République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université A.MIRA-BEJAIA

Faculté des Sciences Exactes
Département de Recherche Opérationnelles
Unité de Recherche LaMOS (Modélisation et Optimisation des Systèmes)

THÈSE

EN VUE DE L'OBTENTION DU DIPLOME DE DOCTORAT

Domaine : Mathématiques et informatique Filière :Mathématiques appliquées
Spécialité : Recherche Opérationnelle et Aide à la Décision

Présentée par
M^{lle} ALKAMA Lynda

Thème

Evaluation et optimisation des performances des réseaux de capteurs d'infrastructures critiques IEEE 802.15.4k

Soutenu le : 22/12/2020 **Devant le Jury composé de :**

Nom et Prénom	**Grade**		
Mr Smail ADJABI	Professeur	Univ. de Bejaia	**Président**
Mme Louiza BOUALLOUCHE-MEDJKOUNE	Professeur	Univ. de Bejaia	**Rapporteur**
Mme Lina BACHIRI	M.C.B	Univ. de Bejaia	**Co-Rapporteur**
Mr Lamri SAYAD	M.C.A	Univ. de Msila	**Examinateur**
Mr Mohand YAZID	M.C.A	Univ. de Bejaia	**Examinateur**
Mr Samra BOULFKHAR	M.C.A	Univ. de Bejaia	**Examinatrice**

Année Universitaire : 2019/2020

Remerciements

Cette thèse a pu voir le jour, grâce à Dieu et au soutien et à l'aide de plusieurs personnes. Je profite de cet espace pour les remercier tous.

Mes premiers remerciements vont à Madame Bouallouche-Medjkoune Louiza pour son encadrement durant ces années de thèse, pour ce thème qu'elle m'a proposé, pour ses orientations et les moyens qu'elle a mis à ma disposition. Elle a été toujours une source inépuisable d'idées, de savoir et d'encouragement. Ce travail n'aurait jamais pu aboutir sans elle, elle a toujours su me guider, me conseiller, et me témoigner son soutien et sa confiance. Je lui transmets l'expression de ma reconnaissance et ma plus profonde gratitude. Je tiens aussi à remercier Madame Bachiri Lina pour ses conseils et son suivi le long de mes années de recherches doctorales. Aussi, grâce à sa confiance, j'ai pu me réaliser complètement dans mes recherches. Elle a été d'une aide précieuse dans les moments les plus délicats, qu'elle trouve ici l'expression de ma profonde gratitude.

Je remercie vivement Monsieur Adjabi Smail, Professeur à l'université de Bejaïa de m'avoir fait l'honneur de présider ce jury. Je suis reconnaissante à Monsieur Sayad Lamri Maître de conférences à l'université de Msila, Monsieur Yazid Mohand Maître de conférences à l'université de Bejaia, Madame Boulefkhar Samra Maître de conférences à l'université de Bejaia d'avoir accepté d'examiner mon travail, je les remercie pour le temps qu'ils consacreraient à la lecture et l'expertise de ma thèse.

Je ne pourrais clôturer ces remerciements sans me retourner vers les deux être les plus chère, qui avaient un rôle essentiel pendant plusieurs années d'études, et qui sans eux aucune réussite n'aurait été possible. J'adresse de tout mon cœur mes remerciements à mon très cher père et ma très chère mère. Merci pour vos sacrifices, votre présence et votre soutien aux moments les plus difficiles. Mes chères sœurs Dina et Narima et mon cher frère Kouceila, merci beaucoup pour vos encouragements.

J'aimerais également remercier tous les membres du l'unité de recherche LaMOS, pour leur aide et pour l'environnement de travail très agréable. Je remercie plus particulièrement Messieurs Atmani Mouloud et Soufit Massinissa pour leur aide précieuse, ainsi que leur encouragement.

Dédicaces

Je dédie ce modeste travail

A mon très cher père, Rezak

A ma très chère mère, Farida

A mon frère Kouceila

A mes sœurs Dina et Narima

A la mémoire de ma grand-mère

A mes amis, collègues, et tout ceux qui ont contribué à la réalisation de ce travail.

Table des matières

Table des figures

Liste des tableaux

Notations et Abréviations

ACK	Acknowledgement
AIFS	Acknowledgment Inter Frame Spacing
ASK	Amplitude Shift Keying
BE	Backoff Exponent
BER	Bit Error Rate
BI	Beacon Interval
BO	Beacon Order
BOP	Beacon Only Period
BPM	Burst Position Modulation
BPSK	Binary Phase-Shift Keying
C4FM	Continuous four-level Frequency Modulation
CAP	Contention Acess Period
CCA	Clear Channel Assessment
CFP	Contention Free Period
CMB	China Medical Band
CSM	Common Signaling Mode
CSMA/CA	Carrier Sence Multiple Access with Collision Avoidance
CSS	Chirp Spread Spectrum
CW	Contention Window
CWPAN	Chinese Wireless Personal Area Network
DBS	Dedicated Beacon Slot
DQPSK	Differential Quadrature Phase-Shift Keying
DSME	Deterministic and Synchronous Multi-channel Extension
DSSS	Direct Sequence Spread Spectrum
EB	Enhanced Beacon
ED	Energy Detection
EDGE	Enhanced Data Rates for GSM

ESD	Extended Superframe Duration
FER	Frame Error Rate
FFD	Full Function Device
FSK	Frequency Shift Keying
GFSK	Gaussian Frequency-Shift Keying
GMSK	Gaussian Minimum Shift Keying
GPRS	General Packet Radio Services
GSM	Global System for Mobile communications
GTS	Guranteed Time Slot
HRP	High Rate Pulse
IEEE	Institut of Electrical and Electronics Engineers
IFS	Inter Frame Space
ISO	International Organization for Standardization
LAN	Local Area Network
LECIM	Low Energy Critical Infrastructure Monitoring
LIFS	Long Inter Frame Space
LLC	Logical Link Control
LLDN	Low Latency Deterministic Network
LMR	Land Mobile Radio
LMSC	Local and Metropolitan area networks Standard Committee
LQI	Link Quality Indication
LRP-UWB	Low Rate Pulse- Ultra Wide Band
LR-WPAN	Low Rate Wireless Personal Area Network
LTE	Long Term Evolution
MAC	Medium Access Control
MBAN	Medical Body Area Network
MDSSS	Multiplexed Direct Sequence Spread Spectre
MIIT	Ministry of Industry and Information Technology
MPM	multi-physical layer management
MPSK	M-ary Phase Shift Keying
MR-FSK	Multi-Rate and Multi-Regional Frequency Shift Keying
MR-OFDM	Multi-Rate and Multi-Regional Orthogonal Frequency Division Multiplexing

MR-O-QPSK	Multi-Rate and Multi-Regional Offset Quadrature Phase-Shift Keying
MSK	Minimum Shift Keying
NB	Number of Backoffs
OOK	On-Off Keying
O-QPSK	Offset Quadrature Phase-Shift Keying
OSI	Open System Interconnection
PAN	Personal Area Network
PCA	Priority Channel Access
PDA	Personnal Digital Assistant
P-FSK	Position-based Frequency Shift Keying
P-GFSK	Position-based Gaussian Frequency Shift Keying
PHY	Physical Layer
PPM	Pulse Position Modulation
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase-Shift Keying
RCC	Rail Communications and Control
RCCN	Rail Communications and Control Network
RCSF	Réseau de Capteurs Sans Fil
RFD	Reduced Function Device
RFD-RX	Reduced Function Device-Receive Only
RFD-TX	Reduced Function Device-Transmit Only
RFID	Radio Frequency Identification
RIC	Réseau d'infrastructures Critique
RSSI	Received Signal Strength Indicator
SAN	Stochastic Automata Network
SD	Superframe Duration
SIFS	Short Inter Frame Slot
SO	Superframe Order
SPC	Super PAN Coordinator
SPC	Stochastic Petri Nnets
SRM	Spectrum resource measurement
SUN	Smart Metering Utility Networks

TDMA	Time Division Multiple Access
TMCTP	TVWS Multichannel Cluster Tree PAN
TSCH	Time Slotted Channel Hopping
TVWS	TV White Space
UMTS	Universal Mobile Telecommunications System
UWB	Ultra Wide Band
WBAN	Wireless Body Area Network
WIMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WPAN	Wireless Personal Area Network
WWAN	Wireless Wide Area Network
WSN	Wireless Sensor Network

Introduction générale

Le système de chauffage, la connexion Internet, l'approvisionnement électrique, l'approvisionnement en eau et l'approvisionnement en gaz que nous utilisons dans nos maisons, sont des services que nous utilisons dans notre vie de tous les jours. Certes leur présence est primordial, mais nous ne pensons jamais aux infrastructures que nous offrent ces services. Si un quelconque problème se produit avec ces infrastructures critiques, ceci aurait un impact négatif significatif sur notre vie. Il est vrai que les interruptions de service ou les dysfonctionnements se produisent très rarement, cependant, en raison des causes artificielles ou naturelles, les services que nous offrent ces installations peuvent être interrompus. De plus, une grande partie de la bonne vie dont jouissent les pays développés dépend fortement du fonctionnement d'un certain nombre d'infrastructures essentielles interdépendantes.

Les infrastructures essentielles représentent les secteurs stratégiques dans lesquels aucune perturbation prolongée ne peut être tolérée, car ils assurent, entre autres, le bon fonctionnement de cette société et, surtout, la sécurité et le bien-être de la population. La plupart des États et groupes d'États, comme l'Union européenne, identifie les infrastructures essentielles, par secteurs. Le choix de secteurs a été inspiré par l'organisation des milieux d'affaires et de l'industrie. D'ailleurs, dans tous les pays, le secteur finance ou économie est toujours présent. Par exemple, au Canada, il existe dix secteurs désignés comme infrastructures essentielles à savoir : Énergie et services publics, Finances, Alimentation, Transport, Gouvernement, Technologies de l'information et de la communication, Santé, Eau, Sécurité et Secteur manufacturier [1]. Si l'une de ces infrastructures échoue, cela peut avoir un effet désastreux se diffusant sur tout le réseau des infrastructures. Par conséquent, ils doivent être protégés et fonctionner 24 heures sur 24, 7 jours sur 7. Pour cela, leur suivi est d'une grande importance. La surveillance de ces infrastructures garantit leur sécurité, réduit les pannes et les coûts de maintenance et accélère la restauration des services interrompus.

Problématique et motivations

Les réseaux de capteurs sans fil (RCSFs) sont l'une des technologies à utiliser pour surveiller les

infrastructures critiques. En effet, ceux-ci peuvent fournir des réseaux de surveillance simples, économiques et faciles à déployer. Les nœuds capteurs doivent rapporter des informations de mesure ou d'état dans un intervalle de quelques minutes à plusieurs heures et de signaler une panne qui se déclenche en urgence.

La norme IEEE 802.15.4-2003 [2] des RCSFs existante ne convient pas à la surveillance des infrastructures critiques. Ainsi, l'organisme IEEE a adopté la norme IEEE 802.15.4k [3] en 2013, afin de redéfinir les protocoles MAC de la norme existante, et de la rendre capable de faire face aux besoins de surveillance des infrastructures critiques. La première version de cette norme a été finalisée en Juin 2013. Des spécifications prometteuses pour la couche MAC et la couche physique (PHY) de l'amendement "k" sont proposées pour les réseaux de surveillance des infrastructures critiques à faible consommation d'énergie LECIM (Low Energy Critical Infrastructure Monitoring). Des mécanismes offrant un accès prioritaire au canal sont définis dans cet amendement, afin de transmettre le message prioritaire comportant les informations nécessaires sur la panne. Cet accès prioritaire permettra ainsi une réparation rapide pour éviter un désastre pouvant se produire. Deux nouveaux mécanismes MAC ont été proposés dans l'amendement "k", à savoir : Carrier Sence Multiple Acess with Collision Avoidance avec backoff Priority Channel Acces (CSMA/CA avec backoff PCA) et ALOHA PCA.

Contributions

Sans perte de généralité, nous allons nous intéresser dans cette thèse à l'analyse de performances des mécanismes MAC proposés dans l'amendement "k" de la norme IEEE 802.15.4, dédiés aux applications de surveillance des infrastructures critiques à faible consommation d'énergie des réseaux de capteurs sans fil. L'évaluation des performances de la norme IEEE 802.15.4k nous permettra ainsi d'illustrer de manière quantitative un ensemble de métriques de performances, telles que, le débit, le délai et la fiabilité.

Le modèle analytique par chaîne de Markov que nous proposons pour le mécanisme CSMA/CA avec backoff PCA slotté de la norme IEEE 802.15.4k est le premier, dans la littérature, considérant un mode beacon, un trafic saturé et une topologie en étoile sous un canal bruité. Notre modèle de chaîne de Markov se compose de deux parties : une chaîne de Markov à deux dimensions pour le CSMA/CA avec backoff PCA slotté et une chaîne de Markov à trois dimensions pour le CSMA/CA

slotté [4]. Le modèle est capable d'estimer la fiabilité, l'énergie consommée, le débit et le délai. Une étude sur l'impact de quelques paramètres sur les métriques de performance étudiées est réalisée. Par la suite, nous réaliserons une analyse comparative du mécanisme CSMA/CA de la norme IEEE 802.15.4k avec le mécanisme CSMA/CA de la norme de base IEEE 802.15.4. Pour une grande taille de paquets, PCA donne une meilleure fiabilité, une énergie consommée réduite, un faible débit, un délai minimal et une petite probabilité d'échec par rapport à CSMA/CA.

Notre deuxième contribution se focalisera sur le mode non beacon des protocoles CSMA/CA avec backoff PCA et CSMA/CA de la norme IEEE 802.15.4k. Notre modèle de chaîne de Markov se compose d'une chaîne de Markov à deux dimensions pour le CSMA/CA avec backoff PCA non slotté et d'une chaîne de Markov à trois dimensions pour le CSMA/CA non slotté. Le réseau considéré suit une topologie en étoile, dans lequel chaque appareil transmet des paquets au coordinateur PAN et reçoit un accusé de réception. Un état saturé du trafic et des conditions du canal idéal et non idéal seront considérées. Une analyse des performances en termes de fiabilité, d'énergie consommée et de débit, est effectuée. De plus, une étude sur l'impact de quelques paramètres sur les métriques de performance étudiées est réalisée. Les résultats montre que PCA non slotté assure une réduction de la consommation d'énergie, offre un débit élevé mais une fiabilité inférieure à celle de CSMA/CA non slotté. En effet, à mesure que l'on augmente le nombre de dispositifs, IEEE 802.15.4k offre une fiabilité réduite, une énergie réduite et un débit réduit. Pour des paquets de grandes tailles, le protocole donne une bonne fiabilité, une très faible consommation d'énergie, une faible probabilité d'échec et un débit plus élevé.

Un premier modèle analytique, dans la littérature, modélisant le mécanisme ALOHA PCA et ALOHA de la norme IEEE 802.15.4k dans un mode beacon sera proposé. Les deux mécanismes seront modélisés chacun par une chaîne de Markov à trois dimensions. Sur la base de notre modèle proposé, nous calculons la fiabilité, la consommation d'énergie, le débit et le délai moyen, pour les deux mécanismes dans des conditions de saturation de trafic et dans un canal idéal. Enfin, une évaluation de l'effet de quelques paramètres sur les performances du réseau est effectuée. Nous constatons que PCA offre par rapport à aloha, une meilleure fiabilité, une énergie consommée minimale, un délai très petit et un faible débit de données. Avec l'augmentation de la taille du réseau et de la taille des paquets, de très bon résultats sont obtenus.

Organisation de la thèse

Dans cette thèse, nous évaluons les performances des mécanismes MAC de l'amendement IEEE 802.15.4k, à savoir les mécanismes (CSMA/CA avec backoff PCA et ALOHA PCA) permettant au nœuds ayant des messages prioritaires à transmettre, un accès prioritaire au canal, et les mécanismes (CSMA/CA et ALOHA) permettant au nœuds ayant des messages non prioritaires à transmettre, un accès au canal ordinaire. Pour ce faire, nous proposons une modélisation analytique à l'aide d'une chaîne de Markov pour chaque mécanisme.

Cette thèse est composée de six chapitres, structurés en deux parties. La première partie est introductive et comporte les trois premiers chapitres. Le premier chapitre est dédié à une présentation générale sur les réseaux de capteurs sans fil, leurs caractéristiques et domaines d'application. Par la suite, nous décrirons la norme IEEE 802.15.4 conçue pour ce type de réseaux, ses topologies du réseau, ses modes de fonctionnement et ses mécanismes d'accès. Une introduction à l'évaluation des performances des RCSFs utilisant soit les méthodes analytiques soit la simulation sera présentée dans ce chapitre. Finalement, nous dresserons une synthèse sur les principaux travaux existants d'évaluation des performances du mécanisme d'accès CSMA/CA en mode beacon et non beacon.

Dans le deuxième chapitre, nous allons présenter la chronique de recherche de type Survey concernant la révolution historique du standard IEEE 802.15.4 au fil du temps depuis sa première apparition jusqu'à aujourd'hui [5]. Une étude critique sur les nouvelles versions sera proposée pour faire face aux limites rencontrées dans la version de base de IEEE 802.15.4-2003. Les amendements sont développés soit pour prendre en charge un type de réseau spécifique, soit pour porter des modifications (sur la couche physique ou sur la sous-couche MAC) ou simplement comme une révision pour les versions précédentes. Un tableau comparatif entre les exigences auxquelles ses amendements répondent sera présenté.

Le troisième chapitre sera consacré aux généralités sur les réseaux d'infrastructures critiques, comprenant leurs domaines d'applications et leurs caractéristiques. La norme IEEE 802.15.4k apparue en 2013, est la norme conçue pour surveiller les réseaux LECIM en utilisant des capteurs surveillant un phénomène précis et alertant toute panne ou danger, en temps réel. Cette alerte se fait par la transmission de l'information en toute priorité vers le coordinateur PAN. La topologie supportée des réseaux LECIM et les protocoles MAC proposés par l'amendement "k" seront présentés. Une

synthèse sur les travaux existants de ces protocoles MAC à savoir le CSMA/CA avec backoff PCA et ALOHA PCA sera aussi présentée.

La deuxième partie de ce travail regroupe nos contributions et comporte les trois derniers chapitres. Le quatrième chapitre sera consacré à la première contribution de la modélisation et l'évaluation des performances des mécanisme d'accès CSMA/CA avec backoff PCA slotté et CSMA/CA slotté de la norme IEEE 802.15.4k en mode beacon. On y trouvera la chaîne de Markov correspondante, sa résolution et les résultats obtenus en termes de fiabilité, d'énergie consommée, de débit de données et du délai moyen, suivis d'une interprétation et d'une comparaison entre les résultats des deux mécanismes.

Le cinquième chapitre se focalisera sur la deuxième contribution concernant la modélisation et l'évaluation des performances des protocoles MAC CSMA/CA avec backoff PCA et CSMA/CA de la norme IEEE 802.15.4k dans le mode non beacon. La chaîne de Markov correspondante au modèle, sa résolution et les résultats obtenus en termes de fiabilité, d'énergie consommée et de débit de données, suivis d'une interprétation et d'une comparaison entre les résultats des deux mécanismes, seront l'objet de ce chapitre.

Dans le sixième chapitre, la même démarche que les deux premières contributions a été entreprise pour présenter la dernière contribution concernant la modélisation et l'évaluation des performances des mécanismes ALOHA PCA et ALOHA de la norme IEEE 802.15.4k dans un mode beacon. Le modèle de chaîne de Markov proposé, sa résolution, ainsi que les résultats obtenus en termes de fiabilité, d'énergie consommée, de débit de données et du délai moyen seront introduits. Une interprétation des résultats et une comparaison entre ses deux mécanismes sera détaillée.

Enfin, notre thèse s'achèvera par une conclusion générale résumant les grands points qui ont été abordés ainsi que les perspectives de recherche dégagées.

Première partie

État de l’art

Chapitre 1

Les réseaux de capteurs sans fil et le standard IEEE 802.15.4

Sommaire

1.1 Introduction

Les progrès récents dans la technologie des systèmes micro-électromécaniques, les communications sans fil, et l'électronique numérique ont permis le développement de petits dispositifs appelés capteurs, peu coûteux, de faible puissance, offrant l'opportunité de communiquer entre eux. Ces derniers communiquent entre eux via une communication sans fil pour le partage d'information et le traitement coopératif. Ils sont déployés aléatoirement dans une zone d'intérêt pour superviser ou surveiller des phénomènes divers (température, humidité, vibration, luminosité, ...). Ces dispositifs coopèrent entre eux pour former une infrastructure de communication appelée réseau de capteurs sans fil (RCSFs).

La norme IEEE 802.15.4 est la technologie sans fil à courte portée la mieux adaptée pour répondre aux exigences de débit et de latence assouplies, destinée pour les réseaux personnels sans fil à bas débit (LR-WPAN).

Dans ce chapitre, nous présenterons dans un premier temps les réseaux sans fil ainsi que leurs catégories. Par la suite, dans la section 1.3, nous enchainerons avec les réseaux de capteurs sans fil, leurs architectures, leurs contraintes ainsi que leurs domaines d'application. Dans un deuxième temps, nous présenterons le standard IEEE 802.15.4 et toutes ses caractéristiques.

Ce chapitre sera aussi consacré à introduire la notion d'évaluation de performances dans les réseaux par modélisation analytique ou par simulation. Par la suite, quelques techniques de modélisation analytique seront introduites ainsi que les métriques de performances dont nous aurons besoin dans la suite de ce manuscrit. Dans la section 1.6, une synthèse sur les études réalisées dans le but d'évaluer les performances de la norme IEEE 802.15.4 a été proposée avant de terminer par une conclusion.

1.2 Réseaux sans fil

Un réseau sans fil permet de communiquer à distance et d'accéder à des applications ou à des informations sans nécessité de connexion filaire. L'utilisateur jouit ainsi d'une réelle mobilité et d'une meilleure accessibilité aux services et aux applications réseau [6]. La communication sans fil n'est pas une idée nouvelle. Elle était déjà pratiquée jadis par les peuples indigènes qui utilisaient des signaux de fumée, ainsi que par les navires qui communiquaient au moyen du code Morse et de signaux lumineux. Mais jamais l'engouement pour cette forme de communication n'a atteint cette proportion que ces dernières années, et ce grâce a l'avancée technologique de la télécommunication [7]. Les réseaux sans fil peuvent avoir une classification selon deux critères, à savoir la zone de couverture du réseau ainsi que son infrastructure [8]. Les réseaux sans fil se déclinent en plusieurs catégories selon le premier critère (voir la figure 1.1).

1.2.1 Les réseaux personnels sans fil WPAN

Les réseaux WPAN (Wireless Personal Area Network) concernent les réseaux sans fil à très faible portée de l'ordre de quelques dizaines de mètres. Ce type de réseau permet de relier des périphériques (imprimante, téléphone portable, appareils domestiques, ...) ou un assistant personnel PDA (Personnal Digital Assistant) à un ordinateur sans liaison filaire. De plus, ils permettent la liaison sans fil entre deux machines très peu distantes. Parmi les technologies permettant la mise en œuvre des réseau WPAN, nous distinguons : Bluetooth, HomeRF, Zigbee ainsi que l'infrarouge. Le standard employé est IEEE 802.15.

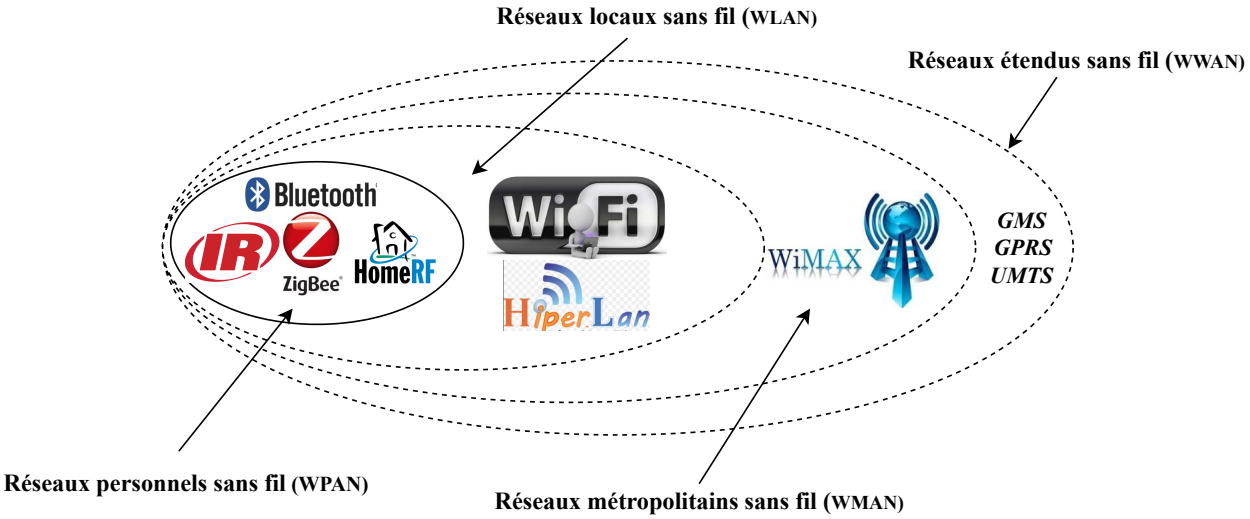


FIGURE 1.1 – Classification des réseaux sans fil selon la zone de couverture.

1.2.2 Les réseaux locaux sans fil WLAN

Les réseaux WLAN (Wireless Local Area Network) sont des réseaux capables d'établir une connexion entre plusieurs appareils informatiques distants d'environ une centaine de mètres. À cause de sa couverture géographique limitée, le WLAN est principalement utilisé pour des réseaux internes et notamment pour établir des connexions rapides entre des ordinateurs comme au sein d'une entreprise, une université ou chez les particuliers, tout en offrant un haut débit.

Ce type de réseau permet un accès au réseau simple et en temps réel, un accès plus rapide et étendu aux bases de données de l'entreprise ainsi qu'à la mise en place des transmissions dans les endroits où la pose de câble est difficile, voire impossible [9]. Comme illustré dans la figure 1.1, ses réseaux sont principalement basés sur les technologies WiFi et HiperLAN 1 et 2. Le standard employé dans les réseaux WLAN est le IEEE 802.11.

1.2.3 Les réseaux métropolitains sans fil WMAN

Les réseaux WMAN (Wireless Metropolitan Area Network) ont pour objectif de créer un ensemble de liens de communication sur une zone étendue sur quelques dizaines de kilomètres (une ville ou une région). Ces liens peuvent servir à interconnecter plusieurs sites d'une même entreprise ou d'une administration. Un WMAN est basé sur la technologie IEEE 802.16 connu sous le nom commercial de WIMAX (Worldwide Interoperability for Microwave Access) offrant un taux de transmission radio théorique pouvant atteindre les 74 Mbit/s.

1.2.4 Les réseaux étendus sans fil WWAN

Les réseaux WWAN (Wireless Wide Area Network) connus sous le nom des réseaux cellulaires mobiles sont les réseaux sans fil les plus répandus, puisque tous les appareils mobiles sont connectés à un réseau étendu sans fil. Les seules technologies des réseaux WWAN disponibles sont les technologies utilisant les satellites géostationnaires ou en orbite basse pour relayer l'information entre plusieurs points du globe [8]. Le peu de technologies existantes à l'heure est : GSM (Global System for Mobile Communications ou en français Groupe Spécial Mobile), GPRS (General Packet Radio Services) et EDGE (Enhanced Data Rates for GSM), UMTS (Universal Mobile Telecommunications System) et LTE (Long Term Evolution). Les WWAN emploient le standard IEEE 802.20.

Lors du déploiement d'un réseau sans fil, il est essentiel de recenser les besoins et de bien choisir le type de technologie qui y répond le mieux [7].

Par rapport au deuxième critère, on peut diviser les réseaux sans fil en : réseaux avec infrastructure (cellulaires) et réseaux sans infrastructure (Ad-hoc) comme illustré dans la figure 1.2. Dans les réseaux avec infrastructure, les communications s'effectuent via une station de base fixe. En revanche, les communications dans un réseau Ad-hoc s'effectuent en absence de toute infrastructure de communication fixe préexistante et tous les appareils communiquent directement entre eux.

Réseau avec infrastructure **Réseau sans infrastructure (Ad-hoc)**

FIGURE 1.2 – Classification des réseaux sans fil selon leur infrastructure.

1.3 Réseaux de capteurs sans fil (RCSFs)

Un réseau de capteurs sans fil RCSF (ou WSN, Wireless Sensor Network) constitue une catégorie particulière des réseaux sans infrastructure. Il est composé de quelques dizaines à plusieurs

milliers d'entités très petites, à faible coût, limitées en ressources énergétiques nommées nœuds capteurs. Ses nœuds sont inter-connectés entre eux, la transmission des données collectées se fait d'un nœud capteur à un autre jusqu'à atteindre une station de collecte appelée Sink (ou station de base). Ensuite, ces données seront transmises par la station à l'aide de l'Internet ou de satellites à l'ordinateur central pour analyser ces données et prendre des décisions, formant ainsi un RCSF.

Dans ces réseaux, chaque nœud est capable de surveiller son environnement et de réagir en cas de besoin en envoyant l'information collectée à un ou plusieurs points de collecte, à l'aide d'une connexion sans fil.

1.3.1 Nœud capteur et son architecture

Un capteur est un petit appareil autonome capable d'effectuer des mesures simples sur son environnement immédiat, comme la température, la vibration, la pression, etc. Il est ainsi dédié à effectuer des tâches bien précises, telles que la détection de la présence ou de la commande d'une électrovanne. Il sert aussi à détecter, sous forme de signal souvent électrique, un phénomène physique afin de le représenter. En d'autre terme, il permet de transformer l'état d'une grandeur physique observée en une grandeur utilisable. Par exemple, transformer l'énergie solaire en énergie électrique ou thermique.

Les capteurs sont dotés d'une batterie limitée et sont capables de communiquer entre eux et de détecter des événements s'ils se trouvent à l'intérieur de leur portée radio. Dans un RCSF, les données devront passer par des étapes de collecte et de traitement et puis les communiquer vers un ou plusieurs points de collecte appelés station de base (SB). Ces étapes seront effectuées par des unités spécifiques du nœud capteur associé à savoir les unités de capture, de calcul, de communication et de gestion de l'énergie, comme illustré dans la figure 1.3. Ces unités effectuent des tâches cruciales en rendant les nœuds capables de communiquer entre eux pour transmettre les données obtenues par leurs capteurs [10]. Le rôle de chaque unité est présenté ci-dessous :

- **Unité de capture (sensing unit) :** est nécessaire pour surveiller le milieu environnant et ses conditions, et de capter quelques phénomènes d'un signal analogique, tels que l'humidité, la pression et les vibrations puis les convertit en signal numérique. Ses signaux numériques seront introduits par la suite dans l'unité de traitement.
- **Unité de calcul (processing unit) :** appelée aussi unité de traitement, composée d'un micro contrôleur assurant le traitement des données et son stockage et d'une mémoire flash. Ce micro contrôleur contrôle les procédures permettant au nœud de collaborer avec les autres

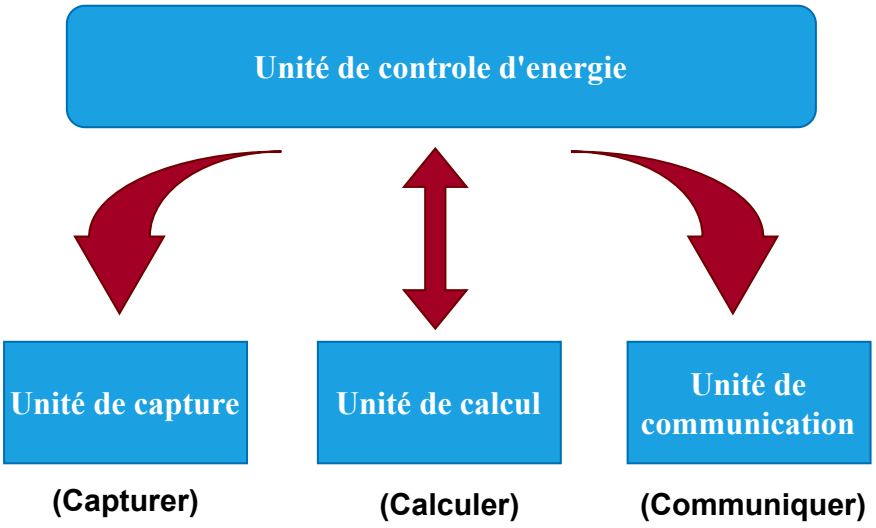


FIGURE 1.3 – Architecture d'un nœud capteur.

nœuds pour effectuer les tâches d'acquisition attribuées.

- **Unité de communications (transceiver unit) :** appelée aussi unité émettrice/réceptrice, elle permet de connecter le nœud au réseau. Cette unité est chargée d'effectuer toutes les opérations d'émission/réception des données vers/depuis les autres nœuds du réseaux.
- **Unité de contrôle d'énergie (power unit) :** représente l'élément primordial de l'architecture du capteur, elle fournit de l'énergie aux diverses unités de nœuds de capteurs citées précédemment. De plus, l'unité de contrôle d'énergie mesure la durée de vie du capteur.

1.3.2 Architecture d'un RCSF

Un RCSF est composé de plusieurs capteurs et d'une passerelle pour fournir une connexion à Internet [10], comme le montre la figure 1.4. L'explication de chaque élément est donnée comme suit [11] :

– **Les nœuds capteurs.** Leurs principaux objectifs sont d'effectuer des mesures locales discrètes sur le phénomène les entourant en communiquant sur des supports sans fil. Ils permettent aussi de collecter des données et de les acheminer vers l'utilisateur via un puits.

– **Le puits.** Le puits appelé aussi passerelle ou station de base, communique avec l'utilisateur via Internet ou par satellite. Il est situé près du champ des nœuds capteurs du réseau. Le puits peut être un capteur ou un autre équipement qui gère le réseau de capteur, tel qu'un PDA, un téléphone portable, etc.

– **Le phénomène.** Le phénomène est une entité d'intérêt pour l'utilisateur qui est détectée et

analysée par les nœuds capteurs.

– **L'utilisateur.** L'utilisateur est celui qui souhaite obtenir des informations sur un phénomène spécifique afin de mesurer/surveiller son comportement.

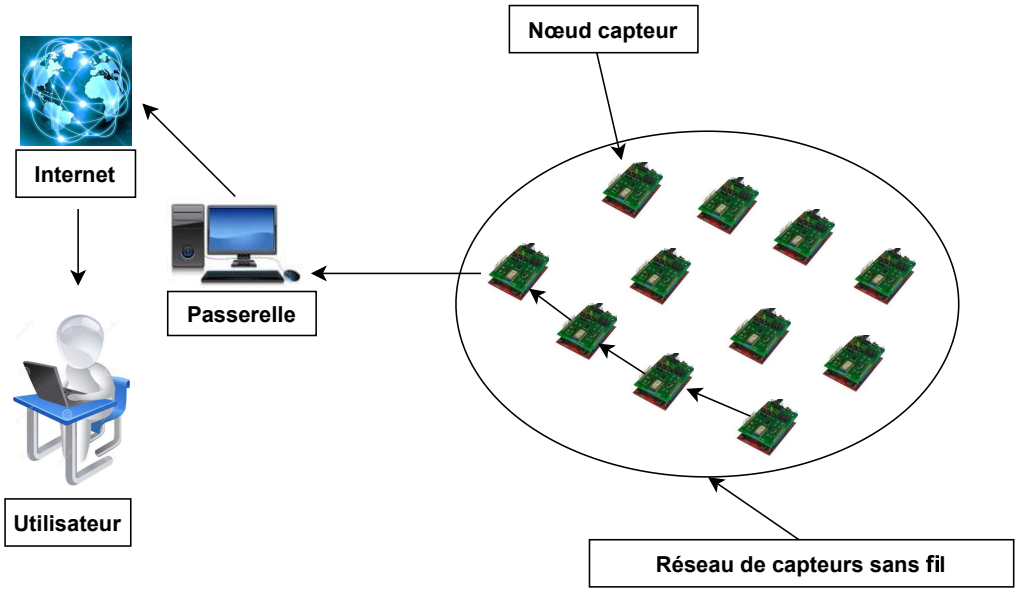


FIGURE 1.4 – Architecture d'un réseau de capteur sans fil.

1.3.3 Les contraintes et les exigences des RCSFs

Les principales caractéristiques et contraintes fondamentale des RCSFs qui ont été abordés par de nombreux chercheurs sont présentés ci-dessous, en se référant aux travaux de [10, 12].

1.3.3.1 Les contraintes des RCSFs

- **Gestion d'énergie.** Les nœuds de capteurs comme mentionné précédemment fonctionnent sur batterie. Vu que la recharge ou le remplacement de ces batteries est une tâche presque impossible, nous pouvons déduire que la durée de vie de chaque nœud dépend éventuellement de la durée de vie de leurs batteries.
- **Contraintes matérielles, et coût de production.** Les RCSFs sont composés d'un très grand nombre de nœuds, et chaque nœud capteur se compose principalement de quatre composants, comme cité dans la sous section 1.3.1. Cependant, le nœud peut également posséder des unités externes et des plug-ins supplémentaires. De nos jours, le prix de chaque nœud est critique et le coût de production du réseau est devenu une véritable contrainte.

- **Contraintes d'environnement.** Les capteurs sont souvent déployés en masse dans des endroits sans avoir recours à des interventions humaines. Par conséquent, ils doivent pouvoir fonctionner sans surveillance dans des régions géographiques éloignées.
- **Topologie du réseau de capteurs.** La latence du réseau ainsi que sa capacité et sa robustesse sont affectées par la topologie du réseau. De plus, la complexité du routage des données dépend de la topologie du réseau.
- **Sécurité.** Les aspects de sécurité des réseaux de capteurs sans fil se concentrent sur les approches de communication centralisées. L'absence de sécurité physique est due à la communication sans fil et à l'absence d'infrastructure centralisée où la probabilité de perte de communications est élevée, et ainsi la gestion d'accès aux ressources du réseau devient très difficile. Un développement d'une approche de sécurité distribuée est donc nécessaire pour ce type de réseau.
- **Qualité de service.** Pour certains types d'applications, la livraison de données dans un délai limité est considérée comme cruciale. Par conséquent, la détection des données après une certaine latence limitée serait parfois inutile.
- **Couverture.** Elle est définie comme la capacité des nœuds de capteurs à couvrir une zone physique qui est limitée en portée et également limitée en précision.
- **Connectivité :** La connectivité réseau est définie par une connexion permanente entre deux nœuds de capteur différents. Ces nœuds sont déployés de manière dense dans un réseau de capteurs.

1.3.3.2 Les caractéristiques et les exigences des RCSFs

– **La tolérance aux pannes.** La tolérance aux pannes (en d'autres termes, la tolérance aux fautes ou bien la fiabilité) d'un nœud capteur est la capacité du capteur à maintenir ses fonctionnalités de réseau sans interruption. Ces interruptions peuvent se produire en raison d'une pénurie d'énergie, de dommages physiques et d'interférences environnementales, ce qui conduira à la défaillance du nœud capteur.

