le prochain saut par ses voisins selon l'algorithme suivant. Pour chaque voisin à portée N_i, ***S*** calcule la distance qui le sépare de N_i. Il choisit alors le voisin N_i dont la distance est plus proche de la distance caractéristique comme le prochain saut.

Le protocole AMERR (*Adaptive MERR*) est une version adaptive de MERR. Si, dans MERR un nœud qui n'est pas à portée du puits n'a pas la connaissance de la distance ***D*** au puits, dans

AMERR tout nœud connait la distance ***D*** qui le sépare au puits. Cette information supplémentaire permet à AMERR de calculer le nombre optimal de sauts au puits en fonction de la distance caractéristique. Le calcul du nombre de saut optimal est détaillé dans (Zimmerling et al., 2008). Avec la connaissance du nombre optimal de sauts, AMERR calcule une distance dite adaptative qui correspond à la distance du nœud au prochain saut.

7.2. Les protocoles de routage hiérarchiques

Les protocoles de routage hiérarchiques sont aussi présents dans les réseaux de capteurs sans fillinéaires. Les protocoles de hiérarchiques se basent sur le partitionnement du réseau en un ensemble de *clusters* afin d'assurer un fonctionnement optimal du réseau par minimisation des ressources en termes d'énergie et de délais d'acheminement. L'implémentation de protocole hiérarchique se fait généralement en trois phases : une phase d'annonce et création des clusters, une phase d'ordonnancement et une phase de transmission. Dans (Jawhar and Mohamed, 2009), les auteurs présentent un protocole de routage hiérarchique pour un réseau de capteur pour surveillance de pipelines à topologie hiérarchique. Comme dans (Jawhar et al., 2011), on trouve des nœuds basiques BSN (*Basic Sensor Node*), des nœuds relais DRN (*Data Relay Node*) et des nœuds d'acheminement des données DDN (*Data Dissemination Node*). L'adressage des nœuds se fait de manière hiérarchique en fonction des niveaux des nœuds. Ainsi, les nœuds DDN ont des adresses de la forme ***NUM_OF_DDN*** où ***NUM_OF_DDN*** est une variable entière qui représente le numéro du DDN dans la liste de nœuds DDN. Les adresses de DRN sont de la forme ***NUM_DRN_PER_DDN*** alors que celles des BSN sont de la forme ***NUM_BSN_PER_DRN***.

La figure 1.15 illustre un exemple d'adressage dans le réseau linéaire considéré. Le nœud BSN mis en évidence est associé au DRN 2 qui lui-même associé au DDN 1. Par conséquent, son adresse est *2.2.1*.

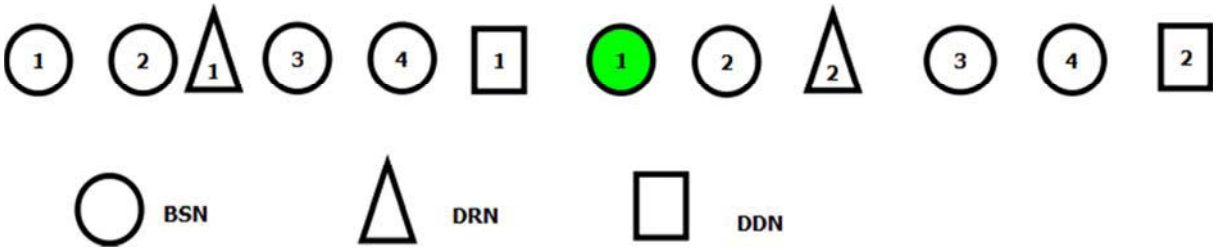


Figure 1. 15 - Illustration de l'adressage hiérarchique.

La communication entre les nœuds se fait de façon hiérarchique sur plusieurs niveaux.

- La communication de BSN à DRN: cette communication est de type *single hop* car les nœuds BSN sont à portée de leur DRN.
- La communication entre DRN et DDN: les nœuds communiquent en utilisant le protocole de routage de Zigbee.
- La communication entre les nœuds DRN: dans cette communication chaque DRN établit une liste de ses voisins directs. Cette liste est mise à jour périodiquement dans le but de gérer les déconnexions des nœuds. Dans le cas où le nœud ne parvient pas à joindre ses voisins directs, (défauts de lien, déconnexion, etc.) deux algorithmes sont proposés pour gérer ce problème : (i) l'algorithme JA (*Jump Always*) dans lequel le nœud augmente sa puissance de transmission afin d'atteindre des nœuds plus lointains. Lorsque le nœud atteint la puissance maximale de transmission sans joindre des voisins alors il « droppe » le paquet en cours ; (ii) l'algorithme RA (*Redirect Always*) est basé sur la redirection des messages. Quand un nœud DRN tombe sur un lien défectueux alors il vérifie si le message en sa possession n'est pas déjà redirigé. Cette information se trouve dans un champ de l'entête du paquet. Si le message est déjà redirigé alors il le supprime, sinon il envoie un message à la source pour l'informer du défaut de lien. Cette dernière renvoie le message en passant par une autre direction.

Un protocole de routage et d'adressage pour des réseaux de capteurs sans fil linéaires longs est proposé dans (Pan et al., 2008). Il est basé sur le protocole de routage de Zigbee et subdivise le réseau linéaire en clusters. Un cluster est composé d'un *clusterhead* qui est le nœud le plus proche du coordinateur, un nœud pont, qui est le plus lointain du coordinateur et des nœuds capteurs basiques. Le nœud pont a la particularité de pouvoir dialoguer avec le *clusterhead*

d'un cluster parmi les clusters fils de l'arborescence du réseau. Après la formation du réseau et l'assignation des différents rôles, le processus d'adressage se fait selon le modèle Zigbee. Ainsi, l'adresse logique d'un nœud formé de 16 bits est divisée en deux parties: une partie représentant l'adresse du cluster et une partie représentant l'adresse du nœud dans le cluster. Le calcul de l'adresse des clusters se fait en utilisant la formule décrite pour Zigbee. Le calcul et l'assignement des adresses des nœuds se font grâce à des requêtes envoyées par les nœuds. Ces requêtes sont traitées différemment soit par les nœuds basiques soit par les nœuds ponts (nœuds relais).

L'établissement de la table de voisinage pour un nœud se fait en utilisant des paquets HELLO. Si un nœud reçoit un paquet avec la destination (C_{dest}, N_{dest}) où C_{dest} est le numéro de cluster et N_{dest} , le destinataire, il le traite. Sinon, il applique les règles suivantes.

- Si le destinataire est dans sa liste de voisins directs, alors il transmet directement le paquet à ce voisin.
- Si le destinataire est dans le même cluster mais pas à portée du nœud, alors il relaie le paquet au nœud de son voisinage le plus proche de la destination.
- Si C_{dest} n'appartient pas au cluster, alors il applique les formules spécifiques pour lr routage de Zigbee pour envoyer les données au *clusterhead* ou au pont selon la position du cluster de destination.

Cette façon d'acheminer les données jusqu'au puits requiert que les nœuds *clusterheads* et les nœuds relais soient tout le temps opérationnels. Cette condition n'est pas tout le temps vérifiée au vu des conditions de propagation aléatoires qui peuvent affecter la connectivité. De plus les caractéristiques matérielles ou logicielles font que les nœuds dysfonctionnent au cours de la durée de vie du réseau. Dans le cas où ce dysfonctionnement concerne les *clusterheads* ou les relais, l'acheminement des données se limite au sein des clusters.

Le protocole DiscoProto (Sarr et al., 2012) propose une technique d'adressage et de routage dynamique basée sur une découverte dynamique des voisins dans un réseau en arbre. La découverte de voisinage se fait à l'initialisation du réseau avec des envois de messages HELLO. Ce processus est répété périodiquement par les nœuds du réseau. La phase d'association se fait à la réception d'un message de type *FatherOffer* qui permet à un nœud de s'associer à un sous-arbre. Il procède d'abord à la collection des nœuds du sous-arbre et si

aucun autre nœud ne répond au message *FatherOffer* par un message *ChallengeOffer* alors il procède à la recherche d'une adresse dans le sous-arbre.

Les adresses sont attribuées de façon hiérarchique par le coordonnateur. Grâce à la propagation de messages entre les nœuds d'un sous-arbre, chaque nœud coordonnateur d'un sous-arbre a connaissance de la taille du sous-arbre. Cette information relayée au coordonnateur principal du réseau lui permet de connaitre la taille du réseau et le nombre d'adresses à attribuer. Quand un coordonnateur de sous-arbre reçoit un bloc d'adresses, alors il délimite sa plage d'adresse de la forme $[a_1+1, a_1+R]$ en fonction de la taille du sous-arbre en s'octroyant la première adresse. R représente la taille du sous-arbre.

8. Conclusion

Dans ce chapitre, nous avons fait un état de l'art sur les réseaux de capteurs sans fil linéaires. Nous avons introduit les caractéristiques de ce type de réseaux telles que le voisinage limité, les possibilités de routage limitées ou encore les zones de couverture longues. Les applications de ces réseaux de capteurs sans fil linéaires sont nombreuses et variées. Nous avons présenté les applications de surveillance les plus usuelles comme la surveillance de pipelines, de route, de train ou encore de frontière. Les caractéristiques spécifiques de ces réseaux font que les recherches de ces dernières années se sont focalisées sur des méthodes d'accès au canal et des techniques de routage adaptées à la linéarité. Par conséquent, nous avons fait un état l'art des protocoles MAC utilisés dans les réseaux de capteurs sans fil linéaires en listant ceux basés sur la contention et ceux basés sur la synchronisation temporelle. Nous nous sommes consacrés ensuite aux protocoles de routage correspondants.

Dans le chapitre suivant, nous proposons deux contributions relatives aux méthodes d'accès : (i) une méthode basée sur la contention consistant en l'intégration du mécanisme RTS/CTS de 802.11 dans le CSMA/CA non slotté de 802.15.4 dans le cas des réseaux de capteurs sans fil linéaires ; (ii) une méthode d'accès basée sur la synchronisation gérée par un jeton qui va donner à un nœud le droit d'accès au canal de transmission.

Contribution relative aux méthodes d’accès

1. Introduction

Nous avons vu que le rôle d'un protocole MAC est la gestion du canal de transmission en proposant des mécanismes d'accès qui améliorent les performances globales du réseau. Dans les réseaux de capteurs sans fil linéaires, les protocoles MAC doivent assurer de bonnes performances relatives aux délais de bout-en-bout et au taux de délivrance des paquets grâce à un accès protégé et efficace au canal. Les protocoles MAC les plus utilisés dans les réseaux linéaires se basent principalement sur la contention et la synchronisation des nœuds comme montré dans le chapitre précédent.

Dans ce chapitre, deux contributions majeures relatives aux méthodes d'accès sont proposées. La première contribution consiste en une intégration du mécanisme RTS/CTS de 802.11 dans la version non slottée du CSMA/CA de 802.15.4 pour un réseau de capteurs sans fil linéaire. Il s'agit d'évaluer dans ce contexte l'apport du mécanisme RTS/CTS dans la contention pour le cas du CSMA/CA. La deuxième contribution est relative à un protocole basé sur la synchronisation des nœuds grâce à l'utilisation d'un jeton. Celui-ci est une trame contenant des informations temporelles sur les temps d'activité et d'inactivité des nœuds. Nous estimons par la suite les performances des protocoles proposés en termes de taux de délivrance, de débit remis au puits et de délais de bout-en-bout afin de déterminer leur pertinence pour les réseaux de capteurs sans fil linéaires.

2. Intégration du mécanisme RTS/CTS dans 802.15.4 non slotté

Dans un environnement sans fil, on ne peut pas être sûr que toutes les stations s'entendent entre elles, et le fait que la station voulant transmettre teste si le support est libre, ne veut pas forcément dire que le support est libre autour du récepteur. Deux stations situées chacune à l'opposé d'une autre station peuvent chacune entendre l'activité de cette dernière mais pas l'une de l'autre car la distance entre elles est trop grande ou un obstacle empêche de communiquer entre elles. Ce phénomène expose le réseau à des collisions, des retransmissions et par conséquent à une dégradation des performances. Ce problème est connu sous le nom de terminal caché.

Le problème du terminal caché est très fréquent dans les réseaux sans fil utilisant CSMA/CA comme méthode d'accès au canal de transmission. Pour résoudre ce problème, le standard 802.11 définit dans la couche MAC le mécanisme RTS/CTS (*Request to send/Clear to Send*) appelé mécanisme de *Virtual Sense* (signal d'occupation virtuel). Une station voulant émettre transmet d'abord une petite trame de contrôle appelé RTS qui porte la source, la destination et la durée de la transaction. La station destinataire répond avec une trame de contrôle appelée CTS, qui inclut les mêmes informations. Ainsi, les stations recevant soit le RTS ou soit le CTS, déclencheront leur indicateur de *Virtual Carrier Sense* pour une certaine durée.

L'objectif de cette partie de nos travaux est d'intégrer le mécanisme RTS/CTS dans la version non slotté du CSMA/CA de 802.15.4 pour un réseau de capteurs sans fil linéaire. Il s'agit d'abord de définir les hypothèses sur lesquelles nous basons notre étude. Ensuite, nous faisons une description de la problématique liée au mécanisme RTS/CTS de 802.11. Puis, nous redéfinissons les algorithmes d'émission intégrant le mécanisme RTS/CTS. Enfin, nous présentons le comportement des files d'attente des nœuds dans le réseau linéaire à travers un modèle de registres à décalage afin de comprendre l'effet de l'intégration du RTS/CTS sur le nombre de paquets supprimés dans le réseau de capteurs sans fil linéaire.

2.1. Hypothèses

On considère un réseau unidimensionnel formé des ***N*** nœuds capteurs et un puits distribués de façon fixe dans un milieu homogène. La distance entre deux nœuds adjacents est égale à *d*. On suppose que tous les nœuds capteurs ont les mêmes caractéristiques matérielles (processeur, mémoire, module radio, etc.) et logicielles (couche physique, MAC, réseau, etc.). Chaque nœud a un rôle de collecteur de données et aussi de relayeur de paquets. L'agrégation des donnés se fait du nœud le plus lointain vers le puits et le routage des données se fait de proche en proche. Les files d'attente sont gérées de manière FIFO et suivant la nature et le sens de circulation des données, une FIFO peut contenir plusieurs types de trafic.

- Un trafic local généré par l'application de surveillance du milieu considéré. Ce trafic est généré par intervalle de temps bien défini.

- Un trafic relayé par son voisin direct en direction du puits.

La couche physique considérée ici est la couche physique de 802.15.4 à 2.4 GHz. On considère le modèle de propagation *Tworayground* (Goldsmith, 2005) dans lequel la puissance de réception est considérée constante pour une puissance d'émission donnée.

2.2. Le problème du terminal caché

Deux problèmes spécifiques aux réseaux de capteurs sans fil sont le problème du terminal caché et celui du terminal exposé. Lorsqu'ils souhaitent communiquer en même temps avec un même nœud, les nœuds commencent par écouter le canal radio. Étant hors de portée l'un de l'autre, ils ne détectent pas d'activité et peuvent donc émettre en même temps. Dans ce cas, les émissions simultanées de ces stations peuvent générer des collisions. La figure 2.1 est une illustration du phénomène du terminal caché. Deux stations A et B qui ne se voient pas, voient par contre toutes les deux une troisième station C. Si A et B veulent quasi-simultanément envoyer des trames à C, A ne voyant pas B et B ne voyant pas A, elles pensent toutes les deux que le medium pour envoyer des informations à C est libre après avoir effectué leur CCA (*Clear Channel Assessment*) (Jordan and Abdallah, 2002). Dans ce cas, des collisions de trames vont survenir dans cette portion du réseau.

Le phénomène du terminal exposé quant à lui survient quand un nœud attend la fin de la transmission d'un autre nœud à portée alors que son nœud récepteur n'est pas à portée du nœud émetteur courant. Ce problème est un résultat de l'utilisation d'antennes omnidirectionnelles et va se traduire par une introduction de délais dans une communication. La figure 2.2 montre une situation de terminal exposé. Le nœud A est entrain de communiquer avec D, le nœud B ne peut pas communiquer avec C car il détecte la communication A->D. Cependant, cette communication B->C pourrait tout à fait avoir lieu. En effet, si les nœuds A et B émettent en même temps cela n'aura pas d'influence au niveau des destinataires car ils sont très éloignés. Les deux communications sont donc possibles car elles ne génèrent pas d'interférences significatives au niveau des récepteurs concernés.

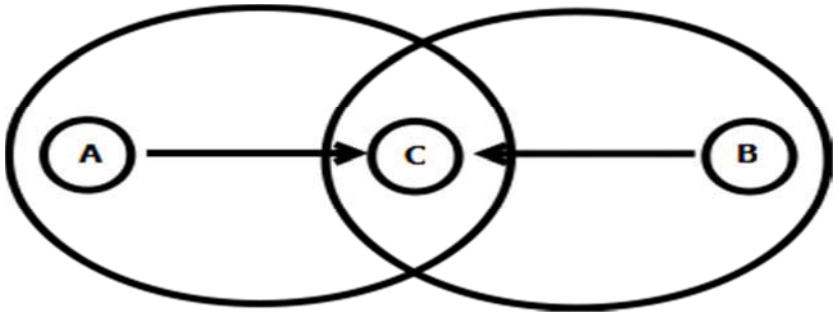


Figure 2. 1 - Problème de stations cachées.

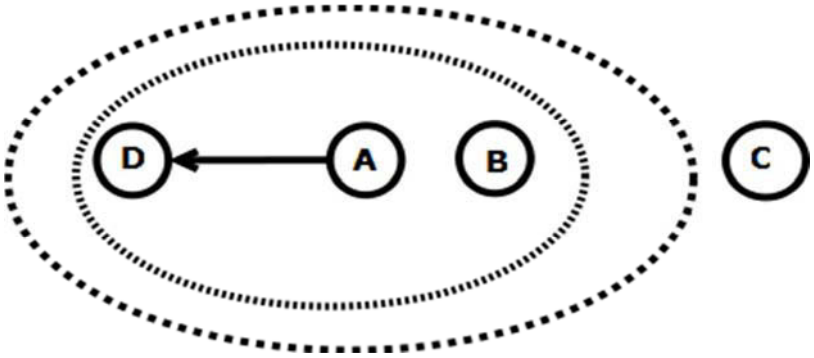


Figure 2. 2 - problème du terminal exposé.

Le terminal caché peut avoir plusieurs conséquences néfastes dans le cas d'un réseau de capteurs sans fils. En effet, il peut être source d'*overhearing*, de retransmission, et de consommation inutile de ressources. Quant au phénomène du terminal exposé les inconvénients sont liés à des pertes de débit et des délais longs.

Une solution pour résoudre le problème du terminal exposé qui nécessite pas de modification de la méthode d'accès au canal, est d'utiliser des antennes directionnelles. En effet, avec ce type d'antenne, le nœud B ne détectera pas la communication A->D et pourra donc émettre simultanément vers C.

Pour la gestion du terminal caché, 802.11 a mis sur place le mécanisme RTS/CTS qui assure une réservation du canal pendant laquelle les stations pouvant interférer avec le récepteur n'émettront pas.

2.3. Le mécanisme RTS/CTS

Pour éviter les effets du terminal caché préjudiciable pour des trames longues (où les retransmissions coûtent du temps et la ressource spectrale), le standard 802.11 définit le mécanisme optionnel du RTS/CTS qui permet de faire des réservations de canal. Ce mécanisme est appelé écoute virtuelle de porteuse. Une station voulant émettre transmet d'abord une petite trame de contrôle appelé RTS, qui porte la source, la destination, et la durée de transmission (c'est-à-dire la durée totale de la transmission de la trame et de son accusé de réception). La station destination répond (si le canal est libre) avec une trame de contrôle de réponse appelé CTS qui porte aussi les mêmes informations sur la durée. Toutes les stations écoutant soit la trame de demande de réservation du canal, soit la trame de réponse de réservation CTS, déclenchent leur indicateur de l'écoute virtuelle (*Virtual Carrier Sense*) appelé NAV pour *Network Allocation Vector* pour la durée de l'échange annoncée par ces nœuds. Grâce à l'envoi de la trame RTS, toutes les stations situées dans la couverture radio de la source sont informées d'une transmission imminente et de sa durée éventuelle. Elles peuvent ainsi mettre à jour leur NAV et passer en mode économie d'énergie pour la dite durée. Le CTS a le même rôle d'annonce mais cette fois autour du récepteur. Ces deux trames sont courtes (20 octets pour RTS et 14 octets pour CTS) et rencontrent donc une faible probabilité de collisions. Ce mécanisme quoique efficace entraîne un surcoût important occasionné par la transmission sur la voie radio des trames de signalisation RTS/CTS. Ce surcoût correspond à autant de bande passante qui n'est pas utilisée pour transmettre des données. C'est pourquoi à ce mécanisme est associé un seuil de déclenchement qui en limite l'usage lorsque le surcoût devient trop important. Si la longueur des données à transmettre est inférieure à ce seuil, la transmission se fera sans utilisation des trames RTS/CTS. Si le seuil est dépassé alors le mécanisme est utilisé pour la transmission. La figure 2.3 suivante illustre l'usage du RTS/CTS et du NAV.

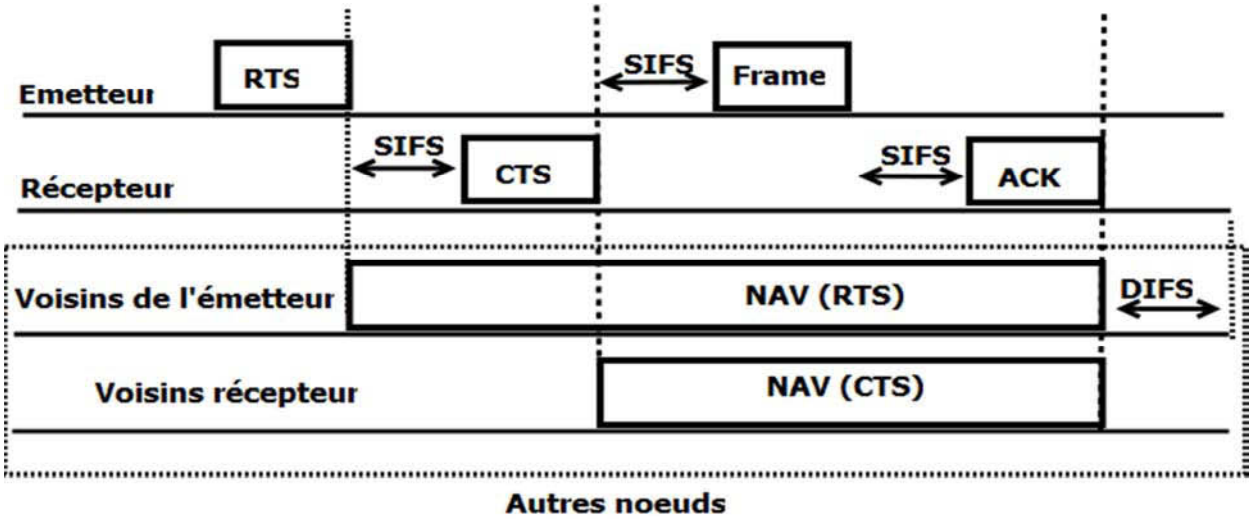


Figure 2. 3 - Le mécanisme de RTS/CTS.

La norme 802.11 définit quatre types d'espace entre deux trames IFS (*Inter Frame Space*). Ils sont classés du plus court au plus long : Le premier, le SIFS (*Short IFS*) est le plus court de tous. Il est utilisé pour la transmission des trames ACK, CTS, etc., lors de la segmentation au niveau trame. Le second PIFS (*PCF IFS*) est utilisé en mode PCF (*Point coordination function*). Il permet aux transmissions PCF de gagner l'accès au médium par l'utilisation d'un IFS plus petit que celui utilisé pour la transmission des trames en DCF (*Distributed Coordination Function*). Le troisième DIFS (*DCF IFS*) est le plus couramment utilisé (avec le SIFS). Il est utilisé en mode DCF (IEEE, 2005) comme temps minimal d'attente avant transmission. Enfin, le quatrième et plus long EIFS (Extended IFS) est utilisé lorsqu'il y a détection de collision. Ce temps relativement long par rapport aux autres IFS est utilisé comme inhibiteur pour éviter des collisions en série.

Ce mécanisme RTS/CTS permet donc de réduire la concurrence entre terminaux cachés mais ne les supprime pas complètement. En effet, dans certaines situations il est possible qu'il y'ait des collisions entre des trames RTS et/ou CTS. La figure 2.4 illustre un exemple de collisions de trames RTS et CTS. Comme indiqué, A veut communiquer avec B et envoie une trame RTS pour accéder au canal de transmission. Le nœud détectant le canal libre, envoie alors une

trame CTS à A qui sera entendu dans le voisinage. Il est possible qu'au même instant, le nœud D qui n'est pas à portée de B envoie une trame RTS à C qui voit arriver deux signaux en même temps. Ces deux signaux vont interférer et finissent par être indéchiffrables pour le nœud C qui ne sera finalement pas informé des transmissions des trames de données de A. À la fin du temporisateur de RTS de D, celui-ci renvoie à nouveau un RTS à C qui répondra par un CTS. En conséquence, il y'a de fortes chances qu'il y'ait collision entre trames de données et CTS au niveau de B.

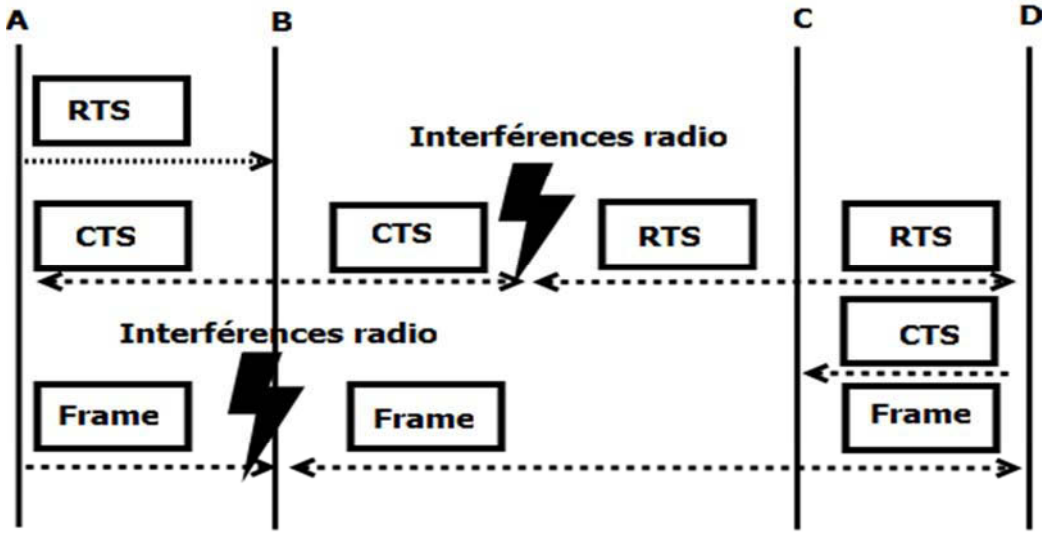


Figure 2. 4 – Exemple d'échec.

L'intégration du mécanisme RTS/CTS dans une version du CSMA/CA est un bon moyen d'éliminer le terminal caché dans un réseau de capteurs sans fil linéaire. En effet, les caractéristiques particulières des réseaux de capteurs sans fil linéaires telles que la disposition des nœuds, leur voisinage et les routes pour l'acheminement des données limitées font que le terminal caché peut avoir des conséquences plus drastiques comparé au réseaux classiques.

Dans ce qui suit, nous allons étudier l'intégration du RTS/CTS dans une version de CSMA/CA non slotté afin de déterminer le gain en termes de collisions et de comportement des files d'attente. Nous évaluerons la pertinence de l'utilisation des accusés de réception avec un tel mécanisme dans le cas spécifique d'un réseau de capteurs sans fil linéaire si l'on sait que les trames RTS, CTS et ACK contribuent à la surcharge du réseau et peuvent affecter les

délais d'acheminement qui constituent un critère de performance très important dans les réseaux de capteurs sans fil.

2.4. Intégration du mécanisme RTS/CTS dans le CSMA/CA non slotté de 82.15.4

L'intégration du RTS/CTS consiste à modifier les algorithmes d'émission et de réception du CSMA/CA en mode « *non beacon enable* » afin que les nœuds puissent faire une réservation du canal avant toute transmission de trames de données. Dans la suite, nous expliquons le choix porté sur le CSMA/CA non slotté et présentons les algorithmes d'émission et de réception intégrant le mécanisme du RTS/CTS. Un modèle construit à base de registres à décalage sera introduit pour expliquer la façon dont les files d'attente des nœuds se remplissent et/ou saturent.

2.4.1 Le choix de la version non slotté du CSMA/CA

Le choix porté sur le CSMA/CA s'explique d'abord par le fait que cette méthode d'accès correspond au mieux au type de réseau de capteurs sans fil linéaire étudié lorsqu'il s'agit de la contention. Ensuite, la difficulté de synchroniser les nœuds dans la version slottée fait que cette version n'est pas adaptée au réseau linéaire. Enfin, le cycle réveil-sommeil de la version slottée ne permet pas de minimiser les délais de bout-en-bout.

La difficulté de synchronisation : il est connu que l'un des problèmes de la version du CSMA/CA en mode slotté est sa difficulté d'implémentation due à la dérive des horloges des nœuds. En effet, le CSMA/CA de 802.15.4 n'implémente pas de mécanisme d'ajustement des horloges deux nœuds capteurs. La conséquence majeure de la dérive des horloges est la désynchronisation des nœuds qui entraine des pertes d'informations mais peuvent aussi provoquer des disfonctionnements pouvant allant jusqu'à mettre fin à la vie du réseau dans le cas précis des réseaux de capteurs sans fil linéaires.

Le cycle réveil-sommeil : les réseaux de capteurs linéaires pouvant s'étendre sur des milliers de kilomètres pour des applications de surveillance parfois très critiques (volcans, pipeline, etc.), il est primordial que les données collectées arrivent dans les meilleurs délais possibles pour être traitées. Le CSMA/CA de 802.15.4 en version slottée ou non, souffre déjà de la contention pour l'accès au canal qui augmente les délais de bout-en-bout. Donc, le cycle réveil-sommeil de la version slottée augmente davantage les délais d'acheminement et ne saurait être adapté pour un tel réseau même si elle permet d'économiser l'énergie.

Les trames balises : les trames de balises échangées lors de la synchronisation dans le CSMA/CA en version slottée peuvent surcharger le réseau dans le cas du réseau de capteurs sans fillinéaires utilisant RTS/CTS pour la réservation du canal de transmission. Donc, dans le souci d'alléger la charge du réseau, il est plus judicieux d'utiliser la version CSMA/CA en version non balise.

2.4.2 Algorithme d'envoi

Le nouvel algorithme d'émission des trames de données fonctionne comme suit. Quand un nœud veut envoyer une trame de donnée, il envoie d'abord un RTS. L'envoi de ce RTS se fait en utilisant l'algorithme CSMA/CA non slotté de 802.15.4. Si le canal est trouvé libre au bout de cinq tests d'occupation du canal, alors le nœud envoie le RTS. Si le nombre de tentatives dépasse cinq occurrences, alors la trame courante est droppée dans le souci de ne pas surcharger le réseau et de ne pas créer une congestion. Quand l'émetteur reçoit le CTS alors il envoie directement la trame de données au destinataire (au prochain saut) et ce dernier répond par un accusé de réception dès réception de la trame. La mise à jour de la NAV au niveau du récepteur est traitée dans l'algorithme de réception dans paragraphe suivant. Les trames RTS et CTS contiennent toutes les informations nécessaires à la réalisation des envois. Les périodes inter-trames comme SIFS et DIFS sont assimilées à une période de backoff de durée 320 µs et correspondent en réalité au temps nécessaire au module radio de passer de l'état réception à l'état transmission et vice-versa dans 802.15.4. Soit :

- T_{RTS}, le temps d'envoi d'une trame RTS,
- T_{CTS}, le temps d'envoi d'une trame CTS,

- T_{ACK}, le temps d'envoi d'un acquittement,
- T_A, le temps nécessaire pour le module radio de passer d'un état à un autre. Il est égal à une période de backoff,
- T_{Data}, le temps d'envoi d'une trame de données.

À l'envoi d'une trame RTS, l'émetteur déclenche un temporisateur d'attente de RTS égale à $T_{RTS} + T_{CTS} + T_A$. De même, après l'envoi de la donnée un temporisateur d'attente d'accusé de réception est déclenché avec une durée de $T_{Data} + T_{ACK} + T_A$. Le fonctionnement de l'algorithme d'envoi est décrit dans la figure 2.5 ci-dessous.

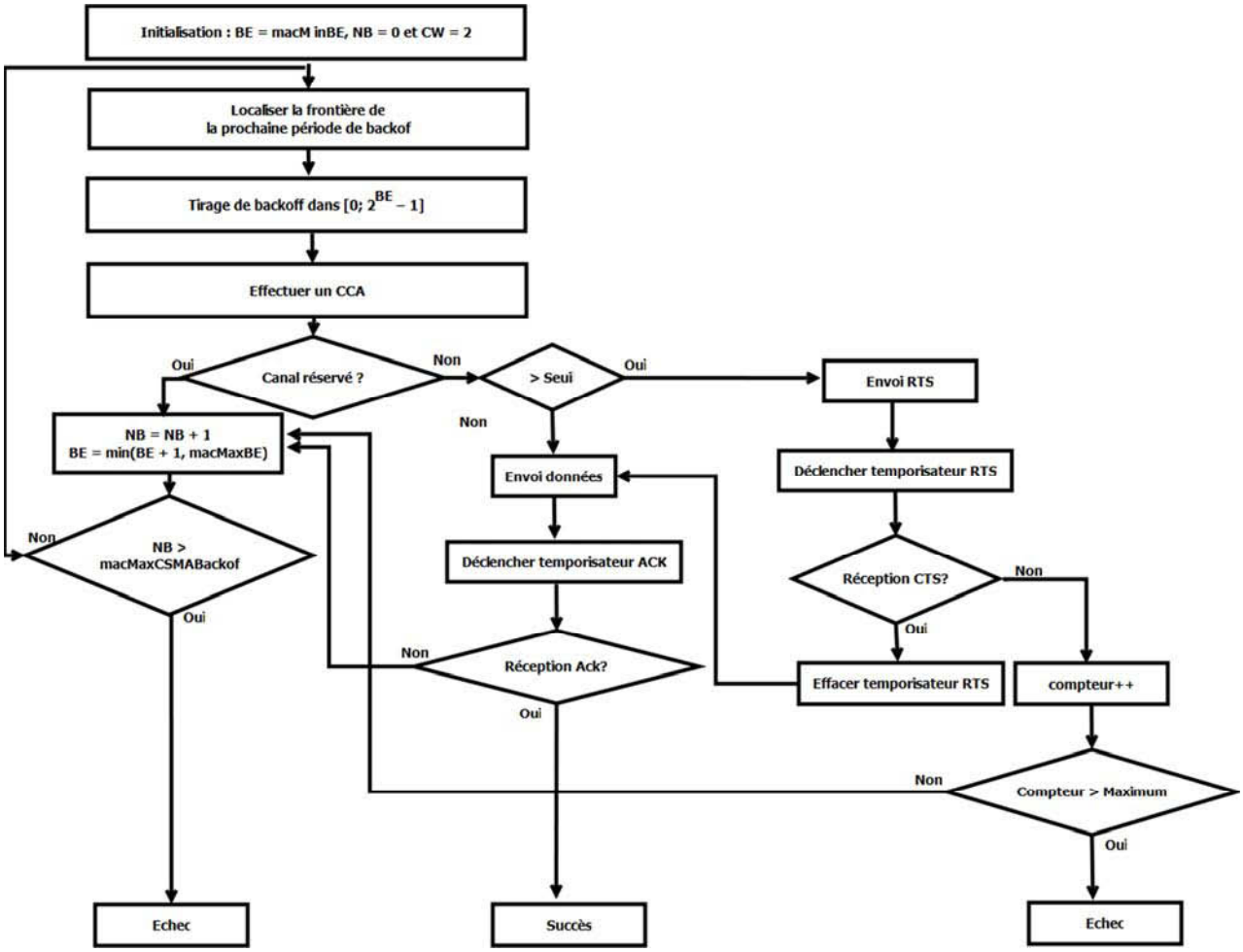


Figure 2. 5 - Algorithme d'envoi.

2.4.3 Algorithme de réception

L'algorithme de réception fonctionne comme suit. Quand un nœud reçoit une trame, il vérifie d'abord la nature de celle-ci. Si c'est une trame RTS alors il bloque le compteur backoff est en cours et vérifie la destination de la trame. S'il est le destinataire de la trame, alors il envoie directement une trame CTS et met à jour son NAV d'une durée égale à $T_{CTS} + T_{Data} + T_{ACK} + 2* T_A$. L'envoi de la trame de réponse CTS se fait sans nécessité d'utiliser le CSMA/CA. S'il n'est pas le destinataire de la trame RTS alors déclenche son NAV d'une durée $T_{CTS} + T_{Data} + T_{ACK} + 2* T_A$. Si la trame reçue est un CTS dont le nœud est le destinataire alors il émet sa trame de données et déclenche un temporisateur d'attente d'accusé de réception égale à $T_{Data} + T_{ACK} + T_{A.}$ Si le nœud n'est pas destinataire du CTS alors il bloque son compteur backoff s'il est en cours et met à jour son NAV d'une durée égale à $T_{Data} + T_{ACK} + 2* T_A$. Le fonctionnement de l'algorithme de réception est décrit figure 2.6.

Le fait de bloquer le compteur backoff en cours est fait pour des raisons d'économie d'énergie des nœuds capteurs. On suppose qu'un nœud qui reçoit une trame CTS ou RTS dont il n'est pas le destinataire durant la consommation de sa période de backoff bloque celle-ci jusqu'à la fin des échanges. Ainsi, à la prochaine période de contention, il continue à consommer la période de backoff qu'il a déjà tiré précédemment. Ceci lui permet d'éviter de recommencer le processus de tirage de backoff qui peut-être couteux dans la consommation.

Cette façon de réserver le canal de transmission dans le but d'éviter le phénomène du terminal caché permet de diminuer les zones de congestion dans la topologie linéaire. La congestion quant à elle est caractérisée par des débordements de files d'attente, des drops de paquets, des difficultés d'accès au canal de transmission. Le comportement des files d'attente dans le temps peut être analysé afin de voir l'apport du RTS/CTS dans le CSMA/CA.