– **Scalabilité ou passage à l'échelle.** D'innombrables nœuds capteurs peuvent être déployés par l'utilisateur pour étudier en collaboration un phénomène qui les intéresse. La scalabilité est la capacité d'un réseau à croître en taille tout en continuant à fournir une qualité de service qui répond aux exigences des applications avec une complexité acceptable. Aussi, lors de la

défaillance d'un nœud capteur, l'utilisateur doit re-déployer un nouveau nœud et l'intégrer au réseau sans perturber son fonctionnement.

- **Agrégation de données.** Connu aussi sous le nom de fusion des données, l'agrégation des données est une fonction utile qui permet de réduire la taille des données ou la taille des informations redondantes transmises à la station de base en les compressant en informations significatives. Cette fusion est accomplie par l'unité de calcul afin de réduire la consommation d'énergie, ce qui améliore la durée de vie du réseau.
- **Auto-configuration.** Un nœud capteur doit avoir des capacités pour s'auto configurer dans le réseau. Étant donné que la défaillance d'un nœud peut se produire dans n'importe quel réseau, de nouveaux nœuds capteurs peuvent rejoindre le réseau afin de réduire les effets négatifs de ces défaillances.
- **Dynamique du réseau.** La mobilité des nœuds de capteur ou de la station de base est essentielle dans un réseau. Du fait que les nœuds de capteurs sont dynamiques, en d'autres termes ils se promènent, de nombreux problèmes ont été soulevés au niveau de la stabilité du routage à l'énergie, de la bande passante, etc.
- **Supports de transmission.** Afin d'établir des liens entre les nœuds, un support sans fil doit être utilisé pour assurer toutes les communications dans le réseau.

1.3.4 Avantages et inconvénients des RCSFs

Comme tout type de réseau, les RCSFs ont des avantages mais bien évidement des inconvénients.

Avantages : comme les RCSFs utilisent la communication sans fil au lieu du câblage dur, ils n'ont pas besoin d'une infrastructure complexe. En raison de la structure sans fil, les RCSFs deviennent moins chers et offre une facilité de déploiement. Ils dépensent moins d'énergie car les appareils sont généralement en sommeil pour économiser l'énergie. De plus, les RCSFs sont compatibles avec les périphériques externes et les nouveaux plug-ins. Cette fonctionnalité augmente leurs zones d'utilisation ainsi que leurs fonctionnalités.

Inconvénients : les RCSFs ont une vitesse de communication relativement faible et une bande passante étroite. De plus, ses réseaux dépendent de la batterie. Dans beaucoup de cas, le déploiement des capteurs se réalise dans un environnement n'offrant pas la possibilité de changer les batteries en cas d'épuisement. Ces caractéristiques constituent l'inconvénient majeur

des RCSFs. Par conséquent, ils sont conçus pour consommer le moins possible d'énergie de fonctionnement. Cependant, une consommation d'énergie moindre peut éviter de prendre des précautions de sécurité essentielles. Étant donné que certaines fuites de sécurité peuvent survenir en raison des politiques d'économie d'énergie, les RCSFs peuvent être attaqués par des attaquants malveillants. De plus, les RCSFs sont affectés par les environnements, tels que les murs et la distance lointaine, etc. Les capteurs possèdent une faible puissance de calcul et une mémoire limitée. La majorité de ceux-ci sont alimentés par des batteries avec une durée de vie restreinte.

1.3.5 Domaines d'application des RCSFs

En raison de leur capacité d'auto-organisation, de leur grande flexibilité, de leur reconfigurabilité, de leur facilité d'installation, de leur maintenance ainsi que le support de communication sans fil utilisé, les RCSFs sont appliqués dans divers domaines d'applications afin de surveiller ou bien de mesurer des paramètres spécifiques [4].

Dans le domaine militaire, les RCSFs sont par exemple utilisés pour détecter les intrusions ou les attaques et pour surveiller les champs de bataille.

Dans l'agriculture, l'objectif principal est d'améliorer la productivité. Pour cela, la collecte, la surveillance et le traitement des informations climatiques, telles que l'humidité du sol, la qualité de l'air, la température, l'humidité, le niveau des précipitations, la vitesse et la direction du vent, le niveau de l'eau et la pression atmosphérique se font par les différents capteurs connectés à un microcontrôleur. De plus, les RCSFs permettent le développement de la culture implantée puis les évaluent et les analysent afin d'anticiper les changements climatiques déjà cités avant leur apparition.

Dans l'industrie, certains problèmes de communications sans fil, tels que le bruit, l'ombrage (shadowing), les effets des évanouissements par trajets multiples (multipath fading) et les interférences peuvent se produire. C'est pourquoi, le capteur surveille et mesure régulièrement certains paramètres critiques. Les mesures obtenues seront transmises à un nœud collecteur qui va permettre de réparer ou de remplacer l'équipement avant que des ossements majeurs ne se produisent. En outre, l'utilisation de la technologie sans fil est devenue un choix privilégié pour l'automatisation industrielle et le contrôle des processus, car elle réduit les tracas d'installation de câbles, les coûts de maintenance et la non-complexité du déploiement.

Dans le domaine médical, les nœuds capteurs sont chargés de surveiller les activités et les actions physiologiques humaines. Ils permettent la collecte de différents paramètres physiologiques

comme la fréquence cardiaque, le taux de glucose, le niveau d'oxygène dans le sang, ... afin de surveiller des patients souffrant de maladies chroniques, des personnes handicapées et des athlètes pendant leur entraînement de gymnastique.

Dans la domotique, ce type de réseaux est également utilisé pour améliorer la qualité de vie, comme la surveillance de l'habitat, le contrôle du climat intérieur et les alarmes intelligentes.

Les applications environnementales exploitent les capteurs pour détecter les catastrophes naturelles (incendies de forêts, tremblements de terre, tsunamis et éruptions volcaniques) et détecter des fuites des produits toxiques (gaz, produits chimiques, pétrole, éléments radioactifs, etc.) dans des sites industriels, tels que les centrales nucléaires et les pétrolières.

Les RCSFs sont également déployés dans des applications de sécurité, de construction et du bâtiment, de transport, de maison intelligente, etc.

1.3.6 Standarisation

L'organisation internationale de normalisation, connue sous le nom de l'ISO (International Organization for Standardization), est un organisme international composé de représentants de divers organismes nationaux qui établissent et publient des normes internationales. Fondée le 23 février 1947, bien avant la naissance des RCSFs, l'ISO promeut des normes mondiales propriétaires, industrielles et commerciales.

Le comité IEEE 802 (IEEE 802 Local and Metropolitan Area Networks Standard Committee) noté par LMSC de l'IEEE (Institute of Electrical and Electronics Engineers), est un groupement de personnes collaborant ensemble sur l'évolution des standards des réseaux locaux, métropolitains, ainsi que d'autres types de réseaux. Les services et les spécifications décrits par ce comité se réfèrent aux deux couches basses du modèle OSI (Open Systems Interconnection) qui en contient sept, à savoir la couche physique (PHY) et la couche liaison de données. L'IEEE 802 découpe la couche liaison en deux sous-couches appelées Logical Link Control (LLC) et Media Access Control (MAC). La figure 1.5 illustre les six groupes du comité travaillant sur différents thèmes pour différents types de réseaux [11].

Des normes pour les réseaux de capteurs sans fil ont été développées tout en exigeant une faible consommation d'énergie. Ces normes définissent les fonctions et les protocoles nécessaires pour que les nœuds de capteurs puissent interfacer avec une variété de réseaux. L'IEEE 802.15 est un groupe de travail axé sur les réseaux personnels sans fil (WPAN) ; il a sept normes différentes approuvées. Comme cité auparavant, toutes les normes 802.15 proposent seulement des couches PHY et des

sous-couches MAC. En revanche, elles ne s'intéressent pas aux couches supérieurs du modèle OSI.

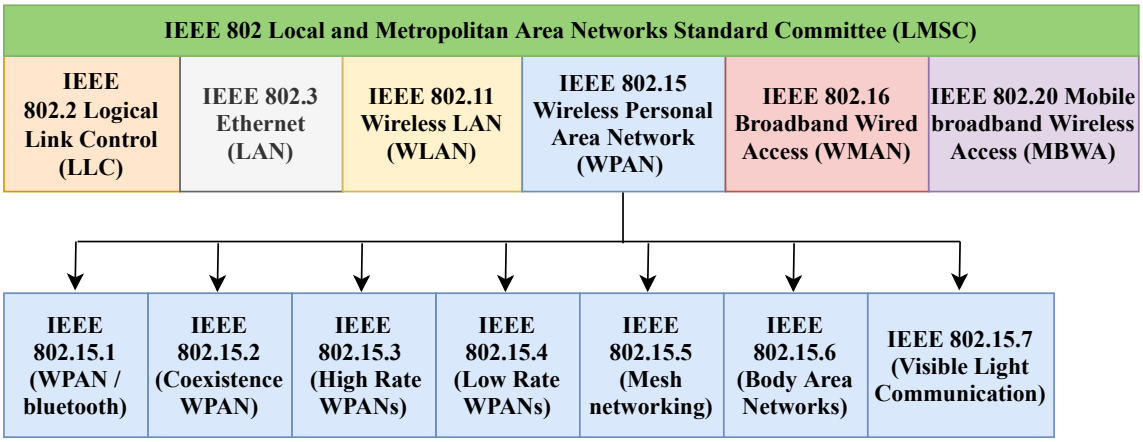


FIGURE 1.5 – Les standards IEEE 802 mettant l'accent sur les normes IEEE 802.15.

Une brève présentation de ses normes est donnée comme suit :

- **La norme IEEE 802.15.1 :** publiée en juin 2002, est une norme des couches de transport inférieures de la pile Bluetooth qui contient des spécifications des couches MAC et PHY.
- **La norme IEEE 802.15.2 :** apparue en 2003, recommandée pour la coexistence de dispositifs WPAN avec d'autres équipements radio dans des bandes de fréquences sans licence.
- **La norme IEEE 802.15.3 :** finalisée en juin 2003, destinée aux WPAN à haut débit (High Rate WPANs) avec des domaines d'application, tels que le multimédia et l'imagerie numérique. Ce groupe de travail avait deux sous-groupes de travail : 802.15.3a et 802.15.3b. Le premier était censé présenter une nouvelle technique radio basée sur la bande ultra-large (UWB), et le second a proposé en 2005 un amendement à la sous-couche MAC.
- **La norme IEEE 802.15.4 :** publiée en Mai 2003, destinée aux réseaux à faible débit de données (Low Rate WPANs) contrairement aux taux de transfert élevés de la norme 802.15.3.
- **La norme IEEE 802.15.5 :** est affrétée pour déterminer les mécanismes nécessaires qui doivent être présents dans les couches PHY et MAC des WPAN pour permettre la mise en réseau maillée.
- **La norme IEEE 802.15.6 :** apparue en 2012, représente la dernière norme internationale conçue pour le réseau corporel sans fil (WBAN). Elle offre des communications sans fil à faible puissance, à courte portée et extrêmement fiables.
- **La norme IEEE 802.15.7 :** publiée en janvier 2009, conçue pour les communications de la lumière visible (VLC).

1.4 Le standard IEEE 802.15.4

1.4.1 Présentation du standard

La norme IEEE 802.15.4 est une technologie sans fil à courte portée, destinée à fournir aux applications des exigences de débit et de latence assouplies dans les réseaux sans fil. Introduite le 1er octobre 2003 [2], IEEE 802.15.4 est destinée pour les réseaux personnels sans fil à bas débit, aussi appelés Low Rate Wireless Personal Area Networks en anglais (LR-WPAN). Les principales caractéristiques de cette norme sont la complexité, les coûts réduits des entités du réseau, une économie d'énergie très avancée et une transmission à faible débit de données qui convient très bien aux besoins des réseaux de capteurs sans fil.

1.4.1.1 Composants d'un réseau IEEE 802.15.4 WPAN

Un réseau IEEE 802.15.4 représente une partie de la famille des standards WPAN qui doit comprendre au moins un coordinateur PAN, en plus d'autres dispositifs. Le coordinateur PAN est le contrôleur principal du réseau personnel PAN, il est le seul nœud autorisé à tisser des liens avec plus d'un périphérique et qui peut être alimenté par le secteur. En revanche, les autres dispositifs seront probablement alimentés par des batteries.

1.4.1.2 Type des dispositifs

La norme IEEE 802.15.4 définit deux types de dispositifs (entités) :

- Dispositifs à fonctions complètes FFD (Full Function Device) : contenant tous les services MAC, et pouvant fonctionner soit comme un coordinateur PAN du réseau ou comme un simple périphérique (dispositif) du réseau. Ces dispositifs peuvent communiquer avec des FFD et des RFD.
- Dispositifs à fonctions réduites RFD (Reduced Function Device) : contenant juste une partie des services MAC, pouvant fonctionner juste comme un simple périphérique du réseau. Ces dispositifs ne peuvent communiquer qu'avec des dispositifs de type FFD.

1.4.1.3 Topologies du réseau

Deux topologies de base sont autorisées dans la norme IEEE 802.15.4, comme illustré dans la figure 1.6.

– La topologie en étoile, formée autour du coordinateur PAN, où les communications se font entre les différents périphériques du réseau via le coordinateur PAN.

– La topologie point à point, où chaque appareil est capable de former de multiples liens directs vers d'autres périphériques de sorte que les chemins redondants soient disponibles.

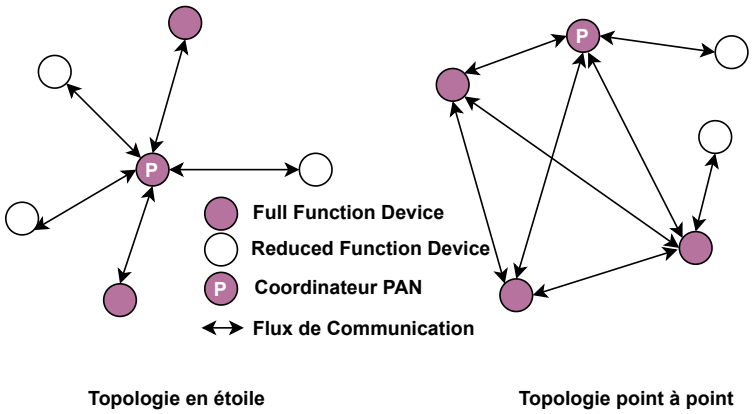


FIGURE 1.6 – Les topologies du réseau LR-WPAN

1.4.1.4 Architecture en couche du réseau IEEE 802.15.4

L'architecture de la norme IEEE 802.15.4 est définie en terme d'un certain nombre de couches du modèle à sept couches de l'OSI.

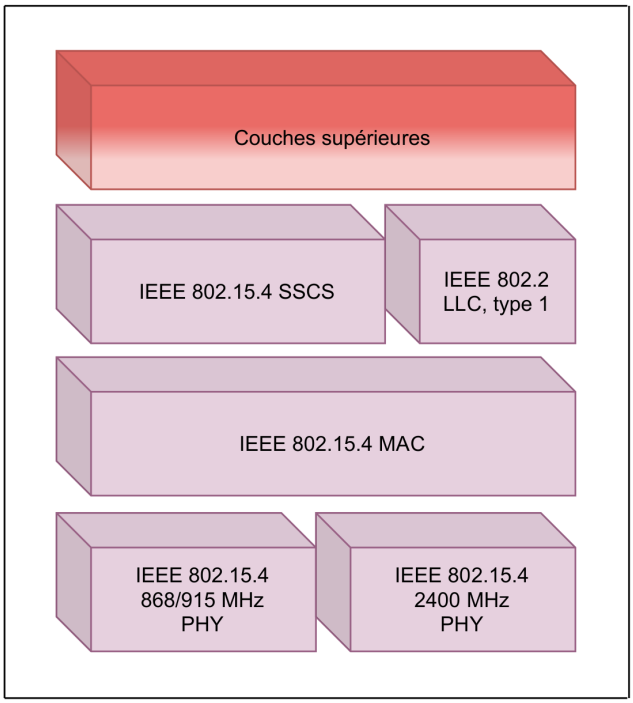


FIGURE 1.7 – Architecture en couche de IEEE 802.15.4.

Le standard fournit les spécificités et les protocoles des couches basses (couche physique et sous-couche MAC) du modèle OSI pour les réseaux WPAN. Un dispositif LR-WPAN comprend seulement la couche PHY et la sous-couche MAC tandis que la définition des couches supérieures n'entre pas dans le domaine d'application de cette norme. Pour cela, la technologie sans fil ZigBee [13] a proposé une pile protocolaire basée sur le modèle de référence OSI, proposant en plus des couches PHY et MAC deux autres couches hautes à savoir la couche réseau et la couche application. La couche réseau fournit la configuration, la manipulation et le routage des messages du réseau, tandis que la couche application fournit les fonctionnalités étendues des composants. En plus, on trouve plusieurs protocoles de haut niveau qui utilisent IEEE 802.15.4, autre que ZigBee comme : WirelessHART [14] et ISA 100.11a [15].

1.4.2 Couche physique de IEEE 802.15.4-2003

La couche physique a pour rôle de gérer le support physique sur lequel seront faites les transmissions. La couche physique dans IEEE 802.15.4 offre les fonctionnalités suivantes [16] :

- **Gestion de l'activation et désactivation du module radio.** Les trois états possibles de la radio sont : réception, émission et éteint. Elle permet à l'émetteur de changer périodiquement d'un état à un autre suite à une demande de la couche MAC. Cette fonction est essentielle pour économiser l'énergie en mettant le module en mode éteint en cas d'absence de réception ou d'émission.
- **La détection de la puissance du signal sur le canal ED.** Le ED (Energy Detection) mesure l'énergie dans le canal. Si cette énergie est importante, cela signifie que le canal est fortement utilisé.
- **Indication de la qualité du lien LQI.** Le LQI (Link Quality Indication) est assuré par un indicateur spécial, permet de caractériser la qualité d'un lien à un instant donné suite à une réception d'une trame. Le résultat de cette mesure sera envoyé à la sous couche MAC qui va l'utiliser et le stocker.
- **La détection de l'occupation ou non du canal CCA :** Le CCA (Clear Channel Assessment) est essentiel pour le fonctionnement des protocoles d'accès au médium de la sous-couche MAC.
- **La sélection d'un canal de transmission.** Puisque la couche physique offre plusieurs canaux de transmission, il est nécessaire de sélectionner un canal précis. Cette sélection est faite à la demande des couches supérieures.

La norme IEEE 802.15.4-2003 spécifie deux PHYs basées sur la technique DSSS (Direct Sequence Spread Spectrum) et opèrent dans les bandes 868/915 MHz et 2450 MHz. Le tableau 1.1 montre les bandes de fréquences disponibles, leurs régions de fonctionnement spécifiques, les techniques de modulation utilisées, les débits de données pris en charge ainsi que le nombre de canaux disponibles.

TABLE 1.1 – Spécifications de la couche PHY de IEEE 802.15.4-2003

PHY (MHz)	Bande de fréquence (MHz)	Modulation	Débit (kbit/s)	Région	Nombre de canaux
868/915	868-868.6	BPSK	20	Europe	1 (0)
	902-928	BPSK	40	Amérique du Nord	10 (1-10)
2450	2400-2483.5	O-QPSK	250	Monde entier	16 (11-26)

La technique de modulation BPSK (Binary Phase Shift Keying) utilise deux phases pour transmettre tandis que la technique O-QPSK (Offset Quadrature Phase-Shift Keying) utilise quatre phases différentes. Un total de 27 (0-26) canaux semi-duplex sont disponibles sur les trois bandes de fréquences citées précédemment.

1.4.3 Sous-couche MAC de IEEE 802.15.4-2003

La sous-couche MAC (Medium Acces Control), comme son nom l'indique, aura pour rôle de gérer l'accès au médium. Cela se fera en utilisant le mécanisme d'accès au canal CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). Elle offre aussi d'autres fonctionnalités de contrôle liées à :

- **La synchronisation avec le coordinateur :** le coordinateur PAN envoie périodiquement des trames balises (beacons) pour synchroniser les membres de son réseau.
- **La création du réseau :** la couche supérieure envoie une requête à la couche MAC pour effectuer un scan actif sur une liste de canaux affin de découvrir les réseaux existants à portée. Une fois le bon canal est sélectionné, la couche supérieure crée un identifiant de PAN et demande à la couche MAC d'initier un PAN avec cet identifiant.
- **L'association et dissociation du PAN :** après avoir effectué un scan (passif ou actif) et puis remonter le résultat à la couche supérieure, cette dernière demande à la couche MAC de s'associer à un PAN spécifique en précisant l'identifiant du PAN et l'adresse du coordinateur correspondant. Suite à cette demande, la couche MAC génère une requête d'association à destination du coordinateur. En revanche, une requête de dissociation est envoyée par la couche

supérieure, par conséquent la couche MAC envoie une indication de dissociation au coordinateur PAN pour l'informer que la station souhaite se dissocier de lui.

- **Les scans :** la couche MAC effectue un des quatre types de scans suivants ; scan d'énergie, scan actif, scan passif et scan orphelin.
- **La génération des trames balises (beacons) :** le dispositif FFD fonctionnant en tant que coordinateur PAN assure cette fonctionnalité.
- **La gestion de l'échange de données :** les trois modes d'échange disponibles sont ; l'échange direct, l'échange indirect et l'échange en GTS.
- **La gestion des acquittements :** ce champ spécifie si la trame de données après sa réception doit être acquittée ou pas.
- **L'allocation et la gestion des slots dédiés et partagés :** par exemple, les allocations GTS sont des slots dédiés pour permettre au nœud un accès garanti au canal.

1.4.3.1 Les trames dans IEEE 802.15.4

Dans le standard IEEE 802.15.4, quatre types de trames sont proposées pour les échanges entre les nœuds [17] :

– Les trames Beacon (Beacon frame) sont envoyées uniquement par les nœuds coordinateurs, afin d'assurer une synchronisation entre les nœuds du réseau, de décrire la structure des supertrames et pour identifier le coordinateur du PAN.

– Les trames de données (Data frame) servent à transférer des données utiles entre les nœuds du réseau.

– Les trames d'acquittement (Acknowledgment frame) servent à confirmer la bonne réception des trames de données.

– Les trames de contrôle (Command frame) servent à effectuer des demandes spécifiques, comme par exemple l'association au réseau.

1.4.3.2 Mode de fonctionnement et mécanismes d'accès au canal

Le standard IEEE 802.15.4 offre deux modes de fonctionnement [2], le mode dit avec beacon (ou avec balise) et le mode sans beacon (ou sans balise), comme le montre la figure 1.8.

1. **Le mode avec beacon (beacon-enabled mode) :** dans ce mode le coordinateur envoie périodiquement des trames Beacon pour synchroniser les nœuds du réseau. Tout membre du

réseau qui entend ce Beacon peut ainsi se synchroniser et se servir de ce coordinateur comme relais. Le choix de ce mode impose aux nœuds de suivre une structure périodique appelée supertrame. Tout nœud souhaitant communiquer doit rentrer en compétition avec les autres nœuds pour gagner l'accès au médium en utilisant le mécanisme CSMA/CA slotté (slotted CSMA/CA).

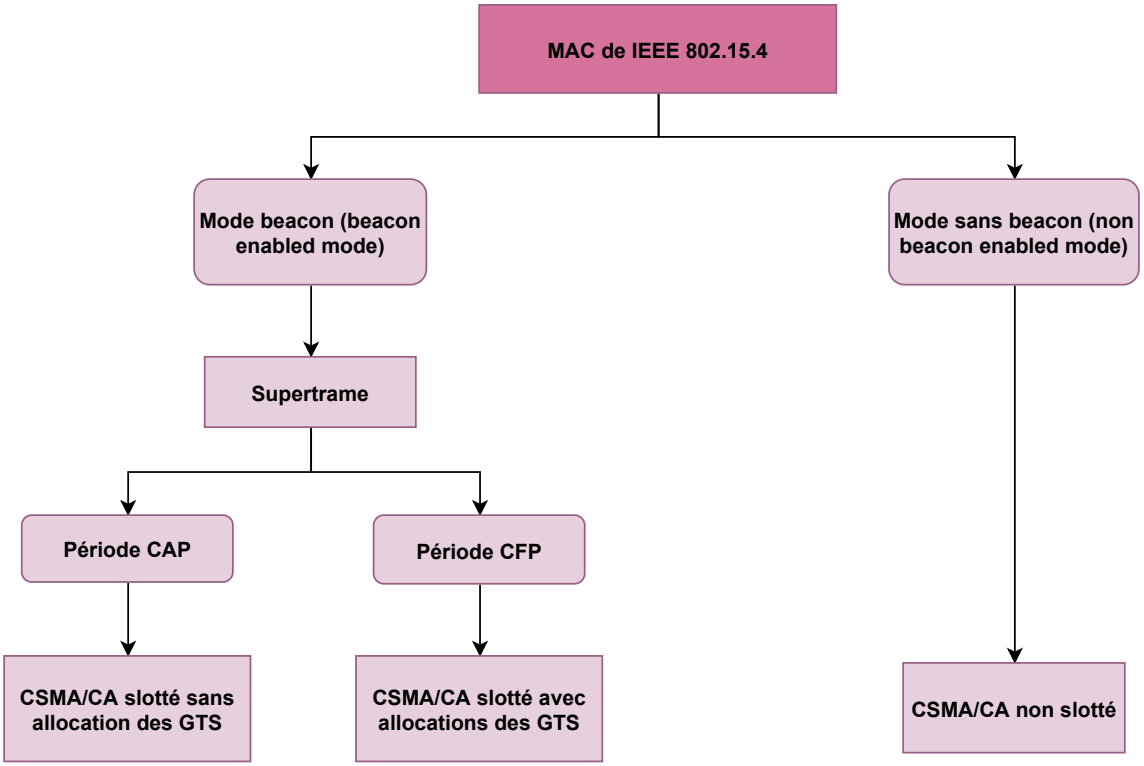


FIGURE 1.8 – Les modes d'accès au médium dans la couche MAC de IEEE 802.15.4.

2. **Dans le mode non beacon (non beacon-enabled mode)**, il y a une absence de synchronisation entre les nœuds du réseau. Ce qui signifie que pour que ces derniers puissent communiquer entre eux, ils doivent laisser leur radio allumée ou se réveiller périodiquement afin d'interroger le coordinateur pour savoir s'il y a des messages en attente. La structure de la supertrame est absente dans ce mode et le mécanisme d'accès au canal utilisé est le CSMA/CA non slotté (unslotted CSMA/CA).

1.4.3.3 Structure de la supertrame dans IEEE 802.15.4

La supertrame est délimitée par deux trames de balise, elle comprend une partie active et une partie inactive (facultative) [2], voir la figure 1.9. La période inactive est destinée aux nœuds qui n'ont pas de paquets à transmettre, par conséquent ils entrent en mode veille pour économiser de l'énergie. La partie active de la supertrame est divisée en 16 slots (emplacements) de temps de taille

égale où le premier slot de temps est occupé par le Beacon.
La période active comprend la période d'accès avec contention CAP (Contention Access Period) et la période sans contention CFP (Contention Free Period).

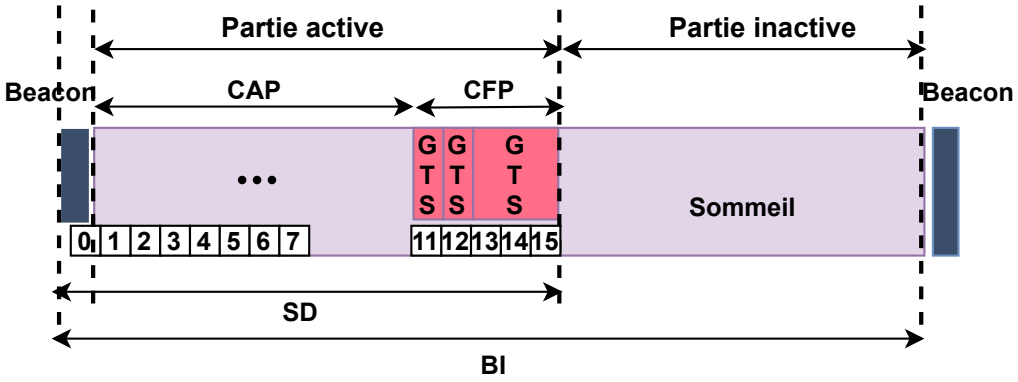


FIGURE 1.9 – Structure de la supertrame IEEE 802.15.4.

Dans le cas où la période CFP qui suit la période CAP est présente, l'accès au médium est garanti par le coordinateur PAN via des allocations appelées créneaux de temps garantis noté GTS (Guaranteed time slots). Jusqu'à sept GTSs peuvent être attribués par le coordinateur PAN dans la norme IEEE 802.15.4 en utilisant un seul canal. Chaque GTS peut occuper plus d'une période de créneau, comme illustré dans la figure 1.9. Notons que les demandes de réservation des GTS qui sont basées sur TDMA, ainsi que les demandes d'association au réseau ne peuvent se faire que durant la période CAP. Chaque nœud capteur souhaitant communiquer dans la période CAP doit rentrer en compétition avec les autres nœuds pour gagner l'accès au canal en utilisant le mécanisme CSMA/CA slotté.

Grâce aux paramètres Beacon Order (BO) et Superframe Order (SO) envoyés dans la trame Beacon, les nœuds pourront calculer les tailles du Beacon Interval (BI) et Superframe Duration (SD) [2].
La taille de BI représente la longueur totale de la supertrame (partie active et inactive) définie comme suit

$$BI = aBaseSuperframeDuration \times 2^{BO} Symboles.$$

La taille de SD représente la longueur de la partie active définie comme suit

$$SD = aBaseSuperframeDuration \times 2^{SO} Symboles.$$

Où : $aBaseSuperframeDuration = 960\ Symboles$ et $0 \leq SO \leq BO \leq 14$.

1.4.3.4 Protocoles MAC de IEEE 802.15.4

Les protocoles MAC utilisés dans le standard IEEE 802.15.4 servent principalement à assurer que le canal de communication est libre (idle) avant de commencer la transmission des données. La consommation d'énergie constitue une contrainte majeure dans les RCSFs, par conséquent les mécanismes d'accès au canal auront pour rôle de réduire les collisions qui sont une source de perte d'énergie. Le protocole CSMA/CA se base sur une unité de temps appelée période de backoff qui doit être égale à $aUnitBackoffPeriod$.

L'algorithme CSMA/CA ne doit pas être utilisé pour la transmission des trames Beacon utilisée dans le mode avec beacon, des trames d'accusé de réception ou des trames de données transmises dans le CFP.

Avant d'entamer la description du fonctionnement des protocoles CSMA/CA slotté et CSMA/CA non slotté illustré dans la figure 1.10, nous devons tout d'abord définir les paramètres et notations prédéfinis dans le standard IEEE 802.15.4 [2] :

- **Backoff :** représente le temps d'attente aléatoire tiré dans l'intervalle $[0, 2^{BE} - 1]$.
- **NB** (Number of Backoffs) : représente le nombre de fois que le protocole CSMA/CA tire aléatoirement un temps backoff pour la transmission en cours, initialisé à zéro avant chaque nouvelle tentative de transmission.
- **BE** (Backoff Exponent) : détermine la période de backoff que doit attendre chaque capteur avant d'évaluer le canal, initialisé à $MacMinBE = 3$ par défaut.
- **MacMinBE** : nombre minimal de l'exposant du backoff, initialisé à 3 par défaut.
- **MacMaxBE** : nombre maximal de l'exposant du backoff, initialisé à 5 par défaut.
- **CW** (Contention Window) : représente la fenêtre de contention qui correspond au nombre de fois que le canal est évalué libre, initialisée à $CW_0 = 2$ avant chaque tentative de transmission.
- **aUnitBackoffPeriod** : unité de temps backoff égale à 20 symboles.
- **macMaxCSMABackoffs** : représente le nombre de fois où le canal est trouvé occupé avant d'abandonner l'émission de la trame, initialisé à 3 par défaut.
- **macMaxFrameRetries** : le nombre maximum de retransmissions autorisé pour chaque trame, initialisé à 4 par défaut.

Le protocole CSMA/CA slotté (slotted CSMA/CA) est le protocole d'accès au médium utilisé dans le mode de communication synchrone avec beacon. Le mode synchrone veut dire que le début

du temps backoff de chaque capteur, qui aligne son début de la supertrame, correspond au début de réception de la trame Beacon envoyée par le coordinateur PAN. Par la suite, chaque nœud doit s'assurer qu'il lui reste assez de temps avant la fin de la supertrame pour achever [1] la transmission.

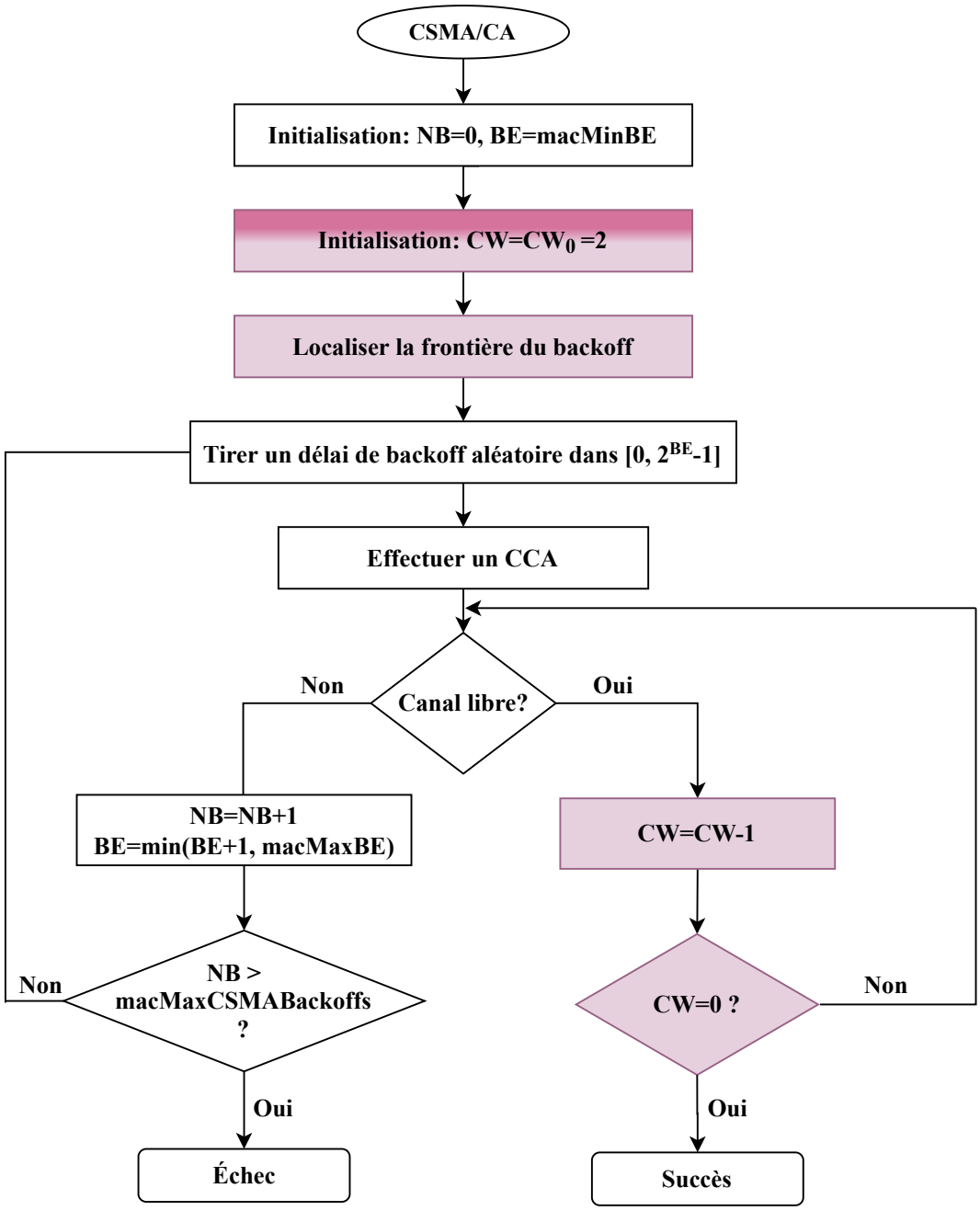


FIGURE 1.10 – Fonctionnement des protocoles CSMA/CA slotté et non slotté du standard IEEE 802.15.4.

Chaque nœud capteur qui utilise ce protocole et voulant accéder au canal de communication

1. Le temps restant est suffisant pour le Backoff, les deux CW et pour transmettre la trame, le CCA, IFS et éventuellement l'ACK si ce dernier est demandé avec son temps d'attente

sans fil suit la démarche suivante.

1. Initialisation des variables NB, CW et BE à leur valeur par défaut 0, 2, 3, respectivement,

2. Le capteur localise la limite du backoff (i.e. le début de la trame Beacon) et tire un temps aléatoire dans l'intervalle $[0, 2^{BE} - 1]$,

3. Le capteur décrémente le compteur du temps backoff jusqu'à atteindre la valeur zéro,

4. À la fin du temps d'attente aléatoire (backoff), la sous-couche MAC demande à la couche physique de vérifier l'état du canal de communication en effectuant un CCA qui dure 8 Symboles de temps,

5. Si le canal est détecté libre, la fenêtre de contention est décrémentée de 1 ($CW = CW - 1$), puis procéder à l'étape suivante. Sinon aller à l'étape 8,

6. Si $CW = 0$, alors procéder à l'étape 11. Sinon procéder à l'étape suivante,

7. Le nœud vérifie l'état du canal pour la deuxième fois en exécutant un autre CCA, puis retourne à l'étape 5,

8. Si le canal est détecté occupé, la variable NB est incrémentée de 1, la fenêtre de contention est réinitialisée à CW_0 et BE est mis à jour à $min(BE + 1, macMaxBE)$,

9. Si NB est inférieur à la valeur de $macMaxCSMABackoffs$, le nœud tire un autre backoff afin de retenter l'envoi de la trame (retourner à l'étape 2). Sinon procéder à l'étape 10,

10. Échec d'accès au canal de communication,

11. Accès au canal de communication réussi, la trame est prête à être envoyée à la frontière du prochain backoff ($UnitBackoffPeriod$).

Dans le cas où deux trames de données successives doivent être transmises d'un nœud au coordinateur PAN, un intervalle de temps appelé IFS (Inter Frame Spacing) est généré entre la transmission des deux trames [2]. Lorsque la première transmission demande un ACK, un AIFS (Acknow-

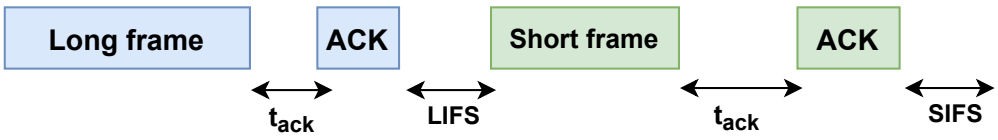


FIGURE 1.11 – Mécanisme de transmission de données avec acquittement.

ledgment InterFrame Spacing) est généré entre la trame d'acquittement et la seconde transmission, comme illustré dans la figure 1.11. La longueur des périodes IFS et AIFS dépendent de la taille de

la trame L qui a été transmise comme suit :

$$IFS = \begin{cases} LIFS & Si\ L > aMaxSIFSFramesize \\ SIFS & Sinon. \end{cases} \quad (1.1)$$

Avec, $SIFS$ (macMinSIFSPeriod) est le plus petit des IFS (12 *symboles*), $LIFS$ (macMinLIFSPeriod) est le plus grand IFS (40 *symboles*) et $aMaxSIFSFrameSize$ est égale à (18 *octets*).

Le protocole CSMA/CA non slotté (unslotted CSMA/CA) est utilisé dans le mode de communication sans beacon (absence de la structure de la supertrame). Son fonctionnement ressemble à celui du protocole CSMA/CA slotté sauf que les étapes coloriées dans la figure 1.10 ne sont pas incluses. Dans CSMA/CA non slotté, la fenêtre de contention (CW) n'est pas utilisée. Donc, il existe un seul test CCA, contrairement au mode beacon, où le canal devra être libre durant deux $aUnitBackoffPeriod$ avant l'émission de la trame. Dans le cas où le canal est libre, le capteur accède au canal et commence la transmission de la trame.

Une autre différence entre ces deux protocoles est que le nœud utilisant le protocole CSMA/CA non slotté ne localise pas la frontière du backoff. Autrement dit, dès que la période de backoff, tirée aléatoirement, expire, le capteur commence l'écoute du canal pendant une durée CCA sans attendre la frontière du prochain backoff.

1.5 Introduction à l'évaluation de performances des réseaux de capteurs sans fil

Les performances du réseau sont les grandeurs qualitatives ou quantitatives qui permettent de caractériser le fonctionnement d'un réseau. Les grandeurs quantitatives sont par exemple le délai de bout en bout, le débit, la fiabilité, etc. Tandis qu'une grandeur qualitative est souvent une propriété comme la convergence ou la stabilité du système. L'étude quantitative doit être précédé par l'étude qualitative.

Le but d'une évaluation de performances est de trouver des indicateurs représentant le comportement du réseau. L'étude de ce comportement avant son déploiement sur le terrain nous permettra de comprendre et de régler les éventuels problèmes qui pourraient affecter le réseau.

Deux classes de méthodes sont généralement utilisées pour évaluer les performances d'un système : les études directement réalisées sur le système lui-même et les études réalisées à l'aide d'un modèle du système. L'approche d'une étude directe nécessite la disponibilité du système physique

à étudier, ou du moins celle d'une copie conforme de lui. L'avantage de cette étude réside dans sa fidélité intrinsèque à la réalité.

Dans de nombreux cas, nous n'avons d'autre choix que d'utiliser la modélisation.

1.5.1 Types de modélisation

En se référant à [18], nous proposons ici les différents types de modélisation de systèmes physiques de natures diverses et en fonction de divers objectifs d'investigation. Un modèle peut être :

- **Statique ou dynamique :** selon la situation, on peut étudier le système à un moment précis ou étudier son évolution dans le temps. La première est appelée modélisation statique et la seconde modélisation dynamique.
- **Stochastique ou déterministe :** selon l'existence ou non d'éléments aléatoires, un modèle peut être déterministe ou stochastique.
- **Continu ou discret :** dans un modèle continu, l'état du système évolue de manière continue dans le temps ; alors que dans un modèle discret, les changements n'ont lieu que ponctuellement à un ensemble d'instants.

Les réseaux informatiques sont des systèmes discrets. Les modèles associés à ce type de réseau sont généralement stochastiques appartenant dans la plupart du temps à la catégorie de la modélisation dynamique.

1.5.2 Approches de la modélisation

Il existe deux approches principales de la modélisation [18] :

1. **Modélisation physique ou mesure :** dans laquelle nous construisons un système réduit du système appelé prototype. Puis à l'aide d'un appareil appelé moniteur, nous réaliseront des expériences en relevant certaines grandeurs significatives sur le prototype (comme de l'émulation) et grâce à l'analyse statistique ou opérationnelle, nous obtenons les métriques de performances attendues. Cette approche est malheureusement souvent assez coûteuse d'où l'intérêt de l'utilisation de l'autre approche ;
2. **Modélisation abstraite :** cette modélisation peut se faire à l'aide d'un :
   - **Modèle mathématique** (ou modèle analytique) que l'on réalise à l'aide des outils de calculs mathématiques, tels que la théorie des files d'attente, les réseaux de Petri, les chaînes de Markov, le coloriage des graphes, etc ;

– **Modèle informatique** (ou simulation) que l'on réalise à l'aide d'un outil logiciel et d'un langage approprié. Dans la pratique, il s'agit souvent de logiciels spécialement conçus pour la simulation comme OMNeT++ et OPNET.

Il est bon de signaler qu'un modèle en général n'est pas une copie conforme du système, les résultats tirés d'une étude par modélisation doivent par conséquent toujours être examinés avec un regard critique quant à leur représentativité. Une modélisation, qu'elle soit mathématique ou bien informatique, est une transcription, plus au moins simplifiée, d'un système réel vers une version virtuelle de celui-ci. Il y a par conséquent toujours un risque de manque de fidélité à l'original.

La modélisation analytique et la simulation ont en commun le besoin de modéliser le système. A ce titre, ils ont tous les deux besoin d'observer, puis d'identifier le comportement du système. Cependant, un modèle analytique, en raison de la maniabilité mathématique, est souvent amené a prendre des hypothèses plus simplificatrices, et par conséquent plus restrictives. Alors qu'une simulation peut modéliser plus finement et s'accorder mieux aux données observées. Ses deux techniques de modélisation sont mieux détaillées ci dessous.

1.5.2.1 Modélisation analytique

L'avantage des méthodes analytiques réside dans leur faible coût d'exploitation et dans le fait qu'elles fournissent rapidement des résultats (elles sont environ mille fois plus rapide que la simulation pour traiter un même problème), mais réclame la disponibilité des experts en mathématiques. De plus, il n'est pas toujours garanti que l'on puisse établir un modèle mathématique applicable, même approximativement, pour un système quelconque. Cette modélisation aboutit à des résultats fermes et généreux, et cela en fournissant plusieurs métriques de performances.

Si l'on veut étudier un nouveau *scenario*, il suffit de recalculer en prenant les paramètres adéquats du *scenario* visé. Cependant, la manipulabilité mathématique impose très souvent une modélisation un peu trop simplificatrice par rapport à la réalité.

Nous allons donner une brève définition de quelques formalismes de modélisation analytique ci-dessous.

– **Files d'attente**

La théorie des files d'attente [19] a été introduite en 1917 par Erlang dans le but de modéliser les réseaux téléphoniques. De nos jours, cette théorie intervient dans de nombreux domaines d'application et particulièrement dans les systèmes informatiques. La dynamique d'un réseau de files d'attente (ouvert ou fermé) est couramment représentée par une chaîne de Markov ergodique. Connaître la

distribution stationnaire de cette chaîne est un enjeu majeur pour celui qui veut étudier le comportement d'un tel réseau.

Quand on ne peut pas calculer directement la distribution stationnaire, pour néanmoins obtenir des informations sur cette dernière, on a recours à des méthodes d'approximation, qui consistent à trouver une solution approchée de la distribution stationnaire, ou à la simulation stochastique, qui englobe : la technique de Monte Carlo, la simulation parfaite ainsi que d'autres méthodes.

– **Les réseaux de Petri stochastiques**

Un réseau de Petri [20] est un graphe orienté composé de places, de transitions et d'arcs. Le graphe orienté est biparti, c'est à dire disposant de deux types de sommets (des places et des transitions) qui sont reliées par des arcs orientés qui forment des chemins alternant place & transition. Les places, les transitions et les arcs sont respectivement illustrés par des cercles, des cases et des flèches. Les places et les transitions dans un réseau de Petri peuvent être reliées par des arcs orientés. Cependant, deux places et deux transitions ne peuvent pas être reliées par des arcs. Les arcs sont identifiés par leurs poids.

Un réseau de Petri est un outil assez général pour modéliser des phénomènes très variés. Il permet notamment : la modélisation des systèmes informatiques, l'évaluation des performances des systèmes discrets, et d'autres.

Un réseau de Petri stochastique (SPN) [21] est un réseau de Petri où l'état change de manière dynamique et aléatoire en choisissant des déclenchements d'événements d'une manière aléatoire soigneusement prescrite. Ce type de réseau occupe une place prépondérante en tant qu'approche d'évaluation des performances des systèmes informatiques ou industriels.

– **Algèbres de processus**

L'algèbre de processus [22] fait référence à une classe de formalismes algébriques pour la modélisation et le raisonnement sur des systèmes de processus concurrents. Les caractéristiques de l'algèbre de processus incluent une collection d'opérateurs pour composer des systèmes à partir de sous-systèmes, et une relation d'équivalence ou de raffinement pour déterminer respectivement quand deux systèmes présentent le même comportement ou quand le comportement d'un système est plus contraint que celui d'un autre.

Les algèbres de processus [23] sont des théories mathématiques qui modélisent des systèmes concurrents par leur algèbre et fournissent un appareil pour raisonner sur la structure et le comportement du modèle. Contrairement aux réseaux de files d'attente ou aux réseaux de Petri, il n'y a pas de notion d'entité ou de flux dans un modèle. Cependant, en récompense, le raisonnement

compositionnel fait partie intégrante du langage.

– **Chaînes de Markov**

Une chaîne de Markov est un processus stochastique à temps discret : à chaque instant, la chaîne prend une valeur aléatoire conditionnellement à la valeur qu'elle possédait à l'instant d'avant. Les chaînes de Markov représentent un formalisme mathématique simple pour modéliser et analyser un phénomène stochastique. Le modèle est basé sur des états et des transitions. Sa simple structure permet de modéliser une large classe de systèmes dynamiques aléatoires.

Les applications des chaînes de Markov peuvent être trouvées dans de nombreux domaines, de la physique statistique aux séries chronologiques financières. Les chaînes de Markov sont des outils bien connus où les nombreux résultats théoriques permettent d'analyser finement le comportement du système modélisé. Elles sont donc un des plus importants outils d'analyse des processus aléatoires dans le domaine de la modélisation.

Dans le cadre d'une modélisation et de l'évaluation de performances, les chaînes de Markov présentent une simplicité et une efficacité incontournable. Dans la littérature, la plupart des modélisations du 802.15.4 utilisent les chaînes de Markov comme outil de modélisation [24, 25, 26, 27, 28, 29]. Nos travaux seront également réalisés à l'aide de cet outil.

– **Les réseaux d'automates stochastiques**

Le formalisme de réseau d'automates stochastiques (SAN) [30] est l'une des méthodes qui permet d'atténuer le problème de dimensionnalité dans la modélisation de chaînes de Markov. La méthode SAN est basée sur la division d'un système en sous-systèmes plus petit. Chacun de ces sous-systèmes est modélisé par un automate séparé. Chaque automate est représenté par une chaîne de Markov, c'est-à-dire un ensemble d'états et des transitions possibles entre eux [31]. Si deux automates interagissent, la transition dans un automate peut dépendre de l'état dans un autre. L'état du système (état global) est l'état compositionnel de tous les automates.

1.5.2.2 Simulation

La simulation fait partie des outils numériques les plus utilisés, aussi bien dans la recherche académique que dans le monde industriel, pour étudier, de manière quantitative, le comportement dynamique des systèmes complexes. Elle nécessite, pour la construction du modèle, un outil de programmation spécialisé et de longues heures de développement. La puissance descriptive apportée par cet outil permet de modéliser de manière très détaillée le système cible. Cependant, pour tirer une conclusion avec une qualité statistique minimale, il est nécessaire de réaliser un certain nombre

de campagnes de simulation. De plus, la conclusion n'est valable que pour une situation donnée. Si nous voulons étudier un nouveau scénario, il est nécessaire de relancer des campagnes de simulation. Le but d'une simulation est de reproduire, par logiciel, un système physique afin que nous puissions entreprendre des expériences statistiques sur celui-ci. Grâce à ces expériences, nous pouvons évaluer les performances du système cible, comme si nous réalisions des expériences sur le système physique réel.

Il existe deux familles de techniques de simulation, la simulation continue et la simulation à évènements discrets [18]. La simulation continue étudie l'évolution dynamique d'un système (phénomènes physiques, mécaniques ou chimiques) qui est décrite par des paramètres à valeurs continues. En revanche, la simulation à évènements discrets convient aux systèmes dont l'évolution n'a lieu que ponctuellement sur un ensemble d'instants spécifiques consécutivement à l'apparition de certains événements.

Les simulateurs peuvent se diviser en deux parties : les simulateurs bas niveau et les simulateurs haut niveau. Les simulateurs bas niveau utilisent des langages de programmation, tels que C, Java, etc. En revanche, les simulateurs à l'intérieur desquels nous pouvons développer de nouveaux mécanismes, protocoles comme NS2, OPNET, JISIM et GLOMOSOM, sont dits de haut niveau. Parmi les simulateurs de haut niveau, il y a des logiciels gratuits (open source comme NS2 et NS3, GLOMOSIM, JSIM) et commerciaux comme OPNET.

La simulation n'est pas une technique exacte (temps infini de simulation) et les résultats obtenus doivent s'accompagner d'un intervalle de confiance qui permet d'estimer le degré d'approximation des résultats. De plus, les logiciels de simulation commerciaux sont souvent assez chers.

1.5.3 Comparaison entre la modélisation analytique et la simulation

Sous les hypothèses retenues, un modèle analytique fournit des formules mathématiquement prouvées. Ce dernier est paramétrique, donc facilement utilisable pour étudier tout scénario d'intérêt. Chaque campagne de simulation est cependant une expérience singulière. Afin de tirer une conclusion statistiquement significative, nous devons effectuer un nombre important de simulations. Le même type de travail doit d'ailleurs être renouvelé à chaque fois que l'on change l'un des paramètres du système. On voit donc la dualité suivante :

– la méthode analytique nécessite l'adoption d'un modèle qui est souvent trop simplifié. En revanche, les résultats sont exacts. Il est donc facile d'examiner diverses situations en faisant varier les paramètres. L'effort intellectuel mis de côté, la modélisation mathématique réclame

peu de ressources physiques ;

– la simulation permet d'obtenir une modélisation plus fidèle. Cependant, l'obtention des résultats est une opération longue et délicate. En effet, plus le modèle est détaillé, plus l'effort de programmation est important et plus la durée de la simulation sera longue. De plus, chaque campagne de simulation est une expérience statistique produisant un résultat qui n'est valable que pour un scénario donné. Son interprétation est sujette à caution et peut toujours présenter un risque d'incertitude.

On voit alors la nécessité de combiner ces deux outils : l'outil analytique pour une étude macroscopique qui permet de tracer les grandes lignes, et l'outil de simulation pour une étude plus ciblée et plus détaillée.

1.5.4 Les Principales métriques de performances des systèmes étudiés

Une métrique de performance est un critère de mesure choisi pour quantifier les performances d'un système. Il existe plusieurs métriques de performance dans la littérature, nous allons citer juste certaines métriques de performance spécifiques aux réseaux de capteurs sans fils qui nous intéressent dans notre évaluation de performance.

– **La fiabilité :** elle est définie comme étant la probabilité de transmission d'un paquet avec succès.

– **L'énergie consommée :** elle représente la quantité d'énergie que consomme un nœud durant tous ses états.

– **Le délai moyen :** il est défini à partir de l'instant où le paquet est enfilé dans la file d'attente jusqu'à ce qu'il soit transmis avec succès. Si le paquet atteint le nombre maximum de retransmissions et il est détruit, alors son temps ne sera pas inclus dans le calcul du temps moyen de transmission.

– **Le débit :** il représente la quantité d'informations transportées par unité de temps.

1.6 Synthèse sur les travaux existants

Dans la littérature, beaucoup de chercheurs s'interessent à la modélisation et à l'évaluation des performances des protocole MAC IEEE 802.15.4. Dans le cas de la modélisation analytique, les chaînes de Markov est l'outil le plus utilisé.

Une grande partie des modèles analytiques proposés jusqu'à présent pour les protocoles MAC basés sur le CSMA/CA sont dérivés du modèle proposé par Bianchi [32]. Dans le cadre de son travail, Bianchi a effectué une analyse de la chaîne de Markov pour estimer le débit de saturation d'un réseau en utilisant le protocole MAC IEEE 802.11 DCF. Compte tenu des bonnes performances de prédiction du modèle de Bianchi et des similitudes entre les mécanismes d'accès IEEE 802.15.4 et IEEE 802.11 DCF, de nombreuses études sur l'IEEE 802.15.4 ont suivi les traces de Bianchi.

1.6.1 CSMA/CA slotté

On trouve beaucoup de travaux sur le protocole CSMA/CA slotté de IEEE 802.15.4 depuis l'apparition du standard jusqu'à aujourd'hui, nous citerons quelques travaux ci dessous :

Modèle de Misic (2004). Dans [24], les auteurs ont proposé le premier modèle mathématique pour le mode beacon de la norme IEEE 802.15.4, en combinant les chaînes de Markov à temps discret et la théorie des files d'attente (système M/G/1/K), sous l'hypothèse d'un réseau non saturé avec considération des ACK. Les auteurs ont obtenu la distribution de probabilité du délai et du débit. L'impact de différents paramètres, tels que le taux d'arrivée des paquets, le nombre de stations, la taille finie des tampons de nœuds individuels, la taille des paquets et la période d'inactivité entre les balises sur les performances du réseau est aussi étudié.

Modèle de Park (2005). Un nouveau modèle analytique basé sur une chaîne de Markov à temps discret du mécanisme CSMA/CA slotté est proposé dans [33], à partir duquel le débit et la consommation d'énergie sont calculés dans des conditions de saturation de trafic, et dans une topologie en étoile. Les résultats analytiques sont validés via des simulations à l'aide du simulateur ns-2.

Modèle de Sahoo (2008). Dans [25], les auteurs ont développé une extension de la chaîne de Markov existante de deux dimensions à une chaîne de Markov à trois dimensions en incluant un troisième processus stochastique, r(t), qui représente le compteur de retransmission maximal. Leur objectif été d'étudier l'impact du nombre maximum de retransmission sur les performances du réseau à savoir la consommation d'énergie et le débit. L'étude s'est faite dans des conditions de trafic non saturé, une topologie en étoile du réseau et prenant en charge les ACKs. La consommation d'énergie et le débit sont analysés pour différents nombres de nœuds afin d'estimer le nombre possible de nœuds offrant les meilleures performances en termes de débit. Les auteurs ont effectué une simulation sous le simulateur ns 2.29.

Modèle de Pollin (2008). Un modèle analytique a été présenté dans [26] pour la couche MAC de la

norme IEEE 802.15.4 basé sur une chaîne de Markov discrète à deux dimensions. Le modèle analytique est utilisé pour prédire la consommation d'énergie ainsi que le débit des réseaux 802.15.4 saturés et non saturés.

Le modèle suppose un nombre limité de terminaux, des conditions de canal idéal et une topologie en étoile avec présence de trames d'acquittements. Les auteurs ont comparé leurs résultats analytiques du débit et de consommation énergétique à des résultats simulés, où les performances prédites par le modèle analytique sont très proches de celles obtenues par simulation. La simulation considérée est la simulation Monte-Carlo de la procédure de contention 802.15.4 avec un développement d'un simulateur vectoriel dans Matlab.

Les auteurs dans [26] étaient les premiers à donner l'expression de la probabilité d'écoute du canal pendant un temps CCA. Il a été démontré que pour les réseaux saturés, il est préférable de choisir une plus grande valeur de backoff. Tandis que pour les réseaux non saturés, les petites valeurs de backoff peuvent améliorer la consommation d'énergie, mais ces économies d'énergie sont très faibles. Il est également montré que, bien que le nouveau mécanisme CSMA/CA diminue considérablement le temps et par conséquent l'énergie dépensée pour écouter le canal, cette consommation d'énergie pendant le CCA représente encore une part importante de la consommation totale d'énergie du système.

Modèle de Park (2013). Dans [34], les auteurs ont proposé un modèle analytique généralisant le mécanisme CSMA/CA slotté en tenant compte des tentatives limitées de retransmission. Ils ont étudié le comportement d'un seul nœud en utilisant une chaîne de Markov tridimensionnels $(s(t), c(t), r(t))$, en s'inspirant du modèle de Sahoo [25]. Où $s(t)$, $c(t)$ et $r(t)$ représentent respectivement l'étage backoff, le compteur backoff et le compteur de retransmission.
Les performances du protocole ont été évaluées en matière de fiabilité, d'énergie et de délai dans un réseau non saturé et en utilisant le mécanisme d'acquittement des trames. La topologie du réseau utilisée est en étoile.

Les auteurs ont montré que le modèle était précis et fiable en le comparant à des simulations qui ont été mises en œuvre sous Contiki OS en utilisant des capteurs TelosB. Les expériences empiriques ont montré que l'approche satisfait considérablement les contraintes de délai et de fiabilité ainsi l'approche garantit une plus longue durée de vie du réseau. Contrairement aux travaux antérieurs, la présence d'un nombre limité de retransmissions, d'accusés de réception, de trafic non saturé, de taille de paquet et de délai de copie de paquet en raison de limitations

matérielles est prise en compte.

Modèle de Tavakoli (2016). Les auteurs de [35] visent à maximiser la durée de vie utile du réseau IEEE 802.15.4 grâce à la veille aléatoire. Pour ce faire, une modélisation par chaîne de Markov à temps discret pour la transmission des paquets utilisant le protocole CSMA/CA slotté a été présentée. Ils ont calculé la fiabilité, le délai des paquets et la consommation d'énergie dans un réseau saturé et dans des conditions de canal non idéal prenant en compte les acquittements.

Modèle de Phan (2018). Dans [36], les auteurs ont proposé des modèles analytiques pour les performances de débit et de latence du protocole MAC IEEE 802.15.4. Ces modèles sont destinés au protocole MAC IEEE 802.15.4 avec acquittements fonctionnant en mode beacon, dans une topologie en étoile avec des conditions de trafic aléatoires et légères. La précision des modèles analytiques est vérifiée au moyen de simulations approfondies à l'aide du simulateur de réseau ns-2. Les résultats de la simulation démontrent que l'augmentation de la taille des paquets dégradera le débit de IEEE 802.15.4 en raison de la nature du mécanisme CSMA/CA, alors qu'une amélioration du débit est généralement attendue.

Modèle de Chen (2020). Les auteurs dans [28] ont analysé les performances du mécanisme CSMA/CA slotté de la norme IEEE 802.15.4 en tenant compte du processus de récupération d'énergie dans chaque appareil IoT. Le réseau considéré suit une topologie en étoile à un seul saut, dans lequel chaque appareil transmet des paquets au coordinateur PAN et reçoit un accusé de réception où l'état du trafic est non saturé. Une analyse des performances, en termes de délai, de débit et de fiabilité a été effectuée. La validité du modèle proposé est prouvée par une simulation développée dans Matlab.

1.6.2 CSMA/CA non slotté

Le mode sans balise est rarement étudié dans la littérature. Voici quelques travaux modélisant les protocoles MAC CSMA/CA non slotté dans un réseau de IEEE 802.15.4.

Modèle de Feo (2011). Dans [37], un nouveau modèle analytique pour le CSMA/CA sans beacon de IEEE 802.15.4 pour un seul nœud a été proposé au moyen d'une chaîne de Markov à temps discret. Les modèles précédents supposent souvent que la probabilité d'une évaluation d'occupation du canal est indépendante de la phase de l'étage du backoff.

Les auteurs ont montré que cette condition ne tient pas pour l'IEEE 802.15.4 et ont proposé une approximation de modélisation. Dans le modèle, la probabilité d'évaluation de l'occupation du canal à la fin de chaque étage du backoff n'est pas considérée comme constante, mais

est calculée en fonction de l'état du trafic du réseau et de la taille de la fenêtre du backoff. Ils ont considéré dans leur analyse, des topologies multi-sauts, un trafic non saturé et une absence d'acquittements.

La précision du modèle est confirmée en comparant les valeurs prédites aux résultats obtenus grâce à des simulations avec le simulateur TOSSIM des réseaux étendues dans un large éventail de scénarios tenant compte des différentes topologies de réseau, du nombre de nœuds et des charges de trafic.

Modèle de Di Marco et al (2012). Dans [38], un modèle généralisé d'un réseau IEEE 802.15.4 hétérogène non slotté est proposé. La chaîne de Markov considérée est la même que celle proposée par Park et al [34], où les tentatives limitées de retransmission et les ACKs sont considérés. La principale contribution de ce modèle, par rapport au modèle de Park et al, est la présence d'un trafic hétérogène avec différents taux de génération de paquets de nœuds, des terminaux cachés et un routage multi-hop. La précision du modèle est évaluée par des simulations de Monte Carlo. L'analyse vise à dériver les métriques de performance du réseau, à savoir la fiabilité en tant que probabilité de réception de paquets réussie, le délai pour les paquets reçus avec succès et la consommation d'énergie moyenne du nœud.

Modele de Chen et al (2016). Une évaluation des performances des réseaux sans balise IEEE 802.15.4 avec mode d'acquittement (ACK) et limites de retransmission dans une unité de temps plus fine a été l'objet de [28]. Un modèle de chaîne de Markov à temps discret et une file d'attente M/M/1/k sont utilisés pour décrire l'algorithme CSMA/CA non slotté dans un réseau sans beacon. Des conditions de trafic saturé et non saturé sont considérés dans un réseau d'une topologie en étoile. Les auteurs ont dérivé des mesures de performance importantes, comme, le débit, le délai et la fiabilité.

Sur la base de la simulation de Monte Carlo et des modèles analytiques proposés, une comparaison entre les performances obtenues de manière analytique et par simulation est donnée. Les résultats extensifs de la simulation montrent la précision des modèles analytiques en ce qui concerne le débit et la fiabilité.

El Korbi et al (2017). Dans [29], l'étude est basée sur l'analyse de la chaîne de Markov à temps discret (DTMC) modélisant le processus du mécanisme IEEE 802.15.4 CSMA/CA non slotté dans le mode sans beacon. Ensuite, des limites probabilistes de consommation d'énergie et la consommation d'énergie moyenne approximative du CSMA/CA non slotté ont été dérivé.

L'étude a été faite dans des conditions de trafic non saturé, où la retransmission limitée et les trames d'acquittements ont été considéré.

Pour valider les bornes probabilistes de la consommation d'énergie données, le simulateur de réseau $OMNET++$ a été utilisé. Les résultats des simulations ont montré la précision de l'approximation proposée.

Modèle de Gamal et al (2020). Dans CSMA/CA non slotté, les nœuds ont tendance à attendre une valeur d'exposant backoff (BE) très limitée, et ne peuvent pas effectuer un CCA jusqu'à ce que la procédure de backoff soit terminée. Par conséquent, la probabilité de collision et le délai moyen sont élevés. Pour améliorer les performances du CSMA/CA non slotté, les auteurs dans [39] ont proposé un protocole CSMA/CA non slotté modifié qui divise le délai du backoff en Backoff Principal et Backoff Secondaire. Dans ce travail, la topologie en étoile est utilisée, tandis que les ACKs, ainsi que les retransmissions ne sont pas considérés. Pour valider le modèle analytique, le délai moyen, la consommation d'énergie et la fiabilité sont calculés à l'aide de $MATLAB$ et comparés aux résultats simulés à l'aide du simulateur $OPNET$. Les résultats sont très proches, et cela prouve la validation du modèle proposé.

1.7 Conclusion

Dans ce premier chapitre, nous avons tout d'abord présenté brièvement les réseaux sans fil et leurs catégories. Nous avons, par la suite, concentré notre étude sur les réseaux de capteurs sans fil, dressé leurs caractéristiques et énuméré leurs contraintes ainsi que leurs domaines d'applications.

Dans un second lieu, nous avons introduit la norme IEEE 802.15.4 adaptée aux applications des réseaux de capteurs sans fil. Elle fournit les spécificités et les protocoles des couches basses physique et MAC. La couche physique de IEEE 802.15.4 propose plusieurs types de modulation, plusieurs canaux de communication et des débits différents. La sous-couche MAC gère l'accès au canal avec les deux mécanismes CSMA/CA slotté et CSMA/CA non slotté. Leur fonctionnement a été présenté en détail dans ce chapitre. Finalement, une introduction à l'évaluation de performances des réseaux de capteurs sans fil permettant de mettre en œuvre les approches existantes dans la littérature, a été présentée. Puis, une synthèse des travaux existants sur la modélisation des protocoles MAC de IEEE 802.15.4 a été élaborée.

Vu les limites de la norme IEEE 802.15.4, différentes versions du standard IEEE 802.15.4 ont été proposées. Son évolution au fil du temps sera l'objet du prochain chapitre.

Chapitre2

La révolution historique du standard IEEE 802.15.4

Sommaire

2.1 Introduction

Depuis 2003, le protocole IEEE 802.15.4 a été conçu pour les réseaux WPAN à faible débit, faible puissance, faible complexité, faible coût et de courte portée. Sa version de base a été publiée le 1er octobre 2003 [2], puis de nombreux amendements et versions ont été proposés pour faire face aux limites rencontrées dans IEEE 802.15.4-2003. Les amendements sont adoptés soit pour prendre en charge un type de réseau spécifique, soit pour porter des modifications (sur la couche physique ou sur la sous-couche MAC) ou simplement comme une révision pour les versions précédentes.

Ce chapitre décrit une synthèse critique sur les nouvelles versions du standard IEEE 802.15.4 [5], étudié dans le premier chapitre, depuis sa première apparition jusqu'à aujourd'hui. Les modifications apportées à la norme de base et quelques travaux connexes existants dans la littérature, seront présentés. De plus, des tableaux comparatifs sur les caractéristiques et exigences de tous les amendements seront établis.

2.2 IEEE 802.15.4-2003

La description de cette norme a été introduite dans le chapitre précédent (voir la section 1.4).

2.3 IEEE 802.15.4-2006

Le 8 septembre 2006 [40], la norme a été révisée pour la première fois pour apporter des améliorations et des corrections spécifiques à la version de base. La résolution des ambiguïtés, la réduction de la complexité inutile, l'augmentation de la flexibilité dans l'utilisation des clés de sécurité et les considérations pour les attributions de fréquences nouvellement disponibles sont les améliorations les plus envisagées dans cette révision.

2.3.1 Spécifications PHY

L'augmentation du débit réalisable sur la bande de basse fréquence a été l'objet de cette révision, par conséquent deux alternatives physiques ont été introduites.

- La bande de 868/915 MHz employant ASK (Amplitude Shift Keying) comme technique de modulation, offre un débit de données de 250 kb/s pour les bandes de fréquences de 868 MHz et de 915 MHz.

- La bande de 868/915 MHz employant O-QPSK comme technique de modulation. Elle offre un débit de données de 250 kb/s pour la bande de fréquence de 915 MHz et de 100 kb/s pour la bande de 868 MHz.

Un nombre de 30 canaux dans la bande 915 MHz et 3 canaux dans la bande 868 MHz ont été rajoutés dans cette version.

2.3.2 Architecture MAC

Concernant la sous-couche MAC, de petits changements ont été ajoutés aux trames MAC pour de nouvelles fonctionnalités de sécurité et des améliorations à cette sous-couche [40]. Sachant que le mécanisme CSMA/CA est le même que CSMA/CA spécifié dans l'IEEE 802.15.4-2003.

2.4 IEEE 802.15.4a-2007

Cet amendement à IEEE 802.15.4-2006 paru le 31 août 2007 spécifie une nouvelle couche physique alternative prenant en charge la télémétrie précise, en plus des PHY spécifiés dans la norme IEEE 802.15.4-2003 [41]. Sachant cela, le choix de la bonne PHY dépend des réglementations locales, de type d'application et des préférences de l'utilisateur.

2.4.1 Spécifications PHY

L'amendement IEEE 802.15.4a-2007 spécifie deux nouvelles options pour la couche physique :

- La bande ultra large UWB (Ultra Wide Band) : prend en charge un débit de données obligatoire de 851 kb/s avec des débits de données en optionnel. Elle fonctionne dans différentes bandes de fréquences avec différents débits de données optionnels comme suit :
  - La bande de sous gigahertz, qui consiste en un seul canal et occupe le spectre de 249,6 MHz à 749,6 MHz offrant un débit de 110 kb/s ;
  - La bande basse, qui se compose de quatre canaux et occupe le spectre de 3,1 GHz à 4,8 GHz offrant un débit de 6,81 Mb/s ;
  - La bande large, qui se compose de onze canaux et occupe le spectre de 6,0 GHz à 10,6 GHz offrant un débit de 27,24 Mb/s.
- La technique d'étalement de spectre CSS (Chirp Spread Spectrum) : prend en charge un débit de données obligatoire de 1000 kb/s et 250 kb/s en optionnel. Il fonctionne dans la bande de fréquence 2450 MHz.

Quatorze canaux qui se chevauchent sur CSS PHY et 16 canaux sur les différents couches PHY UWB sont disponibles [41]. L'UWB utilise la modulation BPM-BPSK qui est une combinaison de modulation BPM (Burst Position Modulation) et de modulation BPSK (binary phase-shift keying). Alors que CSS utilise des techniques CSS en combinaison avec la modulation DQPSK (Differential Quadrature Phase-Shift Keying).

2.4.2 Architecture MAC

Une nouvelle stratégie alternative d'accès aux médium dans la couche MAC nommée protocole ALOHA est introduite en plus du protocole CSMA/CA déjà présenté. En utilisant ce nouveau protocole, le nœud émet quand il le souhaite sans avoir recours à détecter le support ou à attendre un intervalle de temps backoff.

2.4.3 Travaux connexes

Dans [42], un aperçu de la norme IEEE 802.15.4a est présenté. Un aperçu et une comparaison des normes IEEE 802.15.4 et IEEE 802.15.4a sont fournis dans [43]. Les auteurs dans [44] ont présenté une nouvelle méthode d'estimation de la puissance de crête (peak power) plus précise pour les systèmes UWB à impulsions radio. Une telle méthode est un ingrédient crucial dans la conception des nouveaux systèmes sans fil, lorsque il s'agit d'une conception pour une distance maximale réalisable. Dans [45], les performances en termes de taux d'erreur de IEEE 802.15.4a sont étudiées. Des expressions semi-analytiques sont dérivées pour approcher de près le taux d'erreur binaire BER (Bit Error Rate) et le taux d'erreur de trame FER (Frame Error Rate) numériquement, puis évaluées par simulation.

2.5 IEEE 802.15.4c-2009

Cet amendement à la norme IEEE 802.15.4-2006 a été approuvé le 17 avril 2009. Une nouvelle extension alternative de la couche physique pour fournir un fonctionnement dans les bandes de fréquences 780 MHz (779-787 MHz) spécifiques en Chine a été proposée [46]. Seules les spécifications physiques sont prises en compte dans la norme IEEE 802.15.4c-2009 pour les réseaux CWPAN (Chinese Wireless Personal Area Network).

2.5.1 Spécifications PHY

La norme spécifie les alternatives physiques suivantes :

- La bande de 780 MHz utilisant la modulation MPSK et offrant un débit de données égal à 250 kb/s.
- La bande de 780 MHz utilisant la modulation O-QPSK et offrant un débit de données égal à 250 kb/s.

Au total, 8 canaux sont disponibles dans la bande de 780 MHz.

2.5.2 Travaux connexes

IEEE 802.15.4c-2009 a été initialement conçu pour les environnements intérieurs et à faible mobilité. Bien que les auteurs dans [47] aient prouvé que cette norme est également applicable dans des scénarios urbains des RCSFs. Une mesure complète de la qualité des liaisons afin d'évaluer les performances de l'IEEE 802.15.4c-2009 dans des scénarios urbains est proposée. Ces mesures dans différents scénarios typiques ont fourni des ensembles de données empiriques utiles pour les protocoles de couches supérieures conçus pour les RCSFs urbain. De plus, l'influence des obstacles dans le canal sans fil entre l'émetteur et le récepteur et la mesure du taux de réception des paquets est étudiée, avec des plans de test par simulation [47].

2.6 IEEE 802.15.4d-2009

Dans l'amendement IEEE 802.15.4d-2009, une nouvelle extension de couche physique alternative a été approuvée le 17 avril 2009 pour fournir des opérations dans la bande de fréquence 950 MHz (950-956 MHz) spécifique au Japon [48].

2.6.1 Spécifications PHY

La norme spécifie les couches PHYs suivantes :

- La bande de 950 MHz basée sur la technique DSSS utilisant la modulation BPSK et offrant un débit de données égal à 20 kb/s.
- La bande de 950 MHz utilisant la modulation GFSK et offrant un débit de données égal à 100 kb/s.

Un nombre de 22 canaux est utilisé dans la bande 950 MHz.

2.6.2 Architecture MAC

Dans la norme IEEE 802.15.4d-2009, les nœuds tentent d'accéder au canal en utilisant une version modifiée du mécanisme CSMA/CA. La modification est que la valeur de la fenêtre de contention (CW) doit être initialisée à un (dans les amendements précédents, CW est initialisé à deux périodes) avant chaque tentative de transmission, et réinitialisée à un chaque fois que le canal est occupé.

2.7 IEEE 802.15.4-2011

IEEE 802.15.4-2011 approuvée le 5 septembre 2011 représente la deuxième révision de l'IEEE 802.15.4-2003 et la première révision de la norme IEEE 802.15.4-2006 [49]. Elle a été créé pour regrouper les trois amendements précédents (IEEE 802.15.4a, IEEE 802.15.4c et IEEE 802.15.4d) en un seul document.

2.7.1 Spécifications PHY

IEEE 802.15.4-2011 inclut toutes les couches PHY définies dans les versions et amendements précédents (O-QPSK PHY, BPSK PHY, ASK PHY, CSS PHY, UWB PHY, GFSK PHY et BPSK PHY) qui prennent en charge une variété de bandes de fréquences, y compris (868-868,6 MHz ; 902-928 MHz ; 2400-483,5 MHz ; 779-787 MHz et 950-956 MHz) [49].

2.7.2 Architecture MAC

Dans cet amendement, l'accès au canal se fait à l'aide des mécanismes CSMA/CA ou ALOHA.

2.7.3 Travaux connexes

Parmi les études ayant évalué les performances de la norme IEEE 802.15.4 en utilisant soit la simulation, soit la modélisation mathématique ou les deux à la fois, nous citons [50, 51, 34, 52, 38, 53].

2.8 IEEE 802.15.4e-2012

Dans les amendements précédents, les applications industrielles et commerciales n'étaient pas correctement prises en charge. Cela a conduit à la création de l'amendement à IEEE 802.15.4-2011

[49] nommé IEEE 802.15.4e le 16 avril 2012 pour y faire face [54]. Pour cela, des mécanismes MAC supplémentaires (DSME, TSCH et LLDN) et des formats de trame ont été spécifiés dans la norme IEEE 802.15.4e-2012 pour faciliter les applications industrielles, telles que le contrôle de processus et l'automatisation d'usine. Dans cet amendement, seules les modifications MAC sont prises en compte.