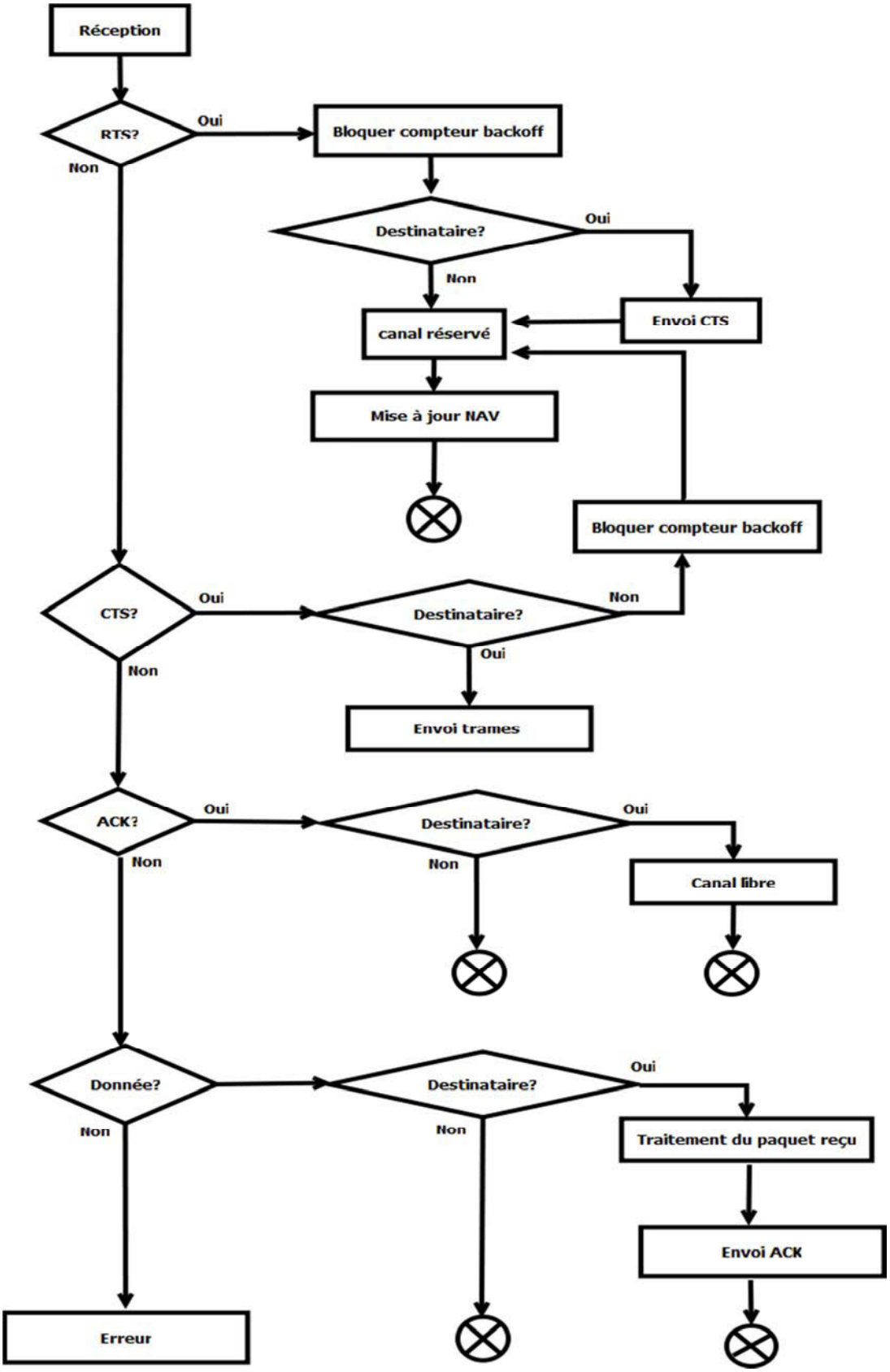


Figure 2. 6 - Algorithme de réception.

2.5. Analyse du comportement des files d'attente des nœuds par un modèle de registres à décalage

Dans cette partie, nous nous intéressons au comportement des files d'attente par une analyse à travers un registre appelé *leacky shift register*. L'objectif est de comprendre les causes principales de la congestion du réseau dans le cas de la méthode d'accès présentée et de définir par la suite une méthode de gestion des paquets dans les files d'attente. Plus précisément, il s'agit de prendre des décisions sur la suppression ou non de paquets dans les files d'attente dans le but d'alléger les charges du réseau et de prévenir ainsi la congestion. Comme indiqué dans nos hypothèses, un nœud reçoit en plus de son trafic local, un trafic descendant et montant de la part de ses voisins de gauche et droite sur la ligne. Ce qui signifie que chaque file FIFO est attachée au moins à deux autres files FIFO, à l'exception des nœuds d'extrémité du puits comme indiqué dans le modèle du *leacky shift register* de la figure 2.7. Dans ce modèle, certains paquets sont soit supprimés, soit perdus, d'où le nom de registre à décalage avec fuite. Le rôle du registre est de permettre de comptabiliser les nombres de paquets perdus, dans le temps pour une file d'attente donnée. Il existe principalement trois raisons de perte ou de supression de paquets.

- **La surcharge du médium** : ceci se produit quand un nœud en possession d'une trame de données trouve que le canal est occupé après cinq tentatives d'envoi de la trame RTS pour faire une réservation locale du canal. Dans ce cas, on dit que le paquet est supprimé.
- **Le débordement des files d'attente :** ceci se produit quand la limite du nombre de paquets que la FIFO peut contenir est dépassée. Ce phénomène se produit si le taux d'arrivée des paquets dans la file d'attente est supérieur au taux de départ. C'est peut-être le cas lorsque le trafic local est produit par intervalles de temps rapprochés dans des zones de congestion. On dit que le paquet est perdu par débordement de file d'attente.
- **Le nombre de retransmissions dépassé:** ce cas arrive quand un nœud ne reçoit pas d'accusé de réception après cinq envois de la même trame de données. Dans ce dernier cas aussi, on dit que le paquet est aussi perdu en raison de la qualité du lien radio.

L'accumulation de trafic dans les zones de congestion est une des causes principales des suppressions et pertes de paquets du fait que l'accès au canal devient difficile pour un nœud donné. Ces zones de congestions sont plus manifestes quand on s'approche du puits. Même pour un réseau de capteurs sans fil linéaire de petite longueur, les effets de la congestion sont drastiques pour les nœuds proches du puits comme en attestent les travaux de (Noori and Ardakani, 2008).

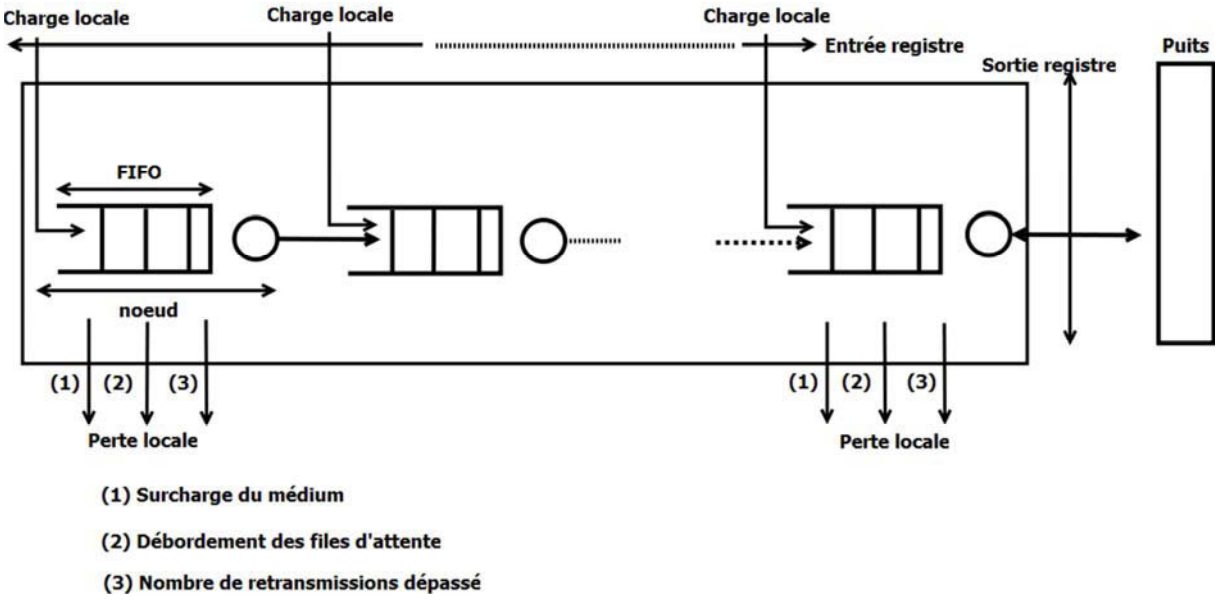


Figure 2. 7 - Représentation du modèle de registre à décalage avec fuite.

L'évaluation du comportement des files d'attente consiste à étudier l'impact des paramètres du registre tels que le nombre de nœuds, la taille des files, la charge locale, etc. sur le nombre de pertes et de déterminer ainsi les périodes de saturation du réseau dans le cas de la méthode d'accès présentée ci-dessus.

2.6. Simulations et résultats

Dans cette partie, nous ferons une simulation du CSMA/CA de 802.15.4 pour voir l'apport de l'intégration du mécanisme RTS/CTS.

2.6.1. Paramètres de simulation

Nous simulons notre contribution au niveau MAC sur NS2 avec la version 2.32. Nous considérons un réseau linéaire unidimensionnel formé de dix nœuds numérotés de 1 à 10 et un puits localisé à l'extrême droite du réseau. Les nœuds sont séparés d'une distance fixe de 30 m et le trafic local est pseudo-périodique en raison de 10 paquets par seconde et par nœud. La taille des paquets est fixe et égale à 100 octets. L'évolution des activités des nœuds se composent de trois phases : une phase de démarrage, une phase de régime établi et une phase de vidage des registres. La figure 2.8 montre les différentes phases d'évolution d'un nœud donné. Ainsi, la génération du trafic démarre à une date choisie aléatoirement dans l'intervalle $[T_1,T_1+\Delta_1]$ et se termine à une date choisie dans l'intervalle $[T_2,T_2+\Delta_2]$. Pour observer le phénomène de la saturation et le comportement des files d'attente, on laisse la simulation continuer jusqu'à T_3 après l'arrêt de la génération du trafic local. Dans ces simulations, on utilise un modèle de propagation déterministe en l'occurrence le modèle *Tworayground*. La puissance de transmission est réglée de façon à ce que la portée du nœud soit de 70 m. Dans ce cas, chaque nœud a exactement deux voisins à gauche et deux voisins à droite. La taille des files d'attente FIFO est limitée à 50 paquets et le routage est effectué en négligeant le trafic descendant dans le cas des simulations. En effet, dans une volonté de simplification des conditions de charge du réseau, on néglige les messages d'alerte et éventuellement de resynchronisation.

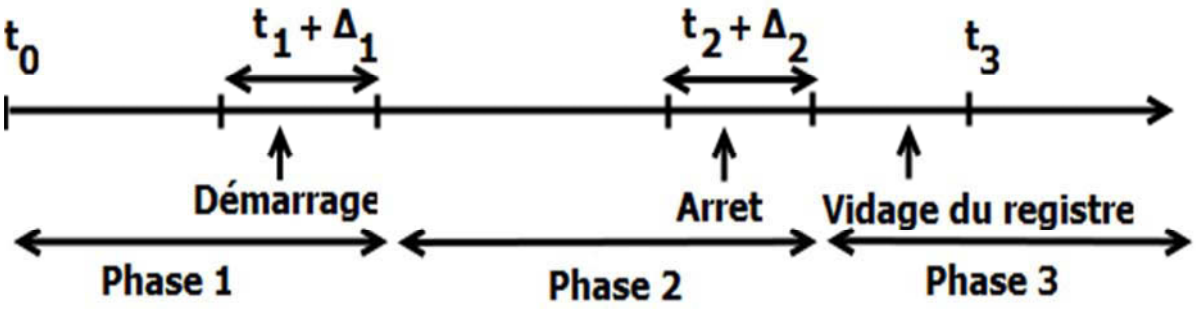


Figure 2. 8 - Les différentes phases de l'évolution de l'activité du nœud.

Trois paramètres de performance sont étudiés. (i) Le nombre de paquets supprimé au cours du temps. Il est égal au nombre de paquets supprimé après un nombre limité de tentatives d'accès au canal avec la méthode d'accès CSMA/CA avec RTS/CTS ou sans RTS/CTS. Dans la figure 2.8, cette métrique est représentée par (1). Dans le comptage du nombre de paquets supprimés, on ne tient pas compte du nombre de paquets supprimés par débordement de file d'attente ni par non réception d'acquittement. (ii) La charge des files d'attente. On définit cette charge comme étant le nombre de paquets contenus dans une file d'attente à un instant donné et pour un nœud précis durant la simulation. Cette métrique est utilisée pour quantifier la surcharge du réseau linéaire. En effet, en examinant la charge des files des nœuds localisés à différentes positions, il est possible de déterminer l'évolution dans le temps des zones de congestion dans le réseau. (iii) Le taux de délivrance qui est le taux de paquets délivré au puits pour un nœud donné. Il représente donc le rapport entre le nombre de paquets reçus et le nombre de paquets envoyés par le nœud. Le taux délivrance dépend de la charge globale du réseau selon la phase de la simulation considérée et du nombre de sauts effectués par les paquets avant d'atteindre le puits.

Dans nos simulations, nous analysons principalement trois nœuds: le nœud 1, le nœud 5 et le nœud 10.

- Le nœud 1 : ce nœud a la particularité d'être le premier nœud à partir de l'extrémité droite du réseau. Il ne reçoit par conséquent pas de trafic venant de sa gauche.
- Le nœud 5 : il a la particularité d'être au milieu du réseau et de recevoir du trafic des nœuds 1 à 4 en plus de son trafic local.

- Le nœud 10 : est le nœud le plus proche du puits. Il accumule le plus de charge dans le réseau mais ne possède que des voisins à sa gauche.

2.6.2. Résultats et discussions

La figure 2.9 montre l'évolution du nombre de paquets supprimé dans le temps. La phase 1 est comprise entre 0 et 10 s. Cette phase est caractérisée par une absence de suppressions du fait que la génération du trafic local ne commence qu'entre 9 et 10 s. Les performances durant la deuxième phase (celle entre 10 et 60 s approximativement) sont dépendantes du nœud. Dans cette période, on note une augmentation progressive des suppressions due au fait que la charge du réseau augmente progressivement aussi. Dans la troisième phase (celle comprise entre 60 s et la fin de la simulation), le nombre de paquets supprimés n'augmente. Cette phase correspond à l'arrêt de la génération du trafic local donc au vidage des files d'attente des nœuds capteurs.

Il est important de noter que c'est le nœud 5 qui a supprimé le maximum de paquets et non le nœud 10 avec ou sans le mécanisme de RTS/CTS. Ceci s'explique par le fait que le nœud 5 se trouvant au milieu du réseau se trouve en compétition avec quatre nœuds pour l'accès au canal alors que le nœud 1 et le nœud 10 ne sont en concurrence qu'avec deux nœuds pour l'accès au canal.

Les effets du mécanisme RTS/CTS sont visibles pour chaque nœud. Il réduit considérablement le nombre de paquets supprimé pour les nœuds 5 et 10. En effet, le nombre de paquets supprimé est passé de 15, 410 et 61 sans RTS/CTS à 13, 325 et 39 avec RTS/CTS respectivement pour les nœuds 1, 5 et 10.

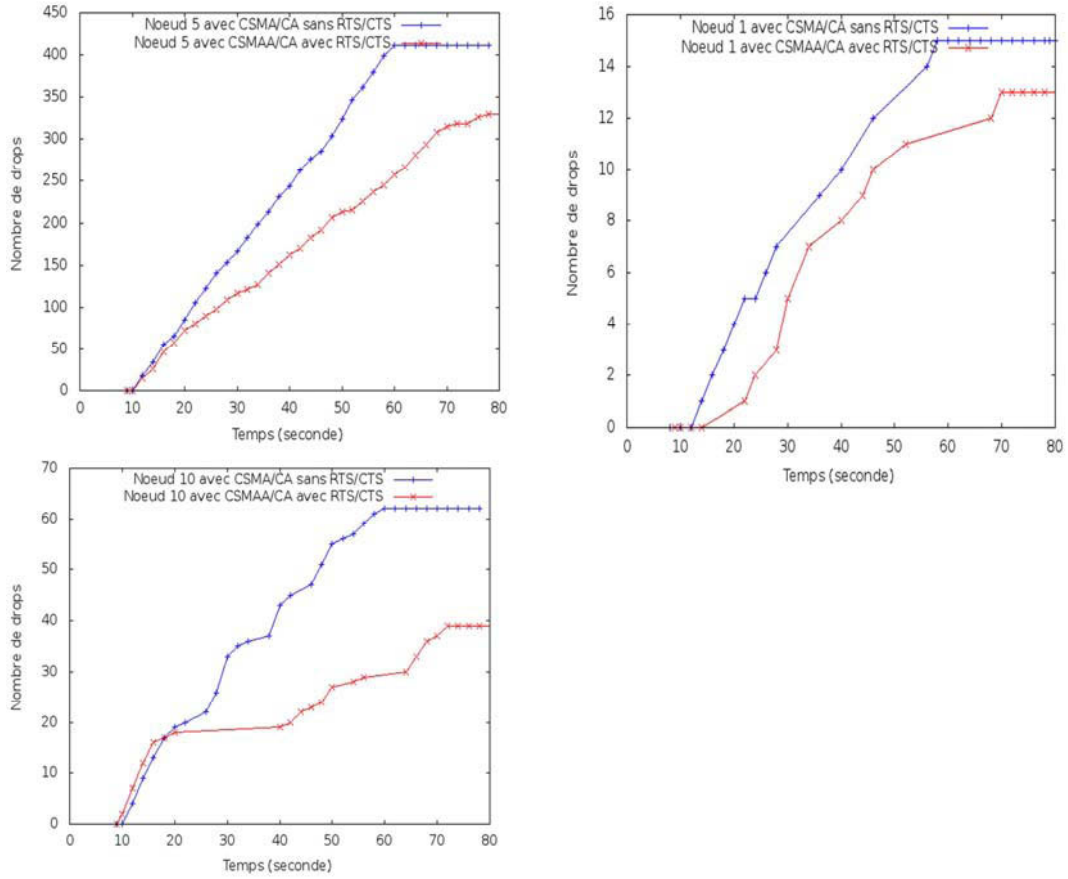


Figure 2. 9 - Comparaison entre le nombre de paquets droppés en mode CSMA/CA avec ou sans RTS/CTS.

La figure 2.10 montre l'évolution des files d'attente dans le temps en version CSMA/CA avec et sans RTS/CTS. On peut identifier l'évolution des FIFO dans les trois phases citées en haut. Dans la phase 1, les files d'attente sont vides du fait qu'il n'ya pas de trafic local généré par l'application des nœuds capteurs. La phase 2 est constituée de deux étapes. La première étape commence à 10 s et finit vers 21 s dépendant du nœud considéré. Durant cette étape, la charge des files d'attente des nœuds augmente progressivement. Ceci s'explique par le fait de la contention qui fait que le taux d'arrivée des paquets est supérieur au taux de départ dans les files d'attente. Donc, ils séjournent plus longtemps dans les files d'attente et par conséquent s'y accumulent dans le temps. La deuxième étape correspond à la période comprise entre 21 s et 62 s. Cette période correspond pour les nœuds les plus proches du puits à une stabilité du registre du fait que les files d'attente atteignent leur maximum. Dans la troisième phase, la production locale de trafic s'arrête et les nœuds commencent à vider leurs files d'attente.

Donc, le canal de transmission devient plus facile d'accès pour les nœuds et par conséquent les files se vident rapidement.

Le nœud 10 accumule le plus de trafic dans ces files d'attente du fait qu'il agrège le trafic venant de tous les autres nœuds. La conséquence de cette situation est le fait que sa file d'attente devient pleine au bout de 21 s. La charge de la file d'attente du nœud 1 ne dépasse pas 12 paquets car il ne gère pas d'autre trafic que celui qu'il produit alors que pour le nœud 10 souffre surtout de la congestion qui fait qu'il supprime beaucoup de paquets.

L'impact du mécanisme RTS/CTS est aussi manifeste dans le comportement des files d'attente. Par exemple, pour le nœud 10, la file d'attente se remplit moins vite en CSMA/CA avec RTS/CTS qu'en mode sans RTS/CTS. La file d'attente se remplit avec 8 s de plus en mode RTS/CTS. Ceci s'explique par le fait que le mécanisme RTS/CTS réduit le nombre de paquets supprimés comme indiqués précédemment. Cependant, le mécanisme augmente les délais dans le réseau du fait qu'il ajoute des trames supplémentaires qui surchargent le réseau. Ceci est visible dans la phase 4 de la simulation. Il faut 4 s pour vider la file d'attente sans RTS/CTS (entre 62 et 66 s) contre 6 s avec RTS/CTS (entre 62 et 68 s).

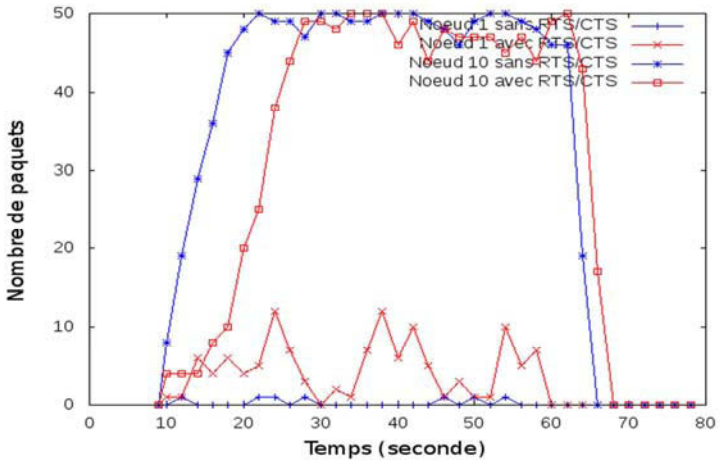


Figure 2. 10 - Évolution des FIFO dans le temps.

Les figures 2.11 et 2.12 montrent le taux de délivrance pour les nœuds 1 et 5 en fonction de la charge globale offerte exprimée en nombre de paquets par unité de temps. On voit que le taux de délivrance pour les deux nœuds est décroissant au fur et à mesure que le réseau est chargé. Cependant, le taux de délivrance du nœud 5 est plus grand que celui du nœud 1. Les paquets

du nœud 5 sont moins exposés aux suppressions du fait qu'ils font moins de chemin que ceux du nœud 1. L'effet du mécanisme RTS/CTS est visible sur le taux délivrance des nœuds. Pour le nœud 1, le taux délivrance maximal est 0.8 avec le RTS/CTS alors qu'il est de 0.11 seulement sans RTS/CTS. Ce taux maximal est respectivement 0.85 et 0.19 pour le CSMA/CA avec RTS/CTS et le CSMA/CA sans RTS/CTS pour le nœud 5. Par contre, lorsque le réseau est très chargé, les nœuds les plus éloignés du puits ont pratiquement les mêmes taux de délivrance et par conséquent l'effet du mécanisme RTS/CTS n'est plus visible.

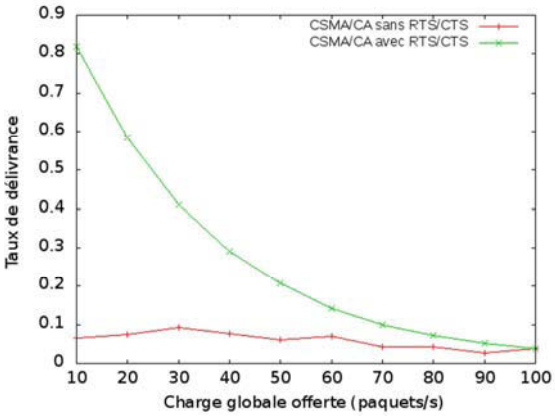


Figure 2. 11 - Taux de délivrance pour nœud 1.

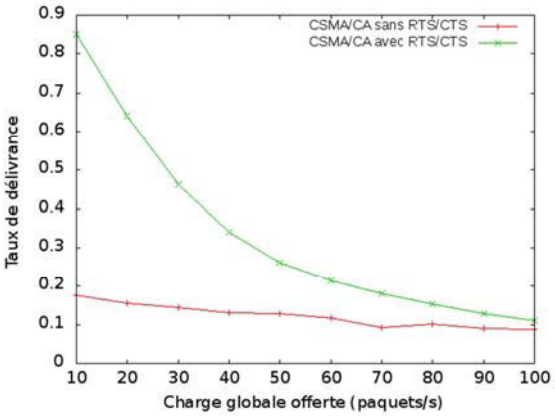


Figure 2. 12 - Taux de délivrance pour le nœud 5

Nous avons vu que les protocoles basés sur la contention pour l'accès au canal se comportent mal dans un réseau linéaire lorsque que celui-ci devient chargé. Dans le cas 802.15.4 avec ou sans RTS/CTS, ce phénomène se manifeste par des zones de congestion lorsqu'on s'approche du puits. Ces dernières sont caractérisées par des files d'attente pleines et une difficulté d'accéder au canal de transmission. Ceci occasionne en même temps des pertes de paquets, des délais de bout-en-bout longs, et peut affecter sérieusement la durée de vie du réseau.

Un protocole MAC pour réseau linéaire doit implémenter de bons mécanismes de gestion des performances réseaux comme les délais de bout-en-bout, le débit au puits, le ratio de délivrance. Il doit être économe en énergie afin d'assurer une longue durée de vie de du réseau. Pour cela, il doit intégrer des mécanismes de gestion d'énergie comme des périodes de sommeil longues. Enfin, du fait de la linéarité et du voisinage limité, le protocole MAC doit aussi assurer la connectivité entre les nœuds pour faire face aux défauts de liens ou de nœuds.

3. LTB-MAC (Linear Token-Based MAC Protocol): Protocole MAC basé sur un jeton

Les protocoles basés sur la synchronisation des nœuds exploitant un jeton sont souvent utilisés dans les réseaux sans fil classiques pour éviter les problèmes de contention rencontrés dans le cas du CSMA/CA (Liu et al., 2013a). Leur implémentation montre par contre qu'ils ne sont pas toujours compatibles aux réseaux linéaires (Liu et al., 2013b). Dans les réseaux linéaires, des protocoles similaires basés sur le jeton ont été proposés (Sun et al., 2013b). Cependant, ceux-ci sont la plupart des cas implémentés dans des réseaux linéaires simples où certaines caractéristiques ne sont pas prises en compte comme le voisinage, le type de trafic et le sens du trafic.

Dans cette partie, nous proposons de mettre en place un protocole MAC basé sur la synchronisation à base de jetons pour l'accès au canal de transmission. Nous appelons LTB-MAC (*Linear Token-Based MAC Protocol*) notre protocole MAC. Dans LTB-MAC, le jeton contient des informations temporelles sur les périodes d'activité et d'inactivité des nœuds. Il donne à un nœud le droit d'émettre pendant un temps borné à ses voisins plus profonds (trafic descendant temps T_1) puis à ses voisins plus proches du puits (trafic montant temps T_2). Le processus de propagation du jeton jusqu'au puits permet de drainer le flux de données au puits, d'assurer la fiabilité, les débits, etc.

3.1. Hypothèses

Il s'agit d'un réseau linéaire de N nœuds capteurs et une méthode d'accès basée sur la circulation de proche en proche d'un droit à la parole géré par un jeton. En fonction du rôle des nœuds capteurs on peut définir trois types de nœuds.

- Le nœud relayeur qui est un nœud simple avec la fonction de relai des données agrégées.
- Le nœud *Token Allocator* ou générateur de jeton qui crée le jeton de façon périodique. Il est généralement situé à l'extrémité opposée à celle du puits. Dans la figure 2.13, il est localisé à l'extrême gauche du réseau. Le *Token Allocator* est aussi un nœud

relayeur avec la particularité de ne pas avoir de voisins descendants (voisins de gauche).

- Le puits est la station chargé de collecter les données agrégées par les nœuds relayeurs.

Dans cette étude, nous considérons un réseau linéaire où le *Token Allocator* est localisé à l'extrême gauche du réseau et le puits à l'extrême droite. Dans ce cas, pour un nœud donné, on définit deux types de voisins : (i) les voisins de gauche plus proche du *Token Allocator* ; (ii) les voisins de droite plus proches du puits. Quand les données transitent du nœud *Token Allocator* vers le puits, on parle alors de trafic montant. Ce trafic correspond aux informations collectées pour l'application de surveillance du capteur (grandeurs physiques, chimiques, environnementales, etc.). Il est relayé par son voisin direct en direction du puits. Les données peuvent aussi transiter du puits vers le *Token Allocator*. On parle dans ce cas de trafic descendant. Ce trafic peut correspondre à des données de pilotage du réseau ou de l'application par exemple. On peut citer des paramètres de synchronisation ou d'alerte.

On suppose que le milieu considéré est homogène et que les conditions de propagation permettent de recevoir le jeton avec une puissance au-delà du seuil de sensibilité définie (-92 dBm dans 802.15.4). Le trafic ainsi que le jeton sont acquittés et les trames de données ont la même taille. On considère trois paramètres de performance : le débit au puits, le taux de délivrance (définis dans la section précédente) et le délai de bout-en-bout. Le délai de bout-en-bout représente la durée entre la mise en file d'attente du paquet et sa délivrance au puits par le nœud qui l'a généré.

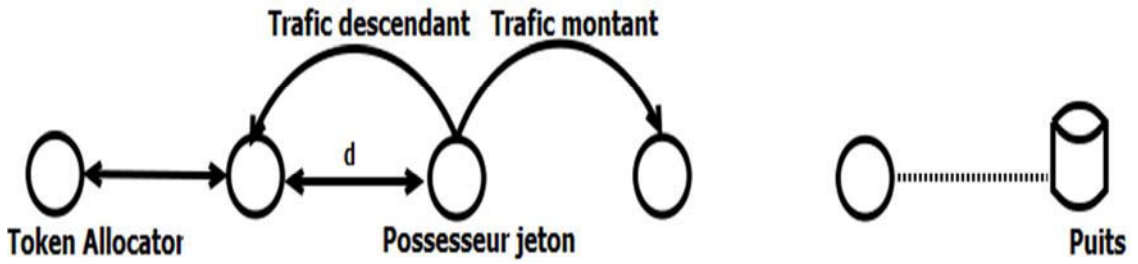


Figure 2. 13 – Présentation des différents types de nœuds nécessaires à un protocole LTB-MAC basé sur le jeton.

3.2. Spécifications

Cette partie fait une description de LTB-MAC. Il s'agit de décrire la structure du jeton en mettant en évidence les différentes informations temporelles et états associés au jeton. Ensuite, nous présentons l'entrelacement des informations temporelles lorsque le jeton traverse le réseau.

3.2.1. Fonctionnement LTB-MAC

Le jeton donne à un nœud donné l'accès au canal de transmission. C'est une trame de données contenant des informations temporelles sur la synchronisation des nœuds. Donc, un nœud est soit possesseur du jeton soit entrain de l'attendre. Quand il est possesseur du jeton alors il accède au canal de transmission pendant un intervalle de temps défini appelé période de transmission. Cet intervalle de temps est divisé comme suit :

- T_1 est le temps dédié à l'envoi du trafic descendant à ses voisins de gauche en direction du *Token Allocator*. Du fait de la nature de ce trafic, T_1 est relativement faible sur la durée de la période de transmission.
- T_2 est le temps dédié à l'envoi le trafic montant en direction du puits. Il constitue la majorité de la durée de la période de transmission.
- T'_2 est le temps d'envoi du jeton qui est presque négligeable par rapport aux temps d'envoi des trafics descendant et montant.

Quand le nœud n'est pas possesseur de jeton, alors il est soit en mode réception soit en mode sommeil. Cette période est divisée en trois parties :

- T_0 est la période d'écoute du trafic montant de son voisin de gauche.
- T'_0 est le temps de réception du jeton à la fin de la transmission du trafic montant.
- T_3 est le temps de réception du trafic descendant de son voisin de droite.
- T_4 est le temps de sommeil.

La figure 2.14.a montre la succession des temps d'activité et d'inactivité pour un nœud dans le cas d'un réseau avec trafic descendant.

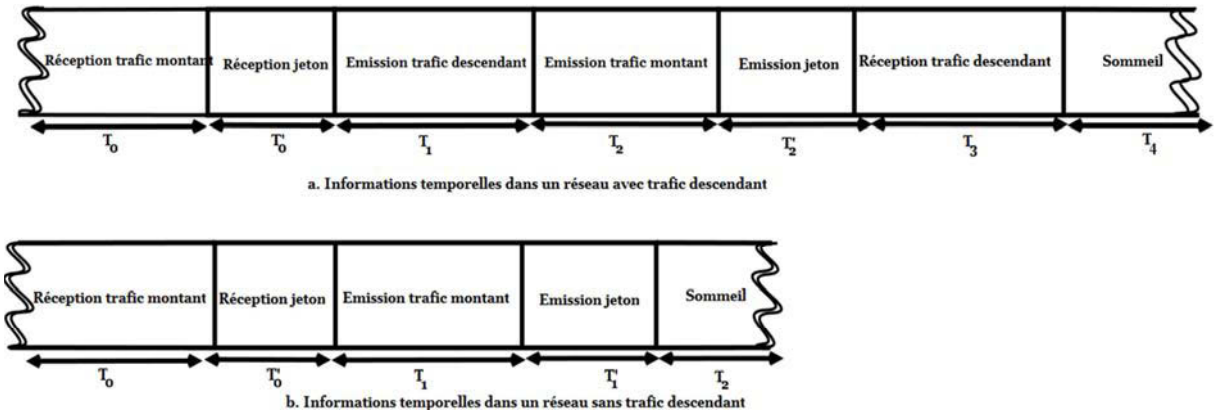


Figure 2. 14 – Les différents états d'un nœud dans LTB-MAC.

Au réveil du nœud, celui-ci se met en mode réception du trafic montant de son voisin de gauche durant T_0 et du jeton durant T'_0. Après la période T'_0, il reçoit le jeton et commence sa période de transmission (T_1+T_2+T'_2). Après la transmission du jeton, le nœud se met en mode réception du trafic descendant de son voisin de droite durant T_3. À la fin de la réception, il se met alors en mode sommeil pour économiser de l'énergie. La figure 2.14.b montre un motif de succession des informations temporelles dans le cas d'un réseau linéaire sans trafic descendant. En effet, suivant les besoins applicatifs, il est possible que le trafic descendant ne soit pas considéré pour des besoins d'optimisation de la charge du réseau et de délais de bout-en-bout.

La production du jeton est périodique avec une fréquence dépendant des caractéristiques du réseau (voir plus loin). Les informations temporelles contenues dans le jeton peuvent varier d'un jeton à un autre. Par conséquent, à la réception d'un jeton, le nœud met à jour ses périodes d'activité et d'inactivité en fonction des informations contenues dans ce dernier. La figure 2.15 montre l'automate d'états d'un nœud courant(le puits et le nœud d'extrémité ne sont pas concernés) et les différents états qui lui sont associés.

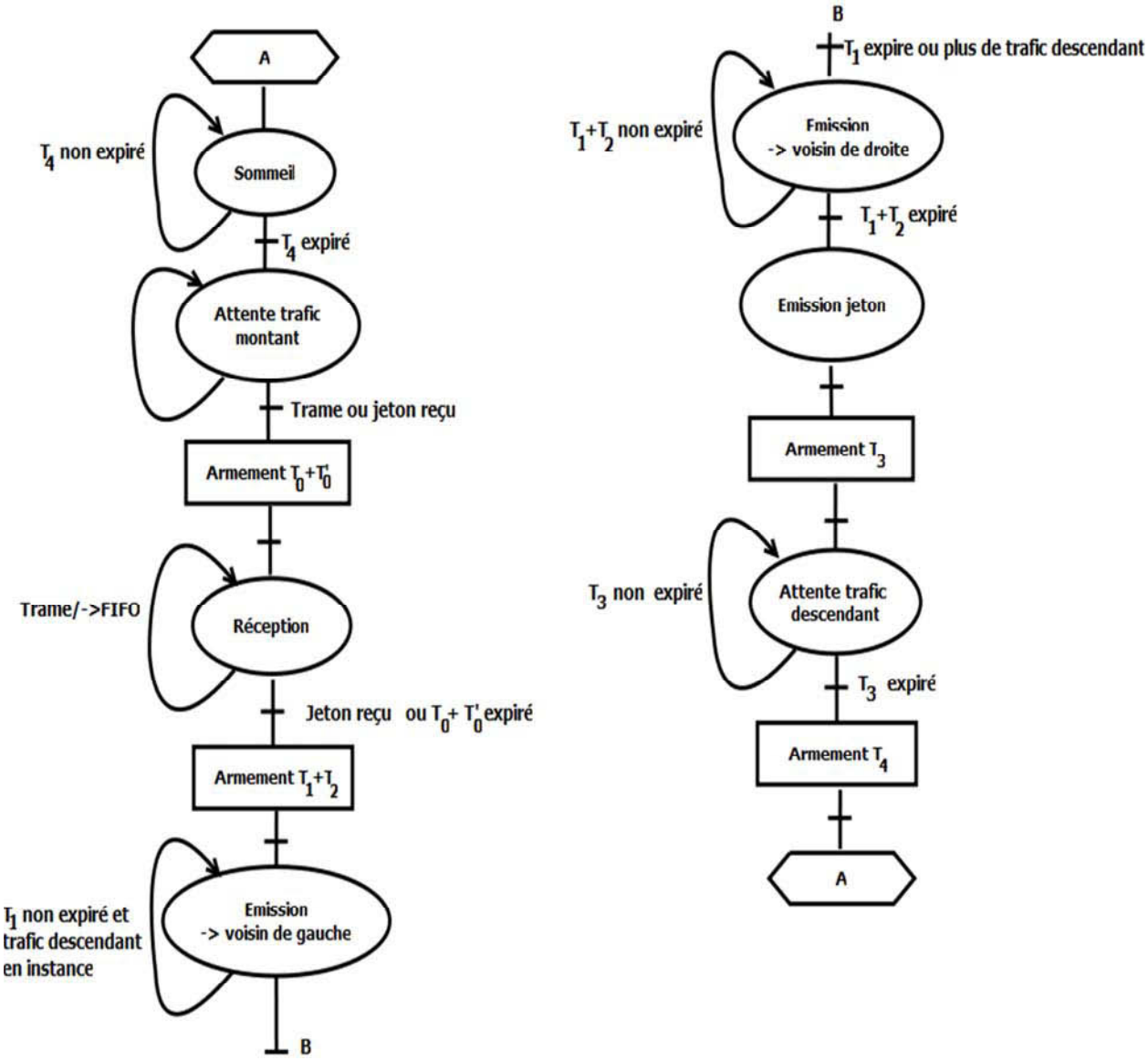


Figure 2. 15 - Automate d'un nœud courant.

3.2.2. Processus de propagation de jeton: la navette

La propagation du jeton de proche en proche jusqu'au puits requiert une synchronisation des nœuds afin d'assurer le drainage des données au puits. L'automate de la figure 2.15 explique comment les nœuds évoluent d'état en état; ceci pour coordonner leurs activités afin d'éviter des désynchronisations sources de pertes de paquets ou de collisions.

Soit la station générique X qui a un voisin à gauche X-1 et un voisin à droite plus proche du puits X+1 comme montré dans la figure 2.16. X est récepteur à l'expiration de T_4 durant T_0, T'_0 et T_3. Il est émetteur pendant T_1, T_2, T'_2. Il peut dormir pendant un temps T_4 déduit des informations portées par le jeton qui contient aussi l'information sur sa fréquence de production. Cette information permet au nœud de déduire la date du prochain passage du jeton et de calculer la durée de la période de sommeil T_4.

Nous avons ainsi la relation suivante :

- $T_2+T'_2$ (X-1) < $T_0+T'_0$(X) le nœud courant est à l'écoute du trafic en direction du puits que lui donne son voisin précédent. Autrement dit, le nœud X-1 n'a pas encore expiré les périodes d'émission liées au trafic montant et au jeton.
- T_3(X-1) > T_1(X) le nœud X-1 écoute le trafic descendant du nœud courant (celui qui a un jeton). C'est-à-dire le trafic descendant que lui donne le nœud courant.

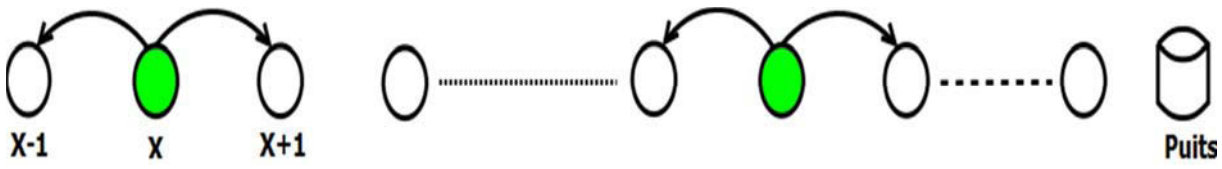


Figure 2. 16 - Token passing appliqué à un réseau sans fil linéaire.

Cette façon de propager le jeton de proche en proche peut être vue comme le passage d'une navette (ou *shuttle*) dans laquelle les nœuds déposent leurs trames d'information en direction

du puits ou du générateur de jeton. Le départ de la navette est ainsi initié par le nœud *Token Allocator*. La figure 2.17 montre un exemple de propagation de la navette en direction du puits. Dans la suite, on ne considère que la navette en direction du puits.