2.8.1 Architecture MAC

Les trois mécanismes MAC définis dans IEEE 802.15.4e-2012 sont :

- Deterministic and Synchronous Multi-channel Extension (DSME) : vise à soutenir les applications industrielles et commerciales avec des exigences strictes en matière de rapidité et de fiabilité. Comme les GTS dans IEEE 802.15.4-2003 sont limités à l'utilisation d'un seul canal, une extension du nombre de GTS pouvant être utilisés dans plusieurs canaux est spécifiée dans IEEE 802.15.4e-2012 utilisant le DSME. Pour atteindre cet objectif, une technique de

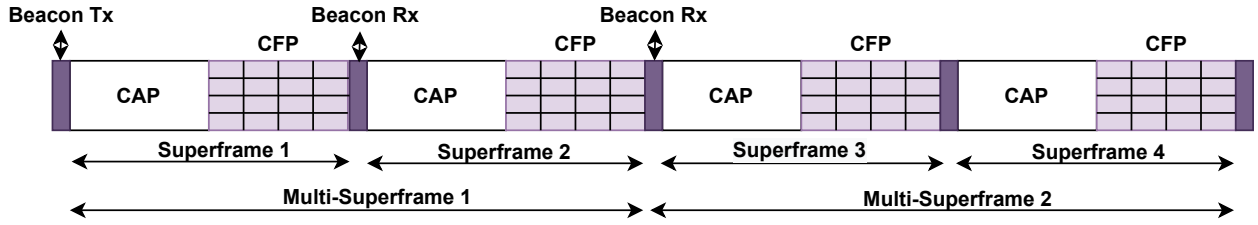


FIGURE 2.1 – Structure de la supertrame IEEE 802.15.4e-2012 DSME

saut de canal et une structure multi-supertrame définie par des coordinateurs sont adoptées, comme le montre la figure 2.1. Une multi-supertrame est un cycle de supertrames répétées qui transmettent périodiquement une balise améliorée EB (Enhanced Beacon).

- Time Slotted Channel Hopping (TSCH) : destiné à des domaines d'application, tels que l'automatisation des processus, l'industrie pétrolière et gazière, les produits pharmaceutiques et chimiques et la climatisation. TSCH combine un accès à intervalles de temps avec un saut de canal sachant qu'un intervalle de temps peut être utilisé par plusieurs liaisons en même temps. En conséquence, la capacité du réseau est augmentée (c'est-à-dire que des communications simultanées peuvent avoir lieu dans le même intervalle de temps).

  Le TSCH peut être utilisé pour former n'importe quelle topologie de réseau et s'exécute en mode sans beacon, où les périphériques sont synchronisés via un slotframe périodique. Un

slotframe est un ensemble de slots de temps qui se répètent au fil du temps. Plusieurs slotsframes sont utilisés pour un réseau donné pour définir différents programmes de communication pour divers appareils.

Lorsqu'un appareil donné fonctionne en mode TSCH, CCA peut être utilisé. La transmission dans la liaison partagée se fait à l'aide de l'algorithme TSCH-CA qui est analogue à celui de CSMA/CA décrit dans IEEE 802.15.4-2003.

- Low Latency Deterministic Network (LLDN) : nécessite une très faible latence (par exemple, automatisation d'usine, contrôle de robot). LLDN ne prend en charge que la topologie en étoile et fonctionne en mode beacon. Afin d'améliorer le mode Beacon, une nouvelle structure de supertrame est utilisée, où le temps est divisé en cycles appelés supertrame LLDN, comme illustré dans la figure 2.2. Dans cette supertrame, il existe deux types de slots de temps : les slots de temps dédiées et les slots de temps partagées. Dans LLDN, plusieurs

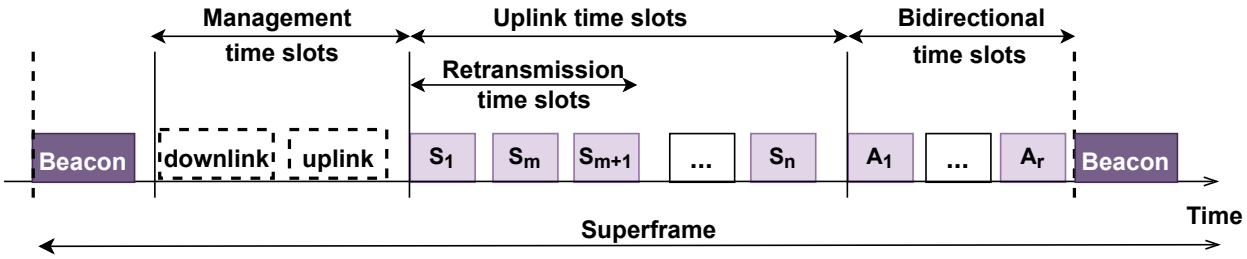


FIGURE 2.2 – Structure de la supertrame IEEE 802.15.4e-2012 LLDN

périphériques peuvent être affectés à un slot de temps. Les appareils utilisent le mécanisme CSMA/CA simplifié qui est le même que le mécanisme CSMA/CA utilisé dans la version de base. Cependant, un seul appareil a le privilège de transmettre dans un slot de temps dédié. Le mécanisme LLDN introduit dans ce nouvel amendement IEEE 802.15.4e offre une retransmission déterministe lorsque la transmission du paquet de données a échoué, sachant que cette opportunité n'était pas possible dans les versions précédentes.

2.8.2 Travaux connexes

Dans [55], un aperçu général de l'amendement IEEE 802.15.4e-2012 est fourni présentant tous les nouveaux modes MAC (LLDN, TSCH et DSME) avec un ensemble d'expériences de simulation. Pour décrire les limites du 802.15.4, de nouveaux protocoles MAC capables de répondre aux besoins émergents des applications industrielles embarquées sont fournis dans [56, 57]. Dans [56],

les performances de l'IEEE 802.15.4e sont évaluées en termes de délai moyen, de taux de perte de paquets et de rendement de bout en bout. La nouvelle version du protocole est implémentée dans l'OMNeT ++ à l'aide du simulateur de réseau ns-2.

Une comparaison entre les performances obtenues en utilisant 802.15.4e et celles obtenues avec 802.15.4 a été réalisée en termes de latence moyenne, de taux de livraison et d'efficacité énergétique, comme présenté dans [57] avec un ensemble d'expériences de simulation utilisant l'outil de simulation ns2.

Les auteurs de [58] évaluent les performances de l'algorithme TSCH-CA dans des conditions de canal non idéal. Les expressions des différentes métriques de performance qui incluent la probabilité de retransmission, le taux de perte de paquets de données, la fiabilité, la consommation d'énergie, le débit normalisé et le délai d'accès moyen ont été obtenues et la précision de l'analyse a été vérifiée par des simulations de Monte Carlo. Dans [59], les auteurs ont proposé d'utiliser plusieurs parents de source temporelle pour améliorer la synchronisation du réseau TSCH. Les auteurs de [60] ont présenté une analyse de DSME et TSCH MAC et l'ont principalement comparé avec le MAC IEEE 802.15.4 via une chaîne Markov. En outre, les auteurs ont analysé le compromis entre le choix d'un mode MAC particulier par rapport aux autres.

2.9 IEEE 802.15.4f-2012

L'amendement IEEE 802.15.4f-2012 [61] approuvé le 20 avril 2012, spécifie deux couches PHY alternatives en plus de ceux de l'IEEE 802.15.4-2011 précédemment cités. Ces PHY prennent en charge les performances et la flexibilité nécessaires pour les futurs déploiements massifs de systèmes RFID (Radio Frequency Identification) actifs et autonomes hautement peuplés partout dans le monde [61]. Un système RFID actif comprend un certain nombre d'étiquettes de transmission uniquement. Dans la norme IEEE 802.15.4f-2012, le paquet transmis périodiquement doit contenir une petite quantité de données et un identifiant unique.

Dans cette version, un RFD peut fonctionner en tant qu'un simple dispositif, un dispositif de transmission à fonction réduite uniquement RFD-TX (Reduced Function Device-Transmit Only) ou un dispositif de réception à fonction réduite uniquement RFD-RX (Reduced Function Device-Receive Only) [61]. Le réseau WPAN de IEEE 802.15.4f-2012 comprend au moins un FFD, fonctionnant en tant que coordinateur PAN ou au moins un RFD-RX fonctionnant en tant que point de terminaison pour les communications RFD-TX [61].

Les deux alternatives PHYs spécifiés dans cet amendement sont présentés dans le tableau 2.1.

TABLE 2.1 – Spécifications PHY de la norme IEEE 802.15.4f

PHY (MHz)	Bande de fréquence (MHz)	Technique de modulation	Débit de donnée (kb/s)	Nombre de canaux
433 MSK	433.05-434.79	MSK	31.25, 100, 250	15
2450 MSK	2400-2483.5	MSK	250	42
LRP UWB	6.2896-9.1856	OOK avec PPM	31.25, 100, 250	3

2.10 IEEE 802.15.4g-2012

Cet amendement a été apporté le 27 avril 2012 pour les réseaux utilitaires SUN (Smart Metering Utility Networks) qui spécifie des PHY alternatives en plus de ceux de la norme IEEE 802.15.4-2011 [62]. La norme IEEE 802.15.4g-2012 a défini un schéma de gestion multi-PHY MPM (Multi-PHY Management) spécifié pour les réseaux SUN afin d'atténuer les interférences ou, en d'autres termes, de faciliter la coexistence inter-PHY. Ce qui signifie que plusieurs et différents PHY SUN peuvent fonctionner au même endroit et dans la même bande de fréquences [62].

2.10.1 Spécifications PHY

Trois couches physiques alternatives sont fournies pour les appareils SUN. Les appareils SUN prennent principalement en charge les applications extérieures, à faible débit de données et sans fil dans plusieurs domaines réglementaires. Des trames physiques d'un minimum de 1500 octets peuvent être transmises sans aucune fragmentation.
Les couches physiques alternatives de SUN fonctionnent à plusieurs débits de données pour prendre en charge les applications SUN dans des bandes allant de 169 MHz à 2450 MHz comme suit :

- Multi-Rate and Multi-Regional Frequency Shift Keying (MR-FSK) PHY : fournit une bonne efficacité de puissance d'émission grâce à l'enveloppe constante du signal d'émission. L'alternative MR-FSK PHY spécifié fonctionne dans de nouvelles bandes de fréquences que celles définies précédemment à savoir 868 MHz, 915 MHz, 780 MHz, 950 MHz et 2450 MHz.
  Les nouvelles bandes de fréquences pour le MR-FSK PHY sont données dans le tableau 2.2, avec leurs débits de données associés, la région où elles fonctionnent et le nombre de canaux disponibles. Le schéma de modulation est soit Filtered 2FSK soit Filtered 4FSK. Notons que la numérotation des canaux $i/j/k/z$ signifie que le nombre de canaux est i (j,k,z) lorsque le mode utilisé est le mode 1 (mode 2, mode 3 ou mode 4), respectivement. Certaines bandes de fréquences fonctionnent soit en mode 1 et mode 2 de FSK, soit en mode 1, mode 2 et mode 3

TABLE 2.2 – Spécifications PHY de IEEE 802.15.4g MR-FSK

MR-FSK PHY (MHz)	Bande de fréquence (MHz)	Débit de données (kb/s)	Région	Nombre de canaux
169	169.4-169.475	4.8/2.4/9.6	Europe	6/6/6
450	450-470	9.6/4.8	États Unis	1599/1599/.
470	470-510	50/100/200	Chine	199/99/199
780	779-787	50/100/200	Chine	39/19/19
863	863-870	50/100/200	Europe	34/17/17
896	896-901	10/20/40	États Unis	399/397/393
901	901-902	10/20/40	États Unis	79/77/73
915	902-928	50/150/200	Europe	129/64/64
917	917-923.5	50/150/200	Corée	32/16/16
920	920-928	50/100/200/400	Japon	38/18/12/12
928	928-960	10/20/40	US	2559/2557/2553
950	950-958	50/100/200/400	Japon	7279/7277/7273
1427	1427-1518	10/20/40	États Unis	33/16/11/11
2450	2400-2483.5	50/150/200	États Unis	416/207/207

de FSK. Tandis que d'autres fonctionnent en plus des modes 1, 2 et 3 de FSK en mode 4 de FSK comme décrit dans le tableau 2.2 .

- Multi-Rate and Multi-Regional Orthogonal Frequency Division Multiplexing (MR-OFDM) PHY : fournit des débits de données plus élevés allant de 50 kb/s à 800 kb/s avec une efficacité spectrale plus élevée.

  Les nouvelles bandes de fréquences pour l'alternative MR-FSK PHY sont données dans le tableau 2.3 avec leur région associée et le nombre des canaux disponibles. Les schémas de modulation utilisés sont BPSC, QPSK et la modulation QAM (Quadrature Amplitude Modulation). Notons que la numérotation des canaux $i/j/k/z$ signifie que le nombre de canaux est i (j, k, z) lors de l'utilisation de l'option 1 (2, 3 ou 4) de l'OFDM, respectivement.

- Multi-Rate and Multi-Regional Offset Quadrature Phase-Shift Keying (MR-O-QPSK) PHY : partage les caractéristiques de l'alternative physique O-QPSK de l'IEEE 802.15.4-2011, rendant les systèmes multi modes plus rentables et plus faciles à concevoir.

  Les MR-O-QPSK PHY sont spécifiés dans le tableau 2.4 avec leur région associée et le nombre de canaux disponible. Le schéma de modulation utilisé est O-QPSK. En plus du mode d'étalement DSSS, un mode d'étalement alternatif nommé MDSSS (Multiplexed Direct Sequence Spread Spectre) est défini dans cette PHY. Les débits de données pris en charge

TABLE 2.3 – Spécifications PHY de IEEE 802.15.4g MR-OFDM

MR-OFDM PHY (MHz)	Bande de fréquence (MHz)	Région	Nombre de canaux
470	470-510	Chine	./../199
780	779-787	Chine	6/9/19/39
863	863-870	Europe	5/8/17/34
915	902-928	États Unis	20/31/64/129
917	917-923.5	Corée	5/8/16/32
920	920-928	Japon	6/9/19/39
950	950-958	Japon	./8/16/33
2450	2400-2483.5	États Unis	64/97/207/416

TABLE 2.4 – Spécifications PHY de IEEE 802.15.4g MR-O-QPSK

MR-O-QPSK PHY (MHz)	Bande de fréquence (MHz)	Région	Nombre de canaux
470	470-510	Chine	99
780	779-787	Chine	4
868	868-870	.	.
915	902-928	Europe	12
917	917-923.5	Corée	3
920	920-928	Japon	38
950	950-958	États Unis	16
2450	2400-2483.5	États Unis	16

dans MR-O-QPSK PHY sont compris entre 20 kb/s et 250 kb/s. Le DSSS est appliqué pour toutes les bandes de fréquences définies dans le tableau 2.4. Alors que pour les bandes 780 Mz, 915 MHz, 917 MHz et 2450 MHz, l'alternative SUN O-QPSK PHY peut prendre en charge l'autre facteur d'étalement MDSSS. La sélection du débit de données est spécifiée par la variable *RateMode* et le mode d'étalement, veuillez vous référer à [62] pour plus de détails.

2.10.2 Architecture MAC

Dans IEEE 802.15.4g-2012, la modification apportée à la sous-couche MAC est l'ajout d'une trame appelée EB (Enhanced Beacon) dans la structure de la supertrame définie dans la norme d'origine [62]. Cette trame contient des informations spécifiques de l'élément considéré IE (Information Element). MPM (Multi-Physical layer Management) est un protocole de gestion des interférences spécifié dans la norme IEEE 802.15.4g conçue pour les réseaux SUN. Il a été mis en œuvre pour résoudre le problème d'interférence potentiel dans les conceptions des couches physiques multiples (PHY) en utilisant un mode de signalisation CSM (Common Signaling Mode) [62].

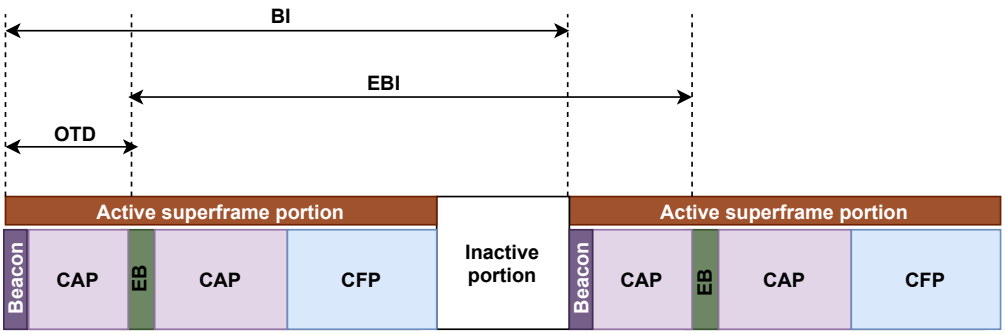


FIGURE 2.3 – Structure de la superframe de IEEE 802.15.4g

Notons que la procédure MPM peut être utilisée conjointement avec le mécanisme CCA pour assurer la coexistence.

Dans un PAN activé par balise (mode beacon), un dispositif SUN fonctionnant en tant que coordinateur doit transmettre un EB [62], en plus des balises périodiques habituelles décrites sur la figure 2.3. Cet EB est transmis à intervalles fixes en utilisant CSM. Alors que, dans un PAN non activé par balise (mode sans beacon), un coordinateur existant doit transmettre un EB périodiquement en utilisant le CSM.

2.10.3 Travaux connexes

Dans [63], la substance spécialisée de la norme IEEE 802.15.4g-2012 est spécifiée, ainsi que la manière dont elle peut être utilisée dans les réseaux de services publics intelligents. Les auteurs de [64] ont effectué un ensemble de mesures expérimentales en utilisant le système d'exploitation Contiki, à la fois dans des contextes ruraux et urbains, pour évaluer la portée de communication et le taux de livraison des paquets dans un environnement réel. Les auteurs de [65] ont résumé les systèmes de communication du réseau sans fil intelligent (Wi-SUN) et leurs spécifications PHY et MAC. En outre, les performances de transmission fondamentales des systèmes Wi-SUN dans la couche PHY et la couche MAC sont évaluées par des simulations informatiques. Dans [66, 67], une performance des appareils SUN basée sur la norme IEEE 802.15.4g-2012 est évaluée par des simulations. L'opération est réalisée à l'aide d'un prototype développé fonctionnant en bande japonaise. Dans [67], les auteurs examinent les performances du MR-OFDM multi-sauts dans le 802.15.4g en utilisant Qualnet pour les outils de simulation de la sous-couche MAC et Matlab pour la couche PHY. Le prototype de station de base nouvellement développé au Japon proposé dans [68], mesure les performances de transmission du système Wi-SUN basé sur IEEE 802.15.4g. Les performances

de transmission incluent l'indicateur de force du signal reçu RSSI (Received Signal Strength Indicator) et le taux d'erreur des paquets. Dans [69], des mesures de portée utilisant la totalité de la norme dans la bande 863–870 MHz, ont été effectuées pour examiner si IEEE 802.15.4g peut être utilisé pour fournir la connectivité pour les déploiements extérieurs.

2.11 IEEE 802.15.4j-2013

Apparu le 27 février 2013, l'amendement IEEE 802.15.4j-2013 [70] spécifie une alternative de la couche physique en plus de ceux des amendements précédents (IEEE 802.15.4-2011, IEEE 802.15.4e-2012, IEEE 802.15.4f-2012 et IEEE 802.15.4g-2012). La sous-couche MAC n'est pas pris en compte dans cet amendement.

Cette alternative PHY est spécifié pour la bande 2360-2400 MHz des réseaux médicaux MBAN (Medical Body Area Network). Les dispositifs MBAN fonctionnant dans cette bande sont conformes à un ensemble de règles, qui limitent l'utilisation de la bande à un usage médical uniquement sous la direction d'un professionnel de la santé [70]. Ces dispositifs doivent protéger tous les utilisateurs principaux et accepter d'éventuelles interférences de leur part [70].

Un coordinateur du réseau MBAN peut exiger que les appareils commutent leur canal et/ou la bande à un moment donné. Avant que l'appareil change ou commute le canal et/ou la bande à un certain moment, il doit informer les autres appareils des changements souhaités à l'aide d'un paramètre d'échange appelé IE.

2.11.1 Spécifications PHY

La norme spécifie une alternative PHY basée sur la technique DSSS à 2380 MHz utilisant une modulation O-QPSK fonctionnant dans la bande 2360 MHz-2400 MHz. O-QPSK PHY est obligatoire lors d'un fonctionnement dans la bande 2380 MHz. Le débit de données du O-QPSK PHY doit être de 250 kb/s. Où 15 canaux sont disponibles sur cette bande de fréquence.

2.11.2 Travaux connexes

Dans la littérature, une brève introduction de l'amendement IEEE 802.15.4j est présentée dans [71, 72]. Dans [73], les performances de IEEE 802.15.4j ont été évalué, en termes de délai et de consommation d'énergie par une méthode de simulation.

2.12 IEEE 802.15.4k-2013

Dans la norme IEEE 802.15.4k approuvée le 14 juin 2013 [3], deux extensions PHYs sont ajoutées pour prendre en charge les applications de surveillance des infrastructures critiques LECIM (Low Energy Critical Infrastructure Monitoring). De nouveaux protocoles MAC sont également mis en œuvre pour transmettre un paquet prioritaire (critique) dans les réseaux LECIM. L'amendement 802.15.4k sera détaillé dans le prochain chapitre.

2.13 IEEE 802.15.4m-2014

La norme IEEE 802.15.4m-2014 a été approuvée le 27 mars 2014 comme un amendement aux versions précédentes apparues entre 2011 et 2014 [74]. Cet amendement spécifie trois alternatives PHY pour prendre en charge principalement les applications de réseau TVWS (TV White Space) qui utilisent des appareils extérieurs, à faible débit et sans fil. Le réseau TVWS fonctionne dans une topologie d'arborescence de cluster, où chaque cluster utilise son propre canal. Ainsi, la collision entre les clusters est réduite [74]. Dans la norme IEEE 802.15.4m-2014, un nouveau périphérique FFD qui fonctionne comme le super coordinateur PAN noté SPC (Super PAN Coordinator), est ajouté [74]. Il a accès à la base de données de géolocalisation des réseaux TVWS, fournit à la fois des services de synchronisation pour le PAN de l'arbre de cluster multicanal TVWS noté TMCTP (TVWS Multichannel Cluster Tree PAN) et les informations de disponibilité des canaux aux autres coordinateurs PAN dans TVWS [74].

Chaque coordinateur PAN peut utiliser un canal différent attribué par ce SPC. Le réseau TMCTP fonctionne dans une topologie d'arborescence de cluster comprenant au moins un FFD, qui fonctionne en même temps comme coordinateur PAN, et comme super coordinateur PAN et d'autres dispositifs de type RFD et de simples dispositifs de type FFD.

2.13.1 Spécifications PHY

Les nouvelles alternatives PHY de TVWS proposées dans IEEE 802.15.4m-2014 prennent en charge plusieurs débits de données dans des bandes allant de 54 MHz à 862 MHz, comme suit :

- TVWS-FSK PHY prend en charge des débits de données allant de 50 kb/s à 400 kb/s. Les techniques de modulation utilisées sont FSK filtré à 2 niveaux (Filtred 2FSK) ou FSK filtré à 4 niveaux (Filtred 4FSK).

- TVWS-OFDM PHY prend en charge des débits de données allant de 390,625 kb/s à 1562,5 kb/s. Les techniques de modulation sont : BPSK, QPSK et 16-QAM (16 Quadrature Amplitude Modulation).
- TVWS-NB-OFDM (TVWS Narrow Band Orthogonal Frequency Division Multiplexing) PHY prend en charge des débits de données allant de 156 kb/s à 1638 kb/s. Les techniques de modulation utilisées sont : BPSK, QPSK, 16-QAM et 64-QAM (64 Quadrature Amplitude Modulation).

2.13.2 Architecture MAC

TVWS permet l'utilisation facultative d'une structure de supertrame dans un TMCTP où une nouvelle trame nommée BOP (Beacon Only Period) est ajoutée à la partie active de la supertrame définie dans IEEE 802.15.4-2011 [74]. Ainsi, la période active est composée des périodes CAP, CFP et BOP, comme illustré dans la figure 2.4. SD (Superframe Duration) est la durée de la supertrame

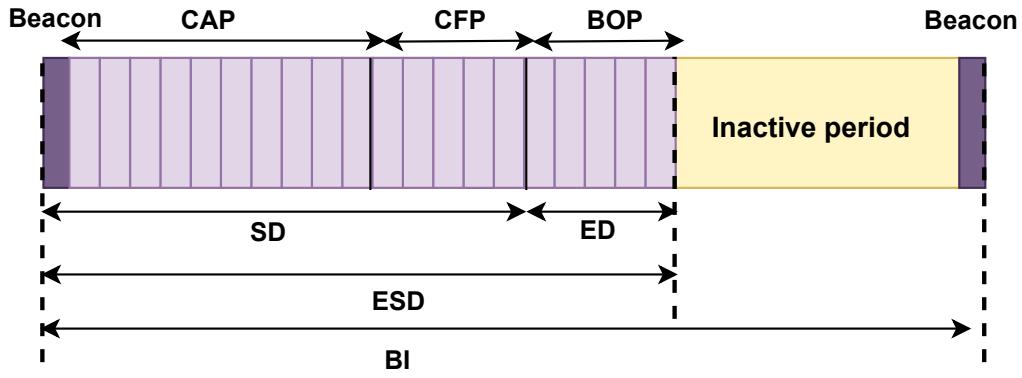


FIGURE 2.4 – Structure de la superframe IEEE 802.15.4m

et ESD (Extended Superframe Duration) est la durée de supertrame étendue. Le BOP est composé d'un ou plusieurs slots de balise dédiés DBS (Dedicated Beacon Slot) où chaque DBS est composé d'un ou plusieurs slots. DBS est utilisé pour communiquer des balises entre un coordinateur PAN parent (SPC) et l'un de ses coordinateurs PAN enfants (FFD) dans un TMCTP. Pendant le BOP, le coordinateur PAN enfant transmet des trames de balise au coordinateur PAN parent sur un canal dédié pendant le DBS.

Dans l'amendement IEEE 802.15.4m-2014, CSMA n'est pas utilisé pour les transmissions des balises. Dans TVWS, un mécanisme capable de réduire la consommation d'énergie et de maintenir des caractéristiques répondant aux exigences réglementaires en même temps est spécifié [74].

2.13.3 Travaux connexes

Pour répondre aux exigences réglementaires de IEEE 802.15.4m, les modifications de la canalisation, de l'architecture réseau et du moteur d'activation MAC sont nécessaires [75]. Alors que pour l'amélioration des performances, des modifications de la conception de la couche PHY et du mécanisme de commutation de bande MAC sont nécessaires. Dans [76], un aperçu sur la formation du premier LR-WPAN fonctionnant dans TVWS suivant la norme IEEE 802.15.4m est fourni. En outre, les principales forces motivant la communauté LR-WPAN à étendre sa bande opérationnelle au TVWS sont aussi présentées.

Les performances du protocole IEEE 802.15.4m peuvent être limitées en raison soit du nombre excessif de canaux et du balayage périodique des canaux, soit du balayage de plusieurs centaines de canaux par chaque appareil afin d'obtenir un message balise du coordinateur PAN comme présenté dans [77, 78]. Dans [79], une analyse de simulation est effectuée afin d'estimer la probabilité de collisions, l'effet du bruit de tir et des interférences en rafales. La simulation a été réalisée en C.

Un nouveau schéma coopératif de détection de spectre et un protocole conçu pour les réseaux IEEE 802.15.4m sont proposés dans [80]. La performance du schéma proposé est évaluée en termes de probabilité de détection et de débit pour un scénario réaliste en utilisant MATLAB.

2.14 IEEE 802.15.4p-2014

La norme IEEE 802.15.4p-2014 approuvée le 27 mars 2014 en tant qu'amendement des versions précédentes (2011 à 2014) est destinée à répondre aux besoins de l'industrie du transport ferroviaire [81]. Les communications et le contrôle ferroviaires RCC (Rail Communications and Control) sont des systèmes faisant référence à un système de communication sans fil utilisé pour les communications entre le véhicule ferroviaire et l'infrastructure fixe [81].

Le réseau de communication et de contrôle ferroviaire RCCN (Rail Communications and Control Network) fonctionne dans des topologies en étoile ou point à point. Il comprend un coordinateur PAN RCCN qui représente la station de base lorsqu'elle est disponible et un point final fixe ou mobile [81].

2.14.1 Spécifications PHY

Les nouvelles alternatives RCC PHY ajoutés doivent être utilisées dans des équipements destinés à répondre aux besoins de l'industrie du transport ferroviaire et à répondre aux exigences

réglementaires en Amérique et dans d'autres parties du monde comme suit :

- Les RCC LMR PHY prennent en charge la radio mobile terrestre LMR (Land Mobile Radio) fonctionnant dans la gamme de fréquences allant de 161 MHz à 928 MHz. Cinq schémas de modulation sont disponibles :
  - GMSK (Gaussian Minimum Shift Keying) offrant des débits de données de 9,6 kb/s ou de 19,2 kb/s ;
  - C4FM (Continuous four-level Frequency Modulation) offrant des débits de données de 9,6/19,2/38,4 kb/s ;
  - QPSK (Quadrature Phase Shift Keying) offrant un débit de données de 16/32 kb/s ;
  - $\frac{\pi}{4}$ DQPSK (Differential Quadrature Phase-Shift Keying) offrant un débit de données de 16/32/36 kb/s ;
  - La technique d'étalement de spectre DSSS (Direct Sequence Spread Spectrum) utilisant la modulation DPSK.
- RCC DSSS BPSK PHY fonctionnant dans les bandes de 4965 MHz, 2450 MHz et 5800 MHz offrant plusieurs débits de données pour une utilisation dans des applications RCC.

2.14.2 Architecture MAC

Dans la norme IEEE 802.15.4p-2014, les périphériques RCC prennent en charge la structure de supertrame RCCN [81]. La figure 2.5 illustre la supertrame RCCN, où des slots de gestion de liaison descendante (management downlink slots) et de gestion de liaison montante (management uplink slots) sont ajoutés dans la partie active entre la trame de balise et le début de la période CAP. Les slots de gestion de liaison descendante sont utilisés par le coordinateur PAN pour envoyer des

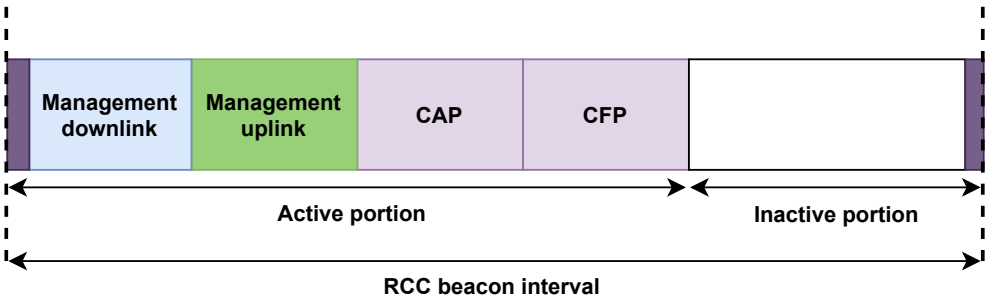


FIGURE 2.5 – Structure de la supertrame IEEE 802.15.4p-2014

trames aux points d'extrémité, tandis que les slots de gestion de liaison montante sont utilisés par les points d'extrémité pour envoyer des trames au coordinateur PAN.

Comme dans IEEE 802.15.4-2011, l'accès au canal est obtenu à l'aide de CSMA/CA [49] et éventuellement de CSMA/CA avec PCA défini dans IEEE 802.15.4k-2013 [3].

2.15 IEEE 802.15.4-2015

En tant que troisième révision de la norme IEEE 802.15.4-2003 et révision de IEEE 802.15.4-2011, la norme IEEE 802.1.4-2015 a été approuvée le 5 décembre 2015 [82]. Cet amendement visait à aborder divers domaines d'application cités dans les amendements précédents tels que, SUN, RCC, TVWS, LECIM, MBAN et RFID. Mais certaines de ces applications ont des exigences uniques qui nécessitent l'ajout d'éléments spécifiques qui sont absents dans les versions précédentes mais définis dans cette norme.

Dans IEEE 802.15.4-2015, le FFD peut fonctionner comme un coordinateur, un coordinateur PAN, un simple dispositif, un dispositif RFD-TX ou comme un dispositif RFD-RX. Alors que le RFD peut fonctionner comme un simple dispositif, un dispositif RFD-TX ou un dispositif RFD-RX.

2.15.1 Spécifications PHY

Plusieurs couches PHYs sont spécifiées dans cet amendement (voir le tableau 2.5) pour les différents espaces d'applications cités précédemment.

2.15.2 Architecture MAC

Pour l'accès au canal, la structure de la supertrame dépend du type du dispositif. Par exemple, lorsqu'un dispositif SUN est disponible, une trame de balise améliorée utilisant MPM est utilisée comme défini dans la section 2.10.

Dans cette version, pour l'accès au canal, les mécanismes spécifiés sont :

- CSMA/CA slotté (ou CSMA/CA non slotté) utilisé respectivement en mode beacon (ou mode sans beacon) ;
- TSCH CCA ;
- TSCH CSMA ;
- CSMA/CA avec PCA ;
- LECIM Aloha PCA.

TABLE 2.5 – Spécifications PHY de IEEE 802.15.4-2015

PHY	Bande de fréquence (MHz)	Modulation	Débit de données (kb/s)
DSSS	780, 868, 2380, 2450	O-QPSK	100, 250
DSSS	868, 915	BPSK	20, 40
PSSS	915	ASK, BPSK	250
CSS	2450	CSS avec D-QPSK	250, 1000
HRP UWB	sous gigahertz	BMP avec BPSK	100, 250
	$3 * 10^3 - 10 * 10^3$	BMP avec BPSK	100, 250
MPSK	780	MPSK	250
GFSK	920	GFSK	100
MSK	433, 2450	MSK	31.25, 100, 250
LRP UWB	780	OOK, PPM	31.25, 250, 1000
SUN FSK	169-2450	2-FSK, 4-FSK	revoir la section 2.10.1
SUN OFDM	470-2450	BPSK, QPSK, 16-QAM	50-800
O-QPSK	40-2450	O-QPSK	20-50
LECIM DSSS	470-2450	BPSK O-QPSK	/
LECIM FSK	169-921	FSK, GFSK, P-FSK, P-GFSK	/
TVWS FSK	54-862	2-FSK, 4-FSK	50-400
TVWS OFDM	54-862	BPSK, QPSK, 16-QAM	390.62-1562.5
TVWS NB-OFDM	54-862	BPSK, QPSK, 16-QAM, 64-QAM	156-168
RCC LMR	161-928	GMSK, C4FM, QPSK DQPSK, DPSK	390.62-1562.5
RCC BPSK	915, 2450, 4965, 5800	BPSK	20, 40

2.16 IEEE 802.15.4n-2016

L'amendement IEEE 802.15.4n-2016 [83] a été approuvé le 29 janvier 2016 par le ministère de l'Industrie et des Technologies de l'information MIIT (Ministry of Industry and Information Technology) de la République populaire de Chine. Il a été défini comme le premier amendement à la norme IEEE 802.15.4-2015 pour prendre en charge la transmission d'informations médicales.

Cette norme définit deux nouvelles alternatives PHY spécifiés pour la bande médicale CMB (China Medical Band). Les dispositifs fonctionnant dans les bandes CMB se conforment à un ensemble de règles, qui restreint l'utilisation de la bande à un usage médical uniquement sous la direction d'un professionnel de la santé [83] comme dans IEEE 802.15.4j-2013 [70]. La sous-couche MAC n'est pas spécifiée dans la norme IEEE 802.15.4n-2016. Les CMB PHY spécifiées présentées ci-dessous fonctionnent dans les bandes de fréquences 195 MHz (174-216 MHz), 416 MHz

(407-425 MHz) et 619 MHz (608-630 MHz).

- CMB O-QPSK PHY utilisant la modulation O-QPSK, offrant un débit de données obligatoire égal à 250 kb/s et un débit de données optionnel de 500 kb/s ;
- CMB GFSK PHY employant la modulation GFSK, offrant un débit de données obligatoire égal à 50 kb/s et des débits optionnels de 100 kb/s ou 200 kb/s.

2.17 IEEE 802.15.4q-2016

La norme IEEE 802.15.4q-2016 [84] a été approuvée le 27 janvier 2016 en tant que deuxième amendement à la norme IEEE 802.15.4-2015 [82] déjà amendée par IEEE 802.15.4n-2016 [83].

Les PHYs fournis dans cet amendement offrent des avantages de faible puissance pour une large gamme d'applications, y compris les étiquettes électroniques, les réseaux domestiques, les systèmes d'irrigation intelligents et les compteurs intelligents [84]. Deux extensions alternatives de la couche PHY sont spécifiées en plus des PHY déjà définies dans IEEE 802.15.4-2015. Elles sont spécifiées pour la bande de 2,4 GHz et plusieurs bandes sous gigahertz (169, 433, 450, 470, 780, 863, 896, 901, 915, 918, 917, 928 et 1427 MHz). Ces PHYs doivent pouvoir prendre en charge la transmission et la réception dans une ou plusieurs des bandes de fréquences déjà citées, en utilisant des débits de données multiples allant jusqu'à 1 Mb/s.

– TASK (Ternary Amplitude Shift Keying) PHY utilise un étalement de séquence ternaire suivi d'une modulation ASK. Elle permet la mise en œuvre d'émetteurs-récepteurs de faible complexité et prend en charge les communications dans des modes de réception à la fois cohérents et non cohérents. Par conséquent, elle permet un compromis entre la complexité du récepteur et les performances.

– RS-GFSK (Rate Switch Gaussian Frequency Shift Keying) PHY basée sur GFSK, utilisant un schéma de modulation GFSK à 2 (2-level GFSK) ou à 4 (4-level GFSK) niveaux. L'alternative RS-GFSK offre des avantages de faible puissance grâce à la disponibilité de débits de données plus élevés, à la réduction des frais généraux dans l'unité PPDU (PHY Protocol Data Unit) et au contrôle de la puissance de transmission. De plus, elle offre des options d'interopérabilité avec l'alternative SUN FSK PHY existante.

2.18 IEEE 802.15.4u-2016

La norme IEEE 802.15.4u-2016 [85] a été approuvée le 22 septembre 2016 en tant que troisième amendement à IEEE 802.15.4-2015 tel qu'amendé par IEEE 802.15.4n-2016 [83] et IEEE 802.15.4q-2016 [84]. Plusieurs recherches et rapports techniques développés en Inde sur M2M/IOT recommandent l'utilisation de bandes inférieures à 1 GHz. Par conséquent, cet amendement définit une nouvelle extension alternative SUN FSK PHY permettant l'utilisation de la bande 866 MHz en Inde [85].