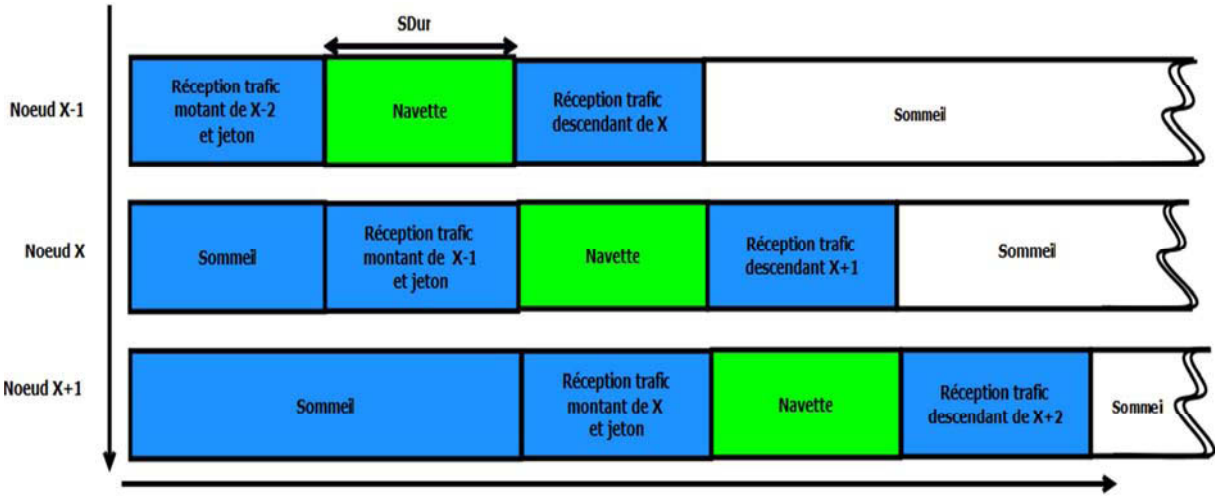


Figure 2. 17 - Processus de passage de la navette.

Nous définissons la durée de la navette ou *Shuttle Duration* (***SDur***) exprimé en seconde et la quantité d'information échangée par un nœud qui dispose de la navette ou *Shuttle Capacity* (***SC***).

- ***SDur*** est égal à $T_1+T_2+T'_2$.
- ***SC*** est fonction de T_1+T_2 .
- Si FD_n désigne la période qui sépare le départ de deux navettes consécutives exprimée en temps et T_x l'instant de réception du jeton le nœud X, alors la prochaine navette devrait arriver à $T_x+ FD_n$. Le temps de sommeil T_4 est alors donnée par : $T_4 = FD_n - (T_1+T_2+T'_2 + T_3)$.

La durée de la navette est un facteur très important sur les performances du réseau linéaire. Suivant les caractéristiques du milieu surveillé et les besoins applicatifs, il est possible d'opter pour une petite ou grande taille de navette. La taille de la navette correspond aussi à la durée exprimée en secondes. Une petite navette a l'avantage de réduire les délais de bout en bout et l'énergie consommée en émission. Cependant, elle diminue le taux de délivrance et le débit au puits. Une grande navette quant à elle augmente le ratio et le débit au puits mais aussi la

consommation d'énergie. Dans tous les cas, il est très important que la taille des files d'attente des nœuds soit adéquatement choisie en fonction de la durée de la navette afin de d'optimiser le drainage des données au puits. En effet, le comportement des files d'attente peut justifier le choix de la durée de la navette et son impact sur les performances.

Pour les besoins de maintien de la synchronisation, on considère qu'un nœud consomme toute la durée de la navette quel que soit la charge et les conditions de propagation. Ainsi, en l'absence de trafic descendant, la période d'envoi du trafic descendant est consommée par le trafic montant.

3.3. L'effet d'écrêtage du trafic

Avec la méthode présentée, le comportement du contenu des files d'attente des nœuds est fonction de la périodicité des jetons et de la durée de la navette. Un nœud donné est émetteur ou récepteur durant des périodes de temps définies dans le jeton. L'activité de la file pour un nœud donné est décrite comme suit :

- la file d'attente de reception d'un nœud se remplit durant $T_0 + T_3$. En effet, durant T_0 le nœud reçoit du trafic montant du voisin à gauche et durant T_3 il reçoit du trafic descendant du voisin de droite.
- durant le passage de la navette, le nœud se vide de son trafic descendant durant T_1 et de son trafic montant durant T_2.
- le trafic local quant à lui est généré tout au long de la période d'activité du noeud. Nous faisons l'hypothèse qu'il est généré périodiquement à une période définie par la couche applicative.

Suivant l'ordre d'arrivée des données en file d'attente, le contenu de la file d'attente peut être décrit comme suit : (i) au fond de la file, on retrouve les paquets qui n'ont pas pu être envoyés suite au dernier passage de la navette. Ce cas se produit lorsque la taille de la file d'attente est assez grande par rapport à la durée de la navette faisant que certains paquets ne peuvent pas être envoyés ; (ii) les paquets produits localement durant la période d'activité du nœud ; (iii) les paquets reçus de ses voisin de gauche et de droite. Parmi ces paquets on retrouve ceux produits par les voisins du nœud et ceux agrégés par ses voisins et venant de voisins lointains.

Le contenu de la file d'attente présenté dans la figure 2.18 peut être considéré comme une structure récursive qui à partir de la quatrième partie de la file contient des paquets qui sont empilés eux-mêmes selon la structure que nous sommes en train de décrire. L'accumulation des données de proche en proche jusqu'au puits entraine une saturation des files d'attente au fur et à mesure que nous nous approchons du puits ou bien lorsque la taille des files n'est pas assez grande pour les vider au passage de la navette. Dans ce cas, le trafic montant est le plus exposé « aux suppressions » car étant toujours en haut de la file d'attente d'après la figure 2.18. Le trafic montant généré par le *Token Allocator* est le premier trafic à être supprimé dans le cas de débordement de file d'attente.

Nous appelons ce phénomène effet d'écrêtage du trafic destiné au puits. Les paquets en provenance du *Token Allocator* sont systématiquement supprimés avant d'atteindre le puits lorsque la charge du réseau linéaire est forte.

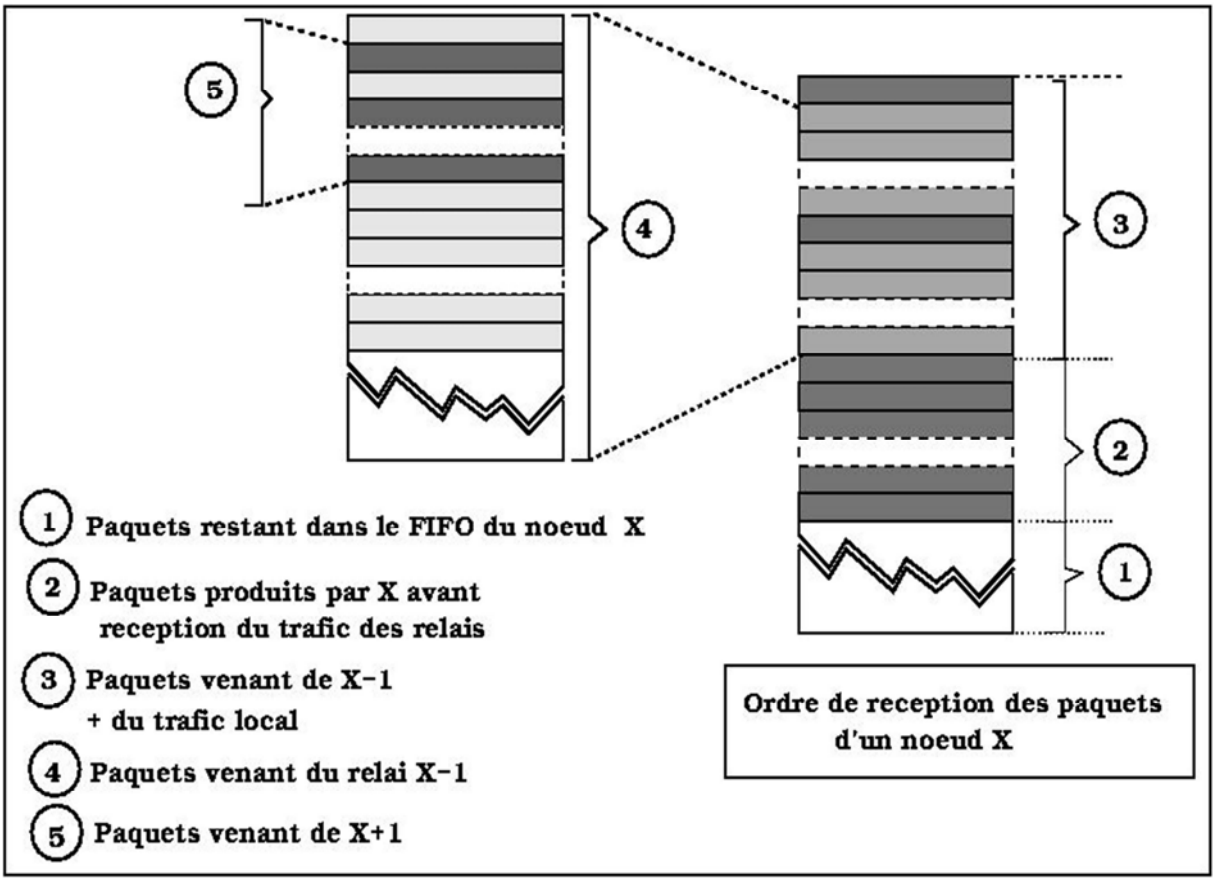


Figure 2. 18 - Comportement du contenu des files d'attente.

Ce constat logique va être validé par simulation dans ce qui suit.

3.4. Simulations et résultats

Dans cette partie, nous présentons les résultats de simulations et discutons les performances du protocole LTB-MAC en le comparant aux protocoles CSMA/CA avec et sans RTS/CTS.

3.4.1. Paramètres de simulation

Cette simulation est basée sur NS2 avec la version 2.32. Nous considérons le réseau linéaire décrit dans la figure 2.9. Le trafic local est généré de façon pseudo-périodique par intervalle de temps et commence de façon indépendante et aléatoire entre 0 et 1 s pour chaque nœud en début de simulation. La puissance d'émission des nœuds est calculée en fonction du modèle de propagation dans le but d'avoir la portée radio désirée. Nous voulons que chaque nœud ait exactement deux voisins: un voisin à gauche et un voisin à droite. Pour ce faire, considérons une puissance de transmission de -5 dBm et une distance ***d*** égale à 70 m. La taille des files d'attente FIFO est considérée comme fixe et égale à 50 paquets. On néglige la possibilité de trafic descendant en supposant que les caractéristiques matérielles du puits lui permettent de recevoir correctement le trafic montant. Dans ce cas, le besoin d'envoyer des messages de resynchronisation ou d'alerte est négligeable. On se focalise sur trois paramètres de performance: le débit au puits, le taux de délivrance et le délai de bout-en-bout pour un nœud donné. On s'intéresse à deux nœuds principalement pour l'étude du taux de délivrance: le nœud 1 et le nœud 5 en raison de leur position sur le réseau linéaire.

On compare le protocole LTB-MAC aux protocoles CSMA/CA avec et sans RTS. La figure 2.19 montre les conditions dans lesquelles nous effectuons les comparaisons. D'après cette figure, la distance minimale entre deux nœuds émetteurs qui ne provoque pas de collisions est égale à trois sauts pour le protocole LTB-MAC et CSMA/CA avec RTS/CTS. Dans ces conditions, on considère que la distance entre deux navettes consécutives est de trois sauts. On considère différentes valeur de ***SDur*** : des valeurs relativement petites 10 ms, 20 ms, etc., une valeur moyenne de 50 ms et une grande valeur de 250 ms. Ces différentes durées de

navette nous permettent de justifier la pertinence d'utiliser le protocole LTB-MAC ou CSMA/CA selon les besoins et la charge du réseau linéaire.

Dans nos simulations, on considère la couche physique 802.15.4. Dans ce modèle, une trame est soit reçue correctement soit perdue. Dans le cas où la trame est perdue, on considère qu'elle est entrée collision avec une autre trame. Donc, le modèle de capture considéré dans nos simulations défini deux états pour une trame en cours de réception : soit elle est reçue soit elle est perdue. On considère que le seuil de capture qui permet de définir l'état d'une trame en cours de réception est égal à 10 dB.

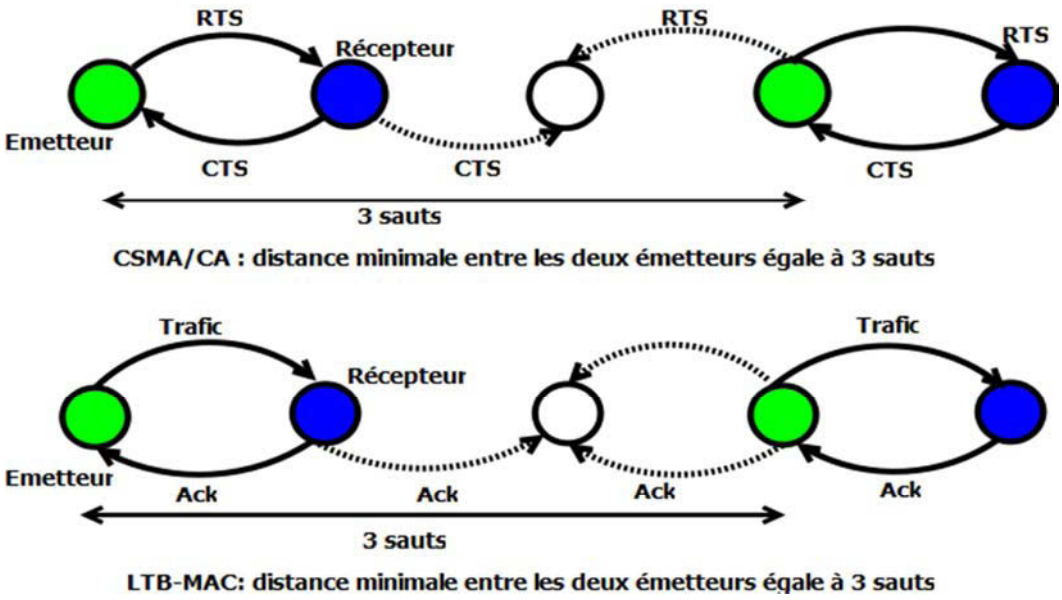


Figure 2. 19 - Critères de comparaison entre LTB-MAC et CSMA/CA.

Les paramètres de simulation sont récapitulés dans le tableau suivant.

Tableau 1 - Paramètres de simulation

Paramètres	**Valeurs**
SDur	10, 20, 30, 50, 250 ms
Taille jeton	11 octets
Taille paquets de données	70 octets
Nombre de répétitions	200
Modèle de propagation	*Tworayground*
Couche physique	802.15.4
Puissance de transmission	-5 dBm
Charge offerte	[8-80] Kbps
Taille FIFO	50-60 paquets

3.4.2. Résultats

La figure 2.20 montre le débit au puits en fonction de la charge globale offerte dans le réseau pour de petites valeurs de la durée de la navette 10, 50 et 250 ms. Elle montre que le protocole LTB-MAC offre de meilleures performances que le CSMA/CA avec ou sans RTS/CTS en termes de débit offert au-delà d'une navette de 10 ms. En effet, pour LTB-MAC le maximum de débit reçu est d'environ 40 Kbps alors qu'il est de 25 Kbps pour CSMA/CA avec RTS/CTS et 15 Kbps sans RTS/CTS.

L'évolution du débit au puits pour le protocole LTB-MAC peut être divisée en deux phases :

- entre 8 et 40 Kbps, de charge offerte (dépendant de la navette): durant cette phase le débit au puits croit en fonction de la charge globale du réseau. Ceci s'explique par le fait que le réseau n'a pas atteint le maximum de sa capacité et par conséquent les files d'attente ne débordent pas. Ainsi, lors du passage de la navette, les nœuds parviennent à envoyer le maximum de données.
- entre 40 et 80 Kbps, le débit du réseau ne varie plus. Cette phase correspond à la saturation qui est la conséquence de la forte charge du réseau. Les données agrégées

durant le passage de la navette restent de taille constante car la navette est pleine quand elle s'approche du puits. Les files d'attente débordent et le débit au puits n'évolue pas.

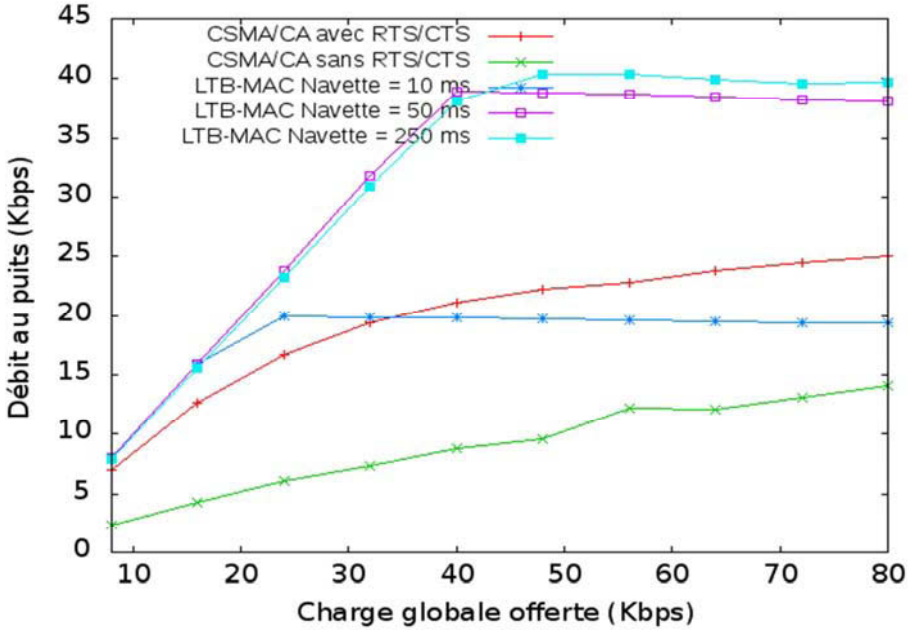


Figure 2. 20 - Comparaison du débit au puits.

La figure 2.21 et la figure 2.22 montrent le taux de délivrance en fonction de la charge du réseau exprimée en nombre de paquets par seconde pour des durées de navettes de 10 ms, 50 ms et 250 ms. Pour les nœuds 1 et 5, on voit que le taux de délivrance de paquets au puits est plus important dans le cas du protocole LTB-MAC que pour les protocoles CSMA/CA avec ou sans RTS/CTS, même dans le cas d'une très navette de durée 10 ms. En effet, pour le nœud 5, le taux de délivrance minimal (resp. maximal) est 0.6 (resp. 1) alors qu'il est de 0.11 (resp. 0.85) et 0.28 (resp. 0.25) respectivement pour les protocoles CSMA/CA avec RTS/CTS et sans RTS/CTS. Pour le nœud 1, le taux minimal observé est de 0.4 pour LTB-MAC alors qu'il est de 0.1 pour les protocoles CSMA/CA avec ou sans RTS/CTS.

Pour le protocole LTB-MAC, l'allure de la courbe nous permet de remarquer qu'elle se divise en deux parties :

- entre 10 et 60, paquets par secondes (dépendant de la navette). Dans ce cas, le taux de délivrance est égal à 1 car le réseau n'est pas saturé. Donc, les paquets ne sont pas victimes de l'effet d'écrêtage du trafic.
- entre 50 et 100 paquets par seconde, le taux de délivrance décroit au fur et à mesure que le réseau est chargé. Ceci s'explique par le fait que les FIFO débordent causant ainsi des drops de paquets. Pour le nœud 1, on remarque cependant que le protocole LTB-MAC et le CSMA/CA avec ou sans RTS/CTS ont le même comportement lorsque le réseau est fortement chargé. En effet, l'effet d'écrêtage du trafic est le même pour le nœud 1 quel que soit le protocole utilisé.

L'allure de la courbe dans le cas du protocole CSMA/CA est décroissante en fonction de la charge globale offerte quand la charge du réseau augmente.

L'effet d'écrêtage du trafic dans le cas du protocole LTB-MAC est visible pour les nœuds 1 et 5. En effet, lorsque que le réseau est chargé, on voit que le taux de délivrance décroît plus lentement pour le nœud 5 que pour le nœud 1 du fait que les paquets du nœud 1 sont plus exposés à l'effet d'écrêtage.

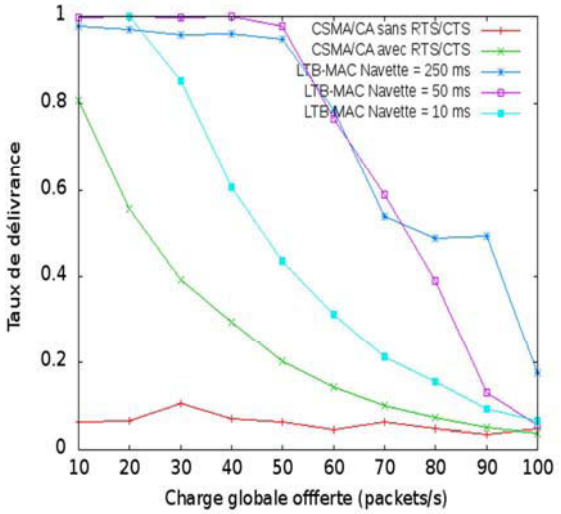


Figure 2. 21 - Taux de délivrance au puits pour les nœuds 1.

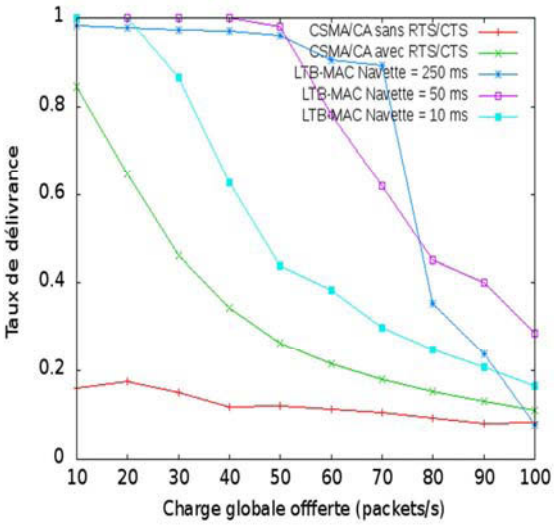


Figure 2. 22 - Taux délivrance au puits pour le nœud 5.

Les figures 2.22 et 2.23 représentent le délai de bout-en-bout en fonction de la charge globale offerte exprimée en termes de paquets par seconde. Ici encore on voit que le protocole LTB-MAC diminue considérablement les délais de bout-en-bout par rapport au protocole CSMA/CA et pour les durées de navette données. Comme dans le cas du taux de délivrance, les délais de bout-en-bout sont plus petits pour le nœud 5 du fait qu'il est plus proche du puits et les trames de données qu'il génère ont un chemin plus court.

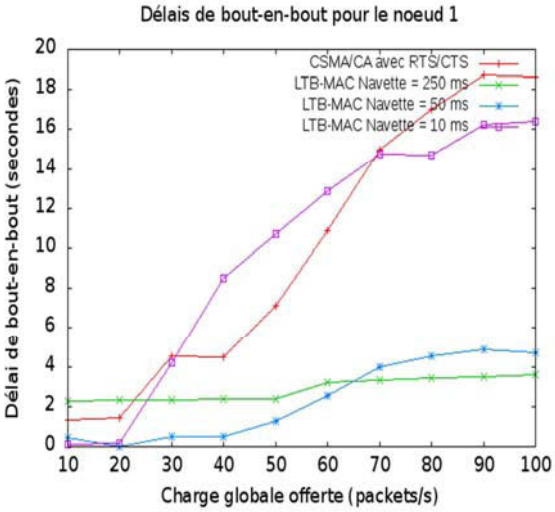


Figure 2. 23 - Délai de bout-en-bout du nœud 1.

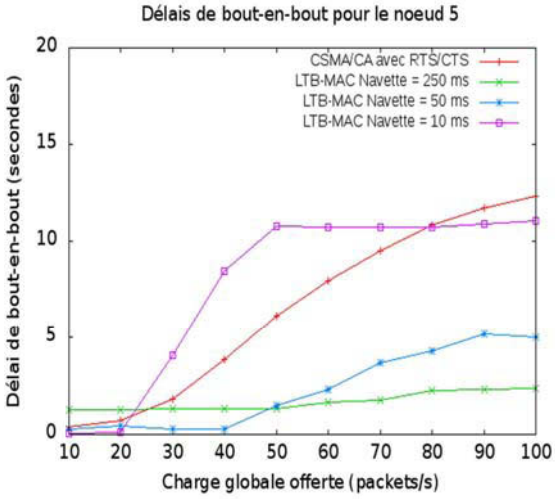


Figure 2. 24 - Délai de bout-en-bout du nœud 5.

Notons qu'à partir de 50 paquets/s la moyenne du temps de transit de bout-en-bout pour le nœud 1 diminue à cause de l'effet d'écrêtage.

4. Conclusion

Les réseaux sans fil souffrent beaucoup du problème du terminal caché quand la méthode d'accès utilisée est basée sur la contention. Ce problème dans le cas dans réseaux de capteurs sans fil linéaires peut être plus drastique vue les caractéristiques spécifiques de ce type de réseau. Dans 802.11, pour éviter le problème du terminal caché ou exposé, on introduit le mécanisme du RTC/CTS qui permet une réservation local du canal de transmission pour un

nœud voulant émettre des données grâce à un échange de petites trames d'information RTS et CTS.

Dans ce chapitre, nous avons fait une intégration du RTS/CTS dans la version non slotté de 802.15.4 pour un réseau de capteurs sans fil linéaire. Nous avons détaillé les nouveaux algorithmes de transmission et de réception et avons par la suite fait des simulations pour montrer l'impact du RTS/CTS sur le nombre de paquets supprimés et sur le comportement des files d'attente. Le mécanisme RTS/CTS diminue considérablement les zones de congestion dans un réseau linéaire et améliore fortement l'usage des files d'attente Cependant, il augmente à la fois les délais de bout-en-bout et la charge du réseau du fait des trames RTS et CTS échangées durant le processus de réservation du canal.

Par la suite, nous avons proposé une méthode d'accès basée sur la génération d'un jeton qui donne à un nœud le droit d'accès au canal de transmission. Le jeton est propagé de proche en proche, en saut par saut, jusqu'au puits. Il est créé par le nœud qui se trouve à l'extrémité opposée de celle du puits et est appelé générateur de jeton ou *Token Allocator*. Le jeton contient des informations sur les périodes d'activité des nœuds. La génération du jeton de proche en proche est comparable à une navette qui passe et dans laquelle les nœuds déposent des informations à destination du puits. La navette détermine la quantité d'informations qu'un nœud peut envoyer lorsqu'il est en possession du jeton.

Par la suite une étude comparative a été faite entre le protocole LTB-MAC et le CSMA/CA en termes de débit, taux de délivrance et délai de bout-en-bout. Nous avons montré grâce à des simulations que le protocole LTB-MAC offre de meilleures performances que le CSMA/CA dans les réseaux de capteurs sans fillinéaires.

Dans ce chapitre, nous avons considéré un réseau linéaire où les caractéristiques des nœuds (puissance d'émission) font que leur voisinage est limité à deux voisins. Dans le chapitre suivant, on se propose d'étudier un réseau linéaire où le voisinage d'un nœud est plus important et avec la possibilité de faire circuler plusieurs jetons en même temps. Dans ce cas, pour un voisinage donné, il est important de définir la distance minimale entre deux nœuds possesseurs de jetons. Il s'agit donc de définir des motifs d'isolement que nous appellerons clusters linéaires afin de protéger les échanges dans le réseau.

Clustering basé sur une exploitation logique du voisinage des nœuds

1. Introduction

Dans le chapitre précédent, nous avons présenté le protocole LTB-MAC basé sur la génération de jetons pour l'accès au canal de transmission. Nous avons considéré le cas le plus simple où la portée d'un nœud donné lui permet d'avoir exactement deux voisins : un voisin à gauche et un voisin à droite. Les nœuds séparés par plus d'un saut d'un nœud en émission ne subissant pas d'interférences significatives. En plus dans le réseau, il n'existe qu'un seul type de trafic : le trafic montant destiné au puits. Dans ce cas, nous avons défini une distance minimale entre deux nœuds possesseurs de jetons afin de protéger les échanges d'éventuelles interférences radios provoquant des collisions. Cependant, il est possible qu'un nœud ait une portée radio qui lui permet d'avoir plusieurs voisins à gauche et à droite. De plus, si on doit considérer la présence de trafic descendant dans le réseau alors il faudra définir un moyen de découper le réseau un plusieurs entités afin de protéger les activités des nœuds possesseurs de jetons des interférences radio. Ceci permet d'optimiser les performances du réseau comme les délais de bout-en-bout et les taux de délivrance. Dans le domaine des réseaux, la technique du clustering (Abbasi and Younis, 2007) est souvent utilisée pour optimiser ces performances. Le clustering consiste à subdiviser le réseau en motifs (patterns) pour assurer une réutilisation spatiale i.e. chacun de ces motifs peut utiliser une ressource commune à ces motifs sans générer d'interférences préjudiciables. Certains algorithmes de clustering se basent sur les caractéristiques des nœuds comme la portée des nœuds (Baker and Ephremides, 1981)(Xu and Gerla, 2002), l'énergie résiduelle (Heinzelman et al., 2000)(Manjeshwar and Agrawal, 2002). D'autres algorithmes quant à eux se fondent sur les caractéristiques du réseau comme la mobilité (Subramanian and Katz, 2000)(Demirbas et al., 2004), la nature des données recueillies en utilisant des fonction de sélection des données (Krishnamachari et al., 2002) ou la topologie du réseau en se basant sur le modèle de déploiement des nœuds (Lindsey and Raghavendra, 2002). Généralement les communications inter-cluster se font en un minimum de sauts. Un nœud dans un cluster est exposé aux interférences radio avec les nœuds de son cluster appelées interférences intra-cluster et avec celles des clusters voisins appelées interférences inter-cluster. Les interférences intra-cluster sont gérées par le mécanisme d'accès au canal de transmission. La technique TDMA est le plus souvent utilisée pour assigner aux nœuds l'accès au canal (Heinzelman et al., 2000)(Santhi and Venkatachalpathy, 2014). Pour les interférences inter-cluster, plusieurs méthodes de gestion sont utilisées comme la

technique du FDMA utilisé dans (Waharte and Boutaba, 2005). LEACH utilise la technique du DS-SS (Shiu et al., 2011) dans tous les clusters. Cette technique consiste à un étalement de spectre et est utilisée dans les communications satellite, les réseaux sans fil afin de rendre les signaux plus résistants aux interférences radio. Dans (Al-Shawaqfeh et al., 2013), les auteurs, présentent une méthode de gestion d'interférences inter-cluster basée sur la technique TDMA.

Cependant, ces techniques même si elles s'avèrent efficaces dans les réseaux WSN ne sont pas adaptées aux réseaux linéaires pour plusieurs raisons. D'abord elles ne garantissent pas totalement l'absence d'interférences. En effet, ces techniques proposent des mécanismes de gestion de l'accès au canal de transmission mais elles ne se focalisent pas de façon catégorique sur la gestion des interférences qui sont de nature diverse et par conséquent ne sont pas seulement liées à l'accès au canal de transmission. Dans le cas des réseaux linéaires, les interférences peuvent être très préjudiciables et impacter significativement sur le taux de délivrance des paquets au puits. Ensuite, l'utilisation des deux méthodes d'accès au canal de transmission l'un entre les nœuds d'un même cluster l'autre entre les nœuds de clusters différents peut ne pas être une solution optimale pour les délais de bout-en-bout dans les réseaux de capteurs sans fil linéaires. En effet, du fait de la longueur souvent importante dans ce type de réseau, il est important que les accès au canal de transmission soient rapide plus réduire les délais de bout-en-bout.

Donc, la notion de clustering, telle que définie dans les WSN, ne convient pas au réseau de capteurs linéaires. Un cluster dans un réseau linéaire doit tenir compte de ses caractéristiques particulières la linéarité, le voisinage limité, les conditions de propagations dans le milieu considéré, les interférences et le facteur de réutilisabilité pour optimiser les performances réseau définis en haut. Récemment des travaux se sont focalisés sur le clustering dans les réseaux linéaires mais sans pour autant satisfaire aux conditions énumérées. Dans(Chakraborty, 2010), les auteurs ont présenté une méthode pour calculer la taille optimale d'un cluster dans un réseau linéaire en se basant sur la connectivité des nœuds capteurs. Cependant, ce calcul se fait sans considération du facteur de réutilisabilité des clusters ni des interférences générées par l'activité des nœuds.

Dans ce chapitre, nous proposons une méthode de clustering dans un réseau de capteurs sans fil linéaire. Il s'agit à partir des conditions de propagation et des caractéristiques des nœuds

capteurs de découper les réseaux en entités dans lesquelles les activités des nœuds sont protégées contre les interférences et les risques de collisions afin d'optimiser les délais de bout-en-bout, les taux de délivrance et les débits.

2. Hypothèses

Nous allons considérer un réseau linéaire constitué de N nœuds placés uniformément sur une même ligne à une distance entre deux nœuds adjacents égale à ***d***. Le mécanisme d'accès au canal considéré est le protocole LTB-MAC et on suppose l'existence de plusieurs accès simultanés au canal de transmission quand la longueur du réseau le permet. Dans ce cas, plusieurs navettes peuvent traverser le réseau linéaire en même temps. Le modèle de propagation considéré dans cette étude est le *Tworayground*. Dans ce cas, pour un lien radio donné, la perte en chemin est considérée comme constante, vu que la variation n'est pas importante. Par conséquent, la puissance de réception pour une puissance d'émission donnée ne varie pas entre l'émetteur et un le récepteur considérés. Donc, dans la topologie linéaire, dans un premier temps nous négligeons les fluctuations environnementales qui pourraient rendre le milieu complexe et difficile à modéliser. Nous focalisons notre étude sur ce point fort pour définir la notion de cluster logique et statique dans les sections suivantes.

Dans ces conditions, chaque nœud a un identifiant allant de 1 pour le Token Allocator jusqu'à N pour le puits. On suppose la possibilité de trafic descendant dans le réseau. Les caractéristiques matérielles des capteurs sont telles qu'un nœud est à portée de un ou plusieurs autres nœuds de son voisinage en fonction de la distance ***d***. Dans ce cas, un nœud peut relayer ses données à son voisin à un saut ou à son voisin le plus lointain à sa portée. Pour plusieurs raisons comme le nombre de retransmissions maximal dépassé (se produit quand un nœud renvoie 5 fois une trame de donnée sans recevoir d'accusé de réception) ou l'effet d'écrêtage du trafic, certains paquets n'arrivent pas au puits.

3. Prise en compte d'un facteur de redondance

Dans cette partie, on se propose de faire une étude de la notion de redondance qui concerne le voisinage dans le réseau linéaire. Il sera ensuite question d'analyser l'impact de cette redondance sur la distance entre les jetons et sur les indicateurs de performance du réseau.

3.1. Définition de la redondance

Soit ***p*** la portée radio exprimée en unité de longueur et ***d*** la distance entre les nœuds adjacents, alors la relation entre ***p*** et ***d*** permet de définir le voisinage en déterminant le nombre de voisins pour un nœud donné. La connaissance du voisinage permet de définir la manière dont les communications sont routées dans le réseau. On définit la redondance pour indiquer le nombre de voisins d'un nœud courant dans le réseau. Cette redondance se différencie de la densité du réseau car elle permet d'exploiter et de tirer avantage de linéarité de la topologie. Cette redondance intervient dans un réseau pour :

- router les paquets : la redondance permet d'avoir plusieurs choix sur les nœuds relais. Si, un nœud a une portée de n nœuds voisins en direction du puits, alors il a n choix pour relayer les paquets.
- assurer la connectivité dans le réseau : la redondance augmente la connectivité de réseau et permet d'améliorer la tolérance aux fautes en cas de nœuds ou liens défectueux. En effet, les conditions d'utilisation des capteurs dues aux besoins des applications de surveillance ou les conditions du milieu surveillé souvent hostiles (mauvaises températures, intempéries,..) font qu'il arrive souvent que des nœuds ou des liens soient défectueux.
- diminuer les zones de congestion dans la topologie linéaire : le drainage du flux de proche en proche à un saut jusqu'au puits est source de congestion dans le réseau lorsqu'on s'approche du puits. Cette congestion se manifeste par des débordements de files d'attente, des pertes et des suppressions de paquets (Ndoye et al., 2013). La redondance permet de drainer le flux en multi-sauts ; ce qui a comme avantage de diminuer les débordements des files d'attente.

En fonction de la relation entre ***p*** et ***d*** on peut définir plusieurs niveaux de redondance dans une topologie linéaire. On dit qu'un réseau linéaire est *R*-redondant lorsque pour un nœud courant donné, il existe au moins *R* voisins à gauche et *R* voisins à droite. L'entier *R* est appelé le facteur de redondance et détermine le nombre de voisins dans chaque direction (droite et gauche), comme indiqué dans la figure 3.1. Cette contribution est basée sur l'hypothèse forte suivante: pour une topologie R-redondant, la relation $R * d < p < (R+1) * d$ est stable, et par conséquent la longueur des liaisons radio d'une telle topologie est relativement constante et uniforme sur toute la ligne. Cette relation signifie qu'un nœud donné a exactement *2*R* voisins comme montré dans la figure 3.1. Cette hypothèse est homogène avec le choix fait pour modéliser les liens radio : conditions de propagation sont déterminées par le modèle déterministe *Tworayground* (Rappaport and others, 1996).

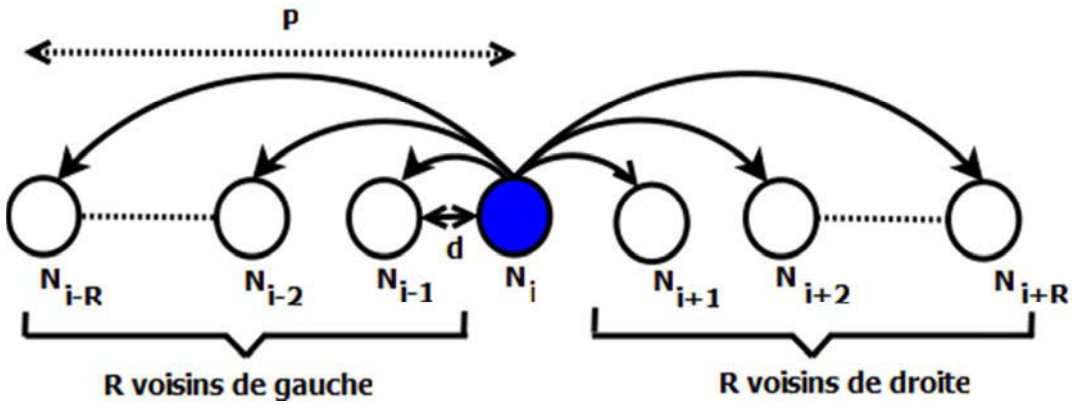


Figure 3. 1 - Connectivité du nœud courant N_i dans un réseau *R*-redondant.

3.2. Quelques exemples de réseaux R-redondant

Selon la valeur de *R*, on peut définir plusieurs types de réseaux *R*-redondant. Dans cette étude, on se limite à la description des réseaux *1, 2 ,3*-redondant.

3.2.1. Réseau 1-redondant

Il est caractérisé par la relation : $d < p < 2 * d$. Dans ce cas, chaque nœud a deux voisins : un à sa gauche et un autre à sa droite. Le réseau 1-redondant est aussi appelé strictement linéaire du fait que le voisinage du réseau est très faible. Le drainage du flux se fait de proche en proche en un saut jusqu'au puits. Pour une telle topologie, si un lien est cassé ou un nœud est en panne, c'est tout le réseau qui se trouve affecté car il n'existe aucune autre possibilité de route. Par conséquent, une rupture provoque un dysfonctionnement global sur toute la ligne.

3.2.2. Réseau 2-redondant

Il est caractérisé par la relation: $2 * d < p < 3 * d$. Dans ce cas, chaque nœud a 4 voisins : 2 à sa gauche et 2 à sa droite. Dans ce réseau, lorsque qu'il existe un nœud défectueux, il est encore possible de transmettre les données au nœud suivant à portée. Autrement dit, pour un nœud donné, il a deux possibilités de nœuds relais pour la transmission des données dans chaque direction. Ce qui lui confère plus de fiabilité dans l'acheminement des données que le réseau *1*-redondant.

3.2.3. Cas du réseau 3-redondant

Dans ce réseau, la relation de voisinage est donnée par la formule: $3 * d < p < 4 * d$. Chaque nœud du réseau a 3 voisins à gauche et 3 à droite et par conséquent a trois possibilités de choix de nœud relais pour une direction donnée. Cette topologie offre plus de solutions pour la tolérance aux fautes que la topologie *2*-redondant en compensant la défaillance de deux nœuds ou de deux nœuds consécutifs.

3.3. Impact de la redondance sur la distance au puits

Dans cette partie, nous allons analyser l'impact de la redondance sur l'acheminement des données au puits. Pour tirer profit de la redondance, on suppose qu'un nœud d'un réseau R-redondant relaie ses données à ses voisins à R sauts suivant la direction considérée. Considérons le flux en direction du puits. Les figures 3.2 et 3.3 permettent de comprendre l'intérêt d'exploiter la redondance pour acheminer le trafic. Dans ces deux figues les flèches en pointillés indiquent le trajet des jetons générés qui suivent systémiquement le chemin A -> B -> C …-> Puits car il est relayé de proche en proche d'un nœud à son voisin. Les flèches pleines indiquent le chemin pris par les paquets de données en direction du puits.

Pour la figure 3.2 du cas *2*-redondant, le trafic généré par A est transmis directement à son voisin à deux sauts en l'occurrence le nœud C pour y être concaténé avec le trafic produit localement. Ce trafic concaténé est ensuite transmis à E et ainsi de suite. Dans un tel réseau, on peut constater l'existence de deux branches (A, C, E, G, I) et (B, D, F, H) qui convergent vers le puits. Dans ce cas, le puits reçoit directement les trafics concaténés par les nœuds I et H.

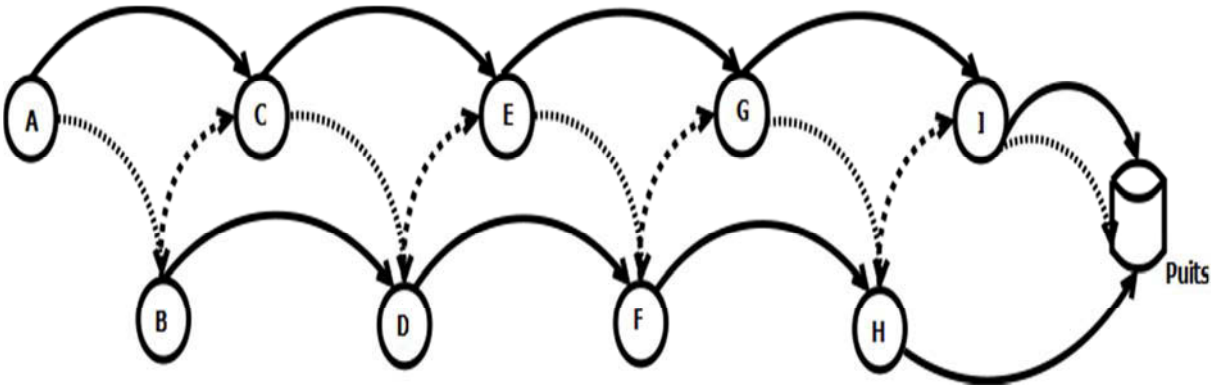


Figure 3. 2 - Formation des branches logiques dans un réseau 2-redondant

Pour la figure 3.3 du cas 3-redondant, le trafic généré par A est transmis directement à D pour y être concaténé avec le trafic produit localement. Ce trafic concaténé est ensuite transmis à G et ainsi de suite. Dans un tel réseau, on peut constater l'existence de trois branches (A, D, G,

J), (B, E, H, K) et (C, F, I, L) qui convergent vers le puits. Ce dernier reçoit les trafics générés par les nœuds J, K et H.

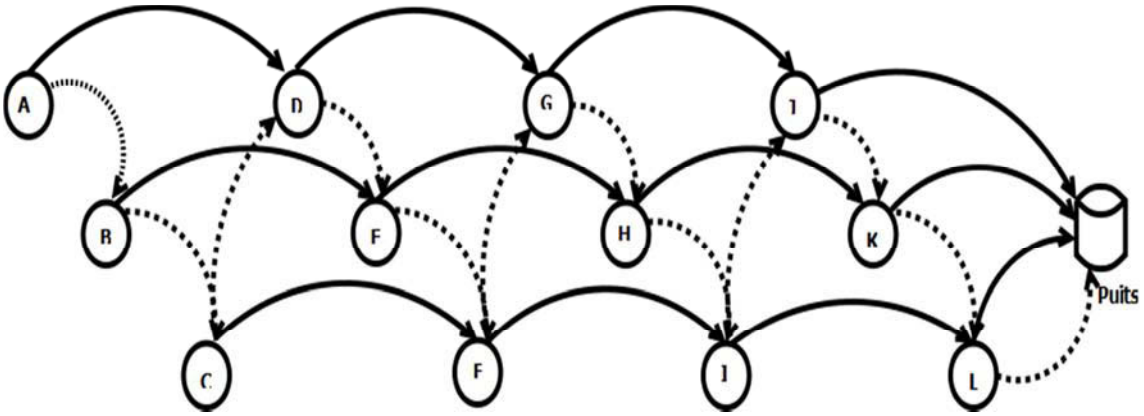


Figure 3. 3 - Formation des branches logiques dans un réseau 3-redondant

Cette façon de ventiler le trafic sur chacun de ces branches a un impact sur les performances en termes de débit.

Considérons la figure 3.3 à l'instant où les stations A et L sont en possession d'un jeton.

A va transmettre ses données à D puis son jeton à B. L va transmettre ses données au puits puis le jeton à M

Nous pouvons remarquer deux choses importantes :

- l'existence d'un jeton permet au puits de recevoir quand ses voisins à portée ont le jeton, pour un 3-redondant : 3 fois (de K, de L et de M).
- l'existence de plusieurs branches permet aux stations à portée du puits de se répartir la charge cumulée à chaque saut. Ainsi, K cumule uniquement le trafic de A de D et de G.

Nous pouvons généraliser cette analyse à un réseau *R*-redondant. En effet, le trafic transmis par un nœud *X* en direction du puits est relayé entre voisins à *R* sauts jusqu'au puits. Le nœud *X* relaie les données à son *X+R* qui le relaie au voisin *X+2*R* ainsi de suite jusqu'au puits. Donc, *X* est associé à la branche (*X, X+R, X+2*R,..., X+n*R*) où *n* est le nombre de nœuds relais associés à *X*. De plus, avec les conditions d'accès au canal de transmission, le puits reçoit du trafic de *R* nœuds à portée. L'impact de la redondance sur la formation des branches se situe principalement sur la répartition équitable de la charge sur les nœuds. La charge

globale du réseau est répartie sur les différentes branches ce qui réduit l'effet de cumul bien connu dans les réseaux linéaires. Ceci permet une meilleure gestion de la congestion.

4. Estimation de la distance entre jetons

Comme indiqué dans nos hypothèses, nous considérons un réseau linéaire composé de *N* nœuds capteurs. Si *N* est assez grand i.e. le réseau linéaire est suffisamment long alors plusieurs jetons peuvent circuler simultanément. Ceci peut avoir plusieurs avantages dans les performances du réseau linéaire :

- augmenter le débit au puits : le passage de plusieurs navettes en même temps dans le réseau permet d'acheminer plus de données au puits. Ceci a un impact significatif sur le débit au puits en ce sens qu'il reçoit plus de données par unités de temps,
- réduire les délais de bout-en bout : lorsque les navettes sont fréquentes les paquets séjournent moins longtemps dans les files d'attente,
- augmenter les taux de délivrance au puits : le passage de plusieurs navettes permet de réduire l'effet d'accumulation de trames dans les files d'attente. Ceci a pour effet de mieux gérer l'effet d'écrêtage du trafic. Par conséquent, le taux de délivrance augmente pour un nœud donné.

Cette situation induit plusieurs zones d'activité distinctes sur le réseau comme introduit dans la figure 3.4. Ces zones d'activités, si elles ne sont pas bien gérées, peuvent générer des interférences entre les nœuds provoquant par la suite des risques de collisions. Autrement dit, il faut que l'activité d'un nœud possédant le jeton (N_i ou N_j de la figure 3.4) ne perturbe pas les autres nœuds disposant eux aussi d'un autre jeton au même moment. Cette question revient à définir une distance minimale entre deux zones d'activité consécutives pour éviter les effets d'interférences, ou plus précisément à définir la distance qui sépare deux nœuds possesseurs de jetons consécutifs afin de protéger les échanges initiés par ceux-ci. Cette situation décrite dans la figure 3.4 nous permet de préciser que le trafic est majoritairement destiné au puits (comme la trame émise par N_i pour N_{i+1}) mais qu'un trafic inverse serait également possible (comme la trame émise par N_j pour N_{j-1}).

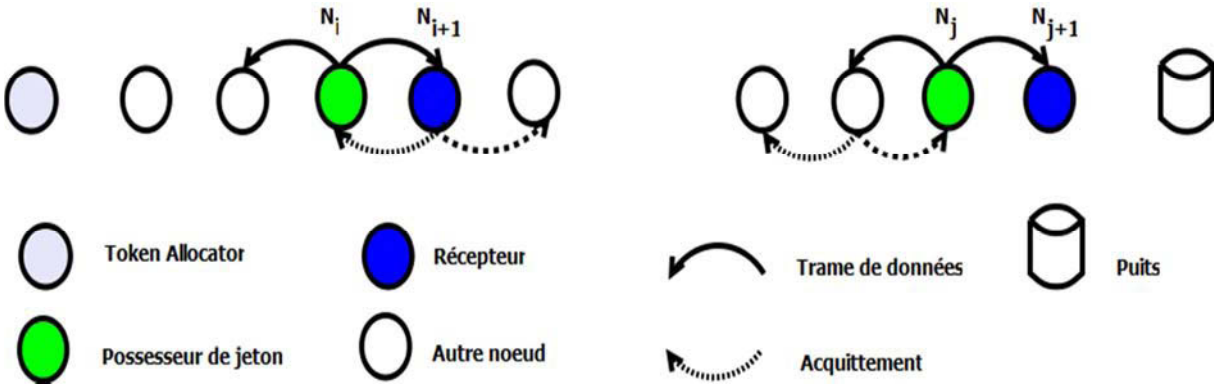


Figure 3. 4 – Exemple de zones d'activités dans un réseau linéaire 1-redondant.

La distance entre deux nœuds possesseurs de jetons en termes de nombre sauts se calcule de façon logique et statique en termes de nombre de sauts sans prise en compte d'un comportement évolutif de la portée d'un nœud. Autrement dit, elle est calculée en fonction de la connectivité du réseau sans considération des fluctuations qui pourraient générer des variations importantes sur les pertes en chemin du signal émis.

4.1. Cas du réseau *1*-redondant

Cette démarche logique suppose que la condition $d < p < 2d$ signifie qu'une trame émise est entendue par le nœud voisin mais ne provoque pas d'interférences significatives pour son voisin à deux sauts comme indiqué dans les hypothèses. La figure 3.5 montre des portions de réseaux avec ou sans trafic descendant. Considérons le cas de l'émission d'une trame montante de A vers B et de l'existence d'un trafic descendant de E vers D quand A et E sont deux porteurs consécutifs du jeton (figure 3.5.a). On considère le cas le plus pessimiste où A envoie du trafic montant à B et E envoie du trafic descendant à D. Dans ce cas, le nœud C est exposé aux interférences des acquittements produits par les nœuds B et D mais ceci n'a pas d'impact puisque C n'est pas le destinataire des trames échangées. Cette hypothèse s'applique quand B acquitte une trame émise par A sans perturber la réception par D de la trame émise par E. Ainsi, dans cette démarche les échanges entre A et B sont protégés des interférences causées par les échanges de E et D. Il est alors facile de voir en exploitant le voisinage que la

distance minimale en termes de sauts entre deux nœuds possesseurs de jetons (ici A et E de la figure 3.5.a) est égale à 4 sauts.

En l'absence de trafic descendant, il est facile de remarquer que le nombre de sauts qui sépare deux nœuds possesseurs de jeton est 3. En effet, comme dans le cas précédent, les échanges entre les nœuds possesseurs de jetons n'impliquent pas le nœud C du fait qu'il n'est pas concerné par les échanges. Cette situation est décrite dans la figure 3.5.b.

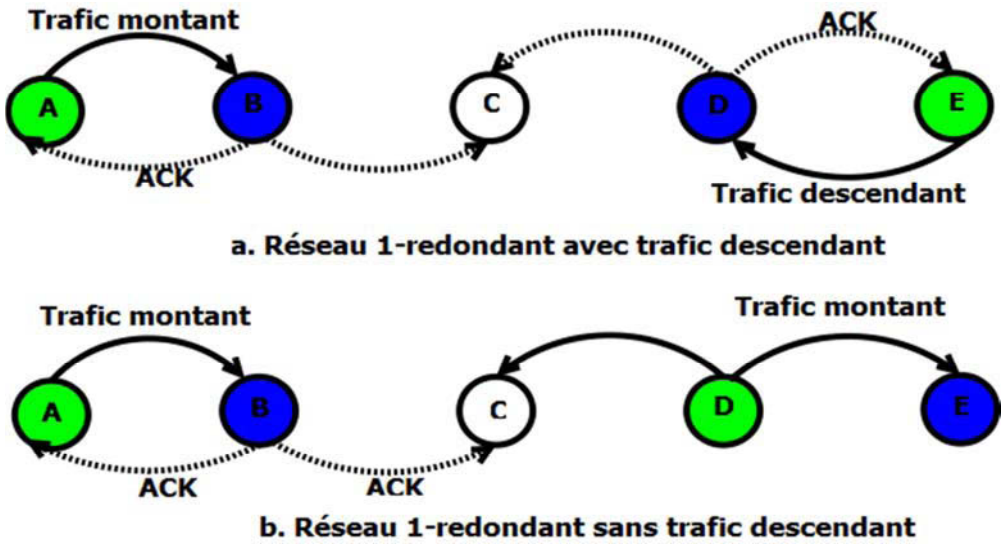


Figure 3. 5 - Distance entre deux possesseurs d'un jeton dans un réseau 1-redondant

4.2. Cas du réseau 2-redondant

Considérons les émissions de trafic montant de A vers C et de trafic descendant de H vers F lorsque A et H sont simultanément possesseurs de jeton. Quand C et F acquittent respectivement à A et à H, les nœuds B, D, E et G sont d'une certaine façon aveuglés par les dans les échanges. Les nœuds D et E sont exposés aux interférences radio générées par les acquittements produits par C et H. Mais ces interférences n'ont pas d'impact sur les nœuds D et E qui ne sont pas destinataires des trafics échangés. De plus, l'hypothèse selon laquelle $2 * d < p < 3 * d$ fait que les acquittements transmis par C à A n'interfèrent pas avec la réception de la trame émise par H à F. Par conséquent, les activités des nœuds A et H

possesseurs de jeton sont simultanément protégées des risques d'interférences dus aux acquittements respectifs des nœuds C et F. En considérant le cas le plus général où deux nœuds possesseurs d'un jeton peuvent générer du trafic montant et descendant, la figure 3.6.a montre que la distance minimale est de 7 sauts. En l'absence de trafic descendant, la figure 3.6.b montre que cette distance est de 5 sauts.

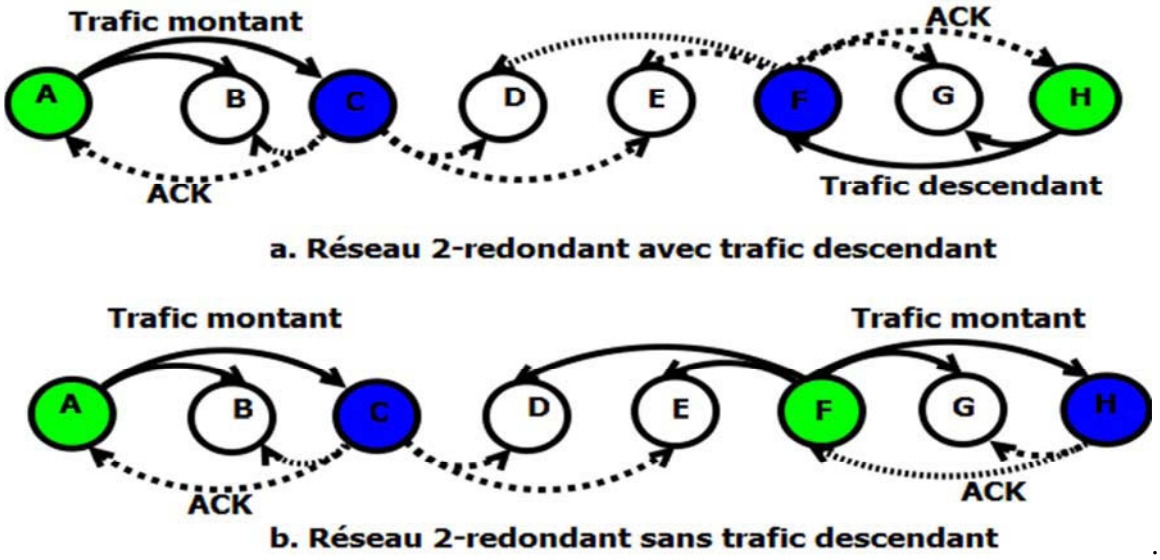


Figure 3. 6 - Distance entre possesseurs de jetons dans un réseau 2-redondant

4.3. Cas du réseau 3-Redondant

Considérons le cas où les nœuds A et K possesseurs de jetons transmettent leurs trafics montant et descendant respectivement aux nœuds D et H comme indiqué dans la figure 3.7.a. Ici, les nœuds intermédiaires concernés par les interférences sont E, F, G. Cependant, ils ne sont pas récepteurs des trafics de A et K. Par conséquent, les risques d'interférences ne sont pas préjudiciables à cette portion du réseau. En effet, avec la méthode d'accès les nœuds cités sont soit en mode sommeil soit en mode *idle* et donc ne participent pas aux échanges à l'initiative des possesseurs de jeton. La figure 3.7.a nous montre que pour un réseau 3-redondant avec trafic descendant, la distance entre deux nœuds possesseurs de jetons est de 10

sauts. Cette distance est de 7 sauts lorsque le réseau est dépourvu de trafic descendant comme montré dans la figure 3.7.b.

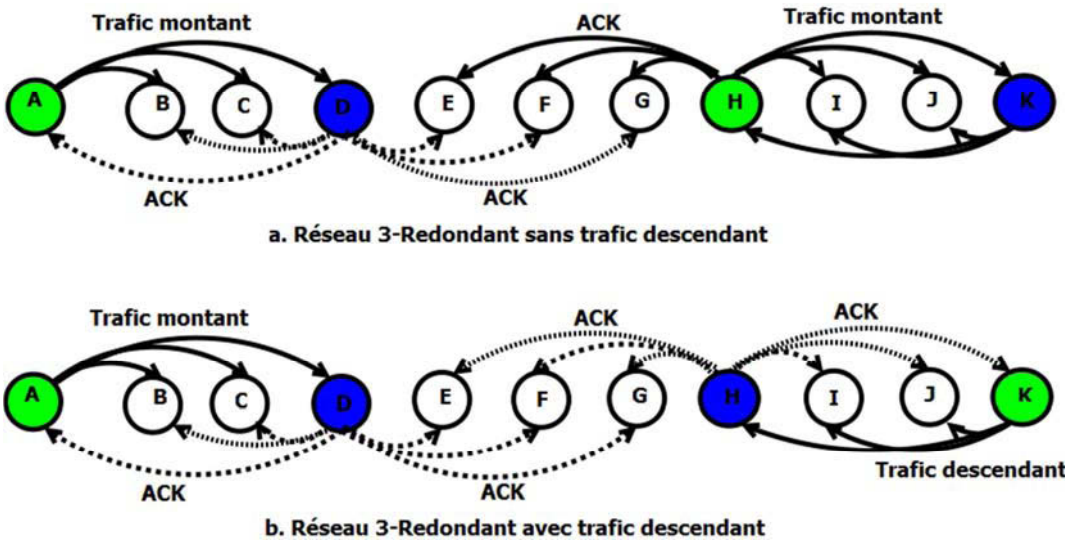


Figure 3. 7 - Distance entre jetons dans un réseau 3-redondant

4.4. Généralisation

Nous pouvons généraliser cette étude à un réseau linéaire *R*-redondant pour estimer la distance entre deux nœuds possesseurs de jeton. Le nombre de nœuds entre les possesseurs de jeton peut être divisé en trois groupes suivant l'impact que les activités des nœuds peuvent avoir sur ces nœuds.

- Les nœuds récepteurs: chaque nœud possesseurs de jeton envoie son trafic à son voisin à *R* sauts. Donc, entre ces deux nœuds il existe deux nœuds récepteurs lorsque le réseau est muni de trafic descendant. S'il n'existe pas de trafic descendant, le nœud récepteur du nœud possesseur de jeton le plus proche ne se trouve pas entre les deux émetteurs. Dans la figure 3.7.b. le récepteur K du trafic de l'émetteur H ne se trouve pas entre H et l'autre émetteur A. En plus, ce nœud est hors portée des nœuds susceptibles d'influencer l'activité de l'autre possesseur de jeton (G, F par exemple de

la figure 3.5.b). Par conséquent, ce récepteur n'est peut être considéré dans le calcul de la distance entre deux possesseurs de jeton.

- Les nœuds entre l'émetteur et le récepteur d'un même échange: ces nœuds ont la particularité d'être concernés uniquement par les échanges entre l'émetteur et le récepteur car ils sont logiquement hors de portée. Ils ne sont pas concernés par l'activité de l'autre émetteur. En plus, ils sont généralement en mode attente de jeton. Pour chaque émetteur, il existe *R-1* nœuds le séparant du nœud récepteur. Dans le réseau *3*-redondant présenté ci-dessus, il s'agit des nœuds B et C pour le nœud A. Donc, au total on a *2*R-2* nœuds entre les deux possesseurs de jetons dans le cas du réseau *R*-redondant où le trafic descendant est assuré. Pour un réseau sans trafic descendant, les *R-1* nœuds du nœud possesseur de jeton le plus proche du puits ne sont pas en fait entre ce nœud et l'autre possesseur de jeton car le trafic va toujours dans le sens du puits. Dans l'exemple du réseau *3*-redondant, il s'agit des nœuds I et J de la figure 3.7.b. Ces nœuds sont en mode attente du jeton et n'ont donc aucune influence sur l'activité des nœuds possesseurs de jetons. Par conséquent, Ces nœuds n'influencent pas la distance entre ces deux possesseurs de jetons et ne sont pas considérés dans le calcul. D'où en réseau *R*-redondant sans trafic descendant le nombre de nœuds de ce type à considérer dans le calcul est de *R-1*.
- Les nœuds entre les deux récepteurs : il s'agit des nœuds qui sont à portée des deux récepteurs. Dans le cas du réseau *3*-redondant avec trafic descendant, il s'agit des nœuds E, F et G. Ces nœuds sont concernés par les acquittements des nœuds récepteurs et par conséquent peuvent être exposés aux interférences radio. Ces nœuds qui forment une zone d'isolement sont en attente du prochain jeton et sont probablement en mode sommeil. Puisque tous les nœuds ont les mêmes caractéristiques, on peut donc compter *R* nœuds dans cette zone d'isolement entre deux récepteurs en se basant sur leur portée.

La figure 3.8 montre la répartition des nœuds entre deux nœuds possesseurs de jeton. Si on appelle Dist la distance entre deux nœuds possesseurs d'un jeton en termes de nombre de sauts, alors la distance en fonction de *R* est donnée par la formule:

$$Dist(R) = \begin{cases} 3 * R + 1 \; avec \;\; trafic \; descendant \\ 2 * R + 1 \; sans \;\; trafic \; descendant \end{cases}$$

Ces deux formules obtenues logiquement sont bien sur vérifiées pour R = 1, 2 et3.

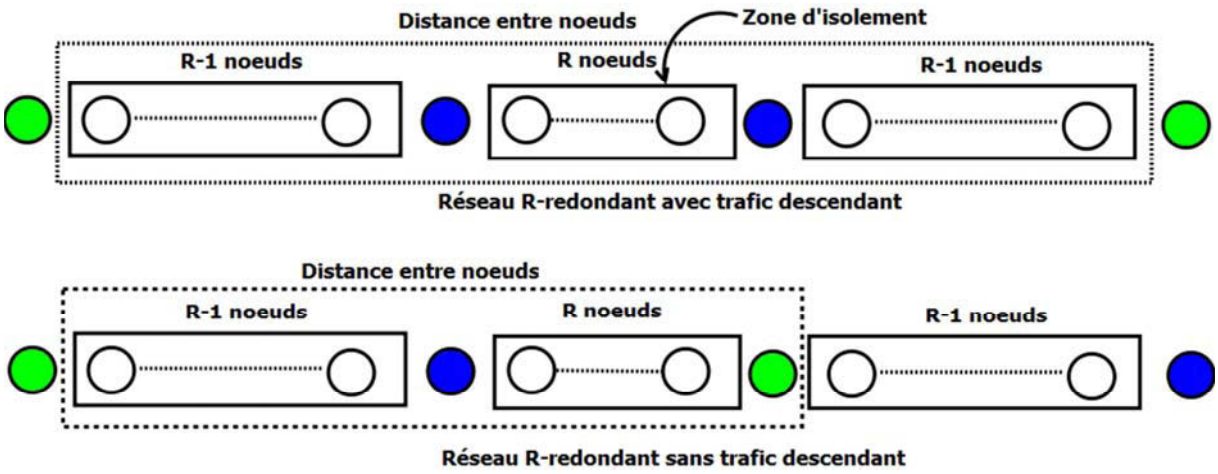


Figure 3. 8 - Distance entre deux nœuds possesseurs d'un jeton dans un réseau *R*-redondant

5. Impact de la distance entre les possesseurs de jeton sur le débit au puits

Dans cette partie, nous allons évaluer le débit maximal au puits pour un réseau R-redondant. Nous nous basons sur les hypothèses suivantes.

- La taille de la navette est juste assez grande pour permettre à un nœud à portée du puits de vider sa file d'attente lors du passage de celle-ci. C'est le cas optimal car tout le temps de possession du jeton est utilisé pour émettre.
- La taille des FIFO des nœuds à portée est assez grande pour stoker les données agrégées des différentes branches du réseau.

Cette évaluation repose sur des trames de longueur constante. Dans le chapitre 2, nous avons défini SDur (*Shuttle Duration*) comme la durée de la navette et SC (*Shuttle Capacity*) comme la capacité de la navette qui définit le nombre de paquets qu'un nœud donné peut envoyer durant le passage de la navette. Nous considérons dans un premier temps les réseaux 1, 2 et 3-redondant.

Nous avons montré que dans le réseau *1*-redondant la distance entre deux nœuds possesseurs d'un jeton est de 4 lorsqu'il existe du trafic descendant et de 3 en l'absence de trafic descendant. Considérons l'existence de trafic descendant dans le réseau. Alors un nœud reçoit le jeton chaque *4*SDur* et envoie un trafic équivalent à *SC* paquets durant un temps de *SDur*.

Puisque dans un réseau 1-redondant un seul nœud est à portée du puits, alors ce dernier reçoit un trafic de *SC* paquet chaque *4* SDur*. Par conséquent, le débit au puits est donné par la formule : $D = \frac{1 * SC}{4 * SDur}$. En l'absence de descendant, le puits reçoit du trafic chaque *3*SDur* , par conséquent, le débit est donné par: $D = \frac{1 * SC}{3 * SDur}$.

Pour un réseau *2*-redondant, on sait qu'il existe deux nœuds à portée du puits et que la distance entre deux possesseurs de jetons est de 7 lorsqu'il existe du trafic descendant. Donc, le puits reçoit 2 fois *SC* paquets par jeton, soit *2* SC* paquets pour *7 *SDur* ce qui donne un débit de : $D = \frac{2 * SC}{7 * SDur}$. Si le réseau est dépourvu de trafic descendant le débit est alors: $D = \frac{2 * SC}{5 * SDur}$.

Pour les mêmes raisons que celles utilisées précédemment, dans le réseau *3*-redondant le puits reçoit 3 fois le trafic *SC* des nœuds à portée lors du passage de la navette tous les *10*SDur* en cas de trafic descendant. Donc, le débit au puits est donné par : $D = \frac{3 * SC}{10 * SDur}$. En l'absence de trafic descendant, le débit au puits est donné par : $D = \frac{2 * SC}{7 * SDur}$.

En passant au cas le plus général du réseau *R*-redondant, nous pouvons affirmer que tout nœud à portée du puits reçoit le jeton chaque *(3*R+1)*SDur* si le réseau contient du trafic descendant sinon il reçoit tous les *(2*R+1)*SC*. Pour chaque nœud à sa portée, le puits reçoit *SC* paquet de données. D'où le débit est données par : $D = \frac{R * SC}{(3 * R + 1) * SDur}$. Si le trafic descendant n'existe pas alors la formule devient : $D = \frac{R * SC}{(2 * R + 1) * SDur}$.

Estimons la suite $\frac{R}{K * R + 1}$ où $K \in \{2 ; 3\}$. La courbe de la figure 3.9 donne une représentation de la suite en fonction du paramètre de redondance *R*. Elle montre que la suite est croissante. Elle démarre à 0.26 et converge vers 0.33 dans le cas du réseau *R*-redondant assurant un trafic descendant. Le rapport *SC/SDur* est constant et indépendant du facteur de redondance. En effet, il dépend uniquement des caractéristiques des nœuds capteurs, des besoins de l'application et du milieu surveillé. Par conséquent, nous pouvons affirmer que le

débit optimum obtenu pour un réseau *3*-Redondant est *12/10* fois supérieur à celui d'un réseau *1*-redondant et *21/10* fois supérieur celui d'un réseau *2*-redondant.

Pour un réseau dépourvu de trafic descendant, la suite démarre à 0.34 et converge vers 0.46. Le rapport du débit optimum entre un réseau 3-redondant et 1-redondant est de *9/7* alors qu'il est de *15/14* entre le *3*-redondant et le *2*-redondant.

Dans tous les cas, on voit que le débit est croissant car il dépend de la valeur de $\frac{R}{3 * R + 1}$ et du rapport *SC/SDur*. D'après la figure de la courbe 3.9, l'effet de la redondance sur le débit est significatif entre les valeurs 1 et 3 de R quel que soit la valeur du rapport *SC/SDur*. Au-delà de 3, l'effet est moins visible car la courbe croit lentement vers la limite.

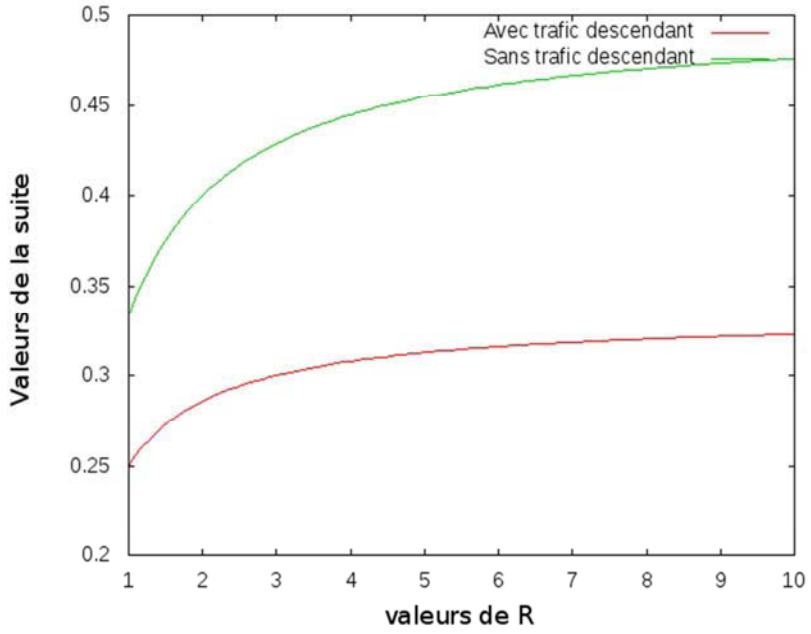


Figure 3. 9 - Courbe représentant l'impact de la redondance sur le débit

Considérons le rapport *SC/SDur*. Il permet de déterminer le nombre de trames qu'un nœud donné peut envoyer par unité de temps lors du passage de la navette. *SC* dépend de la taille du FIFO. Plusieurs situations peuvent se présenter. Si *SC* correspond à une file d'attente de petite taille et la durée de la navette grande, alors le rapport *SC/SDur* est petit et par conséquent on perd du débit. Cette situation se produit lorsqu'un nœud vide sa file d'attente alors qu'il n'a pas fini de consommer le temps de possession du jeton ou durée de la navette.

Considérons la fonction $3 * R + 1$ qui est une fonction croissante de *R*. D'après l'analyse faite ci-dessus, le puits reçoit *SC* paquets chaque *(3*R+1)*SDur*. Ceci signifie que les délais d'acheminement des paquets sont plus longs lorsque *R* est grand.

Le trafic d'une branche d'un tel réseau doit être calculé de façon à ce que les stations à portéedu puits de cette branche contiennent au plus *SC* paquets au passage du jeton. C'est sur cette approche théorique qu'ont été menées des évaluations par simulation qui confirme les gains en débit espérés.

6. Définition d'un cluster logique

Un nœud N possesseur d'un jeton peut dialoguer avec l'ensemble des nœuds de son voisinage dont la taille dépend du facteur *R*. Cet ensemble de nœuds est défini par $\{N_R, N_{R-1}, \ldots, N, \ldots, N_{R-1}, N_R\}$. Considérons $\{N_{A-R}, \ldots N_A \ldots N_{A+R}\}$ et $\{N_{B-R}, \ldots N_B \ldots N_{B+R}\}$ dont les deux nœuds centraux N_A et N_B sont en possession d'un jeton en même temps. Nous pouvons identifier les deux cas où il y a un risque d'interférences sur la trame émise par le nœud N_A, interférences induites par les activités de transmissions des nœuds de l'ensemble $\{N_{B-R}, \ldots N_B \ldots N_{B+R}\}$.

- Si le trafic descendant est possible

La trame reçue avec le moins de puissance émise par N_A est celle reçue par le nœud au plus loin c'est-à-dire N_{A+R} (en limite de portée). Cette trame, la plus fragile, est exposée aux activités provoquées par le cluster de N_B. La linéarité du réseau nous permet d'identifier le nœud du voisinage de N_B le plus agressif pour la bonne réception par N_{A+R} de la trame émise par N_A. Il s'agit de N_{B-R} comme indiqué dans la figure 3.10.a. Ce nœud (l'interférent N_{int}) n'a pas l'initiative d'envoyer des trames mais doit acquitter celles issues de N_B qui lui sont destinées.

- Si le trafic descendant n'est pas assuré

La trame reçue avec le moins de puissance émise par N_A est toujours celle reçue par le nœud au plus loin de N_A c'est-à-dire N_{A+R}. Cette trame la plus fragile est exposée aux activités provoquées par N_B. Seule la partie en direction du puits est concernée par les activités induites

par N_B. Dans ce cas, c'est N_B qui est le nœud le plus agressif (l'interférent N_{int}) quand il émet à $\{N_{B+1}….N_{B+R}\}$. Cette situation est représentée dans la figure 3.10.b.

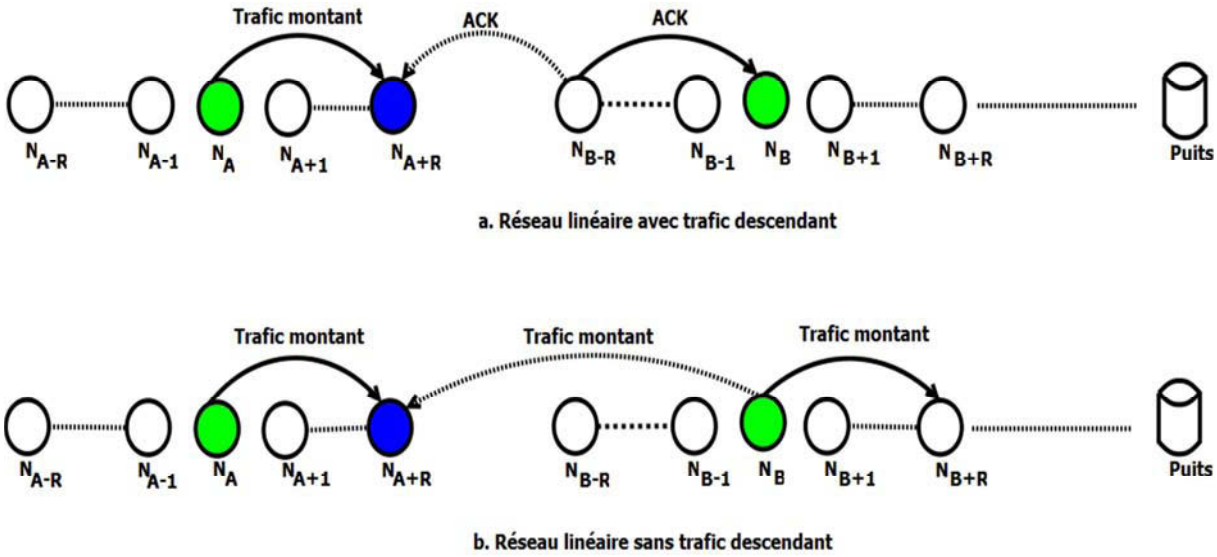


Figure 3. 10 - Identification des interférences

Pour ces deux cas, nous avons évalué dans la section précédente la distance exprimée en nombre de sauts entre N_{A+R} et le nœud interférent N_{int} qui garantisse logiquement une bonne réception. Cette distance a permis de définir un motif d'isolement autour du possesseur du jeton que nous appellerons ***cluster linéaire*** et qui nous permet une réutilisation spatiale des activités sur le réseau linéaire. Nous considérons que le nœud possesseur de jeton est le nœud central du cluster. Il exploite les autres nœuds du cluster qui sont appelés des ressources. La figure 3.11 montre une représentation du cluster.

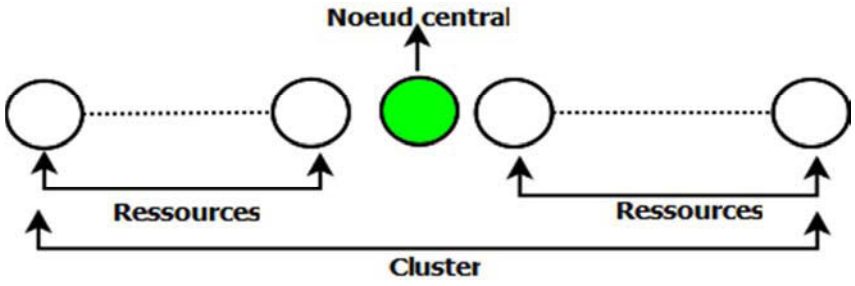


Figure 3. 11 – Représentation du cluster linéaire.

On sait que les conditions de propagation sont telles que les liaisons radio ainsi que la portée des nœuds restent constantes sur toute la ligne. Si on appelle LCSize() la taille du cluster linéaire exprimée en nombre de nœuds nous pouvons affirmer que d'après les conditions de propagation que LCSize est donnée par la formule:

$$LCSize(R) = \begin{cases} 3 * R + 1 \; avec \; trafic \; descendant \\ 2 * R + 1 \; sans \; trafic \; descendant \end{cases}$$

La taille du cluster linéaire dépend uniquement de R et croit linéairement en fonction de ce paramètre. Considérons le cluster de $\{N_{A-R,}\ldots,N_{A,\ldots,}N_{A+R}\}$. A l'instant T_0 le nœud A est possesseur du jeton. Après le passage de la navette à l'instant T_0+SDur le nœud N_{A+1} devient le possesseur du jeton et par conséquent le cluster se déplace et devient $\{N_{A-R+1,}\ldots..,N_{A+1,}\ldots.N_{A+R+1}\}$. Le processus est répété jusqu'au puits. Nous pouvons alors considérer le cluster $\{N_{A-R,}\ldots,N_{A,\ldots,}\ N_{A+R}\}$ comme un cluster se déplaçant en direction du puits par intervalle de temps réguliers équivalent à *SDur*. La figure 3.12 montre le processus de déplacement du cluster vers le puits.