Le tableau 2.6 décrit les informations sur l'alternative SUN FSK PHY spécifiée dans IEEE 802.15.4u-2016. Les débits de données et le nombre des canaux dépendant des techniques de modulation sont aussi donnés dans le tableau 2.6.

TABLE 2.6 – Spécifications PHY de IEEE 802.15.4u-2016

PHY (MHz)	Bande de fréquence (MHz)	Modulation	Débit de données (kb/s)	Nombre de canaux	Région
866	865-867	2-FSK mode 1	50	19	Inde
		2-FSK mode 2	100	10	
		2-FSK mode 3	150	10	

2.19 IEEE 802.15.4t-2017

La norme IEEE 802.15.4t-2017 [86] a été approuvée le 14 février 2017 en tant que quatrième amendement à IEEE 802.15.4-2015. Elle spécifie un débit de données supplémentaire pour le MSK PHY [86] défini dans la norme IEEE 802.15.4-2015 [82]. La nouvelle extension PHY ajoutée dans cet amendement est le FSK PHY fonctionnant dans la bande de 2450 MHz, utilisant la modulation GMSK. La nouvelle alternative 2450 MHz FSK PHY fonctionne dans la plage de 2400 à 2483,5 MHz et prend en charge un débit de données élevé égal à 2 Mb/s, ce qui n'a jamais été introduit auparavant dans les amendements précédents de la norme IEEE 802.15.4.
Un total de 16 canaux de fréquences sont disponibles dans la bande de 2400 à 2483,5 MHz.

2.20 IEEE 802.15.4v-2017

La norme IEEE 802.15.4v-2017 a été approuvée le 12 mai 2017 en tant que cinquième amendement à la norme IEEE 802.15.4-2015. Dans cet amendement, une mise à jour des exigences régio-

nales du 470-510 MHZ et du 863-870 MHz est développée [87]. Dans un autre cas, pour permettre l'utilisation des nouvelles bandes de fréquences que celles définies dans IEEE 802.15.4-2015 dans différents pays, les alternatives SUN PHY ont été modifiées dans cet amendement comme suit :

- SUN FSK PHY fonctionnant dans les bandes de fréquences définies dans le tableau 2.7. Le tableau présente aussi les différents pays de fonctionnement, les débits offerts et le nombre de canaux disponibles dans cette bande. Notons que le nombre de canaux $i/j/k/y/z$ signifie que le nombre de canaux est i (j, k, y, z) lors de l'utilisation du mode 1 (mode 2, mode 3, mode 4 ou mode 5), respectivement. Seul le 2-FSK est utilisé pour la modulation dans toutes ces bandes, contrairement au SUN FSK PHY défini dans IEEE 802.15.4g-2012 qui utilisait à la fois les schémas de modulation 2-FSK et 4-FSK [62].

TABLE 2.7 – Spécifications PHY de FSK IEEE 802.15.4v-2017

PHY (MHz)	Bande de fréquence (MHz)	Débit de données (kb/s)	Région	Nombre de canaux
470	470-510	50/100/150	Chine	199/**99**/**99**
863	863-870	50/100/150	Europe	69/**35**/**35**
867	866-869	50/100/150/200/300	Singapore	29/15/15/7/7
870	870-876	50/100/150	Europe	59/30/30
915-a	902-928	50/100/150/200/300	Amérique du nord	129/129/129/64/64
			Mexique	
915-b	915-928, 902-907.5	50/100/150/200/300	Brésil	91/91/91/45/45
915-c	915-928	50/100/150/200/300	Australie	64/64/64/32/32
			Nouvelle-Zélande	
915-d	915-921	50/100/150/200/300	Europe	29/29/29/15/15
915-e	915-918	50/100/150/200/300	Philippine	14/14/14/7/7
919	919-923	50/100/150/200/300	Malaisie	19/19/9/10/10
920-a	920.5-924.5	50/100/150	Chine	20/20/20
920-b	920-925	50/100/150/200/300	Hong Kong	24/24/24/12/12
			Singapour	
			Thaïlande	
			Vietnam	

- SUN OFDM PHY fonctionnant uniquement dans les nouvelles bandes de fréquences définies dans cet amendement (867 MHz, 870 MHz, 915-a MHz, 915-b MHz, 915-c MHz, 915-d MHz, 915-e MHz, 919 MHz, 920-a MHz et 920-b MHz). Les 470 MHz et 863 MHz ne sont pas pris en compte dans le SUN OFDM PHY.

- SUN O-QPSK PHY fonctionnant dans les mêmes bandes définies précédemment dans SUN OFDM PHY (voir le tableau 2.3). Le DSSS est appliqué pour toutes ces bandes de fréquences, tandis que pour les bandes 915 MHz-a, 915 MHz-b et 915 MHz-c, le SUN O-QPSK PHY peut prendre en charge un facteur d'étalement alternatif MDSSS, déjà introduit dans IEEE 802.15.4g-2012 (voir la section 2.10.1).

2.21 IEEE 802.15.4s-2018

La norme IEEE 802.15.4s-2018 [88] a été approuvée le 15 février 2018 en tant qu'un sixième amendement à IEEE 802.15.4-2015. Cet amendement améliore les fonctionnalités et améliore les performances du déploiement existant défini dans IEEE 802.15.4-2015 afin de réaliser la mesure et la gestion des ressources spectrales SRM (Spectrum Resource Measurement) pour les couches PHY et MAC [88].

Pour la gestion des ressources, un mécanisme normalisé est défini, pour permettre aux dispositifs PAN individuels de se coordonner entre eux. Cela leur permet également de fonctionner plus efficacement là où les appareils sont densément déployés dans des bandes de fréquences partagées sans licence, et où de fortes interférences pourraient limiter les performances globales [88]. Cet amendement permet de mesurer les ressources spectrales.

2.21.1 Spécifications PHY

Seule l'extension SUN O-QPSK PHY est utilisée dans cet amendement et aucune autre information sur la couche PHY n'est présentée.

2.21.2 Architecture MAC

Afin de sélectionner le meilleur PAN disponible pour le trunking et d'assurer une utilisation efficace du spectre radio pour le PAN sélectionné, la collecte d'une variété de données est essentielle pour évaluer les performances des liaisons radio. Cette collecte est possible grâce à la mesure des ressources spectrales SRM. En d'autres termes, SRM permet la mesure, la transmission et la demande d'informations concernant l'état du canal [88]. Dans les systèmes de communication sans fil, de fortes interférences à l'intérieur ou à l'extérieur du réseau peuvent se produire. Ainsi, des procédures et des fonctions ont été spécifiées par SRM pour le bon fonctionnement de ce type de systèmes. Les procédures SRM sont les suivantes :

1. Mesures de performance du réseau comme la détection d'énergie, le pourcentage de temps d'échec de la transmission et de la transmission différée, l'histogramme de la nouvelle tentative, l'utilisation du canal, l'histogramme du bruit, l'indicateur de puissance du canal reçu, l'indicateur du bruit du signal reçu et le délai d'accès moyen ;
2. Mesures des ressources spectrales ;
3. Signalisation : lorsque le mode beacon est pris en charge, les périphériques qui n'ont pas encore rejoint le PAN utilisent les trames beacon améliorées où le SRM IE est acheminé. Une fois les trames beacon reçues, l'appareil peut sélectionner le meilleur PAN puis le rejoindre ;
4. Contrôle de la puissance de transmission TPC (Transmission power control), qui améliore les performances des WPAN et minimise les interférences. Après avoir rejoint le réseau (c'est-à-dire après la procédure de signalisation), le dispositif peut spécifier la puissance d'émission pour les différents types de communication ;
5. Capture des mesures avec des éléments d'information et des structures de données ;
6. Collecte et échange d'informations de mesure de ressources spectrales avec les couches supérieures ou avec d'autres dispositifs avec contrôle de la couche inférieure ou de leurs applications ;
7. Demande/réponse SRM. Le SRM dans le dispositif demande à la couche supérieure d'obtenir des informations qui sont les attributs PIB, puis il répond ;
8. Rapport SRM. Un appareil envoie la commande SRM Report au coordinateur PAN périodiquement ou en fonction d'un événement ;
9. Informations SRM. La notification d'informations SRM peut être envoyée par la balise améliorée.

2.22 IEEE 802.15.4x-2019

La norme IEEE 802.15.4x-2019 [89] a été approuvée le 21 mars 2019 en tant qu'un septième amendement à la norme IEEE 802.15.4-2015. Le but de cet amendement est la prise en charge de débits de données allant jusqu'à 2,4 Mb/s pour l'extension SUN OFDM PHY définis précédemment dans la norme IEEE 802.15.4-2015 [82]. IEEE 802.15.4x OFDM PHY fonctionne dans les bandes de fréquences de 470 MHz, 780 MHz, 863 MHz, 866 MHz, 867 MHz, 870 MHz, 915 MHz, 915-a MHz, 915-b MHz, 915-c MHz, 915-d MHz, 915-e MHz, 917 MHz, 919 MHz, 920 MHz, 920-a MHz et 920-b MHz.

La bande de fréquences 917 MHz allant de 917 MHz à 923,5 MHz est définie uniquement dans l'amendement IEEE 802.15.4q-2016 [84], tandis que les autres bandes de fréquences sont définies dans IEEE 802.15.4v-2017 [87].

2.23 Rectificatif (Corrigendum)

Le premier rectificatif [90] a été approuvé le 15 février 2018 en tant qu'amendement à la norme IEEE 802.15.4-2015. Il contient des corrections substantielles d'erreurs, d'incohérences et d'ambiguïtés de la norme IEEE 802.15.4-2015.

À partir de l'étude réalisée dans ce chapitre, nous pouvons classer les versions du standard IEEE 802.15.4 en trois classes : la classe où les modifications ont été apportées sur la couche physique, les modifications sur la couche MAC ou la classe de versions qui ne sont qu'une révision des normes précédentes, comme indiqué dans le tableau 2.8.

TABLE 2.8 – Classifications des versions du standard IEEE 802.15.4

Classification	PHY	MAC	Révision
Versions			IEEE 802.15.4-2006
	IEEE 802.15.4a-2007	IEEE 802.15.4a-2007	
	IEEE 802.15.4c-2009		
	IEEE 802.15.4d-2009	IEEE 802.15.4d-2009	
			IEEE 802.15.4-2011
		IEEE 802.15.4e-2012	
	IEEE 802.15.4f-2012		
	IEEE 802.15.4g-2012	IEEE 802.15.4g-2012	
	IEEE 802.15.4j-2013		
	IEEE 802.15.4k-2013	IEEE 802.15.4k-2013	
	IEEE 802.15.4m-2014	IEEE 802.15.4m-2014	
	IEEE 802.15.4p-2014	IEEE 802.15.4p-2014	
			IEEE 802.15.4-2015
	IEEE 802.15.4n-2016		
	IEEE 802.15.4q-2016		
	IEEE 802.15.4u-2016		
	IEEE 802.15.4t-2017		
	IEEE 802.15.4v-2017		
	IEEE 802.15.4s-2018	IEEE 802.15.4s-2018	
	IEEE 802.15.4x-2019		

Comme illustré dans le tableau récapitulatif 2.9, nous avons mentionné toutes les versions existantes, leur date de ratification, leur débit maximum supporté, leurs schémas de modulation, les protocoles d'accès au canal utilisés et les types de réseau sur lesquels les appareils fonctionnent. Les caractéristiques de chaque norme sont citées, si elles existent.

TABLE 2.9 – Comparaison entre les standards IEEE 802.15.4

Versions	Date	Type de réseau	Débit max (kb/s)	technique de modulation	Protocole utilisé	Caractéristiques
802.15.4	2003	LR-WPAN	250	BPSK O-QPSK	CSMA/CA	Consommation d'énergie ultra-faible Faible débit de données Utilisation de la sécurité Coût très bas
802.15.4	2006	LR-WPAN	250	ASK O-QPSK BPSK	CSMA/CA	Amélioration de la sécurité La synchronisation des messages diffusés
802.15.4a	2007	LR-WPAN	1000	DQPSK BPM-BPSK	ALOHA	Utilisation simultanée du même canal de fréquence Gamme de précision Prise en charge des liaisons de longue portée
802.15.4c	2009	CWPAN	250	MPSK O-QPSK	/	/
802.15.4d	2009	LR-WPAN	100	BPSK GFSK	CSMA/CA	Coexistence d'écouter avant de parler Coexistence du contrôle de transmission Coexistence du cycle de service
802.15.4	2011	LR-WPAN	1000	Voir la section 2.7	CSMA/CA ALOHA	Modifications rédactionnelles et non techniques
						QoS, sécurité, bande passante

802.15.4e	2012	Industrial LR-WPAN	/	/	DSME LLDN TSCH	déterministe mais flexible Minimisation des collisions Évitement des interférences Multi-canaux, multi-supertrame Haute fiabilité du système
802.15.4f	2012	RFID	250	MSK OOK PPM	ALOHA	Autonomie de la batterie de plusieurs années, des communications fiables, des emplacements de précision
802.15.4g	2012	SUN	800	FSK BPSK QPSK QAM O-QPSK	CCA	Évitement des interférences Sécurité
802.15.4j	2013	MBAN	250	O-QPSK	/	Garder un schéma de canalisation flexible
802.15.4k	2013	LECIM	/	BPSK O-QPSK FSK GFSK P-FSK P-GFSK	CSMA/CA PCA ALOHA PCA	Réduction de la probabilité de collision Bonne efficacité de puissance d'émission Sensibilité plus élevée Priorité Correction d'erreur directe QoS, sécurité
802.15.4m	2014	TVWS	1638	FSK BPSK QPSK 16-QAM 64-QAM	/	Mécanisme de basse énergie Amélioration des performances
				GMSK C4FM QPSK	CSMA/CA	Prise en charge de fixe à fixe,

802.15.4p	2014	RCCN	36	$\frac{\pi}{4}$ DQPSK DPSK BPSK	CSMA/CA PCA	fixe vers mobile et communications mobile à mobile
802.15.4	2015	SUN MBAN RFID LECIM TVWS RCC	1000	Voir la section 2.15.1	TSCH CCA TSCH CSMA CSMA/CA PCA ALOHA PCA	Modifications rédactionnelles et non techniques
802.15.4n	2016	CMB	500	O-QPSK GFSK	/	Transmission d'informations médicales
802.15.4q	2016	/	jusqu'à 1000	GFSK ASK	/	Réduction de la consommation d'énergie, débits de données plus élevés, réduction supplémentaire de la la puissance de crête, compromis entre la complexité et les performances du récepteur
802.15.4u	2016	SUN	150	2-FSK	/	Utilisé pour des niveaux de puissance plus larges sans licence jusqu'à 4 W
802.15.4t	2017		2000	GMSK	/	Débit de données élevé
802.15.4v	2017	SUN LECIM TVWS	300	O-QPSK FSK OFDM	/	Activation des bandes régionales sous-gigahertz
802.15.4s	2018			/	/	Sélection du meilleur PAN disponible Spectre radio efficace
802.15.4x	2019	TVWS	jusqu'à 2400	FSK O-QPSK OFDM	/	Débit de données élevé

2.24 Conclusion

Dans ce chapitre, nous avons présenté un recueil historique de la norme IEEE 802.15.4, la norme la plus utilisée dans les réseaux de capteurs sans fil. La norme a été étendue pour gérer plusieurs types d'applications, telles que les applications industrielles et commerciales, la surveillance, le médical, les services publics intelligents, les communications ferroviaires, les étagères électroniques, l'irrigation intelligente et le comptage intelligent. Une description chronologique des amendements spécifiés par cette norme est présentée. Ces descriptions incluent les modifications apportées soit sur la couche physique, soit sur la sous-couche MAC.

Certains amendements sont proposés pour des pays spécifiques où la norme ne peut pas être utilisée avec les spécifications PHY des versions précédentes. Tandis que les améliorations de la couche MAC traitent de nombreux problèmes fréquentés par les réseaux de capteurs sans fil utilisant la version de base.

Dans cette thèse, nous allons nous intéresser particulièrement aux réseaux d'infrastructures critiques et à l'amendement IEEE 802.15.4k qui prend en charge la transmission des messages critiques dans ce type de réseaux. Un état de l'art sur cela fera l'objet du prochain chapitre.

Chapitre3

Les réseaux d'infrastructures critiques et la norme IEEE 802.15.4k

Sommaire

3.1 Introduction

Les progrès technologiques ont permis de fabriquer des capteurs à une échelle microscopique offrant une vitesse et une sensibilité nettement supérieures à celles des capteurs déjà existants. Leurs tailles et leur bas prix permettent alors de déployer des centaines, voire des milliers d'entre eux dans la zone à surveiller. Néanmoins, ces appareils ont des ressources limitées en termes de mémoire, de puissance de traitement et d'énergie. Par conséquent, pour faire face à ces limitations, des solutions doivent être conçues et mises en œuvre. Ainsi, la solution proposée est l'utilisation de la technologie de réseau de capteurs sans fil. Parmi les réseaux utilisant les appareils reposant sur les RCSFs, nous pouvons citer l'ensemble des grands réseaux indispensables au bon fonctionnement d'une société connue sous le nom des réseaux d'infrastructures critiques RICs.

Dans ce chapitre, nous allons dans un premier lieu donner une vue d'ensemble des réseaux d'infrastructures critiques. Par la suite, nous enchaînerons par leurs caractéristiques, leurs contraintes et exigences, ainsi que leurs domaines d'application. Dans un second lieu, nous présenterons la norme

IEEE 802.15.4k-2013 conçue pour ce type de réseaux, les protocoles MAC utilisés et une synthèse sur les travaux existants sur ses protocoles.

3.2 Les réseaux d'infrastructures critiques RIC

3.2.1 Définition

Étymologiquement, le mot infrastructure vient du mot latin infra-structura qui signifie « au dessous de la construction » et le mot critique vient du mot grec kritikos qui signifie « difficile, décisif » [91]. Selon le rapport de la commission de protection des infrastructures critiques [92], les RICs représentent les infrastructures, les systèmes, les services et les actifs, physiques ou virtuels, qui sont tellement vitaux où leur indisponibilité ou destruction aura un impact néfaste sur la sécurité nationale ou économique, la sûreté et la santé publique. Par exemple, les réseaux de communication sont intrinsèquement essentiels pour les interventions en cas de catastrophe et le contrôle du flux de trafic. Par conséquent, le renforcement et le maintien des systèmes d'infrastructures critiques sûrs et résilients sont un objectif national principal des États-Unis.

Les infrastructures critiques sont connues comme les constructions décisives pour une société en raison de leurs extension à de nombreux secteurs de l'économie, tels que les services financiers, de télécommunication, d'eau et d'égouts, de gaz et de pétrole, de transport et distribution (ferré, routier, aérien ou fluviaux), d'énergie, des services publics, de santé et d'urgences, d'approvisionnement alimentaire, des services de sécurité et des services gouvernementaux essentiels [93].

3.2.2 Les exigences des RICs

La détection des défaillances et des attaques le plus tôt possible est parmi les priorités nationales pour les pays du monde entier. Pour cela la présence d'une technologie évolutive et peu couteuse répondant à ces exigences est indispensable. L'applications des RCSFs apparait comme la technologie potentielle car leur déploiement à une grande échelle est facile et leurs services sont rentables vu les périphériques peu coûteux dont ils disposent. De plus, ils offrent une capacité importante de survie de capteurs dans les situations critiques et fournissent des informations suffisantes sur l'infrastructure critique afin de lancer le processus de récupération lors des pannes et attaques. Parmi les exigences des RICs, nous pouvons citer :

3.2.2.1 L'interopérabilité

L'interopérabilité est expliquée par la capacité des systèmes et des organisations à travailler ensemble impliquant divers aspects sociaux, techniques, politiques et organisationnels, qui jouent tous un rôle essentiel dans la continuité des activités en vue d'atteindre un objectif commun.

3.2.2.2 La scalabilité et l'extensibilité

La scalablilité fait référence à la possibilité d'ajouter ou de supprimer des ressources matérielles tandis que l'extensibilité est liée à la capacité d'étendre ou de modifier les ressources logicielles du système. Le respect des constructions techniques et juridiques telles que les politiques, les normes, les recommandations et les bonnes pratiques est primordiale avant l'ajout ou la modification des ressources. Et cela pour garantir l'interopérabilité et la compatibilité avec les ressources déjà existantes à condition que les nouvelles ressources n'entrainent pas des modifications dans les services fournis par le système critique.

3.2.2.3 Fiabilité et disponibilité

La disponibilité et la fiabilité sont deux concepts étroitement liés. La disponibilité correspond à la probabilité qu'un système fournisse des services quand ils sont requis à n'importe quel instant t, $t \in [t_1, t_2]$. En revanche, la fiabilité correspond à la probabilité qu'un système puisse fournir des services correctement et que leur disponibilité ne diminue pas pendant la période $[t_1, t_2]$.

Cette relation entre les deux propriétés signifie que si un système de contrôle doit effectuer certaines opérations pour exécuter des commandes (par exemple, ouvrir ou fermer une vanne), la séquence normale d'exécution de l'infrastructure d'information et des objets intermédiaires ne doit pas être interrompue ou retardée. Sinon, les services fournis par le système sous-jacent ne seront pas disponibles au moment opportun et le système ne sera donc pas fiable.

3.2.2.4 Résilience et robustesse

La résilience et la robustesse sont des propriétés qui aident à faire face à des situations adverses ou menaçantes. En règle générale, un système sous menace devrait garantir sa fonctionnalité à tout moment, même si certaines parties du système sont sérieusement compromises. Si une telle panne ou menace n'est pas contrôlée correctement, cela peut traverser les limites d'un système critique et, à terme, nuire à la continuité des activités d'autres infrastructures critiques.

3.2.2.5 Sécurité critique

Les aspects critiques pour la sécurité doivent être pris en compte afin de contrôler les effets en cascade. La propriété de la criticité de sécurité implique d'éviter ou d'atténuer la propagation d'effets entre les infrastructures critiques, sachant que ces propagations pourrait entraîner des dommages physiques et physiologiques, des blessures et même la mort. Pour éviter que de telles situations ne se produisent, les réseaux de contrôle devraient incorporer des approches autonomes, dynamiques et intelligentes et assurer la prévention et la réaction de manière efficace et rapide.

3.2.2.6 Convivialité

Tout utilisateur (expert ou non) doit pouvoir interagir avec un système via une interface intuitive. Cela signifie que les interfaces doivent être conçues pour faciliter la compréhension des informations (telles que les alarmes et les lectures de capteurs) et pour faciliter les options permettant d'accélérer les opérations critiques (telles que la gestion des actions sur le terrain).

3.2.2.7 Qualité de service

La qualité de service est également une propriété importante, car une perturbation ou une altération du système due à des pannes, des incidents, des erreurs ou des menaces pourrait compromettre les performances de toute une infrastructure. Pour développer une stratégie de qualité de service adaptée aux systèmes critiques, il est conseillé de prendre en compte des paramètres supplémentaires, tels que le niveau d'hétérogénéité, la nature variable et l'interactivité de l'environnement, la topologie du réseau, les faiblesses associées aux objets, ainsi que les interdépendances entre les nœuds et les systèmes. Cela permettrait d'ajuster les paramètres essentiels et de concevoir des infrastructures robustes capables de contrôler les défaillances et les incidents.

3.2.2.8 Collaboration

La collaboration entre objets est essentielle dans des environnements hétérogènes. Par exemple, tout objet actif dans un système doit savoir comment collaborer avec d'autres objets de manière sécurisée et transparente et comment effectuer ses tâches.

3.2.2.9 Autonomie et auto-réparation

Plus l'autonomie pour la gestion des anomalies est présente, plus grande est la probabilité que les entités opérationnelles puissent lancer une réponse rapide et efficace aux situations d'urgence.

De plus, cette réponse devrait être automatisée lorsque des parties du système sont dispersées dans des emplacements distants avec un contrôle local minimal ou nul, tel que des sous-stations.

La notion d'auto-réparation trouve ses origines dans la recherche sur les systèmes à tolérance aux pannes. Un système d'auto-réparation peut gérer des défauts transitoires ou permanents par des actions locales et individuelles et atteindre un état acceptable. Afin de parvenir à la tolérance aux pannes, il est nécessaire de traiter les problèmes liés à la redondance, à la coordination et à l'auto stabilisation. Pour y parvenir, la coordination doit être soutenue par des mécanismes de synchronisation fondés sur des politiques d'actionnement régulant toutes les actions entre entités.

3.2.3 Les réseaux de surveillance des infrastructures critiques à faible consommation d'énergie LECIM

Les réseaux de surveillance des infrastructures critiques à faible consommation d'énergie LECIM (Low Energy Critical Infrastructure Monitoring) nécessitent une consommation d'énergie extrêmement faible, une longue durée de vie de déploiement, une scalabilité, une fiabilité, une robustesse et une sécurité optimale. Le faible besoin en énergie est dû au fait que les nœuds de capteurs utilisés dans de tels réseaux sont situés dans des endroits très éloignés où le secteur n'est pas disponible. Ces capteurs fonctionnent dans des environnements de propagation extrêmement difficiles, notamment des villes, des zones rurales, des forêts, des montagnes et des lieux de surveillance souterrains ; et ils sont censés travailler pendant plusieurs années sans intervention humaine.

Des méthodes de surveillance périodiques, basées sur des événements ou sur des requêtes sont utilisées. Les nœuds de capteur rapportent des informations de mesure ou d'état dans un intervalle de quelques minutes à plusieurs heures. Certains événements ou changements d'état détectés dans le système peuvent être sensibles au temps, alors les capteurs de détection les signalent en cas d'urgence. Les applications LECIM, en général, nécessitent un grand nombre de points de terminaison, une capacité de diffusion/multi-diffusion, un fonctionnement à très basse énergie, une infrastructure faible, une faible sensibilité du récepteur et un environnement de communication simple et peu coûteux.

3.2.3.1 Caractéristiques des réseaux LECIM

Les principales caractéristiques de LECIM et leur brève description sont énumérées ci-dessous [94], [3].

– **Différence extrême entre les périphériques du réseau**. Le coordinateur PAN et les capteurs

sont les composants des réseaux LECIM. Le coordinateur dispose de capacités beaucoup plus performantes et d'un plus grand apport d'énergie que les capteurs. Pas de mobilité pour les capteurs alors que le coordinateur a une portabilité limitée.

- **Infrastructure minimale**. Le réseau utilise une topologie en étoile pour prendre en charge la communication entre le coordinateur et les nœuds capteurs. À l'exception du coordinateur PAN, tous les nœuds de capteur ne sont pas alimentés par le secteur. Les dispositifs d'extrémité ne peuvent pas communiquer entre eux, et ils peuvent communiquer avec le coordinateur soit directement, soit via le relais PAN.
- **Réseau mis en service**. Les périphériques de ce type de réseau sont configurés pour un réseau spécifique avant le déploiement. De plus, les périphériques sont pré configurés avec des paramètres qui évitent les messages de configuration inutiles.
- **Zone de couverture étendue**. Un réseau LECIM est principalement conçu pour les environnements extérieurs. Les capteurs sont très dispersés et leur portée peut varier de quelques mètres à plusieurs kilomètres. Par conséquent, un réseau LECIM est tolérant à une latence élevée de données (peut être en secondes), à une sensibilité élevée du récepteur et une robustesse aux interférences, et fournit une communication fiable sur un support de propagation en pleine mutation.
- **Faible énergie**. Une fois déployé, le réseau devrait fonctionner pendant plusieurs années sans remplacer les piles de capteurs ni effectuer de maintenance. Les capteurs doivent pouvoir conserver leur énergie limitée. Pour ce faire, LECIM utilise différents mécanismes d'économie d'énergie.
- **Bas débit de données**. Collecter des données planifiées et événementielles, qui sont souvent rares, par les capteurs est l'objectif d'un réseau LECIM. Par conséquent, le débit de données de l'application est limité à moins de 40 kb/s.
- **Coût bas**. Les systèmes LECIM nécessitent des coûts opérationnels faibles (spectre sans licence ou légèrement sous licence), des coûts d'installation faibles, ainsi que des coûts d'infrastructure et de maintenance faibles.
- **Flux de données asymétrique**. La communication sur la liaison montante domine le flux de données avec des besoins limités en données sur la liaison descendante.
- **Adressage**. Les réseaux LECIM peuvent traiter des milliers de nœuds de capteurs connectés.
- **Utilisation dans le monde entier**. De tels réseaux doivent fonctionner dans tous les domaines

réglementaires. La puissance de transmission est faible et conforme à la réglementation internationale.

– **La complexité**. Les réseaux LECIM ont une structure complexe. A titre d'exemple, les réseaux de pipelines de pétrole et de gaz naturel (GN) acheminent le carburant jusqu'aux centrales électriques. Ces réseaux de pipelines comprennent des compresseurs de gaz naturel, des usines de traitement du gaz, des terminaux GN et d'autres sous-systèmes. Ces sous-systèmes complexes sont constitués de données à grande échelle, ce qui est très utile pour analyser les infrastructures critiques.

– **La dynamique**. Les réseaux LECIM sont également très dynamiques. Plusieurs incidents peuvent provoquer une défaillance des réseaux d'infrastructures. Par exemple, une panne d'alimentation, une catastrophe naturelle ou d'origine humaine qui affecte le réseau dans différents états de fonctionnement, variant avec le temps.

3.2.3.2 Domaines d'application des réseaux LECIM

Les RICs sont exploités dans plusieurs domaines d'application que nous pouvons classer en trois catégories [95, 96], comme suit :

a) Surveillance de l'infrastructure

- **Détection des fuites d'eau**. Dans le monde, il y a une pénurie d'eau douce. L'eau est une ressource naturelle rare et souvent trouvée loin de là où elle est utilisée. Elle nécessite un transport de l'alimentation aux consommateurs à l'aide de conduites d'eau. Des dommages au niveau des tuyaux provoquant des fuites d'eau sont très probables. Par conséquent, la détection de ses fuites par ces capteurs en un temps limité est très recommandée. La solution pour remédier à ce problème est de surveiller à distance les systèmes d'exploitation qui sont installés sous terre.

  Le système de surveillance se compose des capteurs qui informent le système de contrôle de l'état de la conduite en envoyant des courts messages de données une fois par jour, ou en envoyant des messages d'alarme en cas de détection d'une fuite. Les avantages des RCSFs dans ce cas sont : la longue portée, la capacité de pénétrer dans les voûtes souterraines, le grand nombre de capteurs déployés sous terre et les faibles coûts d'installation et de maintenance.

- **Surveillance des égouts** [97]. Les installations de traitement des eaux usées constituent une partie importante d'une infrastructure urbaine. Les gouvernements municipaux mettent en place des installations de collecte et de traitement des eaux usées. Ces installations traitent

quotidiennement des millions de gallons d'eaux usées. Leur objectif principal est de veiller à la qualité et à la quantité des eaux usées collectées dans le système de collecte et à atteindre les installations de récupération.

Dans le cas où la surveillance ne se produit pas correctement, des milliers de gallons d'eau coulant sous terre peuvent entraîner un débordement des égouts sanitaires. Par conséquent, une solution intelligente est nécessaire pour la détection et la prévention en temps opportun de toute catastrophe survenant en raison d'une surveillance inefficace des eaux usées. Une technologie de communication souterraine sans fil en utilisant des capteurs est utilisée pour détecter les fuites et les blocages de manière proactive et renvoyer ces données d'événements à une salle de contrôle centrale.

- **Surveillance de l'intégrité des ponts et structures**. Les ponts font partie du réseau routier national. Les maintenir à un niveau de performance élevé induit la sécurité publique, la productivité économique et sa croissance. Par conséquent, les ponts et les structures doivent être inspectés régulièrement pour détecter le plus vite possible les fissures ou les fractures dès leur apparition. Une surveillance efficace de l'état des ponts peut être effectuée à l'aide des RCSFs.

  Les capteurs sont installés sur les parties critiques du pont et sont utilisés pour rapporter des informations de mesure ou d'état sur de longues périodes. Chaque fois qu'un dommage ou une fracture survient dans le pont, tous les capteurs qui détectent l'incident envoient simultanément des messages d'urgence au système de contrôle afin que les actions de correction soient prises à temps.

- **Systèmes de contrôle de l'éclairage public**. Le système de contrôle et de gestion de l'éclairage à distance est un système qui permet de maintenir sous contrôle permanent le réseau d'éclairage public, et ce jusqu'à chaque point lumineux et ne nécessite pas d'intervenir sur l'équipement existant. Ce système permet à un seul opérateur d'effectuer les opérations qui requièrent normalement un nombre important de personnel et de moyens. De plus, ce système permet de réaliser des économies notables sur les coûts d'énergie et de maintenance tout en garantissant un niveau très élevé de fiabilité, de continuité et de qualité de service.

  Cela est devenu possible grâce à la simple connexion d'un dispositif électronique en série à la ligne d'alimentation qui permettra de vérifier les conditions de fonctionnement de chaque lampe : lampe allumée ou éteinte ; lampe fonctionnant en pleine puissance ou en puissance réduite ; lampe en perte de puissance (clignotante) ; lampe en court-circuit ; fusible en panne ;

et absence de courant (circuit lampe non connecté).

- **Indicateurs de circuit de défaut** [98]. Un indicateur de défaut est un dispositif qui fournit une indication visuelle ou à distance d'un défaut sur un système d'alimentation électrique. Il permet de surveiller un système, d'identifier un défaut qui s'est produit et d'identifier le type du défaut ainsi que son emplacement. La détection des défauts joue un rôle important dans les processus coûteux et critiques pour la sécurité. La détection précoce des défauts de processus peut aider à éviter une progression anormale des événements et réduire le temps de recherche des défauts afin que l'alimentation électrique puisse être rapidement rétablie après l'isolation d'un défaut.
- **Surveillance des sols**. Au cours des dernières décennies, la surveillance des sols est devenue de plus en plus importante. Les facteurs environnementaux, tels que le changement climatique, la diminution des ressources en eau et les habitats menacés conduisent à la nécessité de surveiller l'environnement et de mettre en œuvre de meilleures politiques pour le protéger. Des capteurs doivent être installés dans le sol une fois la culture plantée et retirés à la fin de la saison.

  Les capteurs de surveillance de l'état du sol permettent aux agriculteurs de collecter des données sur les précipitations, la température, l'humidité, la poussière, la production de biocarburants, la phytoremédiation, la recharge des réservoirs à partir du manteau neigeux, les séquestrations du carbone dans le sol, les hydrologies des bassins versants, la recherche par satellite au sol, les études de glissements de terrain au fil du temps pour suivre les tendances et prévoir les besoins en irrigation.
- **Surveillance des pipelines de pétrole et de gaz**. Les pipelines de pétrole et de gaz sont d'une grande importance pour le transport du pétrole et du gaz. Ils sont déployés dans les villes, les banlieues et les zones très reculées en surface ou sous terre. La surveillance des pipelines améliore la conformité, la protection de l'environnement, la protection contre les dommages et le vol, la réduction des coûts de remboursement et la fiabilité. Les capteurs installés sur les tuyaux signalent au système de contrôle un problème qui survient avec des courts messages de données programmés ou déclenchés par des événements. Ces problèmes peuvent être des fuites, une forte pression ou vibration, des corrosions ou un incendie dans les tuyaux.

b) Suivi des transports et des actifs

- **Suivi des transports publics** [99]. Les transports publics sont un moyen de transport rapide et pratique, mais il y a de nombreux problèmes qui y sont liés. Les défis du système de transport

public actuel sont les suivants : comment estimer l'heure d'arrivée exacte du véhicule ? et comment suivre réellement son déplacement ?. Le suivi des véhicules nécessite généralement la collecte des données en temps réel, en utilisant un système de positionnement global (GPS), des capteurs, des appareils Internet des objets (IoT), etc.

Après la collecte, l'étape suivante est celle d'analyse et du pré-traitement des données collectées. À ce stade, le système GPS, les capteurs ou les appareils Internet des objets essaient de supprimer le bruit, les valeurs manquantes et la correction des arrêts de bus. Après cela, ils prennent ces données affinées et prédisent l'heure d'arrivée du bus. La procédure de prévision de l'heure d'arrivée comprend le calcul de la vitesse par emplacement et le calcul de la vitesse par tranche de temps. Le capteur envoie la vitesse, l'emplacement, l'horodatage du glissement de la carte et l'embarquement et la descente des passagers.

- **Surveillance des conteneurs** [100]. Le système de suivi des conteneurs permet de déterminer la position actuelle des conteneurs sur la carte du monde. L'application utilisée calcule le temps de stockage dans les ports de transbordement et informe instantanément l'utilisateur de tout retard. Un processeur est utilisé pour recevoir à plusieurs reprises des demandes de suivi, envoyer les demandes à un système informatique de transporteur de conteneurs et recevoir des réponses pour créer plusieurs enregistrements dans une base de données du système de suivi de conteneurs. La base de données comprend plusieurs identifiants d'expédition associés à plusieurs identifiants de conteneurs et associés à d'autres données de suivi des conteneurs.
- **Surveillance de l'état des voies ferrées** [101]. L'industrie ferroviaire a un impact considérable sur l'économie et la consommation d'énergie du pays. La surveillance de l'état de la voie est fondamentale et essentielle pour garantir la sécurité, la fiabilité et la rentabilité des opérations ferroviaires. Les chemins de fer sont obligés d'inspecter et de surveiller toutes les voies en service aussi souvent que deux fois par semaine afin de répondre aux besoins croissants d'amélioration de la sécurité, d'exploitation ferroviaire fiable et à faible coût.

  Pour l'industrie ferroviaire, le processus de surveillance employant des capteurs embarqués sur un véhicule ferroviaire consiste à identifier les défauts, à comprendre leurs causes et à prédire leur occurrence en identifiant et en caractérisant les irrégularités de la voie. Aussi, une inspection de la piste est utilisée pour accumuler des données sur la géométrie de la piste grâce aux technologies de mesure telles qu'un véhicule d'enregistrement de piste ou le transport d'un autocar d'enregistrement de piste.

- **Surveillance de la congestion du trafic** [102]. L'augmentation de la densité du trafic ainsi que la croissance démographique dans le monde ont entraîné de plus en plus de routes encombrées, de pollution atmosphérique et d'accidents. La croissance du nombre total de véhicules dans le monde a augmenté de façon exponentielle au cours de la dernière décennie. La surveillance du trafic dans ce scénario est certainement un grand défi. Un système de surveillance du trafic doit s'attaquer à des problèmes, tels que les embouteillages, la détection des accidents, l'identification/détection des véhicules, le guidage automatique des véhicules, la signalisation intelligente, la criminalistique, la densité du trafic, la circulation sécuritaire des piétons, le transit des véhicules d'urgence, etc.