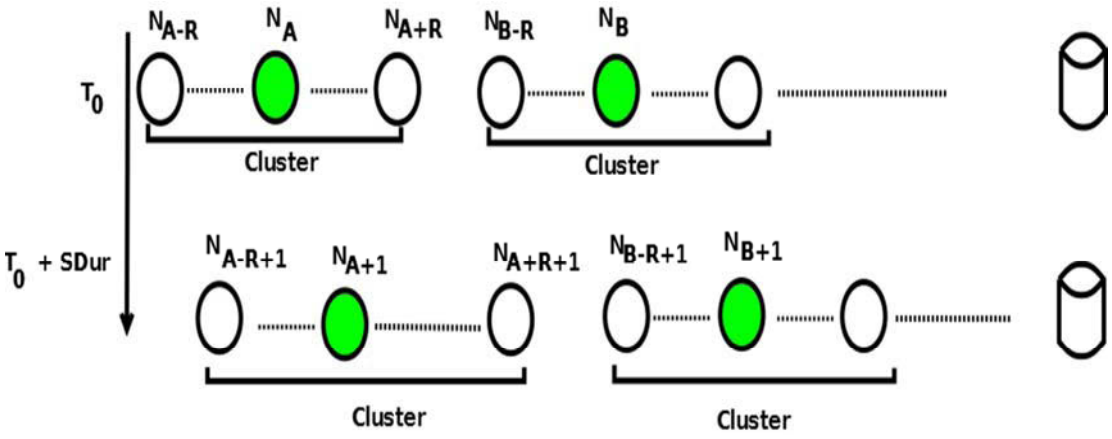


Figure 3. 12 - Processus de déplacement du cluster

Le fait de découper le réseau en clusters linéaires permet de mieux appréhender les échanges faits en parallèle entre certains nœuds du réseau.

7. Simulations et résultats

Dans cette partie, nous présentons les résultats de simulations relatives à la redondance.

7.1. Paramètres de simulation

Nous simulons notre approche de réseau *R*-redondant sous NS2. Nous considérons un réseau linéaire de 15 nœuds répartis de façon fixe en fonction de la redondance et un puits. Nous évaluons les performances d'un réseau *1*-redondant, *2*-redondant et *3*-redondant. Pour ce faire, on considère que les nœuds ont une portée maximale de 75 m. En paramétrant la distance entre les nœuds, il est possible de définir et de contrôler le voisinage des nœuds capteurs. Ainsi, pour un réseau 1-redondant on maintient la distance d à 75 m. Pour un réseau 2-redondant la distance d entre deux nœuds adjacents est fixée à 35 m. Enfin, la distance est fixée à 25 m pour un réseau 3-redondant. On compare les performances de ces trois réseaux en termes de débit au puits, de délais de bout-en-bout et de taux de délivrance. Nous faisons varier la durée de la navette de 50 à 300 ms par pas de 50 afin de déterminer la durée de navette qui optimise les différents paramètres de performances cités. La génération du trafic local commence aléatoirement entre 0 et 1s et s'arrête à 300 s. La simulation quant à elle se termine à 310 s afin de permettre aux différents nœuds de vider leur file d'attente. Chaque scénario est répété 250 fois (afin de déterminer une moyenne) et pour chacun d'eux sont calculés les délais de bout-en-bout, le taux de délivrance des nœuds ainsi que le débit au puits en considérant la moyenne sur les répétitions. Pour le calcul du débit, on fait varier la charge globale du réseau de 8 Kbps à 80 Kbps. Pour les délais de bout-en-bout, on fait varier la charge globale du réseau exprimée en nombre de paquets/s. On s'intéresse aux nœuds 1, 8, 14 et 15 en se basant sur leur position particulière. La taille des FIFO est la même pour tous les nœuds et est égale à 50 paquets.

7.2. Résultats

Les figures 3.13, 3.14 et 3.15 indiquent le débit au puits en fonction de la charge globale du réseau. Elle montre l'impact de la redondance sur le débit. L'évolution de ces courbes est similaire pour tout type de réseau avec une croissance entre 0 et 48 Kbps et un état stationnaire correspondant à la saturation du réseau au-delà de 48 Kbps. Dans la phase de croissance du débit offert, le réseau n'est pas chargé et par conséquent les nœuds parviennent

à vider leur file d'attente. De plus, du fait que la charge n'est pas forte les files d'attente se remplissent lentement au fur et à mesure. L'état stationnaire quant à lui correspond à une charge très forte du réseau qui fait que les files d'attente débordent et par conséquent la quantité de trames de données envoyées par chaque nœuds durant le passage de la navette reste constante d'où la réception constante au niveau du puits.

L'impact de la durée de la navette sur le débit est lui aussi visible sur les différentes courbes. En effet, on voit que le débit croit en fonction de la durée de la navette jusqu'à 250 ms. Au-delà de 250 ms, il n'évolue plus. Nous expliquons ce phénomène par le fait que si la taille de la navette est petite le nombre de trames envoyées par un nœud durant son passage est relativement petit et par conséquent le débit au puits est très faible. Lorsque la durée de la navette est grande comme 300 ms par exemple, les nœuds vident leurs files d'attente avant la fin du passage de la navette et par conséquent du débit potentiel est perdu quand le nœud es possession du jeton n'a plus rien à émettre une partie du passage de la navette. Donc, nous pouvons remarquer qu'avec 250 ms le nombre de trames envoyées par un nœud est optimal. Ceci est pour une taille de paquet constante et unique égale à 100 octets.

Nous pouvons constater l'effet de la redondance sur le débit. En effet, le débit croit avec le facteur de redondance ***R***. Par exemple, pour une charge de 80 Kbps et une navette de 50 ms nous obtenons un débit de 31.1 Kbps, 35.5 Kbps et 45,5 Kbps respectivement pour ***R*** = 1, 2 et 3. Ceci confirme notre analyse théorique.

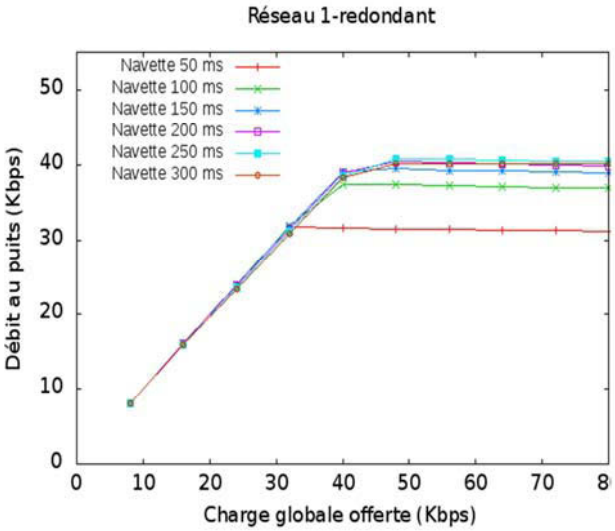


Figure 3. 13 - Débit au puits pour un réseau 1-redondant pour plusieurs navettes

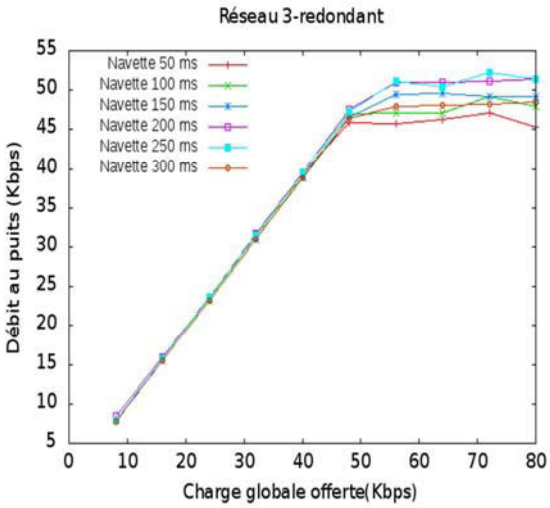


Figure 3. 14 - Débit au puits pour un réseau 3-redondant pour plusieurs navettes

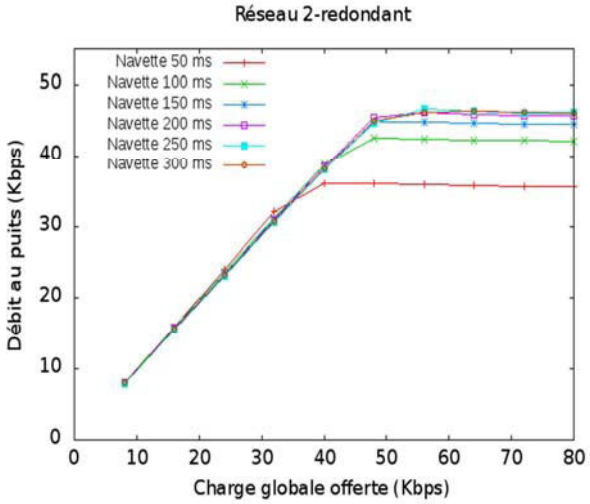


Figure 3. 15 - Débit au puits pour un réseau 2-redondant pour plusieurs navettes

Les figures 3.16, 3.17 et 3.18 représentent le taux de délivrance des nœuds 1, 8, 14 et 15 en fonction de la charge globale du réseau exprimée en nombre de paquets par seconde. On considère une navette de 250 ms et une taille de file d'attente de 50 paquets. L'évolution du taux de délivrance montre l'impact de l'effet d'écrêtage quand le réseau est fortement chargé. Cet effet d'écrêtage est plus significatif pour les nœuds les plus éloignés du puits. Par exemple, pour un réseau 1-redondant, le taux de délivrance du nœud 1 passe de 1 à 0 alors qu'il passe de 1 à 0.58 pour le nœud 8. Pour le nœud 15 le taux de délivrance reste constant et égale 1 du fait qu'il est à portée du puits.

L'impact de la redondance sur le taux de délivrance est visible sur ces courbes. En effet, le taux de délivrance croit en fonction de ***R***. La raison principale est que l'effet d'écrêtage a moins d'impact du fait de la taille du cluster qui croit en fonction de ***R***. Le découpage en cluster du réseau se déplaçant en direction du puits et la création de branches font que les paquets font moins de saut lorsque ***R*** croit. D'où ils sont moins exposés au débordement des files d'attente. Par exemple, le taux de délivrance au puits pour le nœud 8 est 100% à 68% dans le cas du réseau 3-redondant, entre 100% et 62 % dans le cas du réseau 2-redondant et entre 100% et 58% pour le réseau 1-redondant.

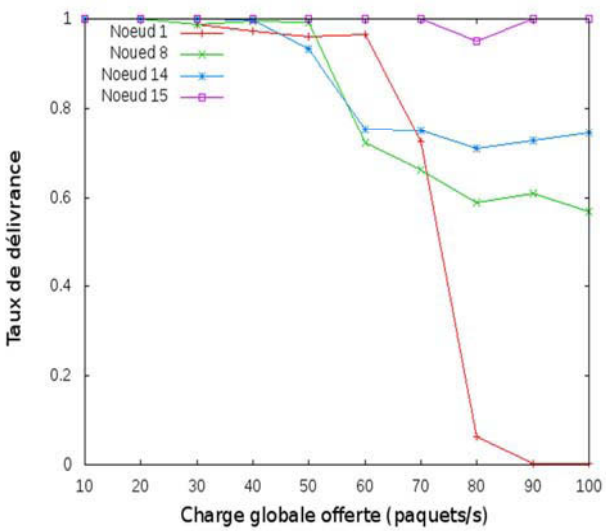


Figure 3. 18 - Taux de délivrance au puits dans un réseau 1-redondant

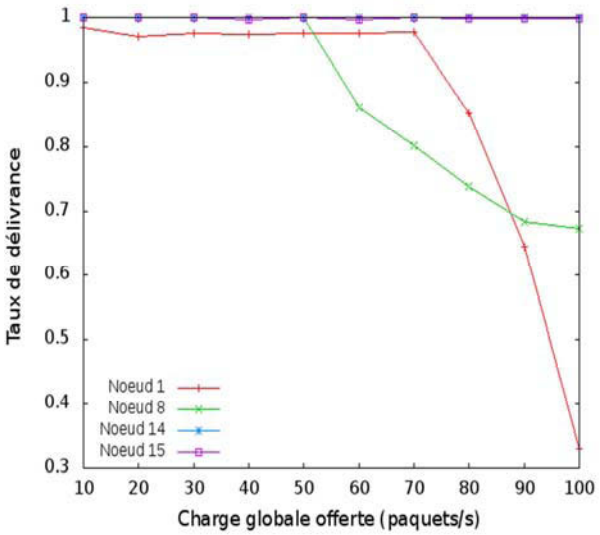


Figure 3. 16 - Taux de délivrance au puits dans un réseau 3-redondant

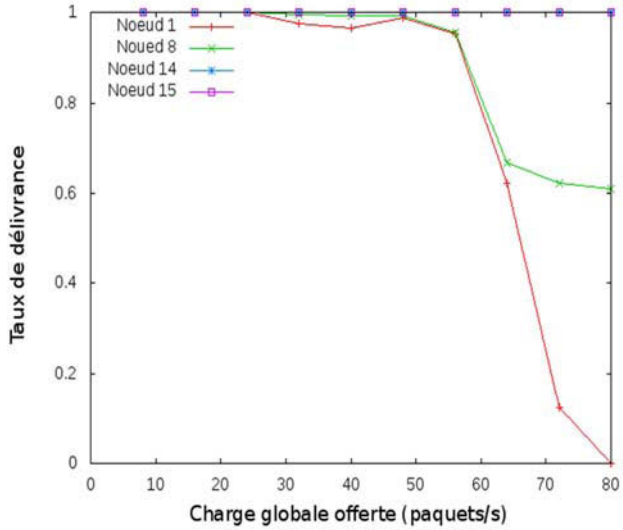


Figure 3. 17 - Taux de délivrance au puits dans un réseau 2-redondant

L'intérêt du *clustering* est visible dans le taux de délivrance au puits. Les résultats de simulation ont montré que la taille du cluster a un impact significatif lorsque la valeur du facteur de redondance croit. Les paquets sont moins exposés à l'effet d'écrêtage du fait de la répartition du réseau en branches d'une part et au *clustering* qui minimise le nombre de sauts qu'un paquet effectue avant d'atteindre le puits d'autre part.

Les figures 3.19, 3.20 et 3.21 présentent le délai de bout-en-bout en fonction de la charge globale du réseau exprimée en nombre de paquets/s pour les nœuds. On voit que les délais sont constants lorsque le réseau n'est pas chargé et qu'il commence à augmenter sous l'effet lorsque le réseau commence à être chargé. L'effet de la redondance est aussi visible dans le délai de bout-en-bout lorsque les nœuds sont proches du puits du fait qu'ils font moins de saut. Dans ce cas, plus le réseau est redondant plus les nœuds font moins de sauts pour atteindre le réseau. Par contre, pour les nœuds un peu éloignés du puits comme les nœuds 8 et 1, les délais de bout-en-bout croissent avec la redondance du fait que la périodicité de passage de la navette est plus petite.

Considérons les paquets qui survivent à l'effet d'écrêtage. Lorsque la taille des files d'attente est plus grande que la capacité de la navette, alors il arrive que certains paquets ne soient pas envoyés et qu'ils doivent par conséquent attendre la prochaine navette. On sait que la périodicité de passage de la navette est une fonction croissante de $\boldsymbol{R}$. D'où le fait que les délais d'acheminement sont plus longs dans le cas du réseau *3*-redondant. Pour optimiser les délais de bout-en-bout, il est possible d'envisager l'étude de l'impact de la mise en place d'une politique de priorité sur les paquets en se basant sur le nombre de sauts.

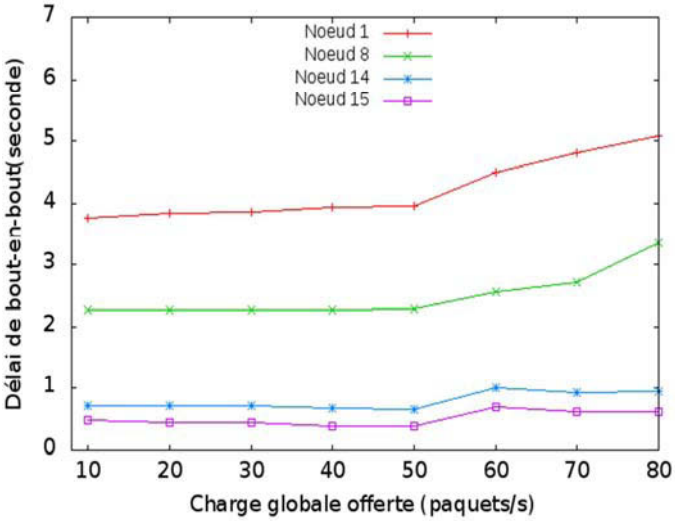


Figure 3. 21 - Délai de bout-en-bout dans un réseau 1-redondant

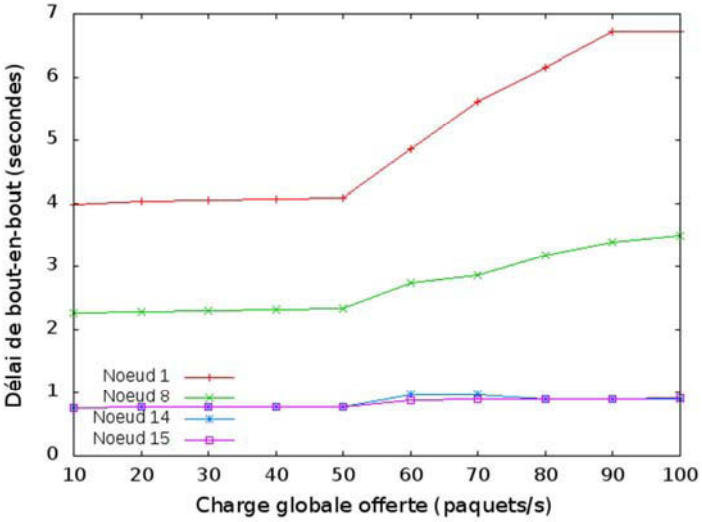


Figure 3. 20 - Délai de bout-en-bout dans un réseau 3-redondant

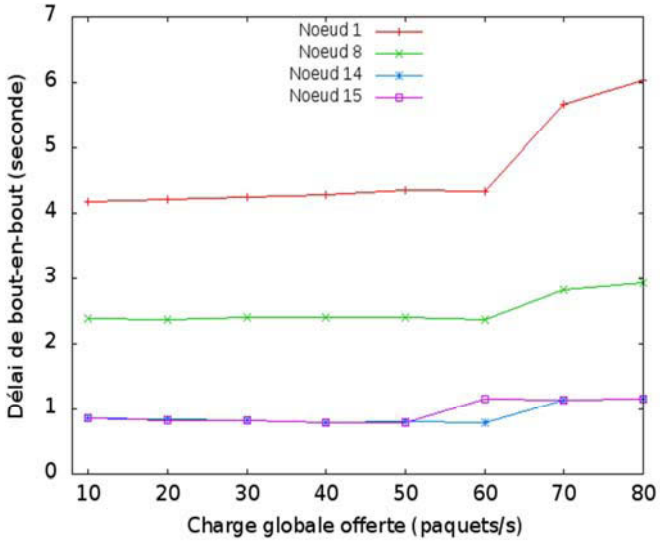


Figure 3. 19 - Délai de bout-en-bout dans réseau 2-redondant

8. Conclusion

Dans ce chapitre, nous avons présenté une technique de découpage d'un réseau linéaire en clusters physiques en considérant la portée comme une grandeur identique et invariante pour tous les nœuds. Nous avons montré que la taille du cluster dans les conditions de propagation choisies dépend du facteur de redondance ***R***. Celui-ci définit le voisinage dans un réseau linéaire i.e le nombre de voisins à gauche ou à droite qu'un nœud donné peut avoir. Nous avons ainsi défini un réseau R-redondant dans lequel un nœud donné est à portée de ***2*R*** nœuds répartis équitablement à sa gauche et à sa droite.

Nous avons montré l'impact du *clustering* sur les performances du réseau. Les paramètres réseaux tels que le taux de délivrance, le débit au puits augmentent avec la taille du cluster linéaire. En effet, le débit et le taux de délivrance sont plus importants pour le réseau 3-redondant, suivi du réseau 2-redondant.

Cependant, la déduction de la taille du cluster de façon logique basée juste sur la connaissance du voisinage i.e. la liste des nœuds à un saut, deux et/ou trois sauts du nœud possesseur du jeton ne garantit pas une bonne modélisation du milieu considéré. Nous allons maintenant voir l'impact d'un modèle de propagation plus réaliste sur la consistance des hypothèses de ce chapitre. Dans le chapitre suivant, il s'agit de bien maîtriser les interactions fortes entre les particularités d'un réseau de capteurs linéaire déployé dans un milieu dont les conditions de propagation sont convenablement représentées par un modèle de type *Log-normal Shadowing*, et exploitant une méthode d'accès au médium basée sur la circulation de jetons. Il s'agit notamment d'évaluer à partir de deux modèles de capture, à quelle distance minimale doivent circuler les jetons afin de ne pas générer de transmissions improductives.

Clustering avec prise en compte de la complexité du milieu

1. Introduction

Dans le chapitre précédent, nous avons présenté une technique de clustering de réseau de capteurs sans fil linéaire dans des conditions où les liaisons radio sont supposées stables et identiques entre nœuds répartis uniformément répartis. Pour ce faire, nous avons considéré le modèle de propagation *Tworayground* dans lequel la puissance de réception pour un lien donné reste constante pour une puissance d'émission donnée. Dans cette démarche, la taille et la distance entre clusters sont calculées de façon logique et statique en fonction de la connectivité du réseau, un lien a un comportement binaire : il est opérationnel ou non. L'expérimentation contredit cette hypothèse par la mise en évidence de liens dont les performances fluctuent ou sont opérationnels par intermittence. Ceci est dû à de nombreuses raisons comme l'instabilité du bruit radio ambiant, les fluctuations des conditions de propagation dans l'air (humidité…), l'impact de la mobilité d'éléments de la zone de déploiement sur l'effet trajets-multiple, etc. La puissance de réception à la disposition du décodeur de l'entité réceptrice ne peut pas être considérée comme parfaitement stable même si le couple émetteur-récepteur est fixe et si la puissance d'émission est constante. Ceci justifie l'existence de nombreux travaux (Iskander and Yun, 2002) qui à partir de mesures dans un environnement donné, proposent un modèle de propagation qui intègre une composante probabiliste pour tenir compte des fluctuations évoquées autour d'un comportement moyen. Le choix que nous ferons pour cette contribution est justifié dans ce chapitre. Par conséquent, un bon formalisme représentant de la taille du cluster dans un réseau linéaire nécessite plusieurs considérations :

- un modèle de propagation qui tient compte de la complexité du milieu considéré en intégrant une composante probabiliste. Dans les réseaux sans fil, le modèle de propagation *Log Normal Shadowing* est souvent utilisé pour modéliser le milieu et sa complexité,
- un mécanisme de gestion des interférences générées par les activités des nœuds possesseurs de jetons à travers un modèle de capture adéquat,

Ce chapitre traite des conséquences des interférences radio entre nœuds disposés régulièrement en ligne (à égale distance les uns des autres). Il s'agit de profiter de cette topologie particulière et simple pour montrer que la définition d'un cluster par l'exploitation du voisinage d'un nœud à un saut, deux et/ou trois sauts ne garantit pas l'absence de collision. Le choix des modèles de propagation et de capture impose une redéfinition de la notion de cluster dans les réseaux de capteurs sans fil linéaires. Il s'agit de proposer une méthode de découpage d'un réseau en cluster en prenant en compte la complexité du milieu. Les clusters qui sont linéaires de par la nature de la topologie, sont formés en adoptant une approche analytique permettant de quantifier les effets du choix de la taille de ces clusters sur les interférences et le nombre de trames correctement reçues.

2. Modélisation des conditions de propagation

Notre contribution s'appuie sur l'existence d'un réseau de capteurs linéaire déployé en extérieur, le long d'un pipeline par exemple, en milieu naturel et relativement homogène. Dans un tel cas, de nombreuses mesures expérimentales (Chen and Terzis, 2011)(Yildiz et al., 2014) ont montré que le choix d'un modèle de type log-normal *Shadowing* (Rappaport and others, 1996) est un compromis satisfaisant. Ce modèle permet d'estimer la perte en chemin PL_{dB} (et sa dispersion) exprimée en dB, à partir d'une perte en chemin mesurée ou estimée à une distance de référence d_0, un coefficient d'atténuation n dépendant du milieu et d'une fonction aléatoire X_σ représentant la diversité des résultats pour une même distance d. Dans les réseaux sans fil, la distance de référence est généralement égale à 1m.

$$PL_{dB} = PL_{dB}(d_0) + 10n\log(\frac{d}{d_0}) + X_\sigma \qquad (1)$$

Par mesures ou à partir de tables de références, il est possible d'évaluer n, la perte à la distance de référence et de choisir la loi de probabilité et ses paramètres (écart type) pour X_σ . Ce modèle nous indique que le comportement moyen PL_A de la perte en chemin entre deux nœuds distants de d est donnée par :

$$PL_A = PL_{dB}(d_0) + 10n\log(\frac{d}{d_0}) \qquad (2)$$

La dispersion autour de ce comportement est donnée par X_σ qui suit une loi gaussienne centrée (de moyenne nulle), avec comme écart type σ en dB. X_σ représente les fluctuations des puissances reçues en raison de la variabilité du milieu traversé par le signal, et d'une incertitude sur l'orientation et le positionnement des nœuds. En d'autres termes, X_σ représente le niveau d'incertitude du modèle donnée en équation 2. $PL_{dB}(d_0)$ représente la perte en chemin à la distance de référence et est calculé à partir de la formule de *Free Space* $(20 * \log_{10}(c/4\pi f d_0))$ (Rappaport and others, 1996). La célérité de la lumière $\boldsymbol{c}$ est une constante égale à $3*10^8$ $m.s^{-1}$. Notons que la couche physique utilisée dans ces travaux est celle de 802.15.4 à la fréquence f de 2,4 GHz.

Dans ce chapitre, les conditions de propagation sont supposées similaires à celles décrites dans (Hakem et al., 2014). Nous nous basons sur le fait que le milieu décrit dans cette référence est assez proche de celui utilisé pour une application utilisant un réseau de capteurs linéaire (mine, pipeline, route…). Nous nous référons sur ces résultats pour choisir une distance de référence d_0 = 1m. Dans ce cas, le calcul de la perte à la distance de référence donne -40,05 dBm. On considère deux coefficients d'atténuation : n = 2 et n = 2,5. Pour ce modèle, l'atténuation de la puissance reçue qui dépend de la distance entre émetteur et récepteur, est corrigée par une composante aléatoire gaussienne.

3. Modélisation des conditions de réception

Nous considérons pour la suite la partie du réseau délimitée par deux nœuds possesseurs d'un jeton consécutifs comme N_i et N_j de la figure 4.1. Nous supposons que le nœud N_i diffuse régulièrement, à puissance constante, des trames vers le nœud N_{i+1}. À chaque trame reçue correctement par ce nœud, est associé un niveau de puissance reçue.

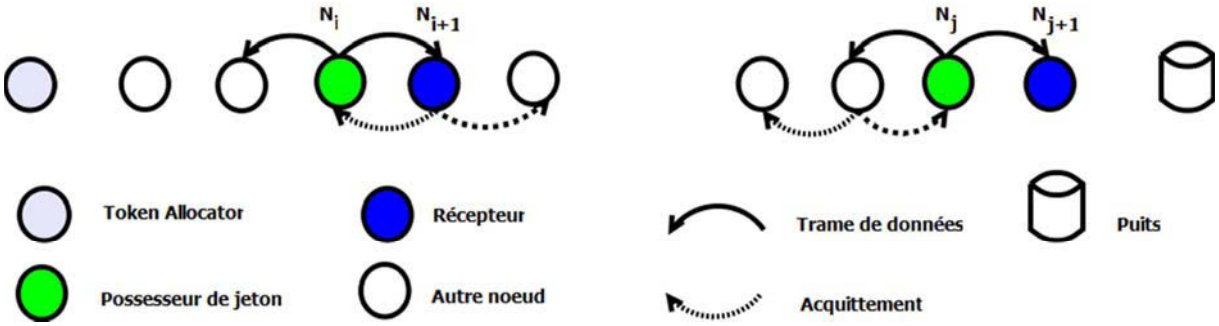


Figure 4. 1 - Activités de deux nœuds possesseurs de jetons

Comme nous l'avons rapidement dit précédemment, nous partons des hypothèses selon lesquelles nous disposons d'un réseau de capteurs linéaire. Nous considérons également que chaque nœud dispose d'une antenne omnidirectionnelle. La puissance de transmission nécessaire au bon fonctionnement d'un lien dépend de la sensibilité du récepteur, de la directivité des antennes, de leur gain, de l'atténuation du signal sur le chemin parcouru par l'onde radio et d'un critère d'exigence qui se traduit par la question suivante : quel pourcentage de trames émises mais non reçues sommes-nous prêts à accepter ? Dans cette partie, nous introduisons une façon de calculer la puissance de transmission pour un nœud possesseur de jeton. Pour cela, il s'agit de présenter d'abord la notion *d'outage probability* qui intervient dans ce calcul.

3.1. *Outage probability*

En l'absence d'interférences, on peut s'attendre à ce que la distribution de la puissance des trames reçues par N_{i+1} soit une cloche de Gauss (centrée sur la puissance moyenne reçue) comme celle donnée dans la figure 4.2 ci-dessous.

Figure 4. 2 - Distribution de la puissance reçue au récepteur à une distance donnée par le modèle *Log Normal Shadowing*

Pour que toutes ces trames aient une chance d'être reçues, il faut donc que toutes les composantes de cette distribution soient supérieures à un seuil, c'est-à-dire à la droite d'une puissance minimale correspondant au seuil de sensibilité du nœud récepteur (voir figure 4.3). Ce choix a deux conséquences.

- Il nécessite une puissance d'émission toujours supérieure à un seuil de transmission calculé en fonction du seuil de sensibilité. Ce choix à une conséquence sur la consommation en énergie des nœuds et peut ne pas être compatible avec leur capacité.

- En considérant les trames reçues avec une énergie qui correspond à la partie droite de cette distribution, les trames reçues avec une énergie excédentaire représentent un risque d'interférences pour le nœud suivant N_{i+i}.

Dans un tel cas, la puissance d'émission nécessairement utilisée par N_i, est calculée selon un compromis basé sur l'efficacité du lien radio [N_i N_{i+1}], qui s'exprime en pourcentage du nombre de trames reçues par N_{i+1} en deçà du seuil de sensibilité, par rapport au nombre de trames envoyées par N_i. C'est le principe de l'*outage probability* qui consiste à admettre

qu'un certain pourcentage de trames émises arrivera au nœud récepteur avec une puissance en deçà du seuil de sensibilité du récepteur.

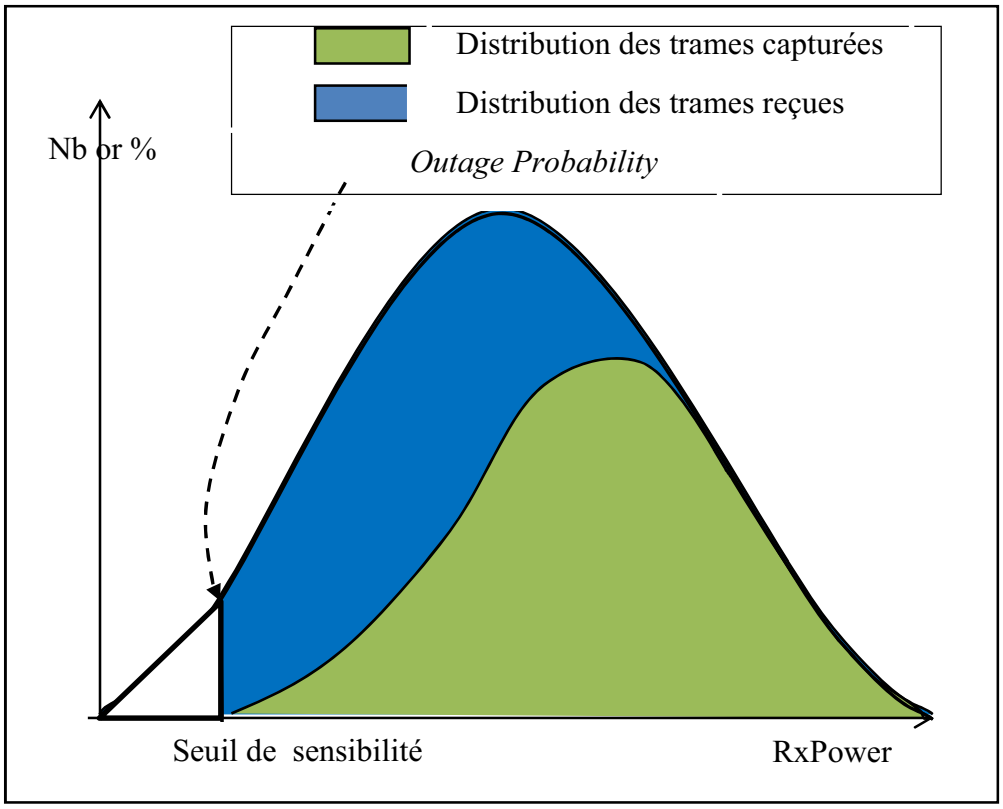


Figure 4. 3 - Représentation de l'*outage probability*

L'*outage probability* est visible sur la figure 4.3 et correspond à la partie de la distribution à la gauche du seuil de sensibilité, c'est-à-dire la surface blanche sous la cloche de Gauss de la distribution. Raisonner à partir de l'*outage probability* consiste à admettre que statistiquement toutes les trames émises ne sont pas forcément reçues. Il convient de choisir la proportion des trames envoyées qui sont reçues avec une puissance suffisante. Celle-ci est matérialisée par le rapport de la surface coloriée en vert sur la surface totale de la courbe de Gauss qui correspond à la distribution de la puissance des trames reçues (coloriée en bleu).

L'*outage probability* est donc la probabilité qu'une puissance reçue soit inférieure au seuil de sensibilité définie. Il représente par conséquent la probabilité de retransmission d'une trame pour un lien donné. Augmenter sa valeur revient donc à diminuer la puissance de transmission

au niveau de l'émetteur et augmente par conséquent les retransmissions de trames. Inversement, une diminution de sa valeur correspond à une augmentation de la consommation d'énergie et à une diminution des trames perdues ou répétées. Dans les réseaux sans fil, les valeurs de références pour l'*outage probability* sont 1%, 5% et 10% (Goldsmith, 2005).

Les trames reçues avec une énergie importante (partie droite de la distribution) sont celles qui vont générer le plus d'interférences pour les voisins de N_i et de N_{i+1}. Les effets de ces interférences sont donc dépendants de la capacité, du destinataire d'une trame, à la capturer malgré le bruit. Une trame reçue avec une énergie forte par rapport au seuil de sensibilité a intuitivement plus de probabilité d'être capturée par son récepteur. Ce comportement « intuitif » est représenté dans la figure 4.3 et va être validé par une approche analytique dans ce chapitre.

3.2. Calcul de la puissance d'émission

La puissance moyenne reçue est donnée par la formule :

$$\mathbf{P_R = P_T - PL_A} \qquad (3)$$

P_R est la puissance reçue et P_T la puissance utilisée à l'émission.

En appliquant la loi Log-normal pour modéliser les fluctuations autour de cette moyenne, nous obtenons :

$$\mathbf{P_{R_\sigma}(P_T) = P_R\ (P_T) - X_\sigma} \quad (4)$$

Soient P l'*outage probability*, P_T la puissance de transmission et P_{seuil} le seuil de sensibilité, on obtient d'après la définition de l'*outage probability* (Goldsmith, 2005) :

$$\mathbf{P(P_{R\sigma}(P_T) \leq P_{seuil}) = P(P_R(P_T) - \chi_\sigma \leq P_{seuil}) = P\left(-\chi_\sigma \leq P_{seuil} - P_R(P_T)\right)} \qquad (5)$$

Posons $z = \frac{X_\sigma}{\sigma}$. On obtient alors :

$$\mathbf{P(P_{R\sigma}(P_T) \leq P_{seuil}) = P\left(z \leq \frac{P_{seuil} - P_R(P_T)}{\sigma}\right) = 1 - Q\left(\frac{P_{seuil} - P_R(P_T)}{\sigma}\right)} \qquad (6)$$

Où $Q(x)$ (Simon, 2007) est la fonction de répartition complémentaire d'une loi de probabilité normale gaussienne centrée et réduite (Papoulis and Pillai, 2002). C'est la probabilité qu'une variable aléatoire gaussienne centrée et réduite z, soit supérieure à la valeur de x.

D'après le tableau de valeurs de la fonction complémentaire, il existe une valeur z_{seuil} telle que :

$$Q(z_{seuil}) = 1 - p(P_R(P_T) \leq P_{seuil}) \quad (7)$$

Par identification, nous avons :

$$z_{seuil} = \frac{P_{seuil} - P_R(P_T)}{\sigma} = Q^{-1}(1 - p(P_R(P_T) \leq P_{seuil})) \quad (8)$$

D'où :

$$P_R(P_T) = P_{seuil} + \sigma . z_{seuil} \quad (9)$$

D'après (1), (8) et (9) on obtient :

$$P_T = P_{seuil} - PL_{dB}(d_0) - 10n \log(\frac{d}{d_0}) + \sigma . Q^{-1}(1 - p(P_R(P_T) \leq P_{seuil})) \quad (10)$$

En se basant sur les résultats présentés dans (Hakem et al., 2014), nous avons estimé la puissance nécessaire à la transmission de trames reçues dans 90%, 95% et 99% des cas pour des nœuds distants respectivement de 25 m, 50 m et 75 m dans le cas d'un lien radio plus ou moins canalisé (n = 2,05 et n = 3). Nous considérons une dispersion modélisée par un écart type de 3.04, une perte en chemin à une distance de référence d_0 de 1 m estimée à -40,05 dB et un seuil de sensibilité de -92 dBm. Le tableau 2 suivant représente différentes puissances de transmission en dBm pour différentes valeurs de la distance et de l'*outage probability*.

Tableau 2: Tableau des puissances d'émission en fonction de la distance et de l'*outage probability*

	Outage probabilty	**25 m**	**50 m**	**75 m**
Puissance de transmission (dBm) pour n = 2,05	1 %	-15.78	-9.61	-6
	5 %	-17.85	-11.68	-8,07
	10 %	-18.95	-12.77	-9.17
Puissance de transmission (dBm) pour n = 2	1 %	-2.5	6.52	11.80
	5 %	-4.57	4.45	9.73
	10 %	-5.67	3.36	8.64

Les valeurs obtenues pour la puissance de transmission varient entre 11,80 dBm et -18,95 dBm. Ces valeurs sont assez similaires aux valeurs de puissance d'émission pratiques dans les réseaux de capteurs sans fil.