  Un système de surveillance du trafic idéal peut être conçu en utilisant des réseaux de capteurs de véhicules où les dispositifs de détection attachés aux véhicules en mouvement se déplacent dans toute la ville pour collecter les informations sur le trafic. Ces dispositifs de détection en mouvement sont attachés les uns aux autres et au centre de surveillance du trafic également. Les informations collectées sont transmises au centre de surveillance du trafic urbain sur la base de communications sans fil de véhicule à véhicule ou de véhicule à infrarouge. Le centre de surveillance du trafic prend les décisions appropriées afin d'assurer une circulation sans tracas.

c) Sécurité et sécurité des personnes

- **Détection de gaz et de matières dangereuses** [103]. Les gaz nocifs pour l'homme à des concentrations définies sont qualifiés de gaz dangereux. Ces gaz ont des effets néfastes sur les organismes vivants et sur l'environnement. Parfois, la présence de gaz dangereux entraîne un incendie, cause des problèmes de santé et même la mort. Bien que la présence de certains des gaz toxiques ou de matières dangereuses puisse être détectée par leur odeur nauséabonde, la présence de ces gaz dans un espace confiné de manière scientifique en utilisant des dispositifs et des technologies électroniques nous aide à éviter les accidents et sauve des vies.

  Un dispositif de détection de gaz (ou de matières dangereuses) identifie la présence d'un gaz particulier (ou matières dangereuses particulières) et peut déclencher une alarme afin que les personnes concernées puissent prendre des mesures contre les fuites et avoir la possibilité de quitter les lieux si nécessaire. Chaque capteur est composé de deux parties : un récepteur de nature hautement spécifique qui améliore la sensibilité de détection et un transducteur qui assure la détection physique ou chimique.

- **Sécurité périmétrique** [104]. Les systèmes de détection d'intrusion de sécurité périmétrique traditionnels utilisent généralement des capteurs radar, infrarouge, micro-ondes ou photoélectriques pour détecter les intrusions. Après la détection et la collecte des informations sur les vibrations externes se produisant dans le système, un dispositif de traitement de signal est utilisé pour extraire et analyser les informations de vibration renvoyées par le câble optique de détection, et pour donner un signal d'alarme à temps lorsqu'un événement d'intrusion se produit.

  Le capteur à fibre optique présente des avantages exceptionnels de fonctionnement passif, une sensibilité élevée, une bonne fiabilité dans des conditions difficiles, une capacité longue distance, une immunité aux interférences électromagnétiques, une résistance à la corrosion, etc. En particulier, ce capteur n'a pas besoin d'alimentation électrique le long de la liaison par fibre optique. Il constitue donc un choix idéal pour les applications de longue ou de moyenne distance dans des environnements de terrain difficiles.

- **Surveillance aux frontières** [105]. La surveillance des frontières et la sécurité sont au cœur des préoccupations de tout pays. Pour maintenir la paix et assurer la sécurité des habitants d'un pays, les frontières doivent être surveillées 24h/24 et 7j/7. L'utilisation de technologies intelligentes modernes renforce la sécurité des frontières. Il est impératif de faire progresser ces technologies pour une meilleure sécurité. Les systèmes de surveillance des frontières à base de capteurs sont utilisés pour surveiller les événements qui se déroulent autour des frontières, et identifier si des activités suspectes sont en cours. Si quelque chose qui suscite des soupçons se produit alors, l'exécution d'un ensemble de tâches prédéterminées aura lieu. Il peut s'agir d'alerter les autorités concernées ou d'invoquer certains autres systèmes en réponse, comme un système d'alerte ou de combat.

  Les systèmes de détection des intrusions font partie intégrante de la surveillance des frontières. Ils sont conçus pour fonctionner dans un environnement hostile pour surveiller, détecter et suivre les intrus (cibles mobiles), 24 heures sur 24. Les principales menaces aux frontières peuvent être généralisées en trois types : les migrants non autorisés, les transports illégaux et les terroristes potentiels.

- **Suivi des premiers intervenants** [106]. Dans les cas d'opérations de sauvetage d'urgence, la sécurité des premiers intervenants est aussi importante que celle des personnes secourues. La possibilité de les suivre en temps réel dans des environnements intérieurs inconnus, contribuerait significativement au succès de leur mission ainsi qu'à leur sécurité. Leur suivi nécessite

un système de localisation et de navigation pour garantir des opérations de sauvetage sûres et sécurisées.

Être capable de suivre avec précision les premiers intervenants dans des environnements intérieurs en utilisant par exemple des véhicules aériens sans pilote, permet à un commandant de l'extérieur pour mieux visualiser et orienter ses intervenants de manière appropriée, ce qui permet non seulement de gérer efficacement la situation, mais aussi d'assurer la sécurité des intervenants eux-mêmes. Les véhicules aériens sans pilote sont guidés de manière autonome, ou par télécommande, ou les deux en même temps et qui transporte des capteurs, des désignateurs de cible, des munitions offensives ou des émetteurs électroniques conçus pour interférer avec ou détruire des cibles ennemies.

3.3 Présentation de la norme IEEE 802.15.4k

Contrairement aux normes WPAN précédentes, IEEE 802.15.4 (LR-WPAN) et ses amendements ont une faible complexité, une faible consommation d'énergie, des infrastructures simples et prennent en charge les applications à bas débit. Cependant, ils ne satisfont pas à toutes les exigences des réseaux LECIM. Leurs inconvénients sont d'avoir des portées courtes, une faible densité de nœuds et la nécessité d'une infrastructure de réseau alimentée, d'un maillage ou de l'absence de mécanismes pour étendre la portée. De plus, ils ne sont pas conçus pour un environnement de propagation extérieur. Pour les utiliser dans de grands réseaux tout en fonctionnant dans des environnements à longue portée et difficiles, ils ont besoin de modifier la sous- couche MAC et la couche PHY des anciennes versions de IEEE 802.15.4.

Afin de pouvoir surmonter les limites de la norme 802.15.4, l'organisme IEEE a proposé la norme IEEE 802.15.4k en 2013 comme la première version destinée à satisfaire les besoins des applications de surveillance des infrastructures critiques à faible consommation d'énergie LECIM. Cet amendement à IEEE 802.15.4-2011 avait pour but de remodeler les protocoles MAC existants de 802.15.4 pour faire face à la transmissions des informations prioritaires et critiques obtenus lors d'une surveillance.

3.3.1 Topologie et composants du réseau

Les réseaux LECIM fonctionnent principalement dans une topologie en étoile déjà abordée dans le chapitre 1 (section 1.4.1.3). Comme dans le réseau IEEE 802.15.4, le réseau IEEE 802.15.4k se

compose d'un coordinateur PAN qui agit comme le maître du réseau et des dispositifs FFD et RFD.

3.4 Couche physique de la norme IEEE 802.15.4k

La norme IEEE 802.15.4k-2013 spécifie deux nouvelles alternatives PHYs.

- LECIM DSSS PHY : fonctionnant dans les bandes de fréquences de 470 MHz, 780 MHz, 863 MHz, 915 MHz, 922 MHz, 917 MHz, 920 MHz, 921 MHz et 2450 MHz. Les techniques de modulation prises en charge sont BPSK et O-QPSK.
- LECIM FSK PHY : fonctionnant dans les bandes de fréquences de 169 MHz, 433 MHz, 470 MHz, 780 MHz, 863 MHz, 915 MHz, 922 MHz, 917 MHz, 920 MHz et 921 MHz. Les techniques de modulation utilisées sont FSK (Frequency Shift Keying), GFSK (Gaussian Frequency Shift Keying), P-FSK (Position-based Frequency Shift Keying) et P-GFSK (Position-based Gaussian Frequency Shift Keying).

3.5 Sous-couche MAC de la norme IEEE 802.15.4k

La sous-couche MAC de IEEE 802.15.4k a pour rôle principal la gestion d'accès au canal prioritaire en utilisant des mécanismes dépendant du mode de fonctionnement du réseau.

3.5.1 Mode de fonctionnement et mécanismes d'accès au canal

Comme le standard IEEE 802.15.4 de base, cet amendement définit deux modes d'accès au support pour la transmission des trames prioritaires à savoir le mode beacon et le mode non beacon. Ses trames accèdent au canal d'une manière prioritaire à l'aide de l'algorithme CSMA/CA avec backoff PCA (Priority Channel Access) ou LECIM ALOHA PCA.

1. **Mode beacon.** Dans le mode beacon, le coordinateur PAN envoie périodiquement des trames Beacon pour synchroniser les nœuds du réseau. Tout membre du réseau qui entend ce Beacon peut ainsi se synchroniser et se servir de ce coordinateur comme relais. Le choix de ce mode impose aux nœuds de suivre une structure périodique de supertrame IEEE 802.15.4k. Tout nœud souhaitant transmettre ses trames prioritaires doit rentrer en compétition avec les autres nœuds pour avoir un accès au médium prioritaire. Dans le mode beacon, les nœuds utilisent le mécanisme CSMA/CA avec backoff PCA slotté ou LECIM ALOHA PCA slotté pour gagner l'accès au canal.

2. **Mode non beacon.** Dans le mode non beacon, la structure de la supertrame n'est pas considérée et les mécanismes utilisés sont CSMA/CA avec backoff PCA non slotté et LECIM ALOHA PCA non slotté.

3.5.2 Structure de la supertrame IEEE 802.15.4k

Lorsqu'un message prioritaire arrive dans un PAN activé par balise (i.e, mode beacon), des allocations de temps de taille fixe appelées PCA (Priority Channel Access) sont dédiées dans la période CAP de la supertrame, comme illustré dans la figure 3.1. Dans le cas où il y a plusieurs allocations PCA par supertrame, la première allocation aura lieu au début du CAP. Les allocations PCA restantes seront réparties dans toute la période CAP de la supertrame. Mais aucune allocation PCA ne doit avoir lieu en dehors du CAP.

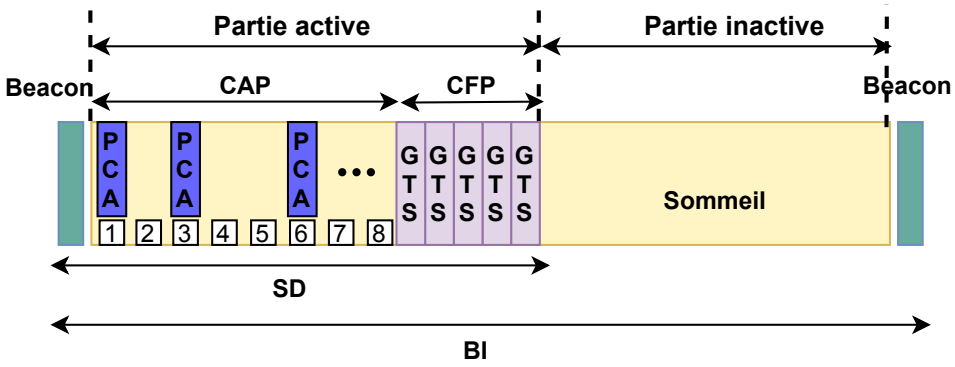


FIGURE 3.1 – Structure de la supertrame IEEE 802.15.4k.

Dans le mode beacon lorsque PCA est activé, ce qui veut dire que il y a des messages prioritaires à transmettre (paramètre macPriorityChannelAccess est vrai), la charge utile de la spécification LECIM PCA IE doit être incluse dans les trames de balise améliorées qui sont envoyées à chaque intervalle beacon. La transmission des trames prioritaires peut commencer dans les allocations prioritaires et se poursuivre pendant toute la durée du CAP.

3.5.3 Protocoles MAC de IEEE 802.15.4k

Deux protocoles MAC sont définis dans l'amendement "k" : le CSMA/CA avec backoff PCA et LECIM ALOHA PCA pour que les dispositifs ayant des messages prioritaires gagnent l'accès au canal de transmission.
Lorsque la trame n'est pas prioritaire, si des balises périodiques sont utilisées alors le dispositif emploie le mécanisme CSMA/CA slotté pour accéder au canal. Dans le cas contraire, le mécanisme

utilisé est le CSMA/CA non slotté. Ces mécanismes sont déjà présentés dans le standard IEEE 802.15.4-2003 (voir la sous-section 1.4.3.4 du chapitre 1). Un nouveau mécanisme appelé ALOHA peut aussi être utilisé dans le mode beacon (ALOHA slotté) ou non becon (ALOHA non slotté) sans avoir recours à vérifier l'état du canal par un CCA. En revanche, lorsque la trame est prioritaire,

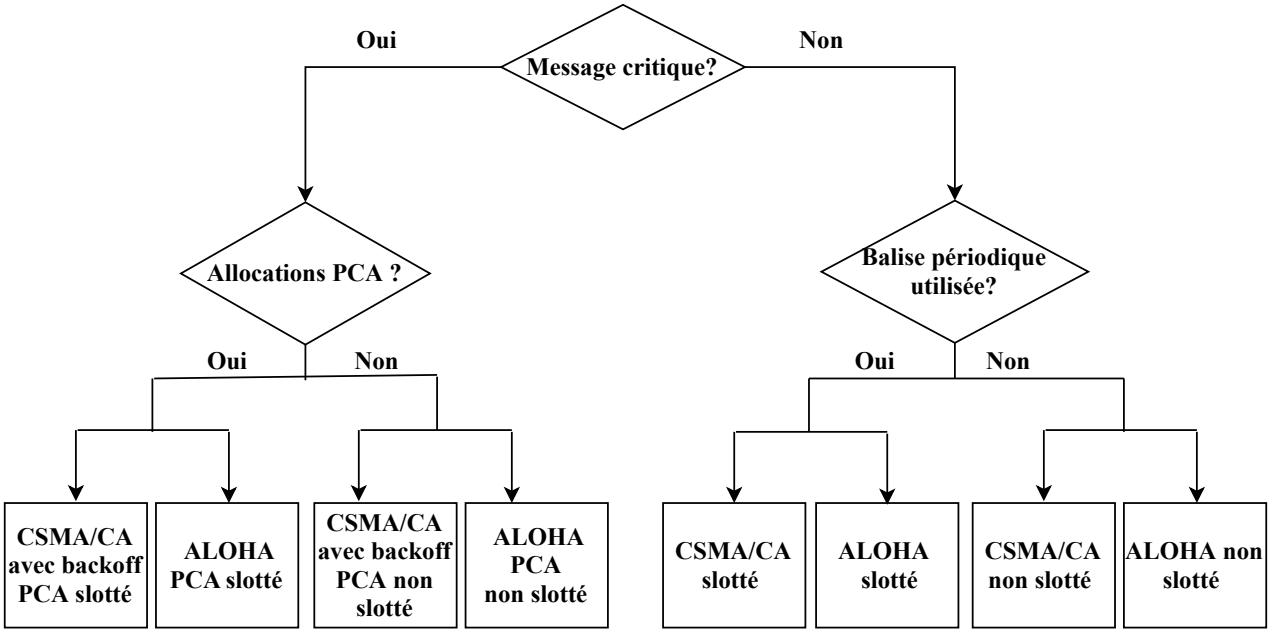


FIGURE 3.2 – Modes d'accès au médium et mécanismes utilisés dans IEEE 802.15.4k MAC.

des allocations PCA peuvent être ajoutées et la transmission commence dans ses allocations et se poursuit dans la partie CAP. Si la trame est priortaire et en plus des allocations PCA existent, alors le dispositif emploie le mécanisme CSMA/CA avec backoff PCA slotté (ou LECIM ALOHA PCA slotté) sinon il emploie le CSMA/CA avec backoff PCA non slotté (ou LECIM ALOHA PCA non slotté), comme le montre la figure 3.2.

3.5.3.1 CSMA/CA avec backoff PCA

L'algorithme CSMA/CA avec backoff PCA présenté dans l'amendement "k" est illustré dans la figure 3.3. Dans le mode beacon, l'algorithme CSMA/CA avec backoff PCA offre des tentatives d'accès au canal persistantes pour un nœud essayant de transmettre un paquet prioritaire. Cela afin d'obtenir un accès immédiat au canal une fois qu'il est détecté libre au moment souhaité (avant d'atteindre *maxDelay*).

Soit *maxDelay* la valeur maximale définie par l'application LECIM représentant le délai qui ne doit pas être dépassé afin d'éviter l'écrasement du paquet. L'algorithme CSMA/CA avec backoff PCA slotté est décrit par les étapes suivantes :

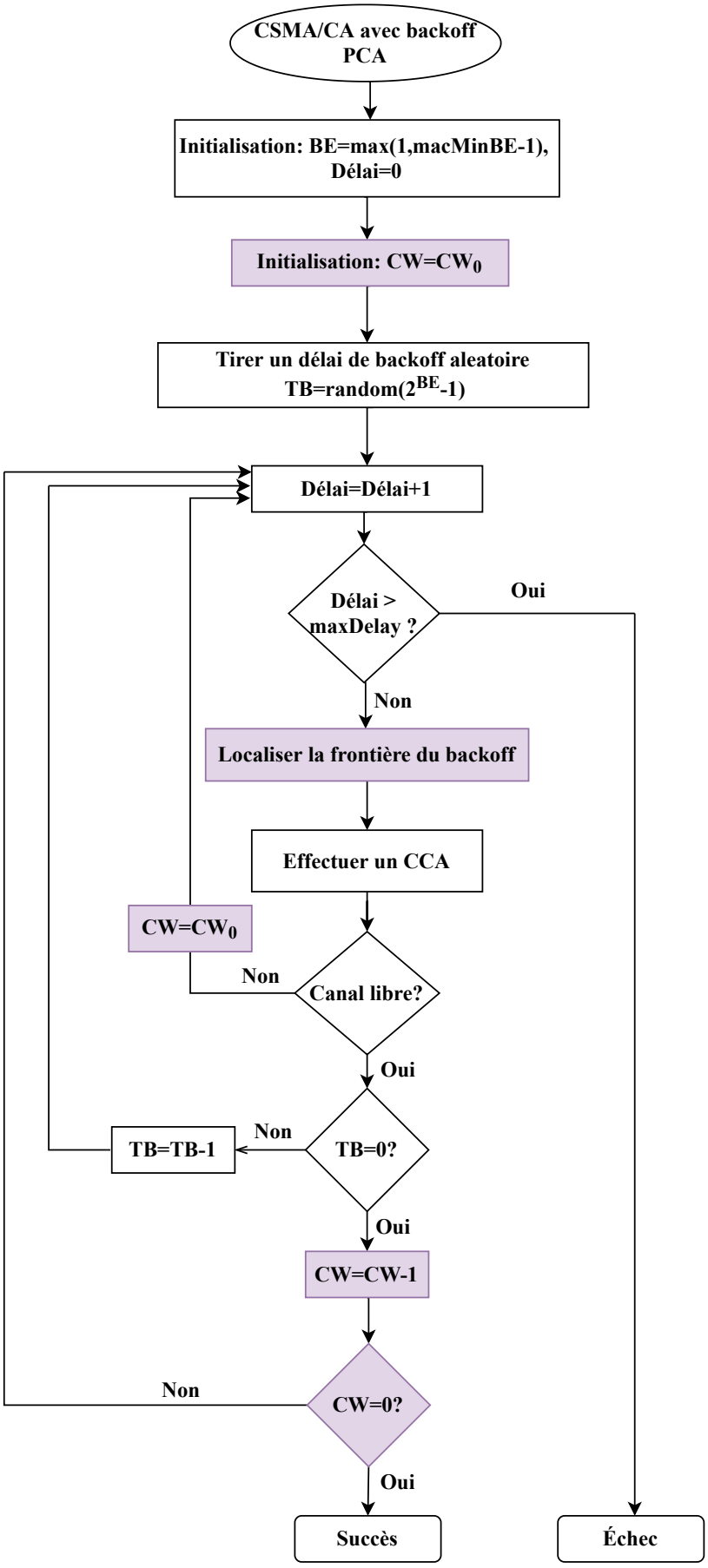


FIGURE 3.3 – Fonctionnement du protocole IEEE 802.15.4k CSMA/CA avec backoff PCA.

Étape 1. Initialisation des variables BE et CW à leurs valeurs par défaut 3 et 2, respectivement. La variable NB n'est pas considérée dans l'amendement "k". De plus, un compteur de délai est initialisé à zéro ($Délai = 0$) à l'arrivée d'un paquet prioritaire,

Étape 2. Le capteur tire un temps aléatoire TB dans l'intervalle $[0, 2^{BE} - 1]$,

Étape 3. Le délai s'incrémente de 1 ($Délai = Délai + 1$),

Étape 4. Si le compteur du délai est inférieur au délai maximum ($maxDelay$), alors procéder à l'étape suivante. Sinon aller à l'étape 9,

Étape 5. Le capteur localise la limite du backoff, puis la sous-couche MAC demande à la couche physique de vérifier l'état du canal de communication en effectuant un CCA,

Étape 6. Si le canal est détecté occupé, la fenêtre de contention est réinitialisée à $CW_0 = 2$, puis retourner à l'étape 3. Sinon aller à l'étape 7,

Étape 7. Si $TB = 0$ alors la fenêtre de contention est décrémentée de 1 ($CW = CW - 1$), puis procéder à l'étape suivante. Sinon décrémenter TB de un et retourner à l'étape 3,

Étape 8. Si $CW = 0$, procéder à l'étape 10. Sinon retourner à l'étape 3,

Étape 9. Échec d'accès au canal de communication, par conséquent la trame est détruite.

Étape 10. Accès au canal de communication réussi, la trame est prête à être envoyée à la frontière du prochain backoff ($aUnitBackoffPeriod$).

Le protocole CSMA/CA avec backoff PCA non slotté (unslotted CSMA/CA with PCA backoff) est utilisé dans le mode de communication sans beacon (absence de la structure de la supertrame). Son fonctionnement ressemble au protocole CSMA/CA avec backoff PCA slotté sauf que les étapes coloriées dans le diagramme de la figure 3.3 ne sont pas incluses dans ce mode. Ces étapes sont l'absence de la fenêtre de contention (une seule tentative d'accès au canal est permise) et l'absence de localisation de la frontière du backoff (dès que TB atteint zéro, l'écoute du canal pendant une durée CCA s'effectue sans attendre la frontière du prochain backoff).

TB (Total Backoff) est le total des backoffs, qui indique le nombre de périodes restantes depuis le début de l'algorithme CSMA/CA avec backoff PCA (ou ALOHA PCA). TB est tiré aléatoirement entre 0 et $2^{BE} - 1$.

3.5.3.2 LECIM ALOHA PCA

La première différence entre le mécanisme ALOHA et CSMA/CA dans le mode beacon est que la fenêtre de contention est initialisée à 1 dans ALOHA, contrairement au CSMA/CA où elle est initialisée à 2. Aussi, la détection de l'occupation du canal est absente dans ALOHA. Dans ALOHA

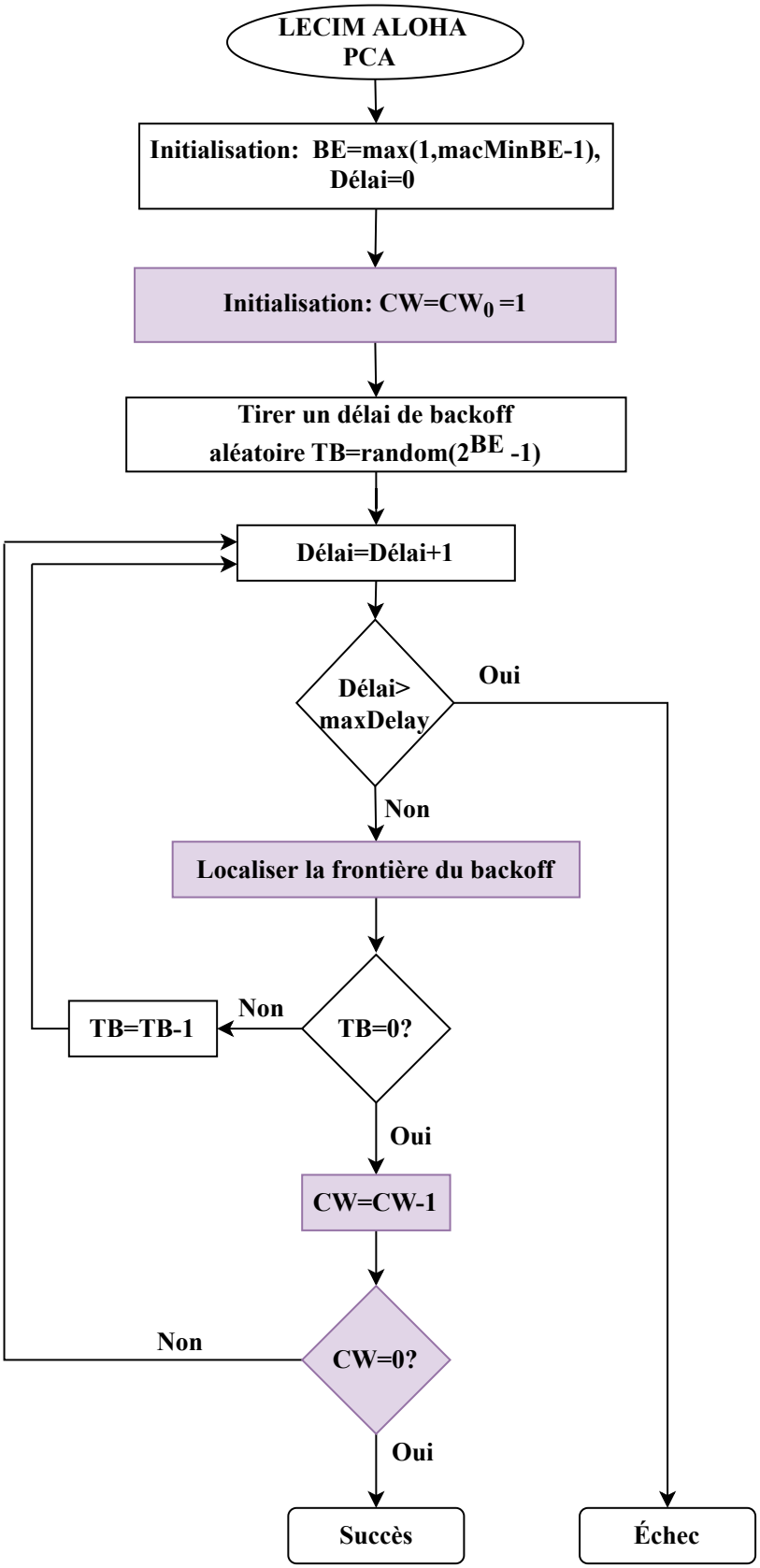


FIGURE 3.4 – Fonctionnement des protocoles LECIM ALOHA PCA IEEE 802.15.4k MAC.

slotté, le dispositif doit suivre les étapes suivantes pour avoir un accès au canal prioritaire :

1. Initialisation des variables BE et CW à 3 et 1, respectivement. Un compteur de délai est initialisé à zéro ($Délai = 0$) à l'arrivée d'un paquet critique,
2. Le nœud tire une période d'attente aléatoire TB dans la plage $[0, 2^{BE} - 1]$,
3. Le délai est incrémenté de un ($Délai = Délai + 1$),
4. Si le compteur du délai est inférieur au délai maximum ($maxDelay$), alors procéder à l'étape suivante. Sinon aller à l'étape 9,
5. Le capteur localise la limite du backoff. Si $TB = 0$, alors la fenêtre de contention est décrémentée de 1, puis procéder à l'étape suivante. Sinon aller à l'étape 7,
6. Si $CW = 0$, aller à l'étape 8. Sinon revenir à l'étape 3,
7. Décrémenter TB de 1 ($TB = TB - 1$) puis retourner à l'étape 3,
8. Accès au canal de communication réussi, la trame est prête à être envoyée à la frontière du prochain backoff ($macLECIMAlohaUnitBackoffPeriod$).
9. Échec d'accès au canal de communication, par conséquent la trame est détruite.

Pour un dispositif tentant d'accéder au canal suivant le mécanisme LECIM ALOHA PCA non slotté, le diagramme des étapes qu'il doit suivre est défini dans le diagramme de la figure 3.4, où les étapes coloriées n'existent pas dans ce protocole. Ici le dispositif ne localise pas la frontière du backoff, il passe directement de l'étape de vérification du délai jusqu'à $TB = 0$. Quand $TB = 0$, l'accès au canal est réussi et l'émission de la trame peut commencer.

Une période d'attente dans le protocole ALOHA IEEE 802.15.4k est définie comme $macLECIMAlohaUnitBackoffPeriod$. Cette période doit être suffisamment longue pour permettre la transmission d'une MPDU de taille maximale, sa période IFS associée ainsi que sa trame ACK, comme indiqué dans l'équation (3.1).

$$macLECIMAlohaUnitBackoffPeriod > aMaxSIFSFrameSize + aMaxSIFSFrameperiod + ACK. \quad (3.1)$$

3.5.3.3 ALOHA

Le mécanisme ALOHA a été défini pour la première fois dans l'amendement "a" en 2007.

Un dispositif ayant un paquet non prioritaire à transmettre à l'aide du mécanisme d'accès ALOHA slotté doit suivre les étapes suivantes (voir le diagramme 3.5) :

1. La sous-couche MAC initialise la fenêtre de contention à une période de temps, BE à $macMinBE$ et NB à zéro,

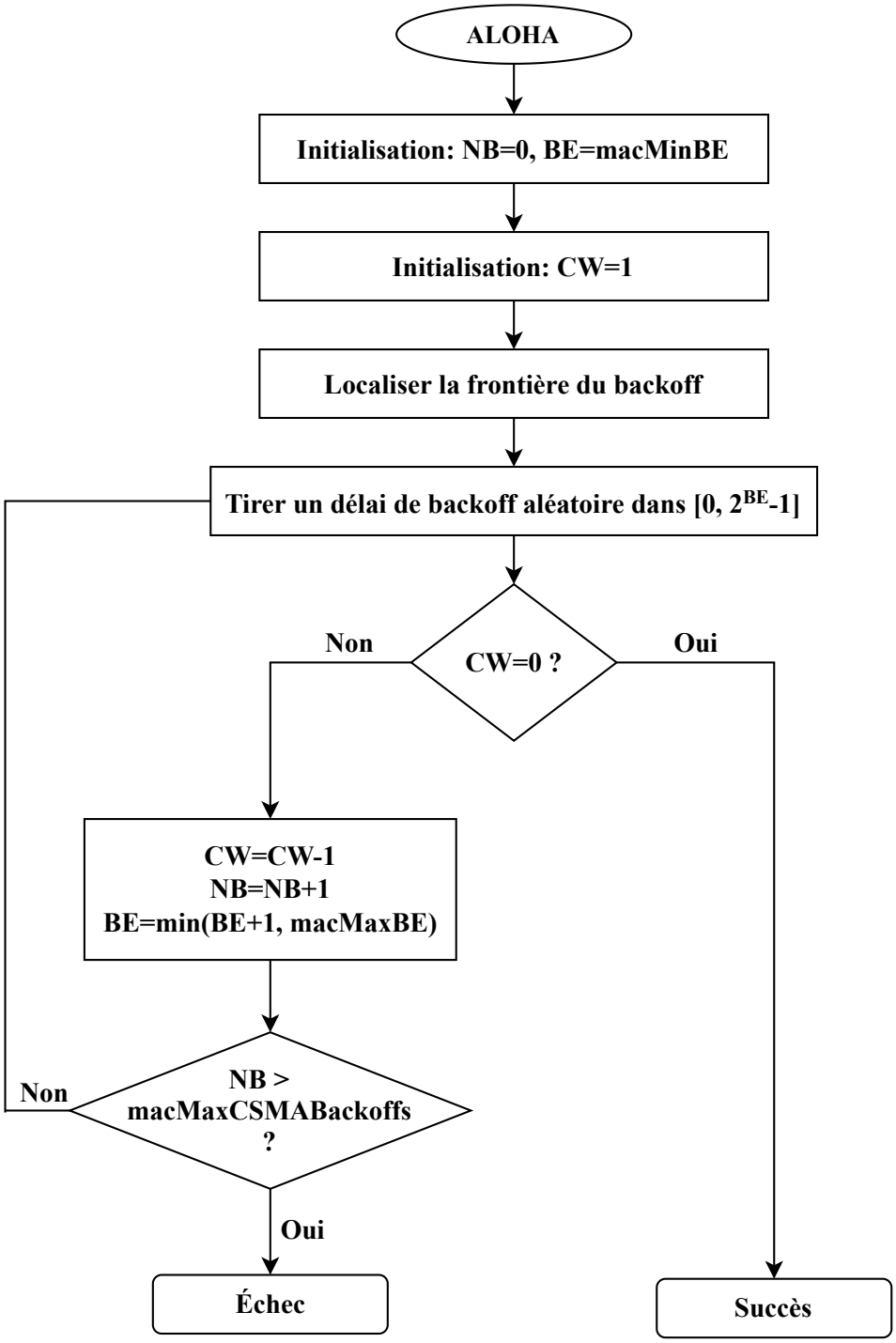


FIGURE 3.5 – Fonctionnement des protocoles MAC ALOHA IEEE 802.15.4

2. Le capteur choisit une période d'attente aléatoire dans la plage $[0, 2^{BE} - 1]$ unités et la décrémente jusqu'à atteindre zéro. Puis procéder à l'étape suivante,
3. Si $CW = 0$, aller à l'étape 7. Sinon procéder à l'étape suivante,
4. Si $CW \neq 0$, les variables d'état sont mises à jour comme suit, $NB = NB + 1$, $CW = CW - 1$, et $BE = min(BE + 1, macMaxBE)$ et procéder à l'étape suivante,
5. Si NB est inférieur à la valeur de $macMaxCSMABackoffs$, le nœud tire un autre backoff afin de retenter l'envoi de la trame (retourner à l'étape 2). Sinon aller à l'étape 6,
6. Échec d'accès au canal de communication,
7. Accès au canal de communication réussi, la trame non prioritaire est prête à être envoyée à la frontière du prochain backoff.

Où NB est le nombre de backoff, initialisée à zéro avant chaque nouvelle tentative de transmission. Lorsque la transmission d'un paquet de données non prioritaire échoue, le mécanisme ALOHA slotté IEEE 802.15.4k offre une possibilité de retransmission.

3.6 Synthèse des travaux existants sur ces deux mécanismes

Depuis l'apparition du nouvel amendement IEEE 802.15.4k, il existe peu d'auteurs qui se sont intéressés aux mécanismes CSMA/CA avec backoff PCA et ALOHA PCA. Dans ce qui suit, nous allons présenter les travaux réalisés sur ces deux mécanismes.

Les auteurs dans [107] ont proposé un protocole MAC basé sur ALOHA slotté encadré (framed slotted ALOHA) dans des réseaux LECIM. Les expressions analytiques de consommation d'énergie et de délai sont dérivées pour analyser et comparer les performances de leur protocole proposé avec les protocoles existants (T-MAC, B-MAC, X-MAC, ZigBee, et WiseMAC).

Dans [108], une implémentation d'un émetteur-récepteur de IEEE 802.15.4k DSSS PHY sur une plate-forme radio GNU avec un périphérique radio logiciel universel (USRP) est établie. Une autre expérience est menée pour évaluer les performances de la coexistence de l'émetteur-récepteur LECIM proposé avec les réseaux LTE-U en place.

Les auteurs de [109] ont évalué le comportement d'un réseau de capteurs sans fil IEEE 802.15.4 mettant en œuvre le mécanisme d'accès au canal prioritaire dans un scénario de surveillance réaliste pour les applications de la santé, en se concentrant sur les transmissions de messages prioritaires. Les évaluations sont basées sur des simulations OMNeT ++. Les résultats de la simulation montrent que

l'adoption de PCA dans le scénario considéré réduit considérablement le taux de perte de paquets ayant des messages prioritaires, sans affecter de manière significative les performances des messages non prioritaires. Ces résultats dépendent de l'algorithme de PCA backoff, qui fournit un taux de perte de paquets plus faible que le CSMA/CA ordinaire aux dépens du délai des messages.

Dans [110], les auteurs ont proposé un protocole de contrôle d'accès moyen basé sur ALOHA slotté encadré (framed slotted ALOHA) dans le mode beacon, destiné aux réseaux LECIM. Une étude sur la consommation d'énergie, la durée de vie de la batterie et le taux de réussite du protocole est élaborée pour différentes tailles de trames et différents taux d'arrivée. Une simulation à l'aide d'un simulateur personnalisé écrit en C ++ est effectuée. Les résultats de la simulation montrent qu'il est efficace en termes de taux de réussite des paquets, de consommation d'énergie et de durée de vie de la batterie. Ces taux de réussite sont satisfaisants et peuvent répondre aux exigences du LECIM.

Dans la littérature, il n'y a qu'une seule étude qui a analysé les performances de IEEE 802.15.4k PHY par l'approche de simulation (la modélisation analytique n'est pas considérée) [111]. Les auteurs dans [111] ont fourni une évaluation des performances du système LECIM DSSS PHY utilisant l'algorithme Slotted ALOHA avec backoff PCA dans un mode beacon dans des conditions de trafic non saturé. Les performances du réseau sont évaluées, en termes de taux de livraison de paquets, de probabilité de succès et du délai du réseau. De plus, un modèle de simulation utilisant le simulateur OPNET est développé. Les résultats de la simulation montrent que l'application d'un accès prioritaire au réseau améliore considérablement les performances du délai de transmission des messages de haute priorité tout en imposant moins d'effet sur les performances globales du réseau concernant les messages de faible priorité. Cependant, les performances de fiabilité suivant PCA sont approximativement les mêmes que les performances de fiabilité d'un schéma qui ne suit pas PCA.

Aussi, il n'y a qu'un seul travail qui évalue les performances des protocoles CSMA/CA avec backoff PCA et CSMA/CA en utilisant la modélisation analytique par chaîne de Markov [112]. Dans [112], les auteurs ont considéré un mode beacon et non beacon, des conditions de trafic non saturé avec des conditions de canal idéal. Une analyse des performances, en termes de fiabilité, de délai de transmission réussie des paquets et de la consommation d'énergie du nœud a été effectuée. La validité du modèle proposé est prouvée par une simulation de Monte Carlo.

Tous les travaux existants sur la norme 802.15.4 ont abordé les collisions comme une source principale pour la perte des paquets. Cependant, ils n'ont jamais considéré les erreurs de transmis-

sion (i.e. conditions de canal bruité) comme une cause de perte de paquets. Contrairement aux études sur les autres normes, telle que IEEE 802.11, quelques auteurs ont considéré des conditions de canal bruité [113, 114].

3.7 Conclusion

Dans ce chapitre, nous avons tout d'abord présenté les réseaux d'infrastructures critiques en particulier et dressé leurs exigences. Puis, nous avons détaillé les réseaux de surveillance des infrastructures critiques à faible consommation d'énergie avec leurs caractéristiques ainsi que leurs domaines d'application. Dans un second lieu, nous avons introduit la norme IEEE 802.15.4k adaptée aux applications de surveillance des réseaux d'infrastructures critiques à faible consommation d'énergie LECIM. Elle fournit deux nouvelles alternatives physiques et de nouveaux protocoles MAC. La sous-couche MAC gère l'accès au canal avec les deux mécanismes CSMA/CA avec backoff PCA et LECIM ALOHA PCA. Leur fonctionnement a été présenté en détail dans ce chapitre.