3.3. Introduction des modèles de capture

Outre les paramètres du modèle de propagation, il est aussi important de mettre en place une bonne politique de gestion des interférences au niveau du récepteur du nœud N considéré. Des réceptions simultanées peuvent conduire : (i) soit à des collisions ; (ii) soit à la réception de la trame destinée à N, ce que l'on nomme capture productive ; (iii) soit à la réception d'une trame non destinée à N, qualifiée de capture improductive (Azimi-Sadjadi et al., 2006). Dans les réseaux sans fil, l'effet de capture est un mécanisme qui a un impact fort sur les performances quand les nœuds récepteurs sont exposés aux effets des interférences. Plusieurs travaux basés sur des analyses, des simulations et des expérimentations ont permis de mettre en évidence l'effet de capture. Il exprime la possibilité de recevoir une trame malgré le bruit

électromagnétique. Celui-ci peut être naturel (orage, soleil, étoiles..) ou artificiel (téléphones mobiles, transmissions radio). Dans le cas d'interférences artificielles causées par les transmissions radio, la capture est généralement basée sur un niveau limite, appelé seuil de capture, exprimé en fonction des puissances reçues du nœud émetteur et des nœuds générateurs de bruit appelés interférents. Ainsi, dans (Lee et al., 2007) les auteurs présentent une étude expérimentale par *testbed* de la capture de 802.11a en se basant sur les puissances reçues. Ils considèrent trois nœuds : S1 comme émetteur, S2 comme nœud interférant et un nœud R comme récepteur des trames émises par S1. En faisant varier les instants d'envoi des trames de S1 et S2 selon plusieurs scenarios afin d'observer le comportement du nœud récepteur R, les auteurs ont pu montrer que l'effet de capture dans 802.11 peut être un phénomène binaire dépendant du rapport entre les puissances des signaux utile et interférents appelé SIR (*Signal-to-Interference Ratio*), ou probabiliste si on ajoute à la capture le paramètre *durée* défini par la longueur de la coïncidence entre les signaux de la trame utile et ceux de la ou des trames interférentes. D'après ces travaux il existe un intervalle de puissances de réception dans lequel il existe une probabilité de recevoir correctement une trame. Cet intervalle est noté intervalle probabiliste. Cette nature probabiliste de la capture peut avoir des avantages sur la gestion des interférences en minimisant le nombre des collisions. Les travaux de (Kosunalp et al.) présentent les effets de la capture dans les réseaux sans fil à partir d'une étude expérimentale utilisant la couche MAC ALOHA et des interfaces radio *Iris* équipées de transmetteur AT86RF230. Les expériences réalisées ont permis aux auteurs de montrer que l'effet probabiliste de la capture dépend du nombre d'octets qui se chevauchent entre les paquets d'un nœud émetteur et ceux des interférents à un moment donné. Plus le nombre d'octets en chevauchement est grand plus la probabilité de capture est faible. Cette probabilité est plus faible quand le nombre de nœuds interférents est plus grand. Dans (Gezer et al., 2010), les auteurs présentent une modélisation et une analyse de l'effet de capture de la couche MAC 802.15.4 en mode *beacon*. Ces travaux ont montré l'impact des paramètres de la supertrame sur la probabilité de capture des paquets en évaluant le rapport entre signal utile (C) et la somme des signaux interférant (I). D'autres mesures expérimentales effectuées (Van Den Bossche, 2007) dans une chambre anéchoïque, montrent l'effet probabiliste de la capture, mais surtout que l'intervalle probabiliste peut être définie d'une manière plus optimiste et plus proche de la réalité que ne le prévoit l'approche binaire prévue dans certaines normes (IEEE, 2003)(IEEE, 2005).

Nous pouvons donc considérer que la capture peut être un phénomène binaire ou probabiliste selon le niveau de finesse de notre étude. Dans la suite, nous détaillons ces types de capture et analysons leur impact dans un réseau de capteurs sans fil linéaire.

3.3.1. La capture binaire

Ce modèle de capture dit binaire est basé sur le fait qu'une trame est capturée ou non selon des considérations de puissance reçues des trames en concurrence au niveau du récepteur. Dans ce cas, l'évolution du récepteur passe brutalement de l'état de collision à celui de capture. Le paramètre utilisé pour déterminer la bonne réception d'une trame ou non au niveau du récepteur est SIR défini ci-dessus. Dans ces conditions, une trame est capturée si le SIR est supérieure à un SIRseuil. On suppose dans ce cas qu'il existe un SIR seuil noté SIR_{seuil} au-delà duquel toute trame reçue avec une puissance supérieure au seuil de réception P_{seuil} est reçue correctement malgré le bruit généré par un signal interférent.

La figure 4.4 illustre la capture binaire. La figure ne concerne bien évidemment que les trames reçues avec une puissance supérieure au seuil de sensibilité P_{seuil}. Pour toute autre trame reçue avec une puissance inférieure à $P_{seuil,}$ on considère qu'elle est perdue et par conséquent la capture ne s'applique pas.

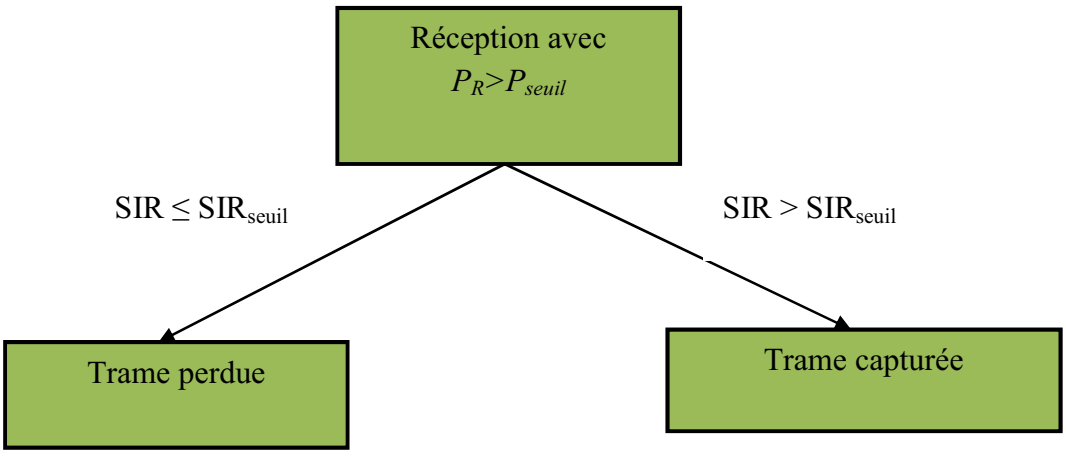


Figure 4. 4 - Représentation de la capture binaire.

3.3.2. La capture probabiliste

Dans le cas de la capture probabiliste, la frontière SIR_{seuil} considérée précédemment est à remplacer par l'intervalle probabiliste définie ci-dessus et dans lequel il existe des chances de capture. Par la suite, nous notons I_{proba} l'intervalle de capture probabiliste. Cet intervalle I_{proba} est défini par $[SIR_{seuilproba}, SIR_{seuilGarantie}]$. $SIR_{seuilproba}$ est la borne inférieure dans l'intervalle I_{proba} et est définie comme le seuil de réception probabiliste. Il représente la valeur du SIR en deçà de laquelle la trame utile est considérée comme non capturée. $SIR_{seuilGarantie}$ est la borne supérieure de I_{proba}, il est défini comme un seuil réception garantie. Il représente la valeur de SIR au-delà duquel on considère que la réception de la trame utile est garantie. La figure 4.5 montre illustre la capture probabiliste. Ici encore, on ne considère que les trames utiles reçues avec une puissance supérieure au seuil de sensibilité.

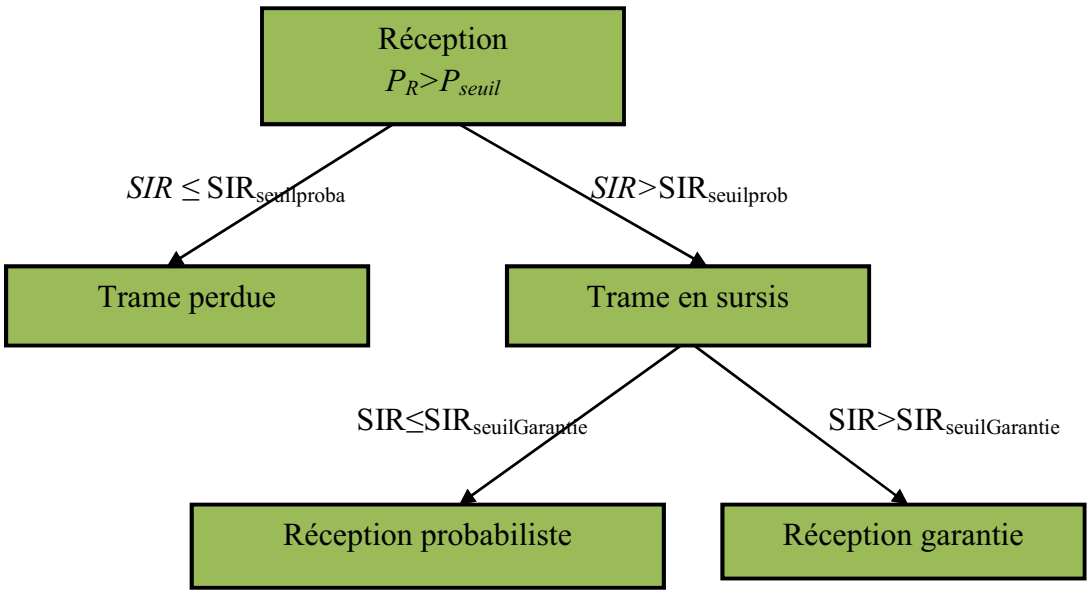


Figure 4. 5 - Représentation de la capture probabiliste.

Dans le cas de la capture probabiliste, il faut identifier trois segments (intervalles) contenant le SIR.

- Si $SIR \in]-\infty, SIR_{seuilProba}[$ alors la trame est perdue.

- Si $SIR \in [SIR_{seuilGrantie}, +\infty[$ alors la trame est capturée.
- Si $SIR \in [SIR_{seuilProba}, SIR_{seuilGrantie}[$ alors la probabilité de capture de la trame est caractérisée par la loi de capture $[SIR_{seuilProba}; SIR_{seuilGrantie}[\rightarrow F_{cap}$.

F_{cap} est une fonction représentant la probabilité de capture. Dans l'intervalle où la capture a un comportement probabiliste il faut considérer pour chaque trame reçue la grandeur $(P_{utile} - P_{interférent})$ qui n'est autre que le SIR et pondérer le nombre de trames de ce type par une probabilité de capture. Dans notre démarche, nous allons déduire les valeurs de cette probabilité de mesures issues de la bibliographie. Donc, nous n'avons pas besoin de faire des hypothèses supplémentaires sur le comportement de la fonction F_{cap}. Le choix fait sur l'intervalle probabiliste sera expliqué un peu plus loin dans ce chapitre.

4. Méthodes et démarches

Considérons le tronçon d'un réseau linéaire représenté par la figure 4.6 et analysons à l'aide du modèle de propagation retenu, l'incidence de la distance du nœud émetteur sur la distribution des trames reçues par la station B (qui sera par la suite notre nœud de référence). Une simulation faite sur l'outil NS2, consistant à faire émettre par A 10 000 trames de taille 100 octets à une puissance de -4.68 dBm, nous donne les résultats de la figure 4.7 qui indique la distribution des puissances reçues par B, C, D et E. Dans le modèle de référence considéré, on suppose que les nœuds émettent avec la même puissance d'émission. Nos simulations sont faite pour $n = 2.5$ et $\sigma = 3$. Dans la suite de ce travail, nous conserverons les mêmes paramètres pour l'étude analytique et pour les simulations.

.

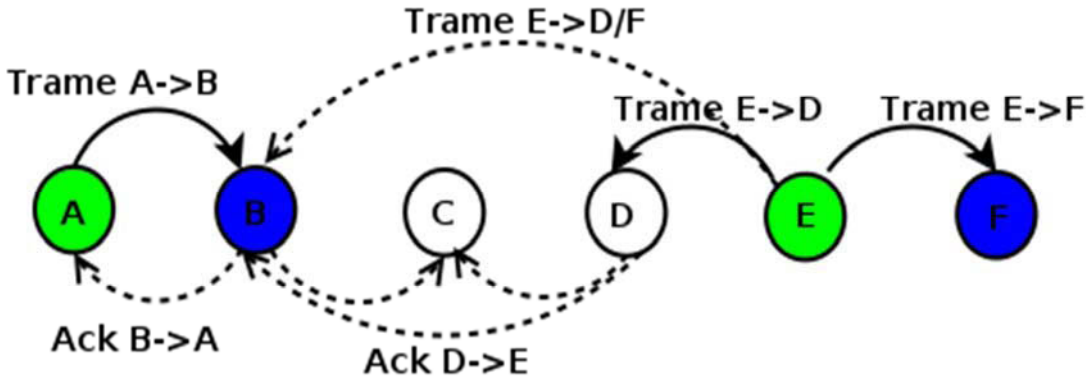


Figure 4. 6 - Conditions de réception de B quand A et E sont possesseurs d'un jeton.

Dans les simulations, nous considérons les puissances reçues sur les intervalles [x_i x_i+1] et la puissance de transmission est calculée pour un lien de distance d de 25 m. Soit :

CpA(x_i) : le nombre de trames reçues de A avec une puissance comprise dans l'intervalle [xi x_i+1] et PrA(x_i) la probabilité de recevoir une telle trame.

CpD(x_j) : le nombre d'acquittements reçus de D avec une puissance comprise dans l'intervalle [x_j x_j+1] et PrD(x_j) la probabilité de recevoir un tel acquittement.

CpE(xj) : le nombre de trames de E reçues avec une puissance comprise dans l'intervalle [x_j x_{j+1}] et PrE(x_j) la probabilité de recevoir une telle trame.

De manière générale, on appelle CpN(x_j) le comptage des trames ou des acquittement reçus par B et venant de N. N représente les nœuds D ou E. PrN(x_j) est la probabilité associée à une telle réception. Les résultats de simulations donnent les différentes répartitions de la puissance reçue en B pour les nœuds A (à 1 saut), D (à 2 sauts), E (à 3 sauts) et F (à 4 sauts) selon le modèle de référence considéré comme indiqué dans la figure 4.7. Ces répartitions montrent la nature gaussienne du modèle de propagation. Pour celle à 1 saut, on voit l'effet de l'*outage probability* défini, soit 1000 paquets reçus en deçà de la sensibilité qui représentent 10% du nombre total de paquets émis.

Si le seuil de sensibilité d'un nœud est de l'ordre de -92 dBm, une activité d'émission à 4 sauts (F) a une influence négligeable sur la capacité de réception en B. En particulier, si A et A' sont deux émetteurs possesseurs consécutifs et actifs au même moment, l'acquittement de B' à A' représente une activité à 4 sauts, ce qui aura un impact négligeable sur les conditions de réception de la trame de A par B.

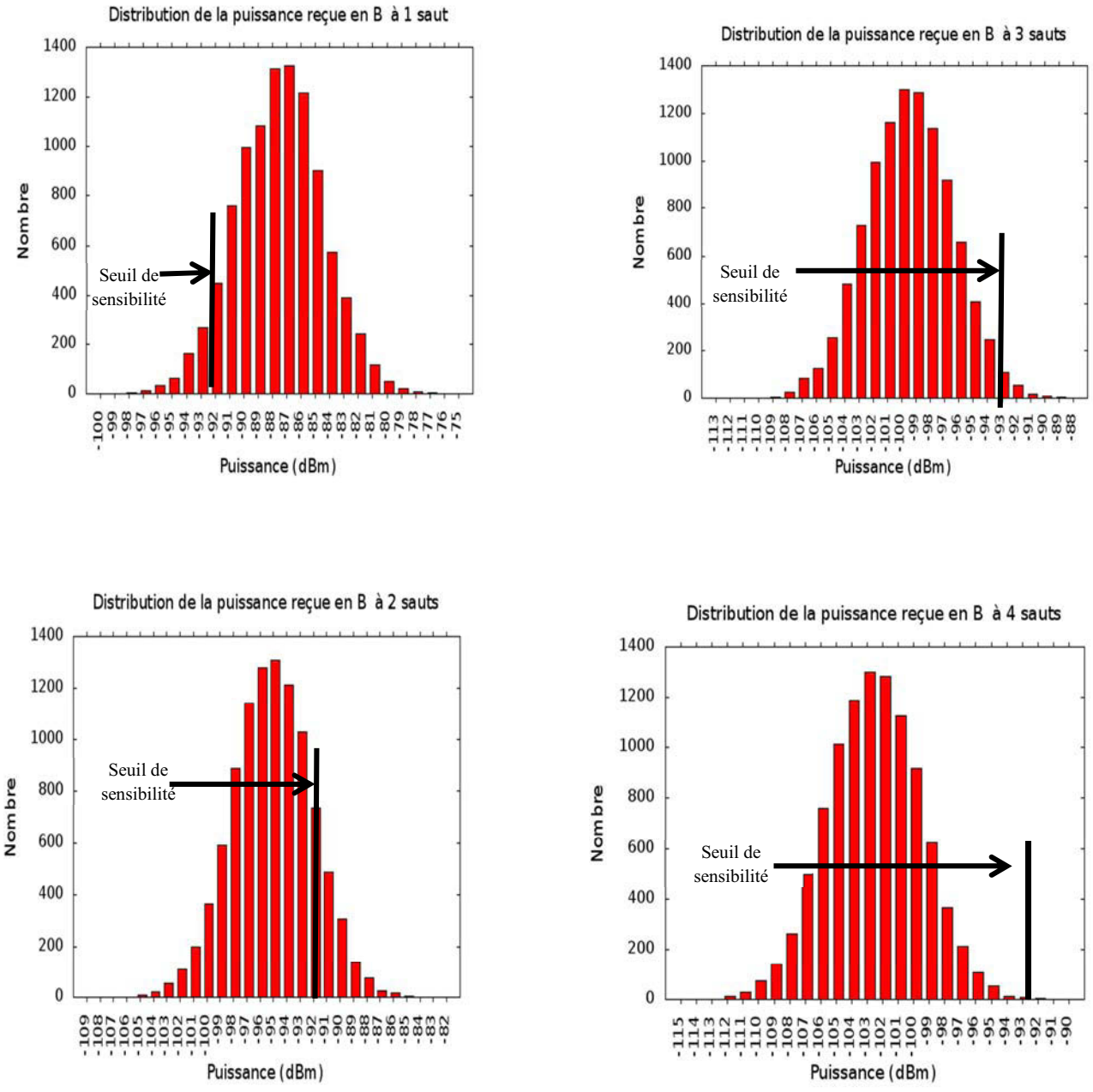


Figure 4. 7 - Distribution de la puissance reçue en B de A.

Nous allons détailler les conditions de réception du nœud de référence B dans ce cluster, quand les nœuds A et E utilisent leur jeton pour échanger des trames acquittées avec leurs voisins à 1 saut. Le cas le plus critique pour B se produit quand A s'adresse à B, et quand E s'adresse à D ; B et D devant acquitter respectivement à A et à E. Un raisonnement dual pourrait être fait pour la station D en raison de la symétrie de la figure par rapport à C. Dans cette partie de notre démarche, nous allons supposer que les trames émises sont de longueurs comparables et que la distance entre deux nœuds adjacents est fixée à d.

Pendant la réception de la trame destinée à notre nœud de référence B, le nœud E peut être en train de finir l'émission de la trame de données qui sera acquittée par D. Dans ce cas, la réception des signaux portant la trame de A sera exposée aux interférences à 3 sauts pendant l'émission de E puis aux interférences à 2 sauts pendant l'acquittement de D (si cet Ack est émis rapidement) si on considère de cluster de taille 4. La coïncidence temporelle de ces activités sera un raffinement apporté à notre contribution dans la partie VI de ce chapitre. En B, peuvent donc interférer la trame issue de A avec celle issue de E (interférences à 3 sauts), et la trame issue de A avec l'acquittement issu de D (interférences à 2 sauts). Ces deux types d'interférences sont décrits à partir de la distribution des puissances qui arrivent à B.

Les puissances reçues par B de A, D et E correspondent aux distributions de la puissance reçue respectivement avec les distances : d, 2*d et 3*d. En comparant ces puissances deux à deux, et en fonction de deux modèles de capture, nous allons déduire le taux de trames reçues par B.

Nous pouvons constater qu'une trame reçue de A par B est exposée aux activités induites par E et D, en particulier quand la puissance reçue de la trame de A est faible et celle reçue de l'acquittement de D est forte. Par conséquent, la réception cohérente de la trame issue de A (sa capture) peut être remise en cause. C'est ce point qui va être étudié dans la suite à partir de deux modèles de capture.

Pour expliquer notre démarche, nous allons travailler en deux étapes qui ont en commun le fait de considérer un intervalle I_{proba} de valeurs du SIR dans lequel le comportement du récepteur passe de la détection de collision à celui de la capture. Dans un premier temps, nous considérons la capture binaire. Dans un second temps, nous introduisons des mesures associées aux évolutions de cette transition dans l'intervalle I_{proba}, nous sommes alors dans le cas de la capture probabiliste.

5. Analyse de l'impact de la distance entre deux nœuds possesseurs jetons

Dans cette partie, nous faisons une analyse de l'impact de la distance entre deux nœuds possesseurs d'un jeton avec les deux modèles da capture définis ci-dessus.

5.1. En capture binaire

Il s'agit ici de faire d'abord une analyse théorique de la capture et ensuite de confirmer cette théorie par une approche de simulation.

5.1.1. Approche théorique

La capture définie à partir d'un seuil SIR_{seuil} a été présenté au paragraphe 3.3 de ce chapitre. Nous allons dans un premier temps évaluer la distance entre B et un interférent qui permet aux trames de A d'être capturées par B. En d'autres termes, si A est à 1 saut, à combien de sauts au moins doit se trouver l'interférent pour que la réception se passe bien dans x % des cas?

Énoncé : La probabilité p_h que le nœud A capture une trame à 1 saut malgré le bruit généré par un nœud à *h* sauts de B est donnée par :

$$p_h = Q\left[\frac{SIR_{seuil} - (P_{T(1-hop)} - P_{T(h-hop)}) - (10 * n * \log h)}{\sigma\sqrt{2}}\right].$$

Où PT représente la puissance d'émission.

Preuve :

On sait que :

$$\begin{cases} P_T = P_{seuil} - PL_{dB}(d_0) - 10n\log(\frac{d}{d_0}) + \sigma . Q^{-1}(1 - p(P_R(P_T) \leq P_{seuil})) \\ P_{R_\sigma}(P_T) = P_T - PL_{dB}(d_d) \pm X_\sigma \end{cases}$$

Soit : PR_σ(1-hop) la puissance reçue de B à 1 saut à une distance de d_1 et PRσ(h-hop) la puissance reçue de B à h (h>1) saut à une distance de d_h. On a :

Clustering avec prise en compte de la complexité du milieu

PR_{σ}(1-hop) $= P_{T(1-hop)} - PL_{dB}(d_1) \pm X_{\sigma 1}$

PR_{σ}(h-hop) $= P_{T(h-hop)} - PL_{dB}(d_h) \pm X_{\sigma h}$

Par conséquent :

$$P_{R_{\sigma(1-hop)}} - P_{R_{\sigma(h-hop)}} = (P_{T(1-hop)} - P_{T(h-hop)}) + (PL_{dB}(d_1) - PL_{dB}(d_h) + (X_{\sigma 1} - X_{\sigma h}))$$

D'après (1) l'équation devient :

$$P_{R_{\sigma(1-hop)}} - P_{R_{\sigma(h-hop)}} = (P_{T(1-hop)} - P_{T(h-hop)}) + (10 * n * \log\frac{d_h}{d_1}) + (X_{\sigma 1} - X_{\sigma h}))$$

En posant $P_{R_{\sigma(1-hop)}} - P_{R_{\sigma(h-hop)}} = SIR$ (en dBm)

On sait que $X_{\sigma 1} \sim N(0, \sigma_1)$ et $X_{\sigma h} \sim N(0, \sigma_2)$, ce qui signifie que $X_{\sigma 1}$ (resp. $X_{\sigma 2}$) suit une loi normale de moyenne 0 (resp. 0) et d'écart type σ1 (resp σ_2).

On sait que la somme (ou la différence) de deux gaussiennes centrées et réduites de même écart type est une gaussienne centrée dont l'écart est doublé. Donc, $X_{\sigma 1} - X_{\sigma h} \sim N(0, 2 * \sigma^2)$

Ce qui entraine que le SIR suit une loi normale de moyenne $\sigma_1 = \sigma_2$ et d'écart $\sigma_1 + \sigma_2$. On sait que type $\sigma_1 = \sigma_2$ car nous sommes dans les mêmes conditions de propagation. Nous donc dire que $SIR \sim N(\mu_{SIR}, 2 * \sigma)$ où $\sigma = \sigma_1 = \sigma_2$.

$$\mu_{SIR} = \left(P_{T(1-hop)} - P_{T(h-hop)}\right) + \left(10 * n * \log\frac{d_h}{d_1}\right)$$

La condition de capture binaire est donnée par : $SIR - SIR_{seuil} \geq 0$ c'est-à-dire :

$$(P_{T(1-hop)} - P_{T(h-hop)}) + (10 * n * \log\frac{d_h}{d_1}) + (X_{\sigma 1} - X_{\sigma h})) - SIR_{seuil} \geq 0$$

Considérons $z = (P_{T(1-hop)} - P_{T(h-hop)}) + (10 * n * \log\frac{d_h}{d_1}) + (X_{\sigma 1} - X_{\sigma h})) - SIR_{seuil}$

$z \sim N(\mu z, 2*\sigma 2)$ avec : $\mu_z = (P_{T(1-hop)} - P_{T(h-hop)}) + (10 * n * \log\frac{d_h}{d_1}) - SIR_{seuil}$

La probabilité de capture p est donnée par la formule :

Clustering avec prise en compte de la complexité du milieu

$$p(z > 0) = p\left(\frac{z-\mu_z}{\sigma\sqrt{2}} > \frac{-\mu_z}{\sigma\sqrt{2}}\right) = Q(\frac{-\mu_z}{\sigma\sqrt{2}})$$.

Donc $p(z > 0) = Q(\frac{SIR_{seuil}-(P_{T(1-hop)}-P_{T(h-hop)})-(10*n*\log\frac{d_h}{d_1})}{\sigma\sqrt{2}})$

En posant : $\frac{dh}{d1} = h$, on obtient :

$$p_h(z > 0) = Q(\frac{SIR_{seuil} - (P_{T(1-hop)} - P_{T(h-hop)}) - (10 * n * \log h)}{\sigma\sqrt{2}})$$

Le seuil de capture est dans ce modèle une constante souvent égale à 10 dB, c'est le cas par exemple dans la norme 802.15.4 (IEEE, 2003) et 802.11 (IEEE, 2005).

Pour des raisons de simplification, nous allons considérer là-aussi que notre objectif est de capturer 90% des trames reçues de A par B.

Dans ces conditions, la valeur de h optimale s'obtient par calcul en posant :

$$Q^{-1}(0,9) = \frac{SIR_{seuil} - (P_{T(1-hop)} - P_{T(h-hop)}) - (10 * n * \log h)}{\sigma\sqrt{2}}$$

Ce qui donne : $\log h = \frac{10-Q^{-1}(0,9)*3*\sqrt{2}}{10*2.5}$ soit h >= 3.

Donc, le rapport h entre les distances du nœud de référence aux nœuds interférents et émetteur définit en réalité de façon analytique la taille du cluster. La figure 4.8 ci-dessous donne la probabilité de capture en fonction de h. La courbe est obtenue à partir de l'étude analytique réalisée si dessus. Ainsi, nous constatons que la valeur de h qui assure un seuil de probabilité d'au moins 90% peut correspondre à plusieurs valeurs entières. Nous passons à une analyse des résultats. Supposons le cas où n = 2,5. Les valeurs envisageables de h sont 3, 4, 5. Nous sommes donc en fait face à un compromis. Si h =3, la probabilité théorique de capture (avec le modèle binaire) ne garantit pas une réception à 90%, mais la taille du cluster est de 4. Si h > 3, la probabilité théorique de capture est au-delà de nos exigences mais la taille du cluster est plus grande. Nous avons de cas le choix entre plusieurs taille de cluster (5, 6, etc) pour lesquelles la condition de bonne réception est vérifiée. Nous sommes confrontés au choix suivant : soit un nombre élevé de perte mais avec une présence des jetons plus fréquente ; soit moins de perte mais avec des jetons plus rares. Ceci nous conduit à approfondir cette étude trop simpliste avec un modèle de capture plus raffiné.

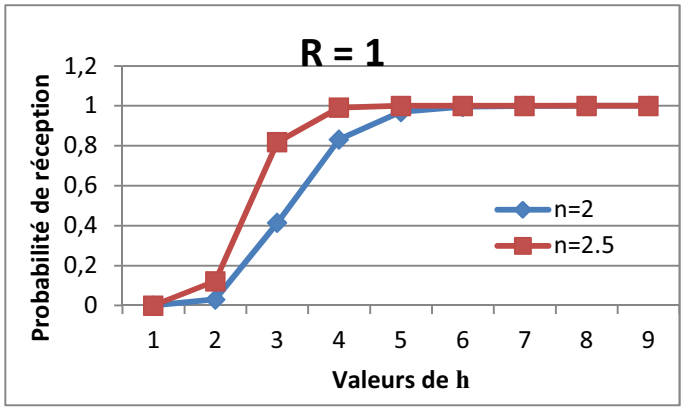


Figure 4. 8 - Probabilité de réception en fonction de la distance de l'interférent

5.1.2. Approche par simulation

La simulation de la capture dans le cas binaire est réalisée de la façon suivante. Toute trame T_A reçue en B avec une puissance dans l'intervalle $[x_i\ x_{i+1}]$, sera capturée si :

- elle est reçue avec une puissance supérieure au seuil de sensibilité P_{seuil},
- la trame T_N arrivant en même temps en B avec une puissance dans l'intervalle $[x_j\ x_{j+1}]$ satisfait à la condition de capture.

Autrement dit, pour un x_i donné, il faut identifier tous les cas pour lesquels x_j satisfait la condition de capture. La probabilité qu'une trame reçue de A avec la puissance x_i soit capturée est donnée donc par :

$$Pr_{cap}(x_i) = \sum_{J=-\infty}^{J=i-SIR_{seuil}} PrA(x_i).PrN(x_j) = PrA(xi)\sum_{J=-\infty}^{J=i-SIR_{seuil}} PrN(x_j)$$

La figure 4.9 donne les résultats obtenus par une simulation quand l'interférent est à 2 et 3 sauts dans le cas de la capture binaire pour un cluster de taille 4. À l'aide de cette figure, nous allons introduire quelle partie de la distribution des trames est affectée par les interférences. Les zones d'interférences sont représentées par les surfaces en vert formées par les intersections des courbes représentant les interférents (2 sauts et 3 sauts) et la courbe représentant le seuil de capture binaire en trait bleu. Cette courbe est en fait un décalage de la courbe à 1 saut de 10 dB. Dans le cas des interférences provoquées par le nœud à 2 sauts, la figure montre que le risque de perte de paquets (collisions et *Outage probability*) concerne

environ 6000 trames .sur les 10 000 envoyées. Ce risque est moindre dans le cas du nœud à 3 sauts de B (environ 1 000 trames). Ces résultats confirment la nature pessimiste en terme de perte de trames de la capture montrée dans le modèle analytique étudié plus haut pour un cluster de taille 4.

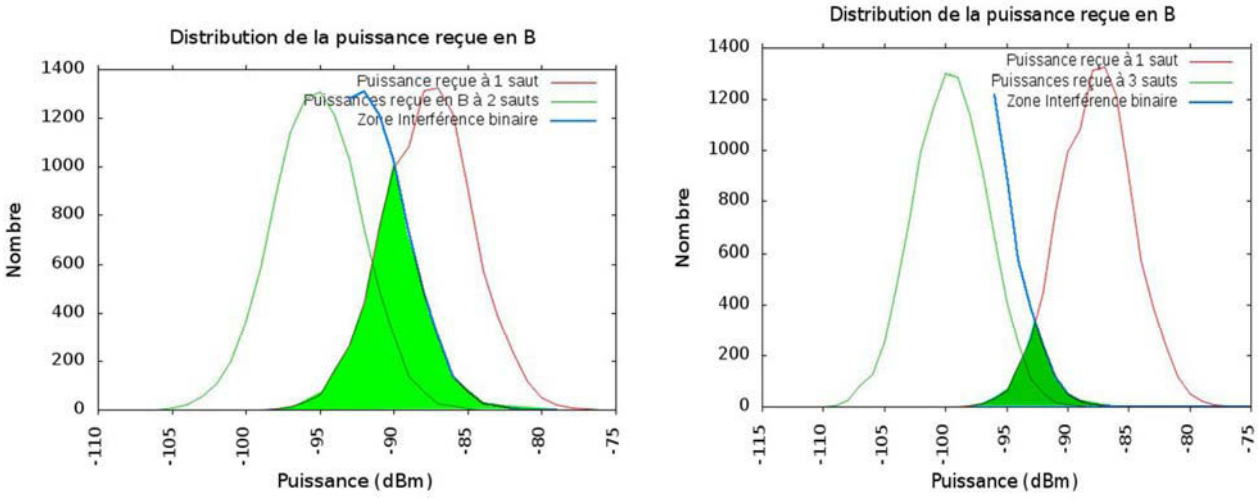


Figure 4. 9 - Impact sur la capture d'une activité à 2 sauts et à 3 sauts

5.2. Cas d'une capture probabiliste

Dans le cas d'un cluster de 4, l'hypothèse d'un comportement de capture binaire donne des résultats assez pessimistes car beaucoup de trames destinées à B ne sont pas capturées si le nœud D ou le nœud E émet en même temps que A. Cette situation correspond aux valeurs de 2 et 3 de h dans la figure 4.8. En effet, on note des probabilités de capture équivalentes à 0.12 et 0.81 pour une activité d'un interférent respectivement à 2 et 3 sauts du nœud B.

Les mesures faites par expérimentation (Lee et al., 2007)(Van Den Bossche, 2007), ont montré que pour la couche physique de 802 .15.4 qui définit la bande passante et la modulation utilisée, la capture suit un comportement probabiliste quand les puissances reçues sont proches, et quasi binaire quand elles sont très différentes. Cette remarque nous permet de récupérer le formalisme introduit pour un comportement binaire et de raffiner notre approche.

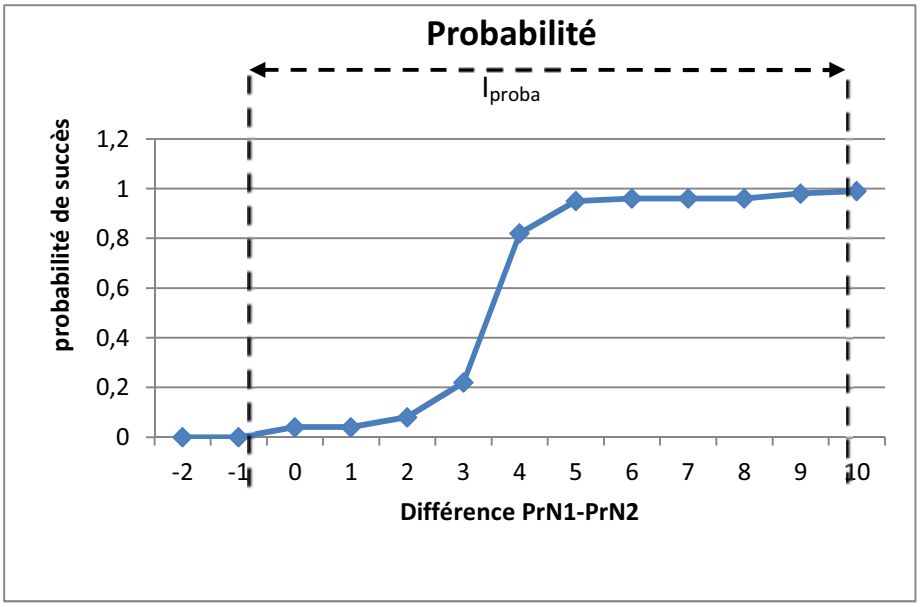


Figure 4. 10 - Intervalle de capture probabiliste

La figure 4.10 montre un exemple d'intervalle de capture probabiliste I_{proba}. Donc, pour tout SIR compris dans -1 et 10 dBm la trame utile a une probabilité (donnée par l'axe des ordonnées) d'être reçue. Nous pouvons formuler cette capture probabiliste de la manière suivante. Soit i la puissance de réception d'une trame reçue d'un nœud émetteur et j la puissance de réception d'une trame reçu d'un nœud interférent, si j est compris entre $i - SIR_{seuilProba}$ et $i + SIR_{seuilGrantie}$ alors il existe une probabilité que la trame de l'émetteur soit capturée au récepteur.

Nous utilisons ce dernier énoncé pour définir la probabilité de capture dans l'intervalle I_{proba}. Dans ce cas, pour chaque paire d'intervalle (x_i, x_j), cette question de capture se pose avec une probabilité : $PrA(x_i).PrN(x_j)$. Comme précédemment, pour un x_i donné, il faut identifier tous les cas pour lesquels x_j satisfait la condition de capture. La probabilité qu'une trame reçue de A en B avec la puissance xi soit capturée est donnée par :

$$Pr_{cap}(x_i) = \sum_{J=i-SIRseuilProba}^{J=i+SIRseuilGarantie} PrA(x_i).PrN(x_j).Fcap(i-j) = PrA(xi).\sum_{J=i-SIRseuilProba}^{J=i+SIRseuilGarantie} PrN(x_j).Fcap(i-j).$$

F_{cap} est la pondération sur $]0,1[$ dont les valeurs sont obtenues grâce à la courbe 4.10.

Nous pouvons généraliser cette formule en définissant F_{cap} sur l'intervalle fermé $[0,1]$. Dans ce cas, nous définissons SIR dans l'intervalle $]-\infty,+\infty[$ et disons que la capture est probabiliste pour tout SIR dans l'intervalle probabiliste I_{proba} et binaire en dehors de cet intervalle. Il est facile de constater que pour tout i supérieur au seuil de sensibilité P_{seuil}, la

probabilité de capture est donnée par : $\mathrm{Pr_{cap}(x_i)} = \mathrm{PrA(X_i)x}\sum_{-\infty}^{+\infty}\mathrm{PrN(x_j)}.\mathrm{Fcap(i\text{-}j)}$. Fcap(i-j) est définie est définie ainsi :

$$\mathrm{Fcap(i-j)} = \begin{cases} 1 \text{ si SIR} \in [SIR_{seuilGaranti}, +\infty[\\ 0 \text{ si SIR} \in]-\infty, SIR_{seuilProba}] \\ a \text{ si } SIR \in I_{proba} \end{cases}$$

Où a est pris dans l'intervalle] 0, 1[et est donné par la courbe 4.10.

Ici, j représente la puissance reçue par le nœud B de ses voisins à N sauts. Dans cette version, la probabilité cumulée est remplacée par une série dans laquelle chaque terme est pondéré par les valeurs données par les mesures réelles de la figure 4.10.

Comme dans le cas de la capture binaire, on obtient :

$\mathrm{Pr_{cap}(x_i)} = \mathrm{Pr_{cap}(x_i|D)} = \mathrm{PrA(xi)}\sum_{-\infty}^{+\infty}.\mathrm{PrD(x_j)}.\mathrm{Fcap(i\text{-}j)}$ si dist(B,N) = 2.d

$\mathrm{Pr_{cap}(x_i)} = \mathrm{Pr_{cap}(x_i|E)} = \mathrm{PrA(xi)}\sum_{-\infty}^{+\infty}.\mathrm{PrE(x_j)}.\mathrm{Fcap(i\text{-}j)}$ si dist(B,N) = 3.d

La figure 4.11 montre une représentation du pourcentage de trames capturées en B lorsque l'interférent est à 3 sauts. La forme de la figure confirme bien notre intuition de départ. La probabilité de capture est un facteur de performance très important dans le modèle de référence considéré. En effet, sa connaissance nous permet d'évaluer le taux de collisions pour un nœud et par conséquent déduire le taux de réception des trames. Dans la suite, nous allons affiner notre approche en prenant en compte l'entrelacement temporel des activités de A et du ou des nœuds interférents. Ceci nous conduit à un nouveau calcul du taux de réception se basant sur la connaissance de la capture et de la vulnérabilité temporelle des nœuds.

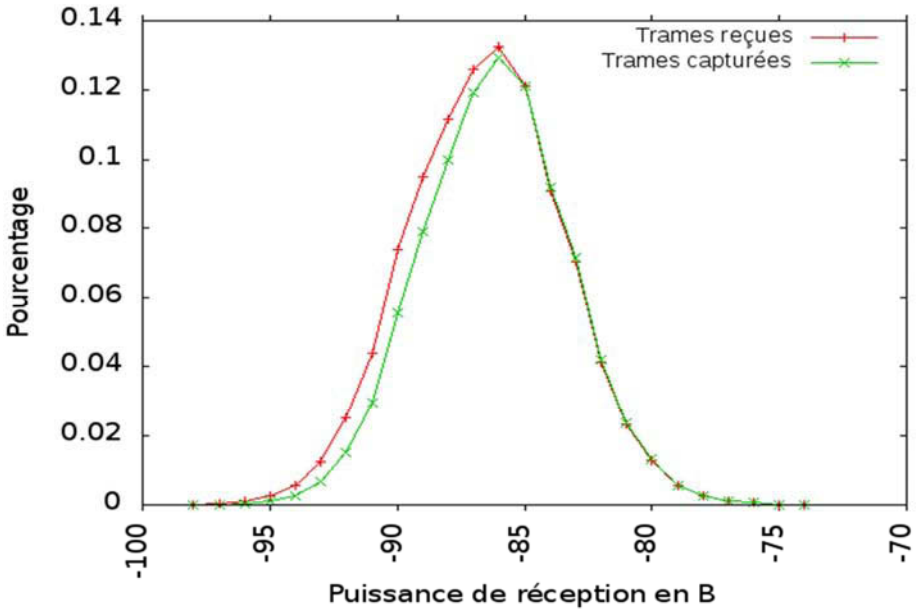


Figure 4. 11 - Pourcentage des paquets capturées

6. Calcul de la probabilité de réception en tenant compte des caractéristiques temporelles de l'échange de trames

Dans cette partie, il s'agit d'évaluer la probabilité de réception par B d'une trame émise par A. Cette probabilité est fortement dépendante de l'activité des autres nœuds voisins à 3 sauts maximum de B (D et E dans cette étude). Si une trame émise par A n'est exposée ni à une activité concurrente du nœud D ni à celle du nœud E, nous dirons qu'elle est non vulnérable. La probabilité recherchée est en fait le pourcentage du nombre de trames émises par A correctement reçues par B.