La modélisation et l'évaluation des performances des mécanismes CSMA/CA avec backoff PCA slotté et CSMA/CA avec backoff PCA non slotté dans des conditions de canal non idéal et LECIM ALOHA PCA dans des conditions de canal idéal seront l'objet des prochains chapitres.

Deuxième partie

Contributions

Chapitre4

Modélisation analytique et évaluation des performances du mécanisme IEEE 802.15.4k CSMA/CA avec backoff PCA slotté

Sommaire

4.1 Introduction

Dans le mode beacon du réseau IEEE 802.15.4k, la transmission d'un message prioritaire se fait grâce au mécanisme CSMA/CA avec backoff PCA slotté et celle d'un message non prioritaire grâce à CSMA/CA slotté. Dans ce chapitre, nous allons proposer un premier modèle de CSMA/CA avec backoff PCA slotté sous un canal bruité [4]. Nous détaillerons notre proposition avec un modèle analytique capable d'estimer les métriques de performance du réseau dont la fiabilité, l'énergie consommée, le débit et le délai dans le cas de saturation de trafic et sous un canal bruité.

Notre modélisation se basera sur une chaîne de Markov à deux et à trois dimensions pour les deux mécanismes CSMA/CA avec backoff PCA slotté et CSMA/CA slotté, respectivement (section 4.2). Nous aborderons notre modélisation par une description générale, qui englobera les hypothèses prédéfinies et les notations utilisées. Par la suite, nous dériverons dans la section 4.3, les expressions des métriques de performances. Enfin, dans la section 4.4.3, nous allons comparer les performances

des deux mécanismes d'accès au canal et voir l'effet de la variation de quelques paramètres sur les mesures de performances. Une analyse comparative entre la norme IEEE 802.15.4 et l'amendement "k" dans le cas du canal idéal sera présentée.

4.2 Modélisation analytique des mécanismes CSMA/CA PCA et CSMA/CA slotté

Dans cette section, nous présentons le modèle analytique de chaîne de Markov (CM) proposé pour les mécanismes CSMA/CA avec backoff PCA slotté et CSMA/CA slotté de IEEE 802.15.4k dans une topologie en étoile, dans des conditions de saturation de trafic, sous un canal bruité avec considération des acquittements [4]. Si la station ne reçoit pas d'acquittement pour une trame donnée, elle considère qu'il y a une collision ou une erreur de transmission sur le canal.

4.2.1 Hypothèses du modèle

Nous supposons les hypothèse suivantes dans lesquelles notre modèle de CM est applicable.

1. N nœuds disposés en topologie en étoile autour d'un coordinateur PAN,
2. Une condition de trafic saturé,
3. Prise en compte des erreurs de transmission (canal bruité),
4. Prise en charge des accusés de réception (ACKs).

4.2.2 Les probabilités utilisées dans le modèle

Les paramètres importants utilisés dans notre modèle sont représentés dans le tableau 4.1

4.2.3 Paramètres et notations utilisés dans le modèle

Dans le tableau 4.2, nous présenterons les différentes notations indispensables à la réalisation de notre modèle.

4.2.4 La chaîne de Markov proposée

Notre modèle de chaîne de Markov proposé se compose de deux modèles : un modèle de chaîne de Markov discrète à deux dimensions pour le mécanisme IEEE 802.15.4k CSMA/CA avec backoff PCA slotté et un modèle de chaîne de Markov discrète à trois dimensions pour le mécanisme IEEE 802.15.4k CSMA/CA slotté. Son graphe de transition est illustré dans la figure 4.1.

TABLE 4.1 – Probabilités du modèle IEEE 802.15.4k CSMA/CA PCA slotté

Probabilités	Description
h_p	La probabilité que le paquet soit prioritaire
α	La probabilité que le canal soit occupé dans le CCA1
β	La probabilité que le canal soit occupé dans le CCA2
τ	La probabilité qu'un nœud tente d'effectuer le CCA1 sur un slot de temps
P_s	La probabilité de résider dans l'état idle
P_c	La probabilité de collision
P_{te}	La probabilité d'erreur
P_e	La probabilité d'échec
$p_{i,k}$	Les probabilités des états de la chaîne de Markov associées à PCA slotté
$b_{i,k,j}$	Les probabilités des états de la chaîne de Markov associées à CSMA/CA slotté

TABLE 4.2 – Paramètres du modèle IEEE 802.15.4k CSMA/CA PCA slotté

Paramètre	Description
N	La taille du réseau
n	Le nombre maximum de retransmissions
m	L'étage maximum du backoff pour CSMA/CA
W_0	La taille minimale de la fenêtre de contention correspondant à la première tentative de transmission pour CSMA/CA
W	Le nombre d'étages de backoff pour CSMA/CA avec backoff PCA
L_p	La taille du paquet
L_s	La taille du paquet reçu avec succès
L_c	La taille du paquet collisioné
L_f	La taille du paquet non reçu
L_{ack}	La taille de l'ACK

Soit h_p la probabilité que le paquet soit prioritaire et $(1 - h_p)$ la probabilité que le paquet soit non prioritaire. Les deux processus stochastiques de notre chaîne de Markov sont décrits comme suit :

- Soit $(c(t), d(t))$ le processus stochastique modélisant la transmission des messages prioritaires en utilisant le mécanisme CSMA/CA avec backoff PCA, où $c(t)$ représente le compteur d'attente backoff et $d(t)$ représente le délai encouru par le paquet. Les états (i,k), $i \in [0, W-1]$, $k \in [1,d]$ représentent les périodes d'attente backoff. Les états $(0,k)$, $k \in [1,d]$ et $(-1,k)$, $k \in [2,d]$ représentent le CCA1 et le CCA2, respectivement. Les états allant de $(-2,0)$ à $(-2, L_s-1)$ et de $(-3,0)$ à $(-3, L_f-1)$ représentent les états de transmission réussie et échouée,

respectivement. Où, L_s et L_f indiquent la taille du paquet reçu avec succès ou non reçu (en raison de collision ou d'erreurs de transmission), respectivement.

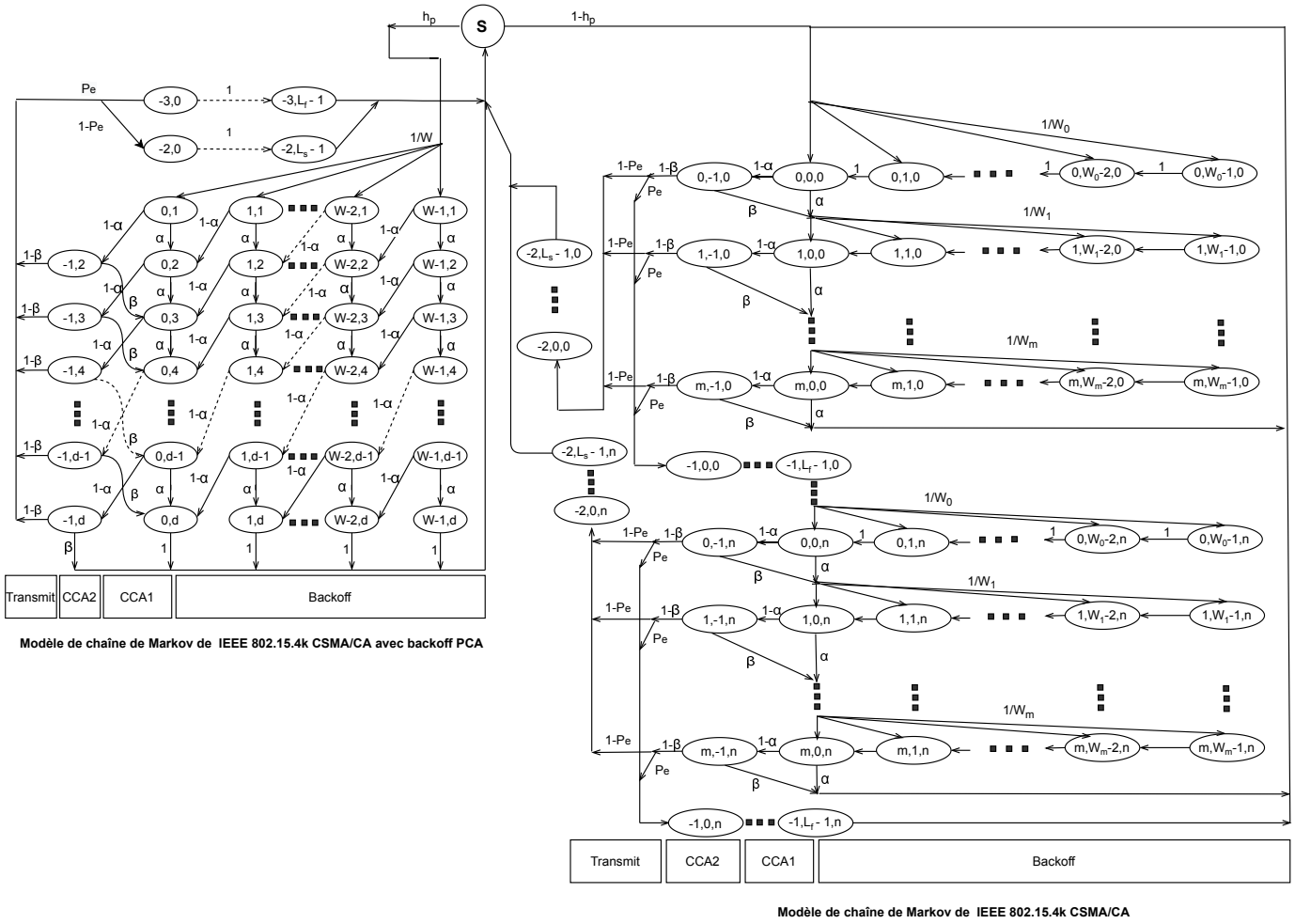


FIGURE 4.1 – Chaîne de Markov des mécanismes de IEEE 802.15.4k slotté

- Soit $(s(t), c(t), r(t))$ le processus stochastique modélisant la transmission des messages non prioritaires en utilisant le mécanisme CSMA/CA où $s(t)$ indique l'étage du backoff à l'instant t, $c(t)$ indique soit la valeur du compteur d'attente backoff ou le CCA1/CCA2 à l'instant t et $r(t)$ indique l'état de retransmission à l'instant t. Les états (i, k, j), $i \in [0, m]$, $k \in [0, W_i - 1]$, $j \in [0, n]$ représentent les périodes d'attente backoff. Les états $(i, 0, j)$ et $(i, -1, j)$, $i \in [0, m]$, $j \in [0, n]$ représentent le CCA1 et CCA2, respectivement. Les états allant de $(-2, 0, j)$ à $(-2, L_s - 1, j)$ et de $(-1, 0, j)$ à $(-1, L_f - 1, j)$ représentent les états de transmission réussie et non réussie, respectivement.

Dans ce modèle, α représente la probabilité que le canal soit occupé dans le CCA1, β la probabilité que le canal soit occupé dans le CCA2 et P_e la probabilité qu'une collision ou une erreur de

transmission se produise.

Soit S l'état des arrivées des paquets et qui se produit à la fin des tentatives d'accès au canal dans les différents cas (succès, échec ou délai dépassé) pour les deux mécanismes. Notons par P_s sa probabilité associée.

4.2.4.1 Probabilités de transition

Les probabilités de transition associées à la chaîne de Markov sont décrites comme suit :

- La probabilité de transition de l'état CCA1 de CSMA/CA avec backoff PCA au slot succès est

$$P(-2, 0|0, k) = (1-\alpha)(1-\beta)(1-P_e), \forall\, k \in [1, d]. \tag{4.1}$$

- La probabilité de transition de l'état CCA1 de CSMA/CA avec backoff PCA au slot échec est donnée par l'équation (4.2).

$$P(-3, 0|0, k) = (1-\alpha)(1-\beta)P_e\ , \forall\, k \in [1, d]. \tag{4.2}$$

- La probabilité de retourner à l'état S après écrasement du paquet est donnée par l'équation suivante

$$P(S\,|i, d) = 1, \forall\, i \in [0, W-1]. \tag{4.3}$$

- La probabilité de transition de l'état CCA1 de CSMA/CA au slot succès est

$$P(-2, 0, j|i, 0, j) = (1-\alpha)(1-\beta)(1-P_e), \forall\, i \in [0, m],\, j \in [0, n]. \tag{4.4}$$

- La probabilité de transition de l'état CCA1 de CSMA/CA au slot échec est exprimée par l'équation (4.5).

$$P(-1, 0, j|i, 0, j) = (1-\alpha)(1-\beta)P_e, \forall\, i \in [0, m],\, j \in [0, n]. \tag{4.5}$$

- Le compteur du backoff décrémente à chaque slot de temps avec la probabilité donnée par

$$P(i, k, j|i, k+1, j) = 1, \forall\, i \in [0, m]\ ,\, j \in [0, n]\ ,\, k \in [0, W_i - 1]. \tag{4.6}$$

4.2.4.2 Probabilités d'état stationnaire

Dans cette sous-section, nous allons calculer la distribution stationnaire qui est essentielle pour dériver les métriques de performance des deux mécanismes, en termes de fiabilité, de consommation d'énergie, de débit et de délai.

Nous représentons par $p_{i,k}$ les probabilités des états de la chaîne de Markov associées à CSMA/CA avec backoff PCA et par $b_{i,k,j}$ les probabilités des états associées à CSMA/CA.

a) La probabilité stationnaire associée à CSMA/CA avec backoff PCA slotté

Pour calculer la distribution $p_{i,k}$, il faut d'abord passer par le calcul de $p_{i,1}$ et $p_{i,2}$, qui signifient que le délai encouru est égal à 1 et 2, respectivement. Selon la chaîne de Markov de CSMA/CA avec backoff PCA (voir la figure 4.1), nous avons

- La probabilité qu'un nœud ayant un paquet prioritaire à transmettre sélectionne l'un des états de backoff aléatoirement est donnée par

$$p_{i,1} = \frac{P_s\, h_p}{W}\ ,\ \forall\ i \in [0, W-1]. \tag{4.7}$$

- La probabilité que le compteur aléatoire soit égal à i et que le délai encouru soit égal à 2 est

$$p_{i,2} = \begin{cases} \alpha\ p_{i,1} + (1-\alpha)\ p_{i+1,1} & i \in [0, W-2], \\ \alpha\ p_{i,1} & i = W-1. \end{cases} \tag{4.8}$$

- En utilisant les équations (4.7) et (4.8) et en exploitant la récurrence, la probabilité de n'importe quel état de backoff dans CSMA/CA avec backoff PCA est donnée par l'expression (4.9).

$$p_{i,k} = \sum_{j=0}^{min(W-1-i,k-1)} C_{k-1}^{j}\ (1-\alpha)^j\ \alpha^{k-j-1} \frac{P_s\, h_p}{W}\ ,\forall\ i \in [1, W-1]\ , k \in [1, d] \tag{4.9}$$

Où $C_u^k = \binom{u}{k}$ représente la combinaison de u objets parmi k à la fois.

- La probabilité que le nœud tente le CCA1 dans l'état $(0, k)$ est

$$p_{0,k} = \sum_{j=0}^{min(W-1,k-1)} C_{k-1}^{j}\ (1-\alpha)^j\ \alpha^{k-j-1} \frac{P_s\, h_p}{W},\ k \in [1, d]. \tag{4.10}$$

- La probabilité que le nœud tente le CCA2 dans l'état $(-1, k)$ est donnée par l'équation (4.11).

$$p_{-1,k} = (1-\alpha) p_{0,k-1}\ ,\forall\ k \in [2, d]. \tag{4.11}$$

- La probabilité d'état succès est donnée par l'expression (4.13).

$$p_{-2,0} = (1-\beta)(1-P_e) \sum_{k=2}^{d} p_{-1,k}. \tag{4.12}$$

- La probabilité d'état d'échec est

$$p_{-3,0} = (1-\beta) P_e \sum_{k=2}^{d} p_{-1,k}. \tag{4.13}$$

b) La probabilité stationnaire associées à CSMA/CA slotté

Selon le modèle de chaîne de Markov de CSMA/CA donné par la figure 4.1 et basé sur [27] mais tenant compte des erreurs de transmission, nous avons obtenu les équations (4.14)-(4.24).

Soit $b_{i,k,j} = \lim_{t\to+\infty} P\Big(s(t) = i, c(t) = k, r(t) = j\Big), i \in [-2, m], k \in (-1, max(W_i - 1, L_s - 1, L_f - 1)), j \in [0, n]$ la probabilité stationnaire de la chaîne de Markov associée au mécanisme CSMA/CA.

Pour $i \in [0, m]$, nous avons

$$b_{i,k,j} = \frac{W_i - k}{W_i}\, b_{i,0,j}\ ,\ \forall\ k \in [0, W_i - 1]. \tag{4.14}$$

Où, la valeur du compteur de backoff W_i est uniformément choisie à l'étage i dans l'intervalle $[0, W_i - 1]$, comme suit

$$W_i = \begin{cases} 2^i\ W_0 & i \le m_b - m_0, \\ 2^{m_b - m_0}\ W_0 & i \in]m_b - m_0, m]. \end{cases} \tag{4.15}$$

Avec $m_b = macMaxBE$ et $m_0 = macMinBE$ (voir le tableau 4.3).

- La probabilité que le nœud tente un CCA1 dans l'état $(i, 0, j)$ est

$$b_{i,0,j} = \Big(\alpha + (1-\alpha)\beta\Big)^i b_{0,0,j} = x^i\ b_{0,0,j}, \forall\ i \in [0, m],\ j \in [0, n]. \tag{4.16}$$

Où $x = \alpha + (1-\alpha)\beta$ représente la probabilité d'échec d'accès au canal dans n'importe quel étage de backoff.

- La probabilité de retransmission après m tentatives échouées d'accès au canal est donnée par l'expression suivante

$$b_{0,0,j} = \left(P_e(1-x)\sum_{i=0}^{m} b_{i,0,j-1}\right)^j = y_p^j\ b_{0,0,0}\ ,\forall\ j \in [0, n]. \tag{4.17}$$

Où $y_p = P_e(1 - x^{m+1})$ représente la probabilité que le nœud obtient l'accès au canal dans les m étages de backoff avec occurrence d'une erreur de transmission ou d'une collision.

- La probabilité de résider dans l'état $(0, 0, 0)$ est donnée par l'équation (4.18).

$$b_{0,0,0} = \frac{(1-h_p)\ P_s}{W_0} + \sum_{k=1}^{W_0-1} b_{0,k,0} = (1-h_p)\ P_s. \tag{4.18}$$

- La probabilité que le nœud tente un CCA2 dans l'état $(i, -1, j)$ est donné comme suit

$$b_{i,-1,j} = (1-\alpha)x^i\ y_p^j,\ \ \forall\ \ i \in [0, m]\ \ j \in [0, n]. \tag{4.19}$$

- La probabilité de l'état succès est

$$b_{-2,0,j} = (1 - P_e)(1 - x^{m+1})\ b_{0,0,j},\ \ \forall\ \ j \in [0, n]. \tag{4.20}$$

- La probabilité de l'état échec est exprimée dans (4.21).

$$b_{-1,0,j} = P_e(1 - x^{m+1})\, b_{0,0,j}, \quad \forall \quad j \in [0, n]. \tag{4.21}$$

c) Calcul de la probabilité de résider dans l'état S

Nous notons que toutes les probabilités tirées du graphe de transition sont données en fonction de la probabilité P_s. Afin de dériver P_s, nous développons la propriété de normalisation dans l'expression (4.22), qui signifie que la somme de toutes les probabilités de la chaîne de Markov est égale à 1. Ensuite, nous dérivons l'expression de chaque terme de cette équation dans les équations (4.23)-(4.29).

$$\sum_{i=0}^{W-1}\sum_{k=1}^{d} p_{i,k} + \sum_{k=2}^{d} p_{-1,k} + \sum_{k=0}^{L_s-1} p_{-2,k} + \sum_{k=0}^{L_f-1} p_{-3,k} + \sum_{i=0}^{m}\sum_{k=0}^{W_i-1}\sum_{j=0}^{n} b_{i,k,j} + \sum_{i=0}^{m}\sum_{j=0}^{n} b_{i,-1,j} +$$

$$\sum_{j=0}^{n}\left(\sum_{k=0}^{L_s-1} b_{-2,k,j} + \sum_{k=0}^{L_f-1} b_{-1,k,j}\right) = 1. \tag{4.22}$$

En utilisant les équations (4.9) et (4.10), le premier terme est donné par

$$\sum_{i=0}^{W-1}\sum_{k=1}^{d} p_{i,k} = \sum_{k=1}^{d} p_{0,k} + \sum_{i=1}^{W-1}\sum_{k=1}^{d} p_{i,k} = \frac{P_s h_p}{W}\left[\sum_{k=1}^{d}\sum_{j=0}^{min(W-1,k-1)} C_{k-1}^{j}(1-\alpha)^j \alpha^{k-j-1} +\right.$$

$$\left.\sum_{i=1}^{W-1}\sum_{k=1}^{d}\sum_{j=0}^{min(W-1-i,k-1)} C_{k-1}^{j}(1-\alpha)^j \alpha^{k-j-1}\right] = S_1 P_s. \tag{4.23}$$

A partir de l'équation (4.11), nous obtenons le second terme exprimé par l'équation (4.24).

$$\sum_{k=2}^{d} p_{-1,k} = (1-\alpha)\sum_{k=2}^{d} p_{0,k-1} = (1-\alpha)\left[\sum_{k=2}^{d}\sum_{j=0}^{min(W-1,k-2)} C_{k-2}^{j}(1-\alpha)^j \alpha^{k-j-2}\frac{P_s h_p}{W}\right] = S_2 P_s. \tag{4.24}$$

Selon les équations (4.12) et (4.13), le troisième et le quatrième termes sont donnés par les expressions (4.25) et (4.26), respectivement.

$$\sum_{k=0}^{L_s-1} p_{-2,k} = L_s(1-\alpha)(1-\beta)(1-P_e)\sum_{k=1}^{d} p_{0,k} = L_s(1-\alpha)(1-\beta)(1-P_e)\frac{P_s h_p}{W}\times$$

$$\sum_{k=1}^{d}\sum_{j=0}^{min(W-1,k-1)} C_{j}^{k-1}(1-\alpha)^j \alpha^{k-j-1} = S_3 P_s. \tag{4.25}$$

$$\sum_{k=0}^{L_f-1} p_{-3,k} = L_f(1-\alpha)(1-\beta)P_e\sum_{k=1}^{d} p_{0,k} = L_f(1-\alpha)(1-\beta)P_e\frac{P_s h_p}{W}\times$$

$$\sum_{k=1}^{d} \sum_{j=0}^{min(W-1,k-1)} C_j^{k-1}(1-\alpha)^j \alpha^{k-j-1} = S_4 P_s. \tag{4.26}$$

En utilisant les équations (4.14) - (4.18), nous obtenons le cinquième terme comme suit

$$\sum_{i=0}^{m} \sum_{k=0}^{W_i-1} \sum_{j=0}^{n} b_{i,k,j} = \sum_{i=0}^{m} \sum_{j=0}^{n} \frac{W_i+1}{2} x^i \, b_{0,0,j} = S_5 P_s.$$

Où,

$$b_{i,k,j} = \begin{cases} \frac{(1-h_p)P_s}{2}\left[\frac{1-(2x)^{m+1}}{1-2x}W_0 + \frac{1-x^{m+1}}{1-x}\right]\frac{1-y_p^{n+1}}{1-y_p}, & si\ m \le m_b - m_0, \\ \frac{(1-h_p)P_s}{2}\left[\frac{1-(2x)^{m_b-m_0+1}}{1-2x}W_0 + \frac{1-x^{m_b-m_0+1}}{1-x} + (2^{m_b}+1)x^{m_b-m_0+1}\frac{1-x^{m_b-m_0+1}}{1-x}\right] \times \frac{1-y_p^{n+1}}{1-y_p}, & si\ m > m_b - m_0. \end{cases} \tag{4.27}$$

A partir de l'expression (4.19), le sixième terme est donné dans (4.28).

$$\sum_{i=0}^{m} \sum_{j=0}^{n} b_{i,-1,j} = P_s(1-h_p)(1-\alpha)\frac{1-x^{m+1}}{1-x}\frac{1-y_p^{n+1}}{1-y_p} = S_6 P_s. \tag{4.28}$$

Finalement, en utilisant les expressions (4.20) et (4.21), le dernier terme est

$$\sum_{j=0}^{n}\Big(\sum_{k=0}^{L_s-1} b_{-2,k,j} + \sum_{k=0}^{L_f-1} b_{-1,k,j}\Big) = P_s(1-h_p)\Big[L_s(1-P_e) + L_f P_e\Big] \times (1-x^{m+1})\frac{1-y_p^{n+1}}{1-y_p} = S_7 P_s. \tag{4.29}$$

Alors, la probabilité P_s s'exprime comme suit

$$P_s = \frac{1}{S_1 + S_2 + S_3 + S_4 + S_5 + S_6 + S_7}. \tag{4.30}$$

Nous pouvons, à présent, exprimer la probabilité τ qu'une entité tente le CCA1 dans un slot de temps choisi aléatoirement par l'expression (4.31).

$$\tau = \tau_{pca} + \tau_{csma} = \sum_{k=1}^{d} p_{0,k} + \sum_{i=0}^{m}\sum_{j=0}^{n} b_{i,0,j}. \tag{4.31}$$

4.2.4.3 Calcul de la probabilité d'échec de transmission

Soit P_e la probabilité d'échec de transmission de données exprimée par l'équation (4.32), pouvant être due à une collision avec la probabilité P_c ou à des erreurs de transmission avec la probabilité P_{te}.

$$P_e = P_c + P_{te}. \tag{4.32}$$

Soit P_c la probabilité qu'au moins une des stations restantes $(N-1)$ transmette sur le même slot de temps donné, provoquant ainsi une collision. Son expression est donnée par l'équation (4.33).

$$P_c = 1 - (1-\tau)^{N-1}. \tag{4.33}$$

Soit P_{te} la probabilité que la transmission comporte des erreurs, donnée comme suit

$$P_{te} = 1 - (1 - BER)^{l}. \tag{4.34}$$

Avec BER (Bit Error Rate) est le taux d'erreur binaire et l est la taille de la trame.

4.2.4.4 Calcul des probabilités que le canal soit occupé

- La probabilité α que le canal soit occupé pendant le CCA1 est donnée par l'expression (4.35). Le canal de communication peut être occupé en raison de la transmission d'un paquet de données avec une probabilité α_1 ou en raison de la transmission d'un acquittement avec une probabilité α_2.

$$\alpha = \alpha_1 + \alpha_2. \tag{4.35}$$

- A partir du graphe de transition de la figure 4.1, les expression de α_1 et α_2 sont données dans (4.36) et (4.37), respectivement.

$$\alpha_1 = L_p\,(1-\alpha)(1-\beta)P_e. \tag{4.36}$$

$$\alpha_2 = L_{ack}\,\frac{N\tau(1-\tau)^{N-1}}{1-(1-\tau)^{N}}(1-\alpha)(1-\beta)P_e. \tag{4.37}$$

Avec L_{ack} est la taille de l'ACK.

- La probabilité β que le canal soit occupé pendant le CCA2 est donnée par

$$\beta = \frac{\left(1-(1-\tau)^{N-1}\right) + \left(1-(1-BER)^{l}\right) + N\tau(1-\tau)^{N-1}}{2-(1-\tau)^{N} + N\tau(1-\tau)^{N-1}}. \tag{4.38}$$

4.3 Calcul des métriques de performances

Dans cette section, nous dérivons les expressions mathématiques de la fiabilité, de délai moyen, de l'énergie consommée et de débit offert par le standard IEEE 802.15.4k pour les mécanismes CSMA/CA avec backoff PCA slotté et CSMA/CA slotté en utilisant la chaîne de Markov précédemment définie dans la figure 4.1 et les formules développées dans la section précédente.

4.3.1 Fiabilité

La fiabilité est la probabilité des transmissions réussies des paquets. Dans notre modélisation, le calcul de cette métrique de performance dépend des probabilités α, β, P_e et τ préalablement déterminées.

4.3.1.1 Fiabilité de CSMA/CA avec backoff PCA slotté

Dans le CSMA/CA avec backoff PCA slotté, un paquet est rejeté en raison du délai dépassé (i.e, d est atteint) ou perdu à cause d'une collision ou d'une erreur de transmission. La fiabilité est donnée par l'expression (4.39).

$$F_{PCA} = 1 - P_{de} - (P_{lc} + P_{lte})(1 - P_{de}). \tag{4.39}$$

Où,

– P_{de} indique la probabilité qu'un paquet prioritaire soit rejeté en raison d'un délai dépassé, son expression est donnée par l'équation (4.40). Les événements A_d et A_c représentent respectivement la probabilité que le paquet soit écrasé en raison d'un délai dépassé et la probabilité que le paquet à envoyer soit prioritaire.

$$P_{de} = P(A_d|A_c) = \frac{\beta p_{-1,d} + \sum_{i=0}^{W-1} p_{i,d}}{h_p} = \frac{\beta(1-\alpha)p_{0,d-1} + \sum_{i=0}^{W-1} p_{i,d}}{h_p}. \tag{4.40}$$

– P_{lc} indique la probabilité de perte de paquet à cause d'une collision, donnée par

$$P_{lc} = 1 - (1 - \tau)^{N-1}. \tag{4.41}$$

– P_{lte} indique la probabilité de perte de paquet à cause d'une erreur de transmission. Son expression est la suivante

$$P_{lte} = 1 - (1 - BER)^{l}. \tag{4.42}$$

4.3.1.2 Fiabilité de CSMA/CA slotté

Dans le CSMA/CA slotté, les paquets sont écrasés en raison d'un échec d'accès au canal ou du nombre limite de tentatives de retransmission atteint. L'expression de la fiabilité de CSMA/CA slotté est donnée par l'équation (4.43).

$$F_{CSMA} = 1 - P_{fca} - P_{fer}. \tag{4.43}$$

Où

– P_{fca} représente la probabilité de perte de paquet à cause d'un échec d'accès au canal dans les $(m + 1)$ étages du backoff. Elle est donnée par

$$P_{fca} = \frac{x^{m+1}(1 - y_p^{n+1})}{1 - y_p}. \tag{4.44}$$

– P_{fer} représente la probabilité que le paquet soit perdu car le nombre de retransmissions est dépassé (i.e, que le nombre maximal de retransmissions n est atteint). Son expression est la suivante

$$P_{fer} = y_p^{n+1}. \tag{4.45}$$

4.3.2 Énergie consommée

Soit P_{cca} l'énergie consommée par le nœud durant les états d'écoute du canal (CCA1 et CCA2), P_i l'énergie consommée durant l'état idle (sommeil) de la période backoff, P_{trans} l'énergie consommée pendant l'état de transmission, et P_{rec} l'énergie consommée pendant l'état de réception. La consommation moyenne d'énergie des deux mécanismes est donnée par les équations (4.46) et (4.47).

4.3.2.1 Énergie consommée par le CSMA/CA avec PCA slotté

En utilisant les équations (4.23)-(4.26), l'énergie consommée E_{PCA} peut être dérivée comme suit

$$E_{PCA} = P_{cca}\Big(\sum_{i=0}^{W-1}\sum_{k=1}^{d} p_{i,k} + \sum_{k=2}^{d} p_{-1,k}\Big) + P_{trans}\sum_{k=0}^{L_p-1}\Big(p_{-2,k} + p_{-3,k}\Big) + P_i\Big(p_{-2,L_p} + p_{-3,L_p}\Big) + \sum_{k=L_p+1}^{L_p+L_{ack}+1}\Big(P_{rec}\ p_{-2,k} + P_i\ p_{-3,k}\Big). \tag{4.46}$$

4.3.2.2 Énergie consommée par le CSMA/CA slotté

A partir des équations (4.27)-(4.29), l'expression de E_{CSMA} est donnée par l'équation (4.48).

$$E_{CSMA} = P_i\sum_{i=0}^{m}\sum_{k=1}^{W_i-1}\sum_{j=0}^{n} b_{i,k,j} + P_{cca}\sum_{i=0}^{m}\sum_{j=0}^{n}\Big(b_{i,0,j} + b_{i,-1,j}\Big) + P_i\sum_{j=0}^{n}\Big(b_{-1,L_p,j} + b_{-2,L_p,j}\Big) + P_{tm}\sum_{k=0}^{L_p-1}\sum_{j=0}^{n}\Big(b_{-1,k,j} + b_{-2,k,j}\Big) + \sum_{j=0}^{n}\sum_{k=L_p+1}^{L_p+L_{ack}+1}\Big(P_{rec}\ b_{-2,k,j} + P_i\ b_{-1,k,j}\Big) \tag{4.47}$$

$$= \tau_{csma}\Bigg[\frac{P_i}{2}\Big(\frac{1-(2x)^{m+1}}{1-2x}\Big)\Big(\frac{1-x}{1-x^{m+1}}\Big) + 1 + P_{cca}\,(2-\alpha) + (1-x)\Big(P_{trans}L_p + P_i + (L_{ack}+1)\times[P_{rec}(1-P_e) + P_iP_e]\Big)\Bigg]. \tag{4.48}$$

4.3.3 Débit

Le débit comme défini dans [115] correspond à la fraction du temps où le canal est utilisé pour transmettre avec succès les charges utiles. Nous considérons les états du canal libre et occupé.

4.3.3.1 Débit de CSMA/CA avec backoff PCA slotté

Soit P_{busy}^{pca} la probabilité que le canal soit occupé, donnée comme suit

$$P_{busy}^{pca} = 1 - (1 - \tau_{pca})^N. \tag{4.49}$$

Soit $P_{success}^{pca}$ la probabilité d'une transmission réussie donnée par

$$P_{success}^{pca} = \frac{N\tau_{pca}(1 - \tau_{pca})^{N-1}}{P_{busy}^{pca}}. \tag{4.50}$$

Soit T_s la durée d'une transmission réussie. Son expression est donnée par (4.51).

$$T_s = L_p + T_{PHY} + T_{MAC} + 2T_{CCA} + T_{LIFS} + t_{ack-wait} + t_{ack}. \tag{4.51}$$

Soit T_e la durée d'une transmission non réussie (due à une collision ou à une erreur de transmission), donnée par

$$T_e = L_p + T_{PHY} + T_{MAC} + 2T_{CCA} + T_{LIFS} + t_{ack-wait}. \tag{4.52}$$

Alors, le débit associé pour CSMA/CA avec backoff PCA slotté est donné par l'expression (4.53).

$$Db_{PCA} = \frac{L_p\, P_{busy}^{pca}\, P_{success}^{pca}}{\sigma(1 - P_{busy}^{pca}) + T_s\, P_{busy}^{pca}\, P_{success}^{pca} + T_e\, P_{busy}^{pca}(1 - P_{success}^{pca})}. \tag{4.53}$$

Avec σ est la durée totale d'un slot de temps, t_{ack} est la durée de la trame ACK et $t_{ack-wait}$ est le temps d'attente avant de commencer la transmission de l'acquittement.

4.3.3.2 Débit de CSMA/CA slotté

Soit P_{busy}^{csma} la probabilité que le canal soit occupé donnée par

$$P_{busy}^{csma} = 1 - (1 - \tau_{csma})^N. \tag{4.54}$$

Soit $P_{success}^{csma}$ la probabilité d'une transmission réussie donnée par l'expression (4.55).

$$P_{success}^{csma} = \frac{N\tau_{csma}(1 - \tau_{csma})^{N-1}}{P_{busy}^{csma}}. \tag{4.55}$$

Alors, le débit associé pour CSMA/CA slotté est

$$Db_{CSMA} = \frac{L_p P_{busy}^{csma}\, P_{sucess}^{csma}}{\sigma(1 - P_{busy}^{csma}) + T_s\, P_{busy}^{csma}\, P_{succes}^{csma} + T_e\, P_{busy}^{csma}(1 - P_{success}^{csma})}. \tag{4.56}$$

Les expressions de T_s et T_e sont données par les équations (4.51) et (4.52), respectivement.

4.3.4 Délai

Le délai moyen pour un paquet reçu avec succès est défini comme l'intervalle de temps à partir de l'instant d'arrivée du paquet jusqu'à la réception de son ACK.

4.3.4.1 Délai de CSMA/CA avec backoff PCA slotté

Le délai moyen d'un paquet prioritaire reçu avec succès comprend le délai d'accès au canal, la durée de transmission du paquet et le temps nécessaire pour la réception de l'accusé de réception. Il est donné par l'expression (4.57).

$$D_{PCA} = T_{ds} + t_{ack} + T_b\, P_{access} \tag{4.57}$$

Où

- P_{access} est la probabilité d'avoir l'accès au canal avec une transmission réussie du paquet

$$P_{access} = \frac{Path_{success}}{(1-\beta)(1-P_e)\sum_{k=2}^{d} p_{-1,k}}.$$

- $Path_{success}$ représente tous les chemins menant de l'état d'arrivée des paquets (S) vers l'état succès.
- $T_{ds} = T_b L_s$ est le temps nécessaire pour une transmission réussie.
- T_b est la durée d'une unité backoff.

4.3.4.2 Délai de CSMA/CA slotté

Selon [34], le délai encouru par un paquet non prioritaire reçu avec succès est donné par

$$D_{CSMA} = T_{ds} + E[\tilde{T}_h] + \left(\frac{y_p}{1-y_p} - \frac{(n+1)\, y_p^{n+1}}{1-y_p^{n+1}}\right)\left(T_{df} + E[\tilde{T}_h]\right). \tag{4.58}$$

Où

- $E[\tilde{T}_h]$ indique le délai approximatif du backoff défini comme suit

$$E[\tilde{T}_h] = 2T_b\left[1 + \frac{1}{4}\left(\frac{1-\gamma}{1-\gamma^{m+1}}\left(2W_0\frac{1-(2\gamma)^{m+1}}{1-2\gamma} - \frac{3(m+1)\gamma}{1-\gamma}\right) + \frac{3\gamma}{1-\gamma} - (W_0+1)\right)\right]. \tag{4.59}$$

- $T_{df} = T_b\, L_f$ indique le temps pris pour une transmission non réussie.
- $\gamma = max(\alpha, \beta(1-\alpha))$.

4.4 Analyse de performances des mécanismes IEEE 802.15.4k PCA et CSMA/CA slotté

4.4.1 Méthode d'analyse et logiciels utilisés

À partir du modèle analytique proposé dans la section précédente (voir la section 4.2.4), nous allons dans un premier lieu résoudre le système d'équations non linéaire formé par les expressions de S_1, S_2, S_3, S_4, S_5, S_6, S_7, P_s, P_e, P_c, τ, α et β en utilisant les deux logiciels Mathcad et Matlab pour obtenir les résultats numériques de CSMA/CA avec backoff PCA slotté et CSMA/CA slotté de IEEE 802.15.4k.

Dans un second lieu, nous calculons les expressions de la fiabilité, de délai, de débit et de la consommation d'énergie dans un trafic saturé et dans des conditions de canal idéal ($BER = 0$) et non idéal ($BER = 4 * 10^{-3}$), et comparer les performances des deux mécanismes d'accès au médium. Après cela, nous évaluons les effets de la variation de la taille du réseau N, de la probabilité que le paquet soit prioritaire h_p, de la taille des paquets L_p et du taux d'erreur binaire BER sur les performances du système. Aussi, une étude comparative entre nos résultats et ceux du modèle de base IEEE 802.15.4 sera présentée.