Cette bonne réception est conditionnée par la règle logique suivante :

(La trame est reçue avec une puissance supérieure au seuil de sensibilité P_{seuil})

ET

((elle bénéficie de l'effet capture) OU (elle est non vulnérable))

Dans un premier temps, il nous faut évaluer les moments correspondants à des émissions concurrentes de A, D et E. Considérons que A et D émettent des trames de même longueur

nécessitant une durée d'émission T_1, le schéma d'activité d'un échange entre les nœuds A et B de notre cluster est basé sur le chronogramme donné figure 4.12.

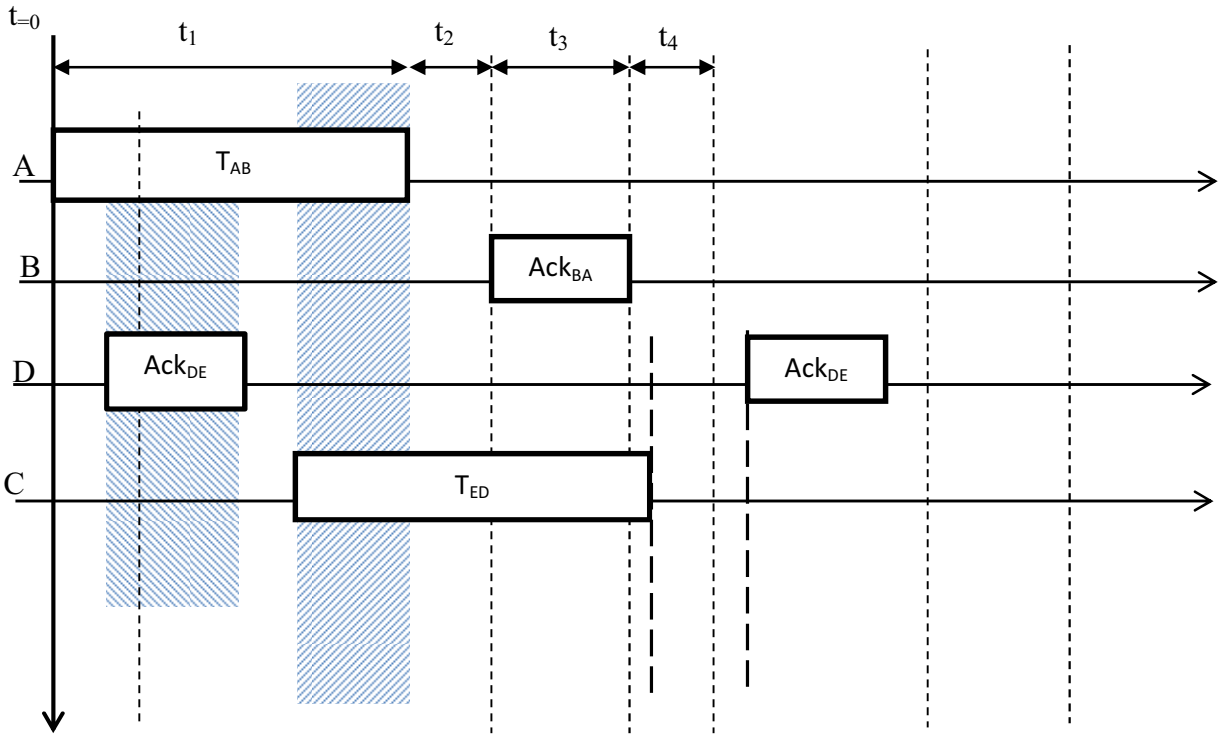


Figure 4. 12 - Chronogramme des échanges entre les nœuds

Quand A est possesseur d'un jeton, l'activité d'émission de A et B se renouvelle périodiquement pour assumer le trafic en direction du puits sur la base du motif temporel (t_1, t_2, t_3, t_4) pour lequel :

- t_1 est la durée nécessaire pour émettre une trame,
- t_2 est la durée définie par la norme 802.15.4 pour permettre à l'émetteur A et au récepteur B de commuter de l'état d'émission à celui de réception (et réciproquement),
- t_3 est la durée nécessaire pour émettre un acquittement géré par le coupleur radio,
- t_4 est la durée nécessaire pour que l'émetteur gère l'acquittement et garnisse le buffer d'émission du coupleur radio pour entreprendre l'émission de la trame suivante (cette durée est souvent négligée dans la simulation alors qu'elle peut être de plusieurs millisecondes).

Si E est aussi possesseur d'un jeton au même moment et s'il a un trafic descendant (à direction de D), alors l'entrelacement de ces motifs temporels peut engendrer des périodes en grisé sur la figure 4.12 qui correspondent à une arrivée simultanée de trames au niveau du récepteur B considéré. C'est durant ces périodes que la trame en cours de réception peut passer de l'état capturée à l'état non reçue sous l'effet d'une collision. Dans notre approche, nous nous appuyons sur les facilitées offertes par le coupleur radio conforme à la norme 802.15.4 qui valide ou non chaque trame reçue à partir de contraintes de synchronisation et du calcul d'un code détecteur d'erreur de type CRC (ceci n'implique pas l'usage de codes auto-correcteurs).

La figure 4.12 correspond au pire cas pour le cluster considéré car elle décrit un scénario durant lequel A émet un trafic vers le puits et E émet un trafic en sens inverse. On observe dans cet exemple d'entrelacement temporel, que la trame issue de A est exposée dans la zone 1 à des interférences « du premier ordre » car provenant d'un nœud à deux sauts, puis dans la zone 2 à celles « du deuxième ordre » car provenant d'un nœud à trois sauts. C'est l'existence de ces zones d'interférences qui permet de se servir des probabilités de capture qui viennent d'être calculées. Soit l'intervalle de temps $T = t_1 + t_2 + t_3 + t_4$ qui est associé à l'échange d'une trame de A vers B, nous allons évaluer le risque que chacune de ces zones d'interférences soient présentes. Ce risque se définit en estimant à partir de l'instant T=0 la plage temporelle qui est concernée par l'existence d'interférences d'ordre 1 et d'ordre 2. Les activités des nœuds A et E étant indépendantes, pour les interférences entre trames, la plage de vulnérabilité relative à l'émission de la trame T_{AB} de la figure 4.12 est d'une longueur $t_1 + t'_1 \cong 2 * t_1$ $2.t_1$, résultat bien connu pour la modélisation d'Aloha (Tanenbaum, 2003). Le risque de ce type d'interférences (avec une trame de E vers D) est donc donné par :

$$P_{\text{vulnerabite}}(A\&E) = \frac{t_1 + t\prime_1}{t1+t2+t3+t4} = \frac{2.t_1}{T}$$

Le risque d'interférences de type 1 (avec un accusé de réception de D vers E) est donné par :

$$P_{\text{vulnerabite}}(A\&D) = \frac{t_1 + t_3}{t1+t2+t3+t4} = \frac{t_1+t_3}{T}$$

Donc, pour une trame reçue par B de A avec une puissance $P_{R_{\sigma(1-\text{hop})}}$, supérieure au seuil de sensibilité, la probabilité de capture (ou de bonne réception) est donnée par :

$$P_{\text{reception}}(P_{R_{\sigma(1-\text{hop})}}) = 1 - P_{\text{vulnerabite}}(A\&D) * (1 - Pr_{\text{cap}}(A\&D)) - P_{\text{vulnerabite}}(A\&E) * (1 - Pr_{\text{cap}}(A\&E))$$

En tenant compte de l'*outage probability*, et en prenant en compte l'ensemble des trames émises par A, la formule devient :

$$P_{reception}\left(P_{R_{\sigma(1-hop)}}\right) = (1 - Outage) - P_{vulnerabite}(A\&D) * (1 - Pr_{cap}(A\&D) - P_{vulnerabite}(A\&E) * (1 - Pr_{cap}(A\&E)$$

Cette formule met en évidence l'impact des paramètres tels que le modèle de capture, l'*outage probability* et le timing des échanges, sur le taux de bonne réception de trames par un nœud dans un contexte simple comme un réseau linéaire dont l'accès au médium est piloté par un jeton circulant.

Dans nos simulations, nous considérons que la capacité de la navette est assez grande pour permettre à un nœud possesseur d'un jeton d'envoyer toutes ses trames. Les durées de transmission des trams (données ou Ack) sont calculées par rapport au débit théorique de la norme IEEE 802.15.4 (250 Kbps au niveau physique) en appliquant la formule $T = \frac{\text{taille trame}}{\text{débit}}$. L'intervalle de temps $T = t_1 + t_2 + t_3 + t_4$ décrit ci-dessus est obtenu de façon expérimentale sur des cartes de type TelosB (Polastre et al., 2005) et est égal à 11,8 ms.

Tableau 3: Valeurs des intervalles de temps pour une taille de trame de 100 octets et un accusé de 11 octets.

Paramètres	Valeurs
T	11,8 ms
t1	4 ms
T2	3,7 ms
t3	0,64 ms
t4	4 ms

Dans la figure 4.13, la capture probabiliste est considérée. Cette figure représente la probabilité de réception de trames en B quand un nœud à trois sauts (nœud E) est possesseur d'un jeton. Cette situation correspond aux échanges E vers D (transmission trafic descendant) et E vers F (transmission trafic montant). Nous remarquons que la probabilité d'une bonne réception augmente avec le nombre de sauts par rapport au nœud B. Il est clair que les nœuds les plus éloignés de B sur le réseau linéaire créent moins d'interférences. En effet, lorsque les interférences en B sont créées par les échanges entre les nœuds à 2 et 3 sauts (cluster de taille 4) c'est-à-dire du trafic descendant de E vers D, le taux de réception maximal en B des

trames du nœud à un saut est un peu au-dessus de 71% pour les trames reçues avec une puissance de -85 dBm par exemple. Ce taux de réception maximal est de 92% lorsque les interférences sont générées par les échanges entre des nœuds à 3 et 4 sauts (trafic montant de E). Notons que le taux de réception des paquets reçus avec une puissance forte (partie droite des courbes) est le même car ses puissances sont supérieures au seuil de réception garantie définie dans la capture.

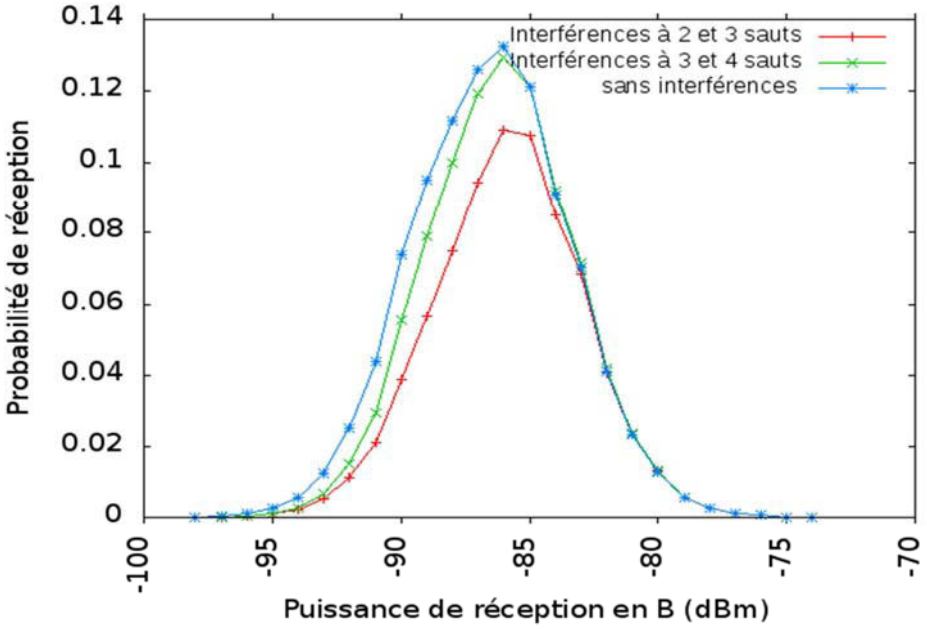


Figure 4. 13 - Probabilité de réception en capture probabiliste

Notons que la courbe représentant la réception en B lorsque les nœuds E et D échangent est très proche de la courbe représentant la réception sans interférences. Ceci prouve qu'avec un cluster de taille 5, la réception en B de trames provenant du nœud à un saut est presque garantie en capture probabiliste.

La figure 4.14 nous donne une idée plus claire sur les effets des interférences créées par les échanges entre nœuds à 2 sauts et 3sauts et entre 3 sauts et 4 sauts. En effet, elle représente le cumul des probabilités de réception au nœud B. Nous remarquons que la probabilité maximale cumulée quand les nœuds à 3 et 4 sauts (cluster de taille 5) sont les sources des interférences, est 0.9 soit 90% des trames reçues par B du nœud à 1 saut, alors que cette probabilité est de 72% lorsque les interférences sont créées par les nœuds à 2 et 3 sauts (cluster de taille 4).

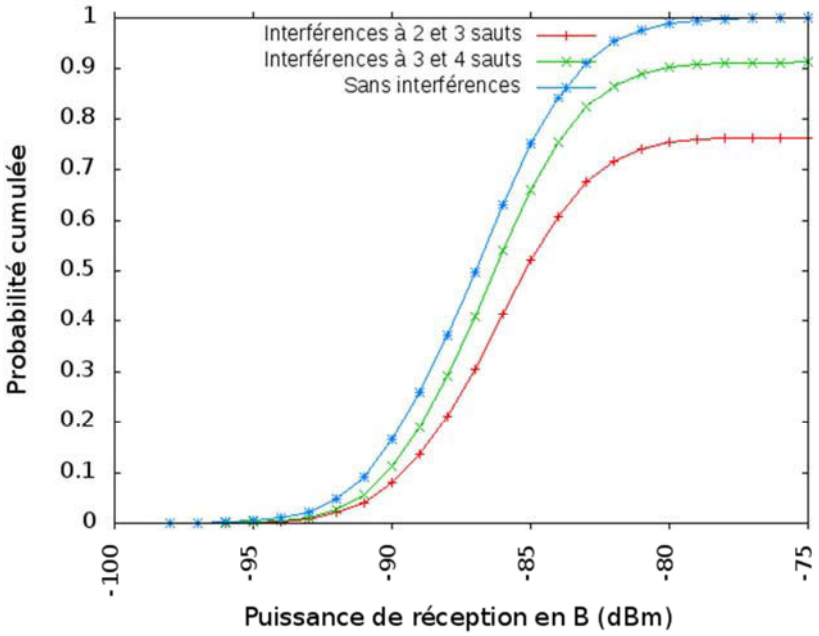


Figure 4. 14 - Cumul des probabilités

En considérant que l'*outage probability* a été choisi à 10%, ceci rend possible cette asymptote à 90 %, nous pouvons estimer que les nœuds à 3 et 4 sauts n'interférent pas dans la réception des trames en B du nœud A à un saut. En effet, la probabilité de réception cumulée totale, étant égale à 90%, correspond au pourcentage des trames au-dessus du seuil de sensibilité défini.

Par contre, les interférences sont pénalisantes lorsque les nœuds à 2 et 3 sauts sont en activité dans le cluster à 4. En effet, on note une probabilité de réception totale de 76% des trames, 24% des trames perdues réparties ainsi :

10% des trames représentant l'Outage probability,

14% perdues par collisions provoquées par les interférences créées par les nœuds à 2 et 3 sauts.

Les échanges avec E et D correspondent au cas d'un cluster à 4 sauts et ceux de E et F au cas d'un cluster à 5. Les résultats montrent l'impact de la capture probabiliste sur un cluster à 4 sauts par rapport à la capture binaire. En effet, on note 24% de perte sur l'ensemble des activités des interférents du cluster alors qu'en simple capture binaire, l'activité du nœud interférent à deux sauts de B seulement génère plus de 50% de pertes par collisions.

Par contre, les performances obtenues en utilisant les deux types de capture sont presque équivalentes dans les cas du cluster à 5, du fait que les interférents sont assez éloignés du nœud récepteur.

7. Formalisation du compromis permettant la définition d'un cluster physique

L'analyse faite précédemment dans le cas particulier du réseau de capteur linéaire 1-redondant montre que pour un seuil de réception fixé, il est possible d'avoir une taille de cluster de 4 ou 5 si l'on considère une valeur coefficient de perte en chemin de 2.5. Dans cette partie, on va considérer le cas le plus général d'un réseau R-redondant pour définir un cluster physique en fonction de la valeur du taux de réception fixé et du facteur de redondance R.

7.1. Estimation de l'influence de la redondance sur l'impact des interférences

Nous allons considérons la figure 4.15 ci-dessous. Le nœud N_{A+R} est récepteur du trafic relayé par N_A . On suppose que N_{int} est un nœud interférent pour N_{A+R} .

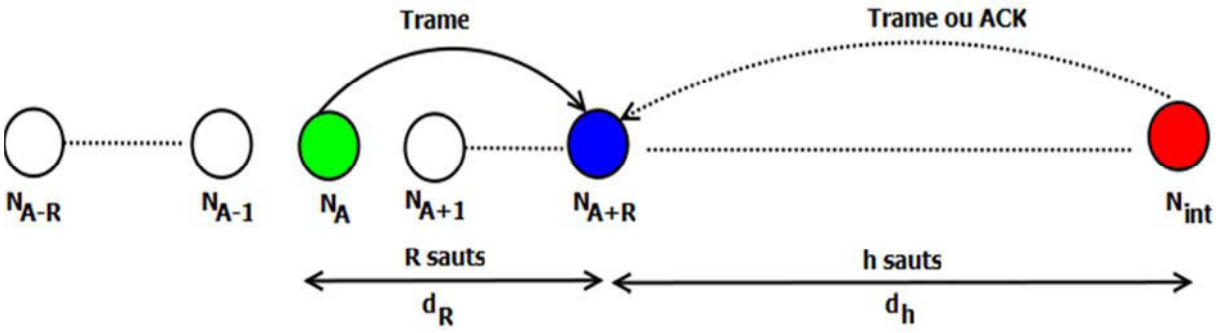


Figure 4. 15 - Représentation d'un nœud et son interférent

Pour le modèle des interférences, on considère que $PR_\sigma(A)$ (resp. $PR_\sigma(int)$) est la puissance reçue par N_{A+R} de N_A(resp. N_{int}). On suppose que le nœud interférent N_{int} se trouve à h sauts de N_{A+R}. Nous appelons d_h la distance N_{int} N_{A+R} en mètres. D'après la définition du facteur de redondance R, le nœud N_A se trouve à R sauts de N_{A+R}. On appelle d_R la distance entre N_A et N_{A+R} exprimée en mètres. Le SIR au nœud N_{A+R} est donné par la formule :

$$SIR = P_{R_{\sigma(A)}} - P_{R_{\sigma(int)}} = (10 * n * \log\frac{d_h}{d_R}) + (X_{\sigma R} - X_{\sigma h}).$$

La condition de bonne réception dans le cas d'une capture au comportement binaire traduit par :

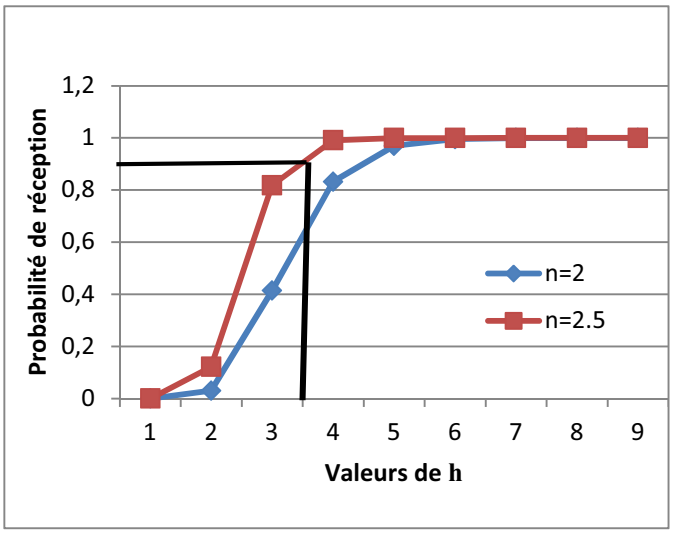
Si $SIR \geq SIR_{seuil}$ alors la trame émise par N_A pour N_{A+R} est bien reçue (capturée). On dit dans ce cas qu'il y'a effet de capture.

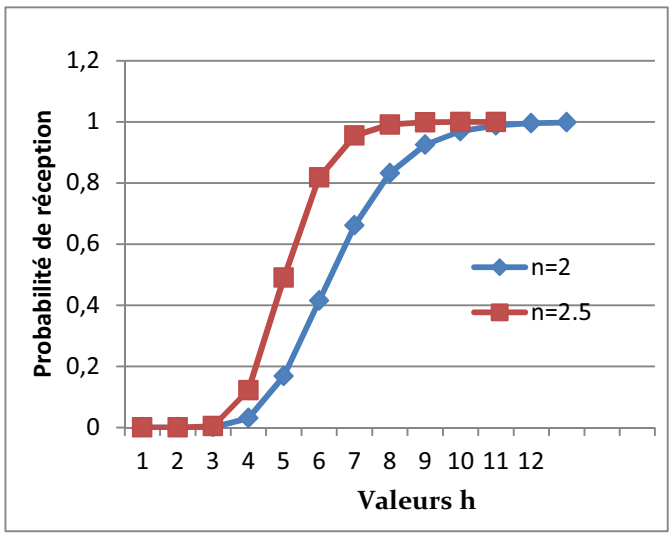
Reprenons la démarche présentée en 5.1.1 de ce chapitre.

Soit $Z=(X_{\sigma R} - X_{\sigma h})/\sigma\sqrt{2}$, $(X_{\sigma R} - X_{\sigma h})$ est une variable aléatoire gaussienne, avec une moyenne nulle et un écart type $\sigma\sqrt{2}$ vu que c'est la différence de deux gaussiennes de moyennes nulles et de même écart σ. Donc Z est une variable gaussienne de moyenne nulle et d'écart type 1. La probabilité d'une bonne réception est donnée alors par:

$$p_h(Z > 0) = Q(\frac{SIR_{seuil} - (10*n*\log\frac{d_h}{d_R})}{\sigma\sqrt{2}}),$$

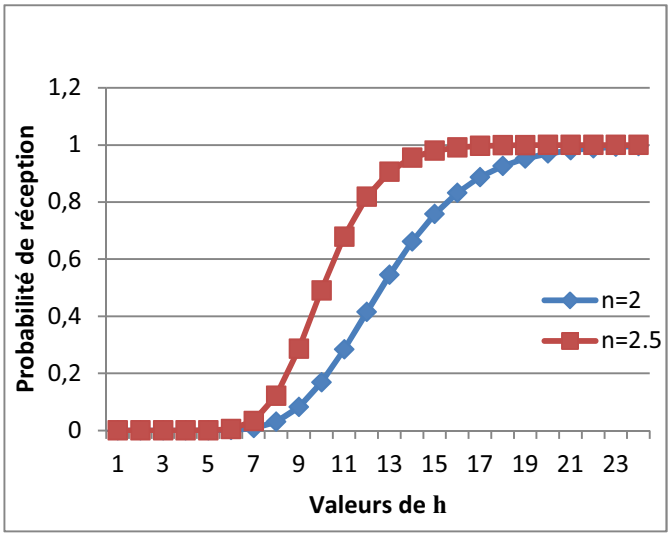
où Q est la fonction complémentaire de la fonction de répartition de la loi normale.

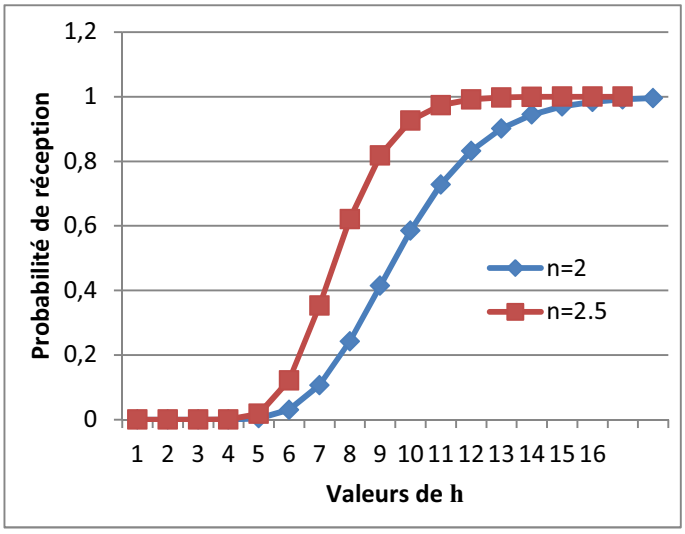




Par définition : d_R= R*d et d_h =h*d.

Donc $h = R\, e^{\left(\frac{SIR_{seuil} - Q^{-1}(P_h)*\sigma*\sqrt{2}}{10*n}\right)}$





Les conditions de propagation sont celles justifiées dans la section 2. De ce chapitre. Les résultats présentés ici sont obtenus pour $\sigma = 3$ dB, SIR_{seuil}=10 dB, et pour deux valeurs du coefficient d'atténuation (pathloss) n = 2 et n= 2,5.

P

Figure 4. 16 - Probabilité de capture pour un réseau R-redondant

La figure 4.16 représente la probabilité de bonne réception d'une trame en fonction de ***h (Number of Hop)*** la distance exprimée en nombre de sauts entre les nœuds N_A et N_{int} tel que nous les avons définis précédemment. La valeur tend vers une asymptote en fonction de la distance séparant N_A et N_{int} d'une façon qui dépend du facteur de redondance.

Si nous fixons 90 % comme le seuil qui ne génère pas d'accumulation de trafic dans les nœuds proche du puits du réseau linéaire, soit un *outage probability* de 10 %, alors d'après la figure, la valeur de h correspondant à ce pourcentage n'est pas entière. Donc, comme tenu de nos hypothèses pour être sûr d'avoir 90 % il faut choisir une valeur parmi tous les entiers à la droite du point d'intersection P défini sur la courbe. Dans la figure 4.16.a correspondant à R = 1, la valeur minimum qui peut être choisie pour h correspond à 4 pour n = 2.5 et à 5 pour n = 2.

Généralement plusieurs valeurs entières satisfont un seuil de 90% avant que la probabilité n'atteigne le 100 %. Supposons que :

- le point P définisse un seuil de taux de bonne réception à 90 % comme montré dans la figure 4.17,
- h_0 soit la première valeur entière à la droite de l'abscisse de P qui nous donne une probabilité de 91 % (x = 0,09)
- h_0+1 désigne la valeur entière suivante sur l'axe des abscisses qui nous une probabilité de 98% (soit y = 0,02),
- $h_0+\alpha$ pour $\alpha > 1$ sont les points suivants donnant des probabilités égales ou très proches de 1.

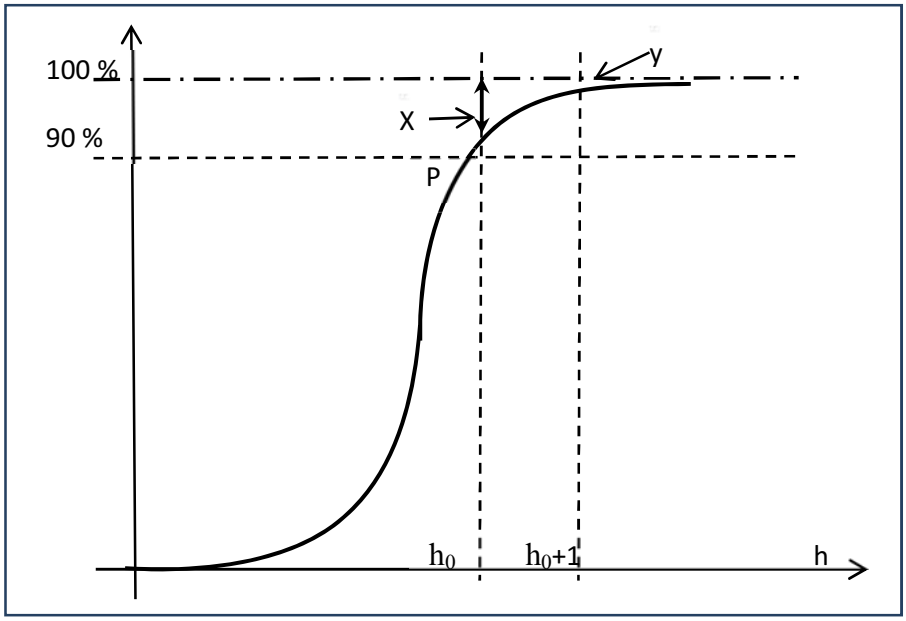


Figure 4. 17 - Représentation de h en fonction du seuil de réception

Dans cette étude, pour des besoins de simplicité et de clarté, nous nous limitons aux deux premières valeurs entières h_0 et h_0+1 en sachant que le raisonnement est le même pour les autres éventuelles valeurs entières correspondant à des valeurs de taux de réception compris entre 90 % et 100 %.

Le fait d'avoir fixé un seuil de taux de bonne réception sur un lien sans fil nous met face à des possibilités de choix pour la valeur de h. La suite de cette contribution traite de la façon de faire ce choix.

7.2. Critères de choix de la taille d'un cluster d'un LSN

Le choix de la valeur de la taille de cluster revient à faire un compromis dépendant des besoins de l'application et des exigences de performance en termes de délais et de taux de

délivrance des paquets au puits. En effet, certaines applications se focalisent plus sur les délais alors que d'autres sont plus exigeantes en termes de taux de délivrance selon les caractéristiques physiques du réseau telles que la longueur du réseau et le milieu à surveiller. Par conséquent, on peut décider de choisir un cluster plus ou moins grand en fonction du type de performances souhaitées. Ce choix dépend principalement de la valeur de h et du seuil de réception souhaité. Deux questions se posent alors:

- Quel est l'impact du choix de h sur la taille du cluster?
- Quelle est l'impact du choix de l'*outage probability* sur la qualité de service offert par le LSN ?

La taille du cluster LCSize (LSN Cluster Size) est fonction de ***R*** et de ***h***. De plus, l'étude faite au chapitre 3 sur la taille du cluster logique, nous permet de déduire la formule de la taille du cluster de la façon suivante :

- $LCSize(R) = \begin{cases} 2 * R + h - 1 & avec\ trafic\ descendant \\ R + h - 1 & sans\ trafic\ descendant \end{cases}$

  R étant le facteur de redondance tel que défini dans cette thèse et ***h*** la distance entre le récepteur et l'interférent.

La taille du cluster croit linéairement avec h. Ceci a un impact sur la fréquence maximale de la distribution des jetons sur le réseau linéaire. Des jetons moins fréquents conduisent à une réduction du débit maximal au puits qui s'exprime par :

Si ***D*** est le débit de paquets délivrés au puits pour un cluster de taille LCSize pour un ***R*** donné, le choix du point suivant pour h nous donne

$D(h_0+1) = D(h_0) * LCSize(R, h_0) / LCSize(R, h_0+1)$

En effet, nous avons déjà montré dans le chapitre 3 que pour une durée de cluster donnée et une capacité SC (SC est le nombre de trames échangées durant la possession d'un jeton) donnée, le puits reçoit du trafic chaque LCSize * SDur. Nous avons :

$D(h_0) = \frac{R*SC}{LCSize(R,h_0)*SDur}$ et $D(h_0+1) = \frac{R*SC}{LCSize(R,h_0+1)*SDur}$ où SC est la capacité de la navette comme défini dans le chapitre 3. Pour un facteur de redondance donné, le rapport $\frac{R*SC}{SDur}$ est constant et ne dépend pas de la valeur de h.

Par conséquent nous avons $D\ (h_0) * LCSize(R,h_0) = D(h_0+1) * LCSize(R,h_0\ +1)$. D'où :

$$D\ (h_0+1) = \frac{D(h_0) * LCSize(R,h_0)}{LCSize(R,h_0+1)}$$

Le choix de h_0 plutôt que h_0+1 semble augmenter le débit et réduire le temps de transit. Ceci doit être modéré quand on prend en compte les effets de l'*outage probability*. Comme sur la figure 4.17 supposons que x soit le taux d'erreurs acceptable pour le point donné par h_0 et y celui donné par le point h_0+1.

Considérons la probabilité d'erreur x sur un lien entre deux nœuds du réseau. Cette probabilité d'erreur peut être définie autrement comme étant la probabilité de retransmission (ou répétition) de trames sur un lien donné. Soit Nb le nombre de répétitions maximal autorisé par le protocole MAC pour un lien donné. Le nombre de retransmissions avant la bonne réception d'une trame peut être représenté par une épreuve de Bernoulli (Papoulis and Pillai, 2002) dans laquelle le succès a une probabilité 1-x et l'échec x. Soit K une variable aléatoire qui comptabilise le nombre de tentatives de transmissions nécessaires avant de recevoir un accusé de réception. Alors, K suit une loi de probabilité géométrique définie par la fonction de masse suivant :

$P(K=n) = (1-x) * x^{(n-1)}$. n=$\in \{1, 2, \dots, \}$.

Ou n est le nombre de tentatives de transmissions. Dans les réseaux sans fil, le nombre maximal de retransmissions est limité pour des besoins d'économie d'énergie ou d'évitement de surcharge du réseau. Dans ce cas, la probabilité de recevoir un accusé après Nb tentatives devient alors :

$$P(K \leq Nb) = \sum_{i=1}^{Nb} P(K=i) = (1-x) \sum_{i=1}^{Nb} x^{i-1} = 1 - x^{Nb}$$

Le nombre moyen d'envoi d'une trame pour chaque lien est déterminé par la formule:

$$E_x(K) = \frac{1}{1-x}$$

D'après la définition du taux de délivrance on peut dire que le taux de délivrance maximal (TD_{max}) sur un lien est donné par: $TD_{max} = \frac{SC}{SC*E_x}$.

Soit pour un saut courant: $TD_{max}(h_0) = 1 - x$ pour h_0 et $TD_{max}(h_0 + 1) = 1 - y$ pour h_0+1.

Il est évident de constater que la fonction E_x est une fonction décroissante de x. Par conséquent, $E_x > E_y$ d'où il est plus judicieux de privilégier le choix de h_0 +1 plutôt que h_0 si nous voulons privilégier le taux de délivrance au puits pour un nœud donné. Cette différence entre les deux moyennes peut paraitre a priori négligeable pour un lien, cependant, cette différence est certainement non négligeable lors de la considération d'un chemin composé de plusieurs de ces liens où l'on verra que le nombre de sauts pour atteindre le puits impacte fortement sur le nœud de délivrance.

En effet, si cette trame est amenée à parcourir PathSize sauts, le nombre moyen de transmissions nécessaire devient PathSize * E_x et PathSize * E_y selon la valeur de h considérée. Donc, le taux de délivrance au puits devient :

- $TD_{max}(h_0) = (1 - x)/PathSize(h_0)$ pour h_0,
- $TD_{max}(h_0 + 1) = (1 - y)/PathSize(h_0 + 1)$ pour h_0 +1.

Par conséquent, si x est petit mais significativement grand par rapport à y, le choix de h_0 a un impact sur le temps de transit. Le paquet arrive plus vite mais avec une probabilité plus grande.

Soit t le temps consommé à chaque retransmission, alors le temps moyen nécessaire pour envoyer une trame E_x*t_x dans le cas de h_0 et E_y*t_y pour h_0+1. Quand le cumul de ces grandeurs dépasse un seuil attaché au temps alloué au possesseur de jeton : une trame peut être différée pour partir la prochaine fois que le nœud émetteur sera possesseur de jeton.

Le choix entre les deux points considérés (h_0 et h_0+1) a un double impact : sur la fréquence des jetons et sur le retard des trames donc sur le délai de bout en bout.

7.3. Synthèse

Ainsi, selon la probabilité de bonne réception attendue, nous pouvons trouver un cluster plus ou moins grand à une unité près en fonction de la valeur de ***h*** souhaitée. Faut-il choisir le petit cluster et répéter certaines trames en ayant un facteur de réutilisation spatial optimum (reuse factor) ou alors prendre le cluster un peu plus grand qui va donner un taux de réception meilleur mais des jetons moins fréquents ? Le raisonnement ci-dessus montre que ce choix est fonction de la QoS requise par l'application de surveillance considérée. Cette QoS est caractérisée par le délai de bout-en-bout, le taux de délivrance au puits, le débit, etc. D'autres facteurs peuvent influencer la QoS et par conséquent la taille du cluster. On peut citer entre autre la taille de la topologie, les caractéristiques du milieu considéré, etc.

L'avantage d'un petit cluster (choix de h_0 plutôt que h_0+1) se trouve dans le fait qu'il y ait plus de jetons qui circulent dans le réseau. Les délais de bout-en-bout sont par conséquent réduits et un débit (une capacité) plus élevé vers le puits est garanti.

L'inconvénient majeur d'avoir un cluster de taille petite se trouve dans la présence de plus d'interférences qui augmentent le taux d'erreur dans les transmissions de paquets et par conséquent réduit le taux de délivrance au puits. Une autre conséquence est la consommation des ressources des capteurs comme l'énergie du fait que les périodes de sommeil des nœuds sont courtes.

L'avantage d'avoir un grand cluster (choix de h_0+1 plutôt que h_0) réside dans le fait qu'il n'a presque pas de zones d'interférences et par conséquent peu de collisions possibles. En effet, dans ce cas il y a moins de jetons donc les activités des zones ne génèrent pas de conflits. Cependant, ce fait peut engendrer une sous-utilisation des ressources des capteurs qui peut créer des pertes de performances. Le tableau ci-dessous récapitule l'étude analytique et montre l'*outage probability* en fonction de h_0 et h_0+1 pour un taux de réception seuil fixé à 90%. Il montre que la probabilité qu'un paquet soit répété est plus grande si la distance entre N_A et N_{int} est fixée à h_0 plutôt que h_0+1. Cette probabilité de répétition augmente avec le facteur de redondance R.

Tableau 4 - Tableau récapitulatif de la taille de cluster. On considère un facteur d'atténuation égal à 2 (la courbe en bleu de la figure 4.16).

Facteur de redondance	**h_0**	**Taille cluster(h_0)**	**Taille cluster(h_0+1)**	**Outage(h_0)**	**Outage(h_0+1)**
R=1	4	5	6	0,00862583	0,00021303
R=2	7	10	11	0,04476727	0,00862583
R=3	10	15	16	0,07378896	0,02643646
R=4	13	20	21	0,09365845	0,04476727

Le point fort de la technique proposée est qu'elle profite de la topologie linéaire et par conséquent prend en compte les risques potentiels d'interférences. De plus, avec cette méthode plusieurs paramètres de performance sont pris en compte et optimisés en même temps :

- la réduction des délais de bout-en-bout: un nœud relaie ses données à son voisin le plus lointain situé à ***R*** sauts ce qui réduit les délais d'acheminement des données au puits,
- l'augmentation des taux de délivrance au puits: on a montré que le cluster créé avec h_0 +1 donne des taux de délivrance meilleurs pour un nœud donné,
- nombre minimal de cluster: l'une des conséquences de la prise en compte des interférences radio dans la méthode proposée est la grande taille de cluster. Ce qui peut diminuer le nombre de clusters exploités en même temps dans un réseau linéaire en comparaison aux méthodes classiques.

8. Conclusion

Dans ce chapitre, nous avons proposé une méthode de calcul qui permet d'estimer le nombre de trames capturées pour un réseau linéaire conforme aux hypothèses que nous venons d'énoncer. Nous avons montré par étude analytique et par simulation que la taille de cluster

dépend du rapport entre la distance du nœud émetteur au nœud récepteur et celle entre le nœud interférent au même nœud récepteur. Ce rapport a un impact significatif sur la capture des trames lorsque les activités des nœuds engendrent des interférences radio. Nous avons donc étudié deux types de modélisation du phénomène de capture : une capture binaire et une capture probabiliste. Les simulations ont montré que la capture probabiliste offre de meilleures performances en termes de taux de réception pour une taille de cluster donnée. En effet, le modèle de capture est binaire et simpliste et est donc pessimiste, alors qu'un modèle plus évolué et probabiliste est plus proche de la réalité car il prend en compte plus finement la capture telle qu'elle existe dans le monde réel. Cependant, ce gain est plus important dans le cas d'un réseau linéaire découpé en grands clusters. Cette remarque nous conduit à un dilemme car, si le cluster est de grande taille, la fréquence des jetons en sera réduite et la capacité de parallélisme sur cette structure linéaire réduite aussi. Là-encore, nous sommes face à un problème de compromis entre les différents paramètres mis en avant dans cette contribution pour satisfaire une qualité de service (le meilleur taux de délivrance des trames au puits, le déterminisme assuré par un risque de collisions minimisé, etc.).

Ce travail met indirectement en avant les limites des méthodes consistant à définir la taille des clusters sur des considérations de voisinage.

Conclusion et Perspectives

Dans cette thèse, nous avons fait une étude des réseaux de capteurs sans fil linéaires. Ils se définissent comme des réseaux de capteurs sans fil dont le déploiement des nœuds se fait sur une ou plusieurs lignes suivant les besoins applicatifs. Les applications de réseau de capteurs sont nombreuses et diverses. On trouve ce type de déploiement pour des applications de surveillance de pipeline, de rails, de routes, de trains, etc.

Les caractéristiques particulières de ce type de réseau comme le voisinage limité, les possibilités de routage réduites ont fait apparaitre de nouvelles problématiques liées aux réseaux linéaires Ces problématiques concernent principalement les mécanismes d'accès au canal de transmission permettant d'assurer des délais de bout-en-bout réduits, des taux de délivrance importants ou encore des débits optimaux. Une autre problématique est la gestion de la connectivité du réseau. Dans un réseau linéaire, le voisinage limité fait que le réseau est très vulnérable au défaut de lien ou de nœud. Donc, il est important de mettre en place un moyen de déploiement des nœuds qui assure la connectivité même en présence de défaut de lien ou nœud.

Dans nos travaux, nous avons proposé deux contributions relatives au protocole d'accès au canal de transmission. Un protocole basé sur la contention des nœuds et un autre basé sur un jeton circulant. Pour la contention, nous avons proposé une intégration du mécanisme RTS/CTS de 802.11 dans le CSMA/CA de 802.15.4. Grâce aux simulations effectuées, nous avons montré que l'intégration du RTS/CTS permet d'augmenter les performances du réseau linéaire en termes de taux de délivrance, de délais ou encore de débit. De plus, elle permet un meilleur comportement des files d'attente des nœuds en retardant le phénomène de débordement par rapport au CSMA/CA sans RTS/CTS. Par la suite, nous avons proposé un protocole MAC basé sur l'exploitation d'un jeton appelé LTB-MAC (Linear Token-Based MAC Protocol). Dans LTB-MAC, l'accès au canal de transmission est conditionné par la possession d'un jeton. Ce dernier est une petite trame contenant des informations temporelles permettant de gérer la synchronisation des nœuds et le drainage du flux au puits de collecte. Il est créé par le nœud situé à l'extrémité opposée du puits et généré de proche en proche jusqu'au puits. Chaque nœud qui le reçoit accède au canal de transmission pendant une durée définie dans le jeton et déduit la date de la prochaine réception de jeton afin de se mettre en mode sommeil après la réception du trafic de son voisin. Cette propagation du jeton de proche en proche entre les voisins à un saut et donnant à un nœud le droit d'accéder au canal de

transmission a permis de définir une navette dans laquelle les nœuds déposent leurs informations en direction du puits. Nous avons montré que la taille de la navette peut avoir un impact significatif sur les paramètres de performances du réseau tels que le taux de délivrance, le débit ou encore le délai de bout-en-bout. Par la suite, nous avons effectué des simulations du protocole LTB-MAC. Nous avons comparé LTB-MAC au CSMA/CA avec RTS/CTS en termes de débit, de taux de délivrance et avons montré qu'il est plus adapté à ce réseau du fait qu'il améliore mieux les performances du réseau en faisant changer la durée de la navette. En effet, en choisissant des navettes de durée petite, moyenne ou grande les simulations ont montré que LTB-MAC offre de meilleurs délais de bout-en-bout, de taux de délivrance et de débit que le CSMA/CA avec RTS/CTS.

Dans la suite de cette thèse, nous avons étudié une technique de gestion de la connectivité du réseau en considérant le protocole LTB-MAC et la possibilité de faire circuler plusieurs jetons en même temps dans le réseau. Nous avons supposé la portée d'un nœud suffisante pour définir la redondance dans un réseau sans fil linéaire, ceci assurant robustesse et possibilités de routage. Ainsi, nous avons défini le facteur de redondance ***R*** comme étant le nombre de voisins qu'un nœud peut avoir dans un sens défini. Dans le cas de plusieurs jetons circulants, la question suivante s'est posée. Quelle est la distance minimale entre deux jetons qui garantit aux trames transmises par des nœuds possesseurs de jetons de bonnes conditions de réception en maitrisant les effets des interférences radio?

Nous avons répondu à cette question en considérant dans un premier temps les conditions de propagation dans le milieu considéré comme étant stables et constantes. Dans ce cas, nous avons défini la distance entre deux jetons en fonction du facteur de redondance. Cette distance minimale permet de protéger les activités des nœuds possesseurs de jetons et créant un motif d'isolement autour nœuds récepteurs que nous appelons cluster linéaire dans cette thèse. Nous avons montré que le facteur de redondance impacte sur le taille du cluster linéaire puisque celle-ci croit en fonction de ce facteur.

Dans un second, temps nous avons considéré un milieu où les conditions de propagation tiennent compte de la complexité de celui-ci en utilisant un modèle de propagation *Log Normal Shadowing*. Dans ce cas, nous avons montré que la taille du cluster dépend du facteur de redondance, de la distance entre un récepteur, de l'*outage probability* et de du modèle de capture choisie. Selon l'*outage probability* fixée, il est possible d'avoir plusieurs tailles de

cluster. Le choix de la taille de cluster dans ce cas dépend des besoins applicatifs en termes de taux de délivrance, de débit ou de délais de bout-en-bout.

Dans nos futurs travaux, nous envisageons de nous focaliser sur plusieurs points relatifs aux réseaux de capteurs sans fil linéaires.

A courts termes, nous comptons estimer les effets de la perte d'un jeton et d'un lien radio sur un réseau R-redondant.

Nous avons vu que dans le protocole LTB-MAC les paquets des nœuds les plus éloignés du puits sont le premiers à être victimes de l'effet d'écrêtage du trafic et à ne pas atteindre le puits. Donc, il serait intéressant de mettre en place une politique de gestion des paquets dans les FIFO. Cette politique va certainement se baser sur une priorité assignée aux paquets. Ainsi, dans la file d'attente les paquets des nœuds ayant effectué le plus grand nombre de sauts sont les plus prioritaires. Pour ce faire, on va associer une valeur entière « saut » au paquet et l'incrémenter à chaque saut du paquet. Avec cette politique de priorité, les paquets ayant fait le plus de sauts auront plus de chance d'atteindre le puits. Ceci aura pour conséquence d'augmenter les taux de délivrance des nœuds les plus éloignés et diminuer l'effet d'écrêtage du trafic de ceux-ci.

Un autre point intéressant est le déploiement en environnement réel du réseau de capteurs sans fil étudié. Il s'agit d'abord d'utiliser des nœuds convenant à un déploiement extérieur sur lesquels on va implémenter le protocole LTB-MAC. Ensuite, nous allons déployer ces nœuds afin de comparer les résultats d'expérimentation aux résultats de simulations. De plus, le formalisme utilisé pour définir un cluster physique dans le cas du réseau R-redondant se base sur le modèle de capture binaire. Nous comptons utiliser l'expérimentation pour d'abord confirmer l'effet probabiliste de la capture et ensuite définir la taille du cluster physique à partir de ce modèle de capture.

Liste des publications

Chapitre livre

- El Hadji Malick Ndoye, Frédérique Jacquet, Michel Misson, and Ibrahima Niang, "Clustering approach based on the redundancy in a Linear Sensor Network using a Token-based MAC protocol", Book chapter, in Advances in Sensors: Reviews, Vol.3, March-April, 2016. (**A paraître)**.

Journal

- El Hadji Malick Ndoye, Frédérique Jacquet, Michel Misson, and Ibrahima Niang, "A Token-based MAC protocol for Linear Sensor Networks", in Sensors & Transducers journal, Vol.189, Issue 6, June 2015, pp. 31-40.

Journal soumis

- El Hadji Malick Ndoye, Nadir Hakem, Frédérique Jacquet, Michel Misson, and Ibrahima Niang, " Clustering approach based on interference avoidance for Linear WSN using Token Passing MAC " journal of Wireless Networks, Springer.

Conférence internationale : article complet

- El Hadji Malick Ndoye, Frédérique Jacquet, Michel Misson, and Ibrahima Niang, "Using a Token Approach for the MAC layer of Linear Sensor Networks Impact of the Redundancy on the Throughput ", in Sensornet, 11-13 Feb., 2015.

- El Hadji Malick Ndoye, Frédérique Jacquet, Michel Misson, and Ibrahima Niang, "Evaluation of RTS/CTS with unslotted CSMA/CA algorithm in linear sensor networks," in NICST 2013, September 2013.

Conférence internationale : article Poster

- El Hadji Malick Ndoye, Frédérique Jacquet, Michel Misson, and Ibrahima Niang, "Using a token approach for the MAC layer of linear sensor networks: Impact of the node position on the packet delivery," in IEEE Wireless Days, 12-14 Nov 2014.

Conférence nationale :

- El Hadji Malick Ndoye, Frédérique Jacquet, Michel Misson, "Architecture et méthode d'accès pour réseaux de capteurs linéaires", JNCTT, 3-4 Novembre, 2011.

Annexe A : Présentation de NS2

Source (www.developpez.com)

Le simulateur NS est un outil logiciel de simulation de réseaux informatiques, développé dans le cadre du projet VINT, ce dernier est un projet en cours de développement avec la collaboration de plusieurs acteurs (USC/ISI, Xerox parc, LBNL et UCB) dans l'objectif principal de construire un simulateur multi-protocole pour faciliter l'étude de l'interaction entre les protocoles et le comportement d'un réseau à différentes échelles.

Le projet contient des bibliothèques pour la génération de topologies réseau, des trafics ainsi que des outils de visualisation tels que l'animateur réseau NAM (network animator).

NS est un outil logiciel de simulation de réseaux informatiques. Il est essentiellement élaboré avec les idées de la conception par objets, de la réutilisation du code et de modularité. Il est aujourd'hui un standard de référence en ce domaine, plusieurs laboratoires de recherche recommandent son utilisation pour tester les nouveaux protocoles.

Le simulateur NS actuel est particulièrement bien adapté aux réseaux à commutation de paquets et à la réalisation de simulations de grande taille (le test du passage à l'échelle). Il contient les fonctionnalités nécessaires à l'étude des algorithmes de routage unicast ou multicast, des protocoles de transport, de session, de réservation, des services intégrés, des protocoles d'application comme FTP. A titre d'exemple la liste des principaux composants actuellement disponibles dans NS par catégorie est :

- application : Web, ftp, telnet, générateur de trafic (CBR...) ;
- transport : TCP, UDP, RTP, SRM ;
- routage unicast : Statique, dynamique (vecteur distance) ;
- routage multicast : DVMRP, PIM ;
- gestion de file d'attente : RED, DropTail, Token bucket.

NS-2 ne permet pas de visualiser le résultat des expérimentations. Il permet uniquement de stocker une trace de la simulation, de sorte qu'elle puisse être exploitée par un autre logiciel, comme NAM. NAM est un outil de visualisation qui présente deux intérêts principaux : représenter la topologie d'un réseau décrit avec NS-2, et afficher temporellement les résultats d'une trace d'exécution NS-2. Par exemple, il est capable de représenter des paquets TCP ou UDP, la rupture d'un lien entre nœuds, ou encore de représenter les paquets rejetés d'une file d'attente pleine. Ce logiciel est souvent appelé directement depuis les scripts TCL pour NS-2, pour visualiser directement le résultat de la simulation.

Pour l'installation du ns2, on doit tout d'abord installer les paquets suivants :

- build-essential ;
- autoconf ;
- Automak ;
- libxmu-dev.

Cela par la commande suivante (sous Fedora pour Ubuntu vous allez utiliser apt-get au lieu de yum):

```
su -
yum install build-essential autoconf automake libxmu-dev
```

Le téléchargement du NS2 se fait par la commande suivante :

```
wget http://nchc.dl.sourceforge.net/sourceforge/nsnam/ns-allinone-vX.tar.gz
```

Après la décompression de l'archive avec la commande tar -xzvf ns-allinone-X.tar.g , vous tapez la commande d'installation suivante après l'accès au dossier ns-allinone-X :

```
./install
```

L'étape la plus importante est la gestion des variables d'environnement qui s'affichent après la fin d'installation. La déclaration de ces variables se fait dans le fichier .bashrc comme suivant (il faut changer les X, Y, Z, T par les versions que vous avez) :

```
# LD_LIBRARY_PATH
OTCL_LIB=/home/<votre dossier personnel>/el>/ns-allinone-X/otcl-Y
NS2_LIB=/home/<votre dossier perso>/ns-allinone-2.31/lib
X11_LIB=/usr/X11R6/lib
USR_LOCAL_LIB=/usr/local/lib
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$OTCL_LIB:$NS2_LIB:$X11_
LIB:$USR_LOCAL_LIB
# TCL_LIBRARY
TCL_LIB=/home/<votre dossier personnel>/ns-allinone-2.31/tclZ/library
USR_LIB=/usr/lib
export TCL_LIBRARY=$TCL_LIB:$USR_LIB
# PATH
XGRAPH=/home/<votre dossier perso>/ns-allinone-2.31/bin:/home/<votre dossier perso>/
ns-allinone-X/tclZ/unix:/home/<votre dossier perso>/ns-allinone-2.31/tk8.4.14/unix
NS=/home/<votre dossier perso>/ns-allinone-X/ns-X/
NAM=/home/<votre dossier perso/-allinone-X/nam-T/
PATH=$PATH:$XGRAPH:$NS:$NAM
```

Après chaque changement au niveau du fichier .bashrc, on doit le recharger sinon on est obligé de redémarrer le terminal avec la commande :

```
$ source ~/.bashrc
```

Pour tester l'installation il suffit de lancer la commande ns qui affichera un % indiquant le bon fonctionnement de notre simulateur NS2. Une étape optionnelle de validation qui va tester des exemples de simulation déjà implémentés (cette étape prend plus ou moins de temps selon la puissance de la machine) :

```
cd ns-X
 ./validate
```

Annexe B : Quelques fonctions importantes de LTB-MAC

1. La fonction *generateToken*()

Cette fonction est utilisée par le *TokenAllocator* pour créer et initier la génération du jeton de proche en proche jusqu'au puits. Cette fonction permet de fixer la fréquence de passage du jeton selon que le réseau est 1, 2 et 3-redondant.

```
void MACPROTO::generateToken(){
Packet *p=Packet::alloc();
struct hdr_macproto_token * token = HDR_MACPROTO_TOKEN(p);
struct hdr_cmn * ch = HDR_CMN(p);
ch->size()+=SIZEOF_MACPROTO_TOKEN;
ch->direction()=hdr_cmn::DOWN;
 ch->ptype()=PT_MACPROTO_TOKEN;
token->nextTokenOwner=index_+1;
token->shuttleDuration=SHUTTLE_DURATION;
if(isStrictlinear){
token->tokenFrequence=4*token->shuttleDuration;
                        }
else{
        if(is2Redundant){
        token->tokenFrequence=7*token->shuttleDuration;}
        else {
        token->tokenFrequence=10*token->shuttleDuration;
                        }
                        }
tokenFrequence=token->tokenFrequence;
                        for(int i=0;i<numberOfPacketsUp;i++){
token->timeForNetxWakeup=TX_TIME(SIZE_OF_MACPROTO_DATA_PKT)+TX_TIME(SIZE_OF_MACPROTO_ACK);
                                }
Scheduler::instance().schedule(downtarget_, p, 0);
isWaitingForDowTraffic=true;
sleepTimer->resched(tokenFrequence);
if(!IsFirtGeneration){
```

```
		IsFirtGeneration=true;
}
else{
		}
SavedToken=p;
timerForToken=TX_TIME(SIZEOF_MACPROTO_TOKEN)+TX_TIME(SIZEOF_MACPROTO_ACK);
AckTimerForToken->resched(timerForToken);
		}
```

2. La fonction *sendToken*()

La fonction *sendToken()* est utilisée par tout autre nœud différent du générateur de jeton. Cette fonction est appelée après le passage de la navette. Elle permet à un nœud donné de relayer le jeton à son voisin direct.

```
void MACPROTO::sendToken(Packet * p) {
			Packet * copy = p->copy();
struct hdr_macproto_token * token = HDR_MACPROTO_TOKEN(copy);
struct hdr_cmn * ch  = HDR_CMN(copy);
ch->direction()=hdr_cmn::DOWN;
token->nextTokenOwner=index_+1;
if(!isSink){
		if(!IsFirtGeneration){
			IsFirtGeneration=true;
				}
}
token>timeForNetxWakeup=TX_TIME(SIZEOF_MACPROTO_DATA_PKT)+TX_TIME(SIZEOF_MACPROTO_ACK);
Scheduler::instance().schedule(downtarget_, copy, 0);
isWaitingForDowTraffic=true;
if(isStrictlinear){
			sleepTimer->resched(tokenFrequence-shuttleDuration);
		}
else{
		if(is2Redundant){
			sleepTimer->resched(tokenFrequence-2*shuttleDuration);
				}
```

```
            else {
                        sleepTimer->resched(tokenFrequence-3*shuttleDuration);
                    }
}
UpComeFromDirectNeighbor=false;
DownComeFromDirectNeighbor=false;
SavedTokenForNode=p;
AckTimerForToken->resched(timerForToken);
isReceivedToken=false;
            }
```

3. La fonction sendUptraffic()

Cette fonction permet à un nœud d'envoyer des trames de données en direction du puits au passage de la navette. Elle est appelée après l'envoie du trafic descendant. Elle prend en paramètre

```
void MACPROTO::sendUpTraffic(Packet * p) {
Packet * copy = p->copy();
struct hdr_malick_pkt * data = HDR_MALICK_PKT(copy);
struct hdr_cmn * ch  = HDR_CMN(copy);
hdr_ip *ih = hdr_ip::access(copy);
data->isType=1;
ch->direction()=hdr_cmn::DOWN;
ch->ptype()=PT_MALICK_PKT;
ch->size()=SIZEOF_MACPROTO_DATA_PKT;
ch->error() = 0;
if((isSendingUpTraffic)&&(isAcknowledgedUp)){
savedPacketUp=copy;
Scheduler::instance().schedule(downtarget_,copy, 0);
isAcknowledgedUp=false;
AckTimerForUpTraffic->resched(timerForUptraffic);
                        }
            }
```

4. La fonction receiveToken()

Cette fonction permet à un nœud donné d'occuper le canal. En effet, à la réception du jeton, le nœud va armer un *timer* d'envoi égal à la durée de la navette définie.

```
void MACPROTO::receiveToken(Packet * p) {
struct hdr_macproto_token * token = HDR_MACPROTO_TOKEN(p);
struct hdr_cmn * ch  = HDR_CMN(p);
if (isSink)  {
            Packet::free(p);
}
if(index_==token->nextTokenOwner){
hasNotreceiveToken=false;
sendAckForToken();
if(!hasReceivedToken){
isInReceiveingState=false;
hasReceivedToken=true;
DownTrafficTime=computeDownTrafficTime();
BeforeSendingTimer->resched(TX_TIME(SIZEOF_MACPROTO_ACK));
shuttleDuration=token->shuttleDuration;
tokenFrequence=token->tokenFrequence;
timeForNetxWakeup=token->timeForNetxWakeup;
SavedTokenForNode=p;
if(DownTrafficTime>0){
            isSendingDownTraffic=true;
            isAcknowledgedDown=true;
            if(numberOfPacketsDown>0){
            downtrafficTimer->resched(DownTrafficTime);
            sendDownTraffic(FIFODown[0]);
            time_for_downtraffic_finish=Scheduler::instance().clock()+DownTrafficTime;
                                    }
            }
            else {
            uptrafficTimer->resched(shuttleDuration-sendTokenTime);
            time_for_uptraffic_finish=Scheduler::instance().clock()+shuttleDuration-sendTokenTime;
            isAcknowledgedUp=true;
            isSendingUpTraffic=true;
                        }
}
```

```
        else{
                Packet::free(p);
                }
}
 }
```

Glossaire

Branche

L'ensemble des nœuds impliqué dans le relai d'une trame de donnée jusqu'au puits.

Capture

Elle définit la possibilité de recevoir un signal utile malgré la présence d'un signal interférent.

Cluster

Un ensemble composé d'un nœud central qui exploitent d'autres nœuds appelés ressources.

Connectivité

Elle permet d'améliorer la tolérance aux fautes en cas de nœuds ou liens défectueux.
.

Interférences

Il y'a interférences lorsque deux signaux se rencontrent et interagissent l'une avec l'autre créant ainsi une collision.

Jeton

Une petite trame de contrôle contenant des informations temporelles sur la période de transmission de données, sa fréquence de création, etc... Il donne à un nœud donné le droit d'accéder au canal de transmission.

Navette

La navette représente la période de transmission du trafic montant et descendant. Elle commence à la réception du jeton.

Portée

Champs de vision d'une entité réseau.

Puits

Dans le réseau, c'est l'entité qui est chargée de collecter les informations récoltées par les nœuds.

Qualité de service

Capacité à véhiculer dans de bonnes conditions un type de trafic donné, en termes de débit, délais de transmission, taux de perte de paquet, etc…

Redondance

La possibilité d'exploiter plusieurs liens radio en fonction de la portée des nœuds.

Token Allocator

Dans la topologie linéaire, c'est le nœud qui se trouve l'extrémité opposée du puits. Il est chargé de créer le jeton. Il est aussi appelé générateur de jeton.

Trame

Paquet d'informations délimitées par des fanions.

Liste des abréviations

ADC-SMAC, Adaptive Duty Cycle SMAC 45
AMERR, Adaptive MERR 48
BI, Beacon Interval 28
BO, Beacon Order 28
BSN, Basic Sensor Node 49
CAP, Contention Access Period 29
CCA, Clear Channel Assessment 56
CFP, Contention Free Period 29
CMAC-T, Chain-type MAC Protocol based on Token 37
CSMA/CA, Carrier Sense Multiple Access with Collision Avoidance 29
DDN, Data Dessimination Node 24
DIFS, DCF IFS 59
DiS-MAC, Directional Scheduled MAC 34
DRN, Data Relay Node 49
DS-SS, Direct-sequence spread spectrum 92
EEDA-MAC, Energy-Efficient and Delay-Aware MAC 47
EIFS, Extended IFS 59
FDMA, Frequency Division Multiple Access 92
FIFO, First In First Out 55
GTS, Guaranted Time Slot 29
IFS, Inter Frame Space 59
JA, Jump Always 50
LC-MAC, Long-Chain MAC 35
L-CSMA, Linear CSMA 42
LDP, Location Detect Package 36
LR WPAN, Low Rate Wireless Personal Area Network 27
LTB-MAC, Linear Token-Based MAC Protocol 74
MAC, Medium Access Channel 12
MERR, Minimum Energy Relay Routing 48
MTF-MAC, Multi Frame Transmission MAC 40

NAV, Network Allocation Vector 58
PAN, Personal Area Network 27
PCF, Point coordination function 59
PIFS, PCF IFS 59
PRI-MAC, pipelined-forwarding, Routing-integrated, and effectively-Identify MAC 43
RA, Redirect Always 50
RTS/CTS, Request to send/Clear to Send 55
SC, Shuttle Capacity 80
SD, Superframe Duration 28
SDur, Shuttle Duration 80
SIFS, Short IFS 59
SIR, Signal-to-Interference Ratio 129
S-MAC, Sensor MAC 45
SO, Superframe Order 28
TDMA, Time division multiple access 30
WiWi, Wireless Wire 38
WLSN, Wireless Linear Sensor Network 12
WSN, Wireless Sensor Network 92

Bibliographie

Abbasi, A.A., and Younis, M. (2007). A survey on clustering algorithms for wireless sensor networks. Comput. Commun. *30*, 2826–2841.

Agha, K.A., Chalhoub, G., Guitton, A., Livolant, E., Mahfoudh, S., Minet, P., Misson, M., Rahmé, J., Val, T., and Bossche, A.V.D. (2009). Cross-layering in an Industrial Wireless Sensor Network: Case Study of OCARI. J. Netw. *4*.

Agrawal, D., and Zeng, Q.-A. (2015). Introduction to Wireless and Mobile Systems (Cengage Learning).

Al-Shawaqfeh, M., Abu-El-Haija, A., and Abdel Rahman, M.J. (2013). Collision Avoidance Slot Allocation Scheme for Multi-cluster Wireless Sensor Networks. Wirel Netw *19*, 1187–1201.

Azimi-Sadjadi, B., Sexton, D., Liu, P., and Mahony, M. (2006). Interference effect on IEEE 802.15. 4 performance. In Proceedings of 3rd International Conference on Networked Sensing Systems (INNS), Chicago, IL, (Citeseer),.

Baker, D.J., and Ephremides, A. (1981). The Architectural Organization of a Mobile Radio Network via a Distributed Algorithm. IEEE Trans. Commun. *29*, 1694–1701.

Baldus, H., Klabunde, K., and Müsch, G. (2004). Reliable Set-Up of Medical Body-Sensor Networks. In Wireless Sensor Networks, H. Karl, A. Wolisz, and A. Willig, eds. (Springer Berlin Heidelberg), pp. 353–363.

Buratti, C., and Verdone, R. (2015). L-CSMA: A MAC Protocol for Multi-Hop Linear Wireless (Sensor) Networks.

Chakraborty, G. (2010). Optimum Cluster Size for Cluster-Based Communication in Wireless Sensor Network. Fourth Int. Confrence Mob. Ubiuitous Comput. Syst. Serv. Technol.

Chen, Y., and Terzis, A. (2011). On the implications of the log-normal path loss model: an efficient method to deploy and move sensor motes. In Proceedings of the 9th ACM Conference on Embedded Networked Sensor Systems, (ACM), pp. 26–39.

De Caneva, D., Montessoro, P.L., and others (2010). A synchronous and deterministic MAC protocol for wireless communications on linear topologies. Intl J Commun. Netw. Syst. Sci. *3*, 925.

Demirbas, M., Arora, A., and Mittal, V. (2004). FLOC: A fast local clustering service for wireless sensor networks. In Workshop on Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks (DIWANS/DSN 2004), (Citeseer), pp. 1–6.

Dudek, D., Haas, C., Kuntz, A., Zitterbart, M., Krüger, D., Rothenpieler, P., Pfisterer, D., and Fischer, S. (2009). A Wireless Sensor Network for Border Surveillance. In Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems, (New York, NY, USA: ACM), pp. 303–304.

Fang, C., Liu, H., and Qian, L. (2011). Lc-mac: An efficient mac protocol for the long-chain wireless sensor networks. In Communications and Mobile Computing (CMC), 2011 Third International Conference on, (IEEE), pp. 495–500.

Felemban, E. (2013). Advanced border intrusion detection and surveillance using wireless sensor network technology.

Fitzsimons, M. (2005). The langeled approach. World Pipelines *5*, 24–26.

Gezer, C., Buratti, C., and Verdone, R. (2010). Capture effect in IEEE 802.15. 4 networks: Modelling and experimentation. In Wireless Pervasive Computing (ISWPC), 2010 5th IEEE International Symposium on, (IEEE), pp. 204–209.

Goldsmith, A. (2005). Wireless communications (Cambridge university press).

Hakem, N., Delisle, G., and Coulibaly, Y. (2014). Radio-wave propagation into an underground mine environment at 2.4 GHz, 5.8 GHz and 60 GHz. In Antennas and Propagation (EuCAP), 2014 8th European Conference on, (IEEE), pp. 3592–3595.

Hartong, M., Goel, R., and Wijesekera, D. (2008). Security and the US rail infrastructure. Int. J. Crit. Infrastruct. Prot. *1*, 15–28.

Heinzelman, W.R., Chandrakasan, A., and Balakrishnan, H. (2000). Energy-efficient communication protocol for wireless microsensor networks. In Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, 2000, p. 10 pp. vol.2 – .

IEEE (2003). Part 15.4: wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (LR-WPANs). IEEE Comput. Soc.

IEEE (2005). Part 11: wireless medium access control (MAC) and physical layer (PHY) specifications: medium access control (MAC) quality of service (QoS) enhancements. IEEE 80211 E Stand.

Iskander, M.F., and Yun, Z. (2002). Propagation prediction models for wireless communication systems. Microw. Theory Tech. IEEE Trans. On *50*, 662–673.

Jawhar, I., and Mohamed, N. (2009). A hierarchical and topological classification of linear sensor networks. In Wireless Telecommunications Symposium, 2009. WTS 2009, pp. 1–8.

Jawhar, I., Mohamed, N., and Agrawal, D.P. (2011). Linear wireless sensor networks: Classification and applications. J. Netw. Comput. Appl. *34*, 1671–1682.

Jordan, R., and Abdallah, C.T. (2002). Wireless Communications Networking: and An Overview.

Karpiriski, M., Senart, A., and Cahill, V. (2006). Sensor networks for smart roads. In Pervasive Computing and Communications Workshops, 2006. PerCom Workshops 2006. Fourth Annual IEEE International Conference on, (IEEE), p. 5 – pp.

Karveli, T., Voulgaris, K., Ghavami, M., and Aghvami, A.H. (2009). DiS-MAC: A MAC protocol for sensor networks used for roadside and highway monitoring. In International Conference on Ultra Modern Telecommunications Workshops, 2009. ICUMT '09, pp. 1–6.

Kennedy, J.L. (1993). Oil and Gas Pipeline Fundamentals (PennWell Books).

Komar, C., Donmez, M.Y., and Ersoy, C. (2012). Detection quality of border surveillance wireless sensor networks in the existence of trespassers' favorite paths. Comput. Commun. *35*, 1185–1199.

Kosunalp, S., Mitchell, P., Grace, D., and Clarke, T. Experimental Study of the Capture Effect for Medium Access Control with ALOHA.

Koubaa, A., Alves, M., and Tovar, E. (2006). A comprehensive simulation study of slotted CSMA/CA for IEEE 802.15.4 wireless sensor networks. (IEEE), pp. 183–192.

Krishnamachari, B., Estrin, D., and Wicker, S. (2002). Modelling data-centric routing in wireless sensor networks. In IEEE Infocom, pp. 39–44.

Lee, E., Jwa, J.W., and Kim, H. (2013). MFT-MAC: A Duty-Cycle MAC Protocol Using Multiframe Transmission for Wireless Sensor Networks. Int. J. Distrib. Sens. Netw. *2013*, e858765.

Lee, J., Kim, W., Lee, S.-J., Jo, D., Ryu, J., Kwon, T., and Choi, Y. (2007). An experimental study on the capture effect in 802.11 a networks. In Proceedings of the Second ACM International Workshop on Wireless Network Testbeds, Experimental Evaluation and Characterization, (ACM), pp. 19–26.

Lee, S.H., Lee, S., Song, H., and Lee, H.S. (2009). Wireless sensor network design for tactical military applications : Remote large-scale environments. In IEEE Military Communications Conference, 2009. MILCOM 2009, pp. 1–7.

Lee, W., Lee, J., Henderson, C., Taylor, H.F., James, R., Lee, C.E., Swenson, V., Atkins, R.A., and Gemeiner, W.G. (1999). Railroad bridge instrumentation with fiber-optic sensors. Appl. Opt. *38*, 1110–1114.

Lin, P., Qiao, C., and Wang, X. (2004). Medium access control with a dynamic duty cycle for sensor networks. In Wireless Communications and Networking Conference, 2004. WCNC. 2004 IEEE, (IEEE), pp. 1534–1539.

Lindsey, S., and Raghavendra, C.S. (2002). PEGASIS: Power-efficient gathering in sensor information systems. In Aerospace Conference Proceedings, 2002. IEEE, (IEEE), pp. 3–1125.

Liu, J., Suzuki, M., Lee, D., and Morikawa, H. (2013a). A Token Scheduled High Throughput Multi-Channel Data Collection Protocol for Wireless Sensor Network. In Vehicular Technology Conference (VTC Spring), 2013 IEEE 77th, pp. 1–5.

Liu, J., Suzuki, M., Lee, D., and Morikawa, H. (2013b). Implementation and evaluation of token-scheduled collection protocol in wireless sensor network. In 2013 19th Asia-Pacific Conference on Communications (APCC), pp. 178–183.

Mainwaring, A., Culler, D., Polastre, J., Szewczyk, R., and Anderson, J. (2002). Wireless sensor networks for habitat monitoring. In Proceedings of the 1st ACM International Workshop on Wireless Sensor Networks and Applications, (ACM), pp. 88–97.

Malan, D., Fulford-Jones, T., Welsh, M., and Moulton, S. (2004). Codeblue: An ad hoc sensor network infrastructure for emergency medical care. In International Workshop on Wearable and Implantable Body Sensor Networks,.

Manjeshwar, A., and Agrawal, D.P. (2002). APTEEN: A hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks. In Ipdps, (IEEE), p. 0195b.

Musaloiu-e, R., Terzis, A., Szlavecz, K., Szalay, A., Cogan, J., and Gray, J. (2006). Life under your feet: A wireless soil ecology sensor network. In Proc. 3rd Workshop on Embedded Networked Sensors (EmNets 2006), (Citeseer),.

Ndoye, E.H.M., Jacquet, F., Misson, M., and Niang, I. (2013). Evaluation of RTS/CTS with unslotted CSMA/CA algorithm in linear sensor networks. NICST.

Noori, M., and Ardakani, M. (2008). Characterizing the traffic distribution in linear wireless sensor networks. Commun. Lett. IEEE *12*, 554–556.

Pan, M.-S., Fang, H.-W., Liu, Y.-C., and Tseng, Y.-C. (2008). Address Assignment and Routing Schemes for ZigBee-Based Long-Thin Wireless Sensor Networks. In IEEE Vehicular Technology Conference, 2008. VTC Spring 2008, pp. 173–177.

Papoulis, A., and Pillai, S.U. (2002). Probability, random variables, and stochastic processes (Tata McGraw-Hill Education).

Polastre, J., Szewczyk, R., and Culler, D. (2005). Telos: enabling ultra-low power wireless research. In Information Processing in Sensor Networks, 2005. IPSN 2005. Fourth International Symposium on, (IEEE), pp. 364–369.

Porter, J., Arzberger, P., Braun, H.-W., Bryant, P., Gage, S., Hansen, T., Hanson, P., Lin, C.-C., Lin, F.-P., Kratz, T., et al. (2005). Wireless Sensor Networks for Ecology. BioScience *55*, 561–572.

Rappaport, T.S., and others (1996). Wireless communications: principles and practice (prentice hall PTR New Jersey).

Santhi, S.G., and Venkatachalpathy, K. (2014). Multiple Cluster Tree Routing and Schedu ling for Collision Avoidance in 802.15.4. Sensor Networks.

Sarr, M.D., Delobel, F., Misson, M., and Niang, I. (2012). Automatic discovery of topologies and addressing for Linear wireless sensors networks. In Wireless Days (WD), 2012 IFIP, pp. 1–7.

Shiu, Y.-S., Chang, S.Y., Wu, H.-C., Huang, S.C.-H., and Chen, H.-H. (2011). Physical layer security in wireless networks: a tutorial. IEEE Wirel. Commun. *18*, 66–74.

Shuai, M., Xie, K., Ma, X., and Song, G. (2008). An on-road wireless sensor network approach for urban traffic state monitoring. In Intelligent Transportation Systems, 2008. ITSC 2008. 11th International IEEE Conference on, (IEEE), pp. 1195–1200.

Simon, M.K. (2007). Probability distributions involving Gaussian random variables: A handbook for engineers and scientists (Springer Science & Business Media).

Simon, G., Maróti, M., Lédeczi, Á., Balogh, G., Kusy, B., Nádas, A., Pap, G., Sallai, J., and Frampton, K. (2004). Sensor Network-based Countersniper System. In Proceedings of the 2Nd International Conference on Embedded Networked Sensor Systems, (New York, NY, USA: ACM), pp. 1–12.

Stoianov, I., Nachman, L., Madden, S., Tokmouline, T., and Csail, M. (2007). PIPENET: A wireless sensor network for pipeline monitoring. In Information Processing in Sensor Networks, 2007. IPSN 2007. 6th International Symposium on, (IEEE), pp. 264–273.

Subramanian, L., and Katz, R.H. (2000). An architecture for building self-configurable systems. In 2000 First Annual Workshop on Mobile and Ad Hoc Networking and Computing, 2000. MobiHOC, pp. 63–73.

Sun, T., Yan, X.J., and Yan, Y. (2013a). A Chain-type Wireless Sensor Network in Greenhouse Agriculture. J. Comput. *8*, 2366–2373.

Sun, T., Yan, X.J., and Yan, Y. (2013b). A Chain-type Wireless Sensor Network in Greenhouse Agriculture. J. Comput. *8*.

Tanenbaum, A.S. (2003). Computer networks, 4-th edition. Ed Prentice Hall.

Tong, F., Ni, M., Shu, L., and Pan, J. (2013). A Pipelined-forwarding, Routing-integrated and effectively-Identifying MAC for large-scale WSN. In Global Communications Conference (GLOBECOM), 2013 IEEE, (IEEE), pp. 225–230.

Van Dam, T., and Langendoen, K. (2003). An adaptive energy-efficient MAC protocol for wireless sensor networks. In Proceedings of the 1st International Conference on Embedded Networked Sensor Systems, (ACM), pp. 171–180.

Van Den Bossche, A. (2007). Proposition d'une nouvelle méthode d'accès déterministe pour un réseau personnel sans fil à fortes contraintes temporelles. Université Toulouse le Mirail-Toulouse II.

Virone, G., Wood, A., Selavo, L., Cao, Q., Fang, L., Doan, T., He, Z., and Stankovic, J. (2006). An advanced wireless sensor network for health monitoring. In Transdisciplinary Conference on Distributed Diagnosis and Home Healthcare (D2H2), pp. 2–4.

Waharte, S., and Boutaba, R. (2005). Performance Comparison of Distributed Frequency Assignment Algorithms for Wireless Sensor Networks. In Network Control and Engineering

for QoS, Security and Mobility, III, D. Gaïti, S. Galmés, and R. Puigjaner, eds. (Springer US), pp. 151–162.

Wu, H., Cheng, S., Peng, Y., Long, K., and Ma, J. (2002). IEEE 802.11 distributed coordination function (DCF): analysis and enhancement. In IEEE International Conference on Communications, 2002. ICC 2002, pp. 605–609.

Xu, K., and Gerla, M. (2002). A heterogeneous routing protocol based on a new stable clustering scheme. In MILCOM 2002. Proceedings, pp. 838–843 vol.2.

Yildiz, H.U., Kurt, S., and Tavli, B. (2014). The Impact of Near-Ground Path Loss Modeling on Wireless Sensor Network Lifetime. In Military Communications Conference (MILCOM), 2014 IEEE, (IEEE), pp. 1114–1119.

Yu, H., and Guo, M. (2015). Energy-Efficient and Delay-Aware MAC Protocol in Wireless Sensor Networks for Oil and Gas Pipeline Monitoring. Power *5*, 10.

Zimmerling, M., Dargie, W., and Reason, J.M. (2008). Localized power-aware routing in linear wireless sensor networks. In Proceedings of the 2nd ACM International Conference on Context-Awareness for Self-Managing Systems, (ACM), pp. 24–33.