4.4.2 Valeurs des paramètres utilisés

Le tableau 4.3 nous donne les différents paramètres utilisés pour l'analyse des performances.

TABLE 4.3 – Paramètres utilisés pour IEEE 802.15.4k CSMA/CA PCA slotté

Paramètre	Valeur	Paramètre	Valeur
$n, W, macMinBE$	3	$t_{ack-wait}$	$[1 - 1.32]\ ms$
m, d	5	T_{LIFS}	0.32 ms
$W_0, macMaxBE$	8	T_{CCA}	0.128 ms
N, h_p, L_p, BER	Variant	T_b	0.32 ms
P_{cca}	40 mW	t_{ack}	1 ms
P_i	0.8 mW	*Physical header length*	6 bytes
P_{trans}	30 mW	*MAC header length*	16 bytes
P_{rec}	40 mW	$L_c = L_f = L_s$	7 bytes
σ	0.96 ms	L_{ack}	1 byte
		l	20 bytes

4.4.3 Résultats, analyses et comparaisons

Dans cette sous-section, nous présentons les résultats analytiques obtenus pour les deux mécanismes CSMA/CA avec backoff PCA slotté et CSMA/CA slotté, en termes de probabilité d'échec, de fiabilité, de consommation énergétique, de débit et de délai, dans des conditions du canal idéal et non idéal. Par la suite, nous analysons l'impact de la variation du nombre de nœuds N, de la taille du paquet L_p, de la probabilité h_p et du taux d'erreur binaire BER sur les performances du réseau. De plus, nous comparons les performances de l'amendement "k" à celles de la norme de base.

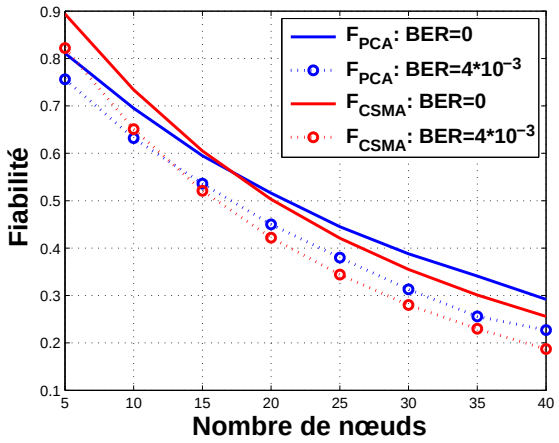
4.4.3.1 Performances du réseau en fonction de sa taille

La figure 4.2 trace les performances du réseau avec la variation de la taille du réseau. Où, $L_p = 8\ bytes$, $L_s = L_f = 7\ bytes$ et $h_p = 0,3$.

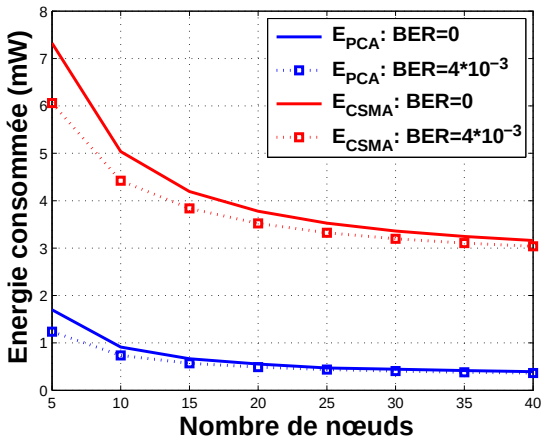
La figure 4.2(a) montre que lorsque nous augmentons le nombre de nœuds, la fiabilité diminue à la fois pour CSMA/CA avec backoff PCA et CSMA, quelles que soient les valeurs de BER. Ceci est dû à l'augmentation de la probabilité de collision et des erreurs de transmission lorsque la taille du réseau est importante. Nous notons également que CSMA/CA offre une fiabilité nettement meilleure par rapport à CSMA/CA avec backoff PCA lorsque $N < 17$ pour $BER = 0$, et lorsque $N < 15$ pour $BER = 4 * 10^{-3}$. Une dégradation des fiabilités F_{PCA} et F_{CSMA} est observée dans le cas du canal non idéal que dans le canal idéal.

En augmentant la taille du réseau N, une diminution de la consommation d'énergie pour les deux mécanismes et pour différents BER est observée sur la figure 4.2(b). Ceci est confirmé par le fait que lorsque N devient de plus en plus grand, le canal se trouve dans la plupart du temps occupé, et par conséquent, le nœud consomme moins d'énergie dans l'état idle (P_i). L'énergie consommée par CSMA/CA avec backoff PCA dans le cas du canal idéal ou non idéal est négligeable par rapport à CSMA/CA en raison de la possibilité de retransmission qui donne une consommation d'énergie supplémentaire pour le mécanisme CSMA/CA. Les résultats obtenus dans les conditions de canal non idéal sont meilleurs que ceux calculés dans des conditions de canal idéal.

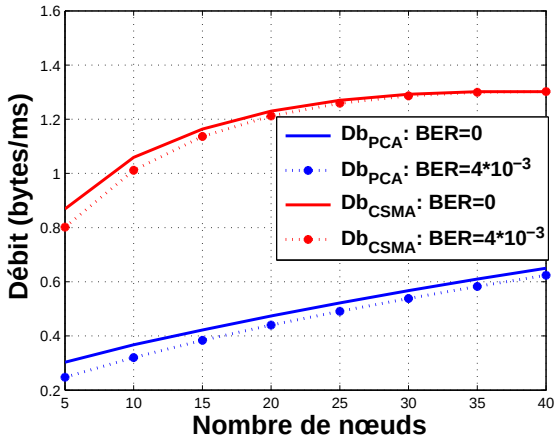
Dans la figure 4.2(c), nous représentons les deux débits Db_{PCA} et Db_{CSMA} par rapport à la variation de la taille du réseau avec des valeurs différentes de BER. Cette figure montre que le débit augmente avec l'augmentation de la taille du réseau, car la bande passante est de plus en plus utilisée. Nous notons que Db_{PCA} et Db_{CSMA} sont plus élevés pour $BER = 0$ (canal idéal) que pour $BER = 4 * 10^{-3}$ (canal non idéal). Le débit obtenu par CSMA/CA est plus élevé que celui obtenu par CSMA/CA avec backoff PCA à cause de la retransmission autorisée ($n = 3$) pour ce mécanisme.



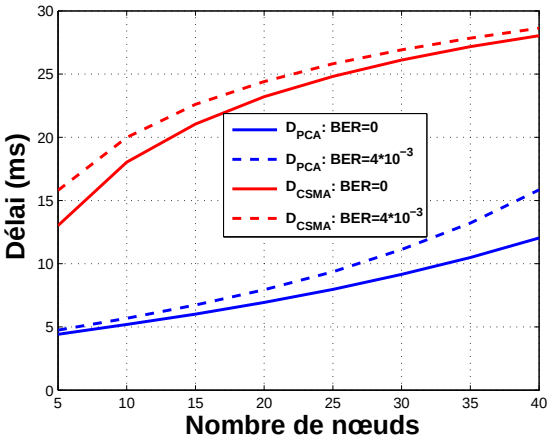
(a) Fiabilité Vs Nbre de nœuds



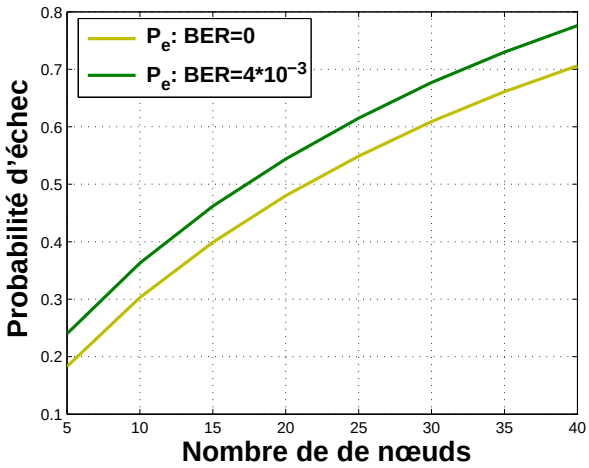
(b) Energie Vs Nbre de nœuds



(c) Débit Vs Nbre de nœuds



(d) Délai Vs Nbre de nœuds



(e) Probabilité d'échec Vs Nbre de nœuds

FIGURE 4.2 – Performances du PAN activé par balise Vs Taille du réseau.

Sur la figure 4.2(d), nous rapportons que le délai de CSMA/CA avec backoff PCA et celui de CSMA/CA augmentent avec l'augmentation de la taille du réseau, ce qui s'explique par le fait que le nœud dépense beaucoup de temps dans l'état du backoff (c-à-d. la probabilité de canal occupé est plus élevée) lorsque le nombre de nœuds est plus grand. CSMA/CA offre un délai plus élevé par rapport à CSMA/CA avec backoff PCA, car pour un nœud ayant un paquet prioritaire à transmettre, l'accès au canal sera plus rapide et le délai maximum pour l'accès au canal sera de d. Tandis que dans CSMA/CA, un délai de plus est dépensé lors des retransmissions. Nous notons également une légère augmentation des délais D_{PCA} et D_{CSMA} pour $BER = 4 * 10^{-3}$ par rapport à $BER = 0$.

La figure 4.2(e) montre la variation de la probabilité d'échec P_e par rapport à la taille du réseau avec différentes valeurs de BER. Lorsque N augmente, la probabilité de défaillance associée augmente en raison du risque élevé d'apparition des collisions et d'erreurs de transmission. Nous notons également que lorsque nous augmentons la valeur de BER, la probabilité P_e sera plus élevée que pour des valeurs plus petites.

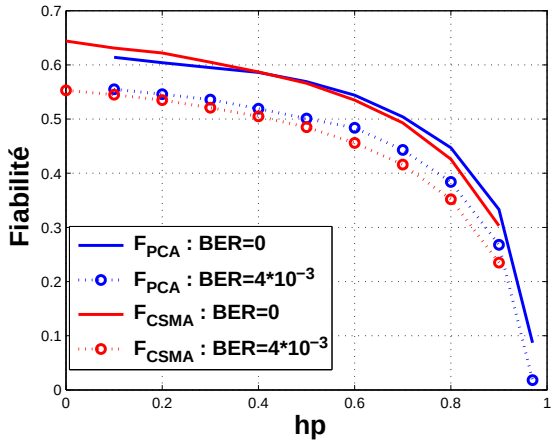
4.4.3.2 Performances du réseau en fonction de la probabilité que le paquet soit prioritaire

La figure 4.3 trace les performances du réseau avec variation de h_p dans des conditions de canal idéal et non idéal. Où, $L_p = 8\ bytes$, $L_s = L_f = 7\ bytes$ et $N = 15$.

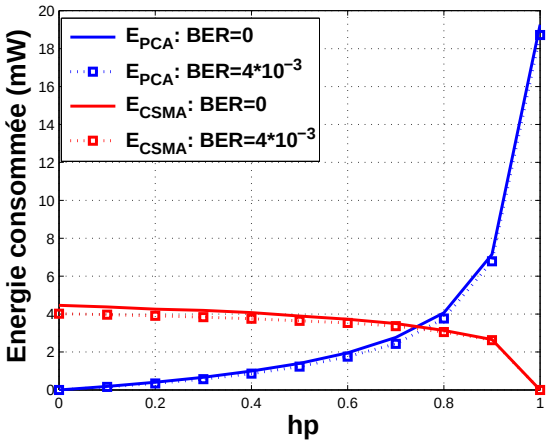
La figure 4.3(a) trace les fiabilités F_{PCA} et F_{CSMA} pour les deux valeurs de BER et pour différentes valeurs de h_p. Pour $BER = 0$, nous rapportons que la fiabilité offerte par CSMA est supérieure à celle offerte par PCA lorsque la probabilité que le paquet soit prioritaire est inférieure ou égale à 0.4 ($h_p \leq 0.4$), car il y a plus de paquets qui ne sont pas prioritaires dans la file d'attente que ceux qui sont non prioritaires. En revanche, elle est inférieure à celle de PCA quand $h_p > 0,4$, car il y'a plus de paquets prioritaires que ceux qui sont non prioritaires. Pour $BER = 4 * 10^{-3}$, la fiabilité offerte par PCA est supérieure à la fiabilité de CSMA/CA. Nous rapportons également une très forte diminution de la fiabilité à la fois pour CSMA/CA avec backoff PCA et pour CSMA/CA pour $BER = 4 * 10^{-3}$ que pour $BER = 0$, peu importe la valeur de la probabilité h_p.

Sur la figure 4.3(b), nous notons que chaque fois que nous augmentons le nombre de paquets prioritaires, E_{PCA} augmente. Par conséquent, E_{CSMA} diminue. L'énergie consommée dans le canal non idéal est légèrement inférieure à celle dans le canal idéal pour les deux mécanismes.

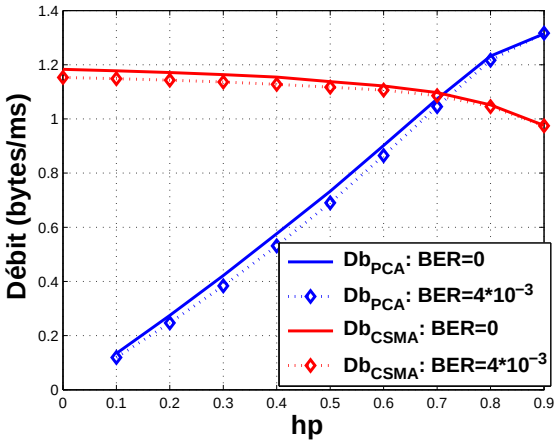
La figure 4.3(c) montre une augmentation significative du débit Db_{PCA} avec l'augmentation du nombre de paquets prioritaires. En revanche, une légère diminution de Db_{CSMA} est observée. Nous notons également que les débits de données pour les deux mécanismes sont meilleurs pour $BER = 0$



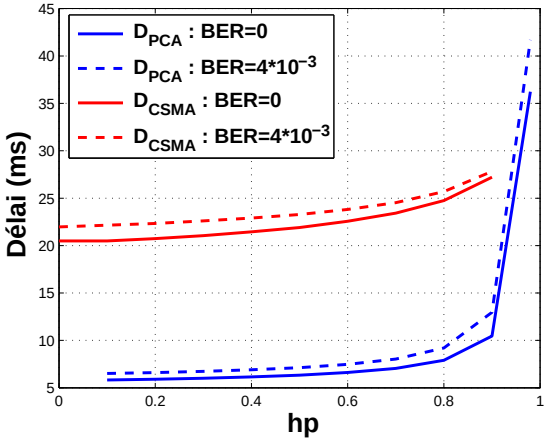
(a) Fiabilité Vs Probabilité h_p



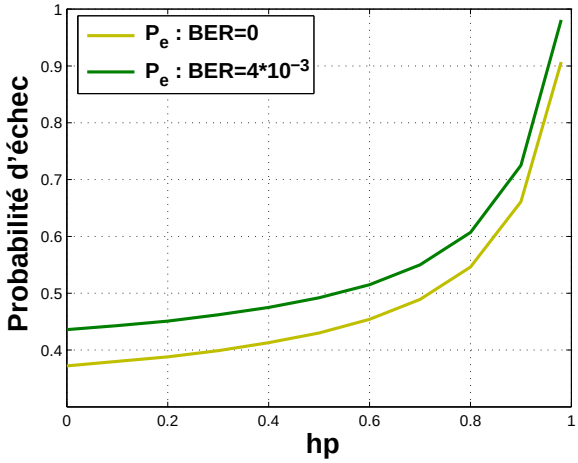
(b) Energie consommée Vs Probabilité h_p



(c) Débit Vs Probabilité h_p



(d) Délai Vs Probabilité h_p



(e) Probabilité d'échec Vs Probabilité h_p

FIGURE 4.3 – Performances du PAN activé par balise Vs probabilité que le paquet soit prioritaire h_p

que pour $BER = 4 * 10^{-3}$.

Sur la figure 4.3(d), le délai moyen augmente à mesure que h_p augmente pour les deux mécanismes. Comme la retransmission est autorisée pour le mécanisme CSMA/CA, le délai moyen offert par CSMA/CA est donc plus important que celui offert par CSMA/CA avec backoff PCA. Lorsque les erreurs de transmission sont considérées ($BER = 4 * 10^{-3}$), nous constatons une augmentation moyenne du délai par rapport au cas où les erreurs de transmission ne sont pas considérées ($BER = 0$).

La figure 4.3(e) trace la probabilité de défaillance avec l'augmentation de h_p. La probabilité P_e augmente avec l'augmentation de h_p. Nous notons une proportion directe avec l'augmentation de BER et l'augmentation de la probabilité de défaillance.

4.4.3.3 Performances du réseau en fonction de taux d'erreur binaire

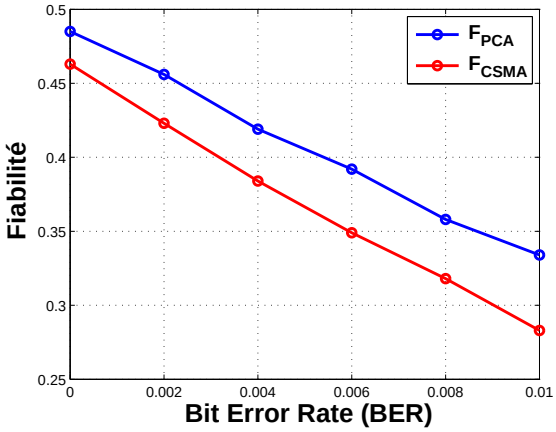
La figure 4.4 trace les performances du réseau avec la variation de BER. Les paramètres du modèle sont : $L_p = 8\ bytes$, $L_s = L_f = 7\ bytes$, $h_p = 0,3$ et $N = 20$.

Avec l'augmentation du BER, nous rapportons une diminution importante de la fiabilité pour CSMA/CA avec backoff PCA et pour CSMA/CA. En outre, PCA offre une fiabilité significativement meilleure que CSMA/CA, comme le montre la figure 4.4(a).

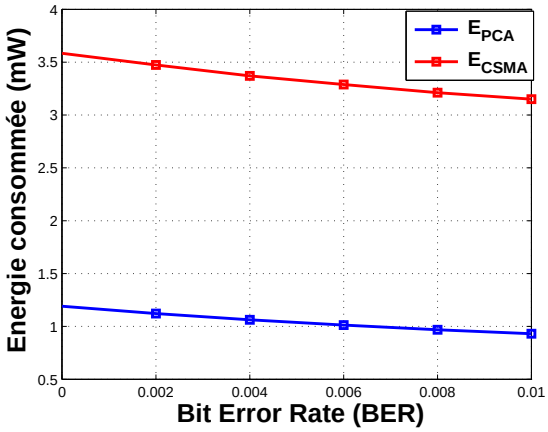
Sur la figure 4.4(b), nous notons une légère diminution de l'énergie consommée par IEEE 802.15.4k pour les deux mécanismes avec l'augmentation de BER. Rappelons que le mécanisme CSMA/CA permet une retransmission des paquets de données après l'échec de leur première tentative, par conséquent, l'énergie consommée par un paquet non prioritaire est très importante par rapport à l'énergie consommée par un paquet prioritaire.

La figure 4.4(c) montre l'effet de l'augmentation du BER sur le débit pour les deux mécanismes. Nous rapportons une légère diminution pour Db_{CSMA} mais une diminution significative de Db_{PCA}. Le débit offert par CSMA/CA est nettement supérieur à celui de PCA, car il y a beaucoup de paquets non prioritaires que de prioritaires ($h_p = 0.3$). Par conséquent, le nombre de paquets non prioritaires transmis avec succès dans une milli-seconde est nettement grand.

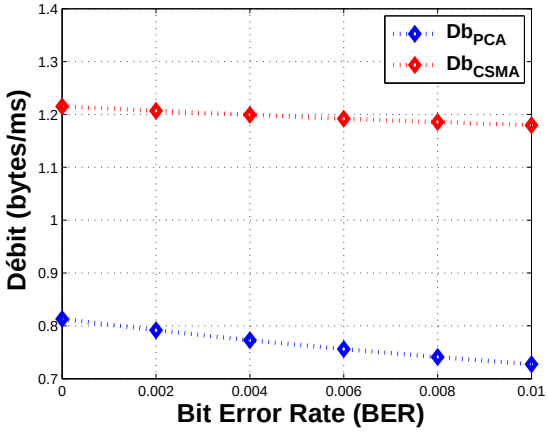
Dans la figure 4.4(d), nous rapportons une augmentation du délai moyen avec l'augmentation du taux d'erreur binaire. Le délai moyen offert par CSMA/CA avec backoff PCA est négligeable par rapport à celui offert par CSMA/CA, car le délai maximum de l'accès au canal pouvant être atteint par le mécanisme PCA est de d. Tandis que CSMA/CA perd beaucoup de temps dans chaque transmission et retransmission.



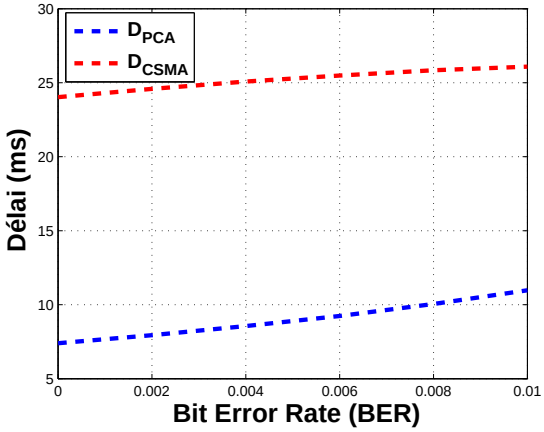
(a) Fiabilité Vs BER



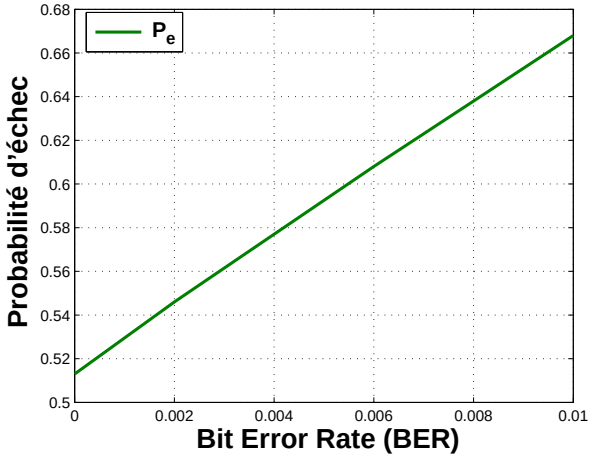
(b) Energie Vs BER



(c) Débit Vs BER



(d) Délai Vs BER



(e) Probabilité d'échec Vs BER

FIGURE 4.4 – Performances du PAN activé par balise Vs BER.

La figure 4.4(e) montre la probabilité de défaillance par rapport à BER. À mesure que nous augmentons le BER, la probabilité d'erreur de transmission augmente, donc la probabilité de défaillance augmente.

4.4.3.4 Performances du réseau en fonction de la taille du paquet

La figure 4.5 trace les performances des deux mécanismes de IEEE 802.15.4k avec une variation de la taille du paquet. Où, $L_s = L_f = 7\ bytes$, $h_p = 0,3$ et $N = 20$.

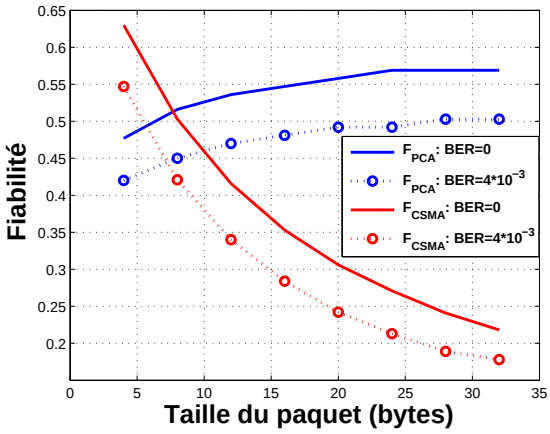
Dans la figure 4.5(a), nous rapportons que le $F_{CSMA/CA}$ diminue et le F_{PCA} augmente en augmentant la longueur du paquet de données, quelle que soit la valeur de BER. De plus, la fiabilité dans le canal idéal est plus élevée que dans le canal non idéal pour différentes longueurs de paquet de données.

La figure 4.5(b) trace la variation de la consommation d'énergie en fonction des différentes tailles du paquet de données. Nous notons que l'énergie consommée pour les deux mécanismes diminue en augmentant la longueur du paquet de données dans les conditions du canal idéal et non idéal, car les collisions et les erreurs de transmission sont plus probables lorsque la taille du paquet devient grande. L'énergie E_{PCA} est moins importante que le E_{CSMA} en raison de la possibilité de retransmission offerte pour le mécanisme CSMA/CA.

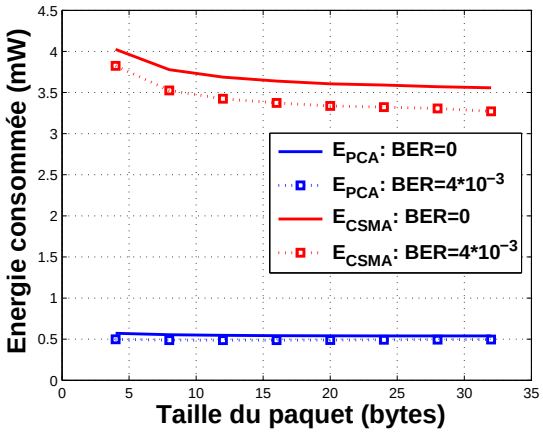
Lorsque la longueur des paquets devient de plus en plus importante, la quantité de données transmise augmente, comme le montre la figure 4.5(c). Nous notons que Db_{CSMA} est plus important que le Db_{PCA} à cause de la retransmission ($n = 3$). Le débit IEEE 802.1.4k offert dans un canal non idéal est légèrement inférieur à celui offert dans des conditions de canal idéal en raison des erreurs de transmission.

La figure 4.5(d) trace la variation du délai en fonction de la taille du paquet. Avec l'augmentation de la taille des paquets, les délais de transmission D_{CSMA} et D_{PCA} augmentent. Nous notons une grande différence entre le délai offert par CSMA/CA et CSMA/CA avec backoff PCA car lorsque un paquet non prioritaire subit un échec de transmission, trois autres possibilités de retransmission sont offertes. Comme le montre la figure, les résultats obtenus pour $BER = 0$ sont meilleurs que ceux pour $BER = 4 * 10^{-3}$.

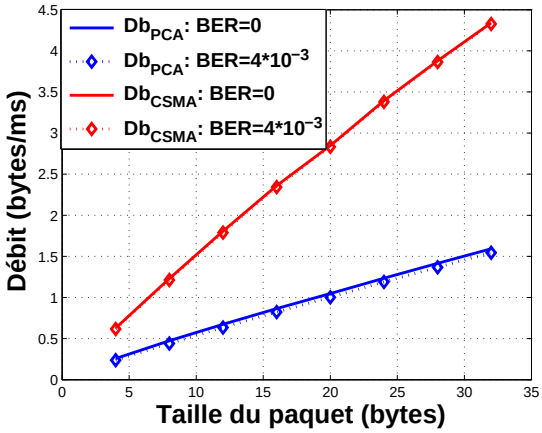
Dans la figure 4.5(e), nous rapportons que la probabilité d'échec diminue avec l'augmentation de la longueur du paquet pour les deux valeurs BER. P_e est plus élevé dans le canal non idéal par rapport aux conditions de canal idéal.



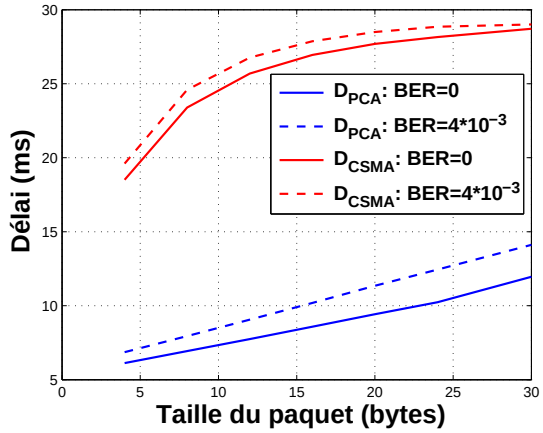
(a) Fiabilité Vs Taille du paquet



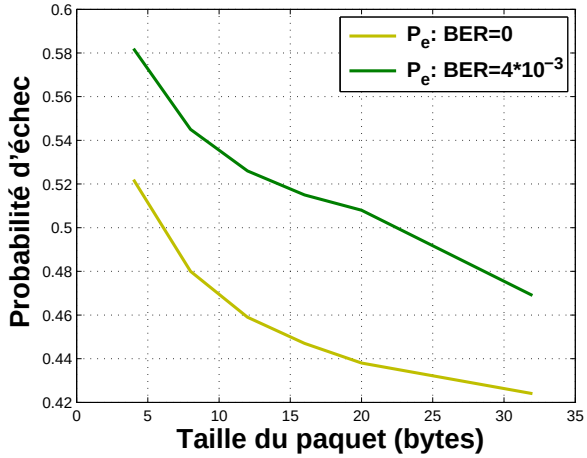
(b) Energie Vs Taille du paquet



(c) Débit Vs Taille du paquet

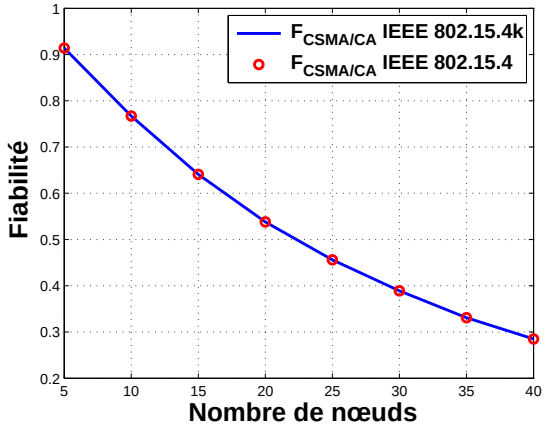


(d) Délai Vs Taille du paquet

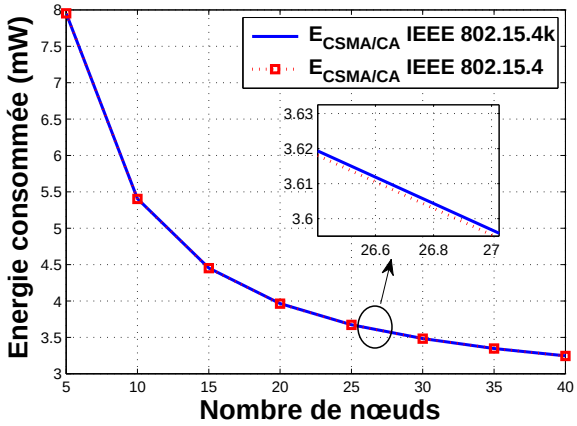


(e) Probabilité d'échec Vs Taille du paquet

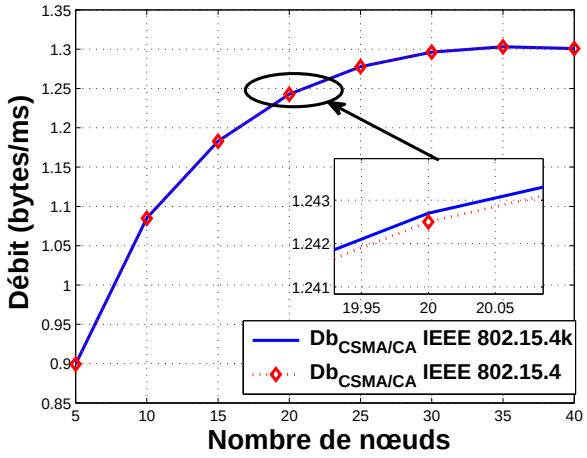
FIGURE 4.5 – Performances du PAN activé par balise Vs Taille du paquet



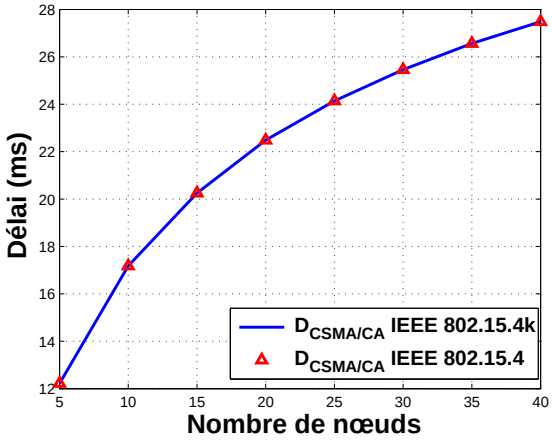
(a) Fiabilité Vs Nbre de nœuds



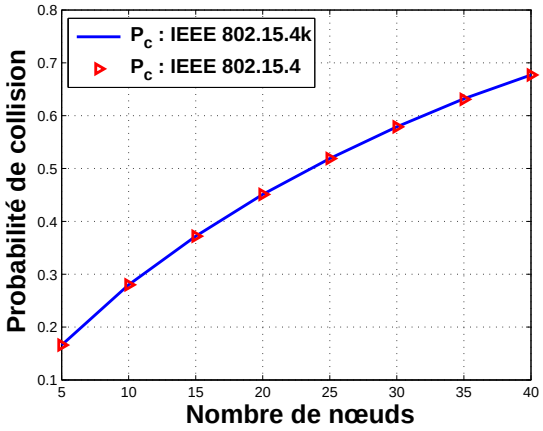
(b) Energie Vs Nbre de nœuds



(c) Débit Vs Nbre de nœuds



(d) Délai Vs Nbre de nœuds



(e) Probabilité de collision Vs Nbre de nœuds

FIGURE 4.6 – Performances de IEEE 802.15.4k CSMA/CA et IEEE 802.15.4 CSMA/CA Vs Taille du réseau

4.4.3.5 CSMA/CA IEEE 802.15.4k et CSMA/CA IEEE 802.15.4

Une comparaison entre notre modèle IEEE 802.15.4k CSMA/CA et celui du modèle IEEE 802.15.4 CSMA/CA de base sera présentée, dans des conditions de trafic saturé et sous un canal idéal. Le modèle de base considéré est celui dans [27], mais considérant un état de trafic saturé au lieu d'un trafic non saturé. En plus, nous supposons qu'il n'y a pas de paquets prioritaires dans le réseau ($h_p = 0$).

La figure 4.6 trace les performances du réseau pour les deux mécanismes de IEEE 802.15.4k CSMA/CA et IEEE 802.15.4 CSMA/CA en fonction de la variation de la taille du réseau. Les paramètres du modèle utilisés sont : $L_p = 8\ bytes$ et $L_s = L_c = 7\ bytes$.

Nous notons que les résultats obtenus pour la fiabilité et le délai de IEEE 802.15.4k sont exactement les mêmes que les résultats du standard de base comme le montrent les figures 4.6(a) et 4.6(d), respectivement.

Sur les figures 4.6(b) et 4.6(c), il y a une légère augmentation de l'énergie consommée et du débit offert par la norme IEEE 802.15.4k par rapport à la norme IEEE 802.15.4, car la valeur P_s est un peu plus élevée que la valeur $b_{0,0,0}$.

4.5 Conclusion

Dans ce chapitre, nous avons présenté un nouveau modèle analytique basé sur une chaîne de Markov pour analyser les performances des deux mécanismes slotté de IEEE 802.15.4k. Le modèle proposé prend en compte un nombre fixe de nœuds disposés en topologie en étoile, un trafic saturé, des conditions de canal bruité, un mécanisme d'accusé de réception et des limites de retransmission. Nous avons dérivé les expressions mathématiques de fiabilité, de consommation d'énergie, de délai moyen pour une transmission de paquets réussie et de débit offerts par la norme IEEE 802.15.4k en mode beacon pour les paquets prioritaires et non prioritaires. Nous avons analysé l'impact de la variation de la taille du réseau, la probabilité que le paquet disponible soit prioritaire, le taux d'erreur binaire et la longueur du paquet sur la probabilité d'échec et les métriques étudiées.

A l'issue de cette étude, nous avons constaté qu'à mesure que nous augmentons la taille des paquets, la probabilité d'une transmission réussie des paquets prioritaires augmente en parallèle. Avec l'augmentation de la taille du réseau, une fiabilité plus élevée, un délai plus faible, une consommation d'énergie négligeable et un débit plus faible sont observés pour les paquets prioritaires par rapport aux non prioritaires.

Chapitre5

Modélisation analytique et évaluation des performances du mécanisme IEEE 802.15.4k CSMA/CA avec backoff PCA non slotté

Sommaire

5.1 Introduction

Dans le cas d'absence de la structure de la supertrame, la transmission d'un message prioritaire se fait dans un mode non beacon grâce au mécanisme CSMA/CA avec backoff PCA non slotté et celle d'un message non prioritaire grâce à CSMA/CA non slotté du standard IEEE 802.15.4k. Une modélisation mathématique par chaîne de Markov et une évaluation de leurs performances seront présentées dans ce présent chapitre. Notre modèle mathématique est le premier, dans la littérature, réalisé dans des conditions de canal bruité. Des conditions de saturation de trafic seront considérées dans un réseau de topologie en étoile. De plus, pour tester l'efficacité de notre modèle, nous allons analyser l'impact de la variation de la taille du réseau, de la probabilité que le paquet disponible soit prioritaire, du taux d'erreur binaire et de la taille des paquets sur la fiabilité, la consommation d'énergie et le débit, afin de comparer les performances des deux mécanismes.

5.2 Modélisation analytique des mécanismes d'accès au canal CSMA/CA PCA et CSMA/CA non slotté

Dans cette section, nous présentons le modèle analytique proposé pour les mécanismes CSMA/CA avec backoff PCA non slotté et CSMA/CA non slotté de IEEE IEEE 802.15.4k dans des conditions de saturation de trafic, sous un canal bruité avec considération des acquittements. Comme soulignée dans le chapitre 4, si la station ne reçoit pas d'acquittement pour une trame donnée, elle considère qu'une collision ou une erreur de transmission a eu lieu sur le canal.

5.2.1 Hypothèses du modèle

Nous considérons les hypothèses suivantes dans lesquelles notre modèle de CM est applicable.

1. N nœuds disposés en topologie en étoile autour d'un coordinateur PAN,
2. Une condition de trafic saturé,
3. Prise en compte des erreurs de transmission (canal bruité),
4. Prise en charge des accusés de réception.

5.2.2 Paramètres et notations utilisés dans le modèle

Les paramètres importants dans notre modèle sont représentés dans le tableau 5.1.

TABLE 5.1 – Paramètres du modèle IEEE 802.15.4k CSMA/CA PCA non slotté

Paramètre	Description
N	La taille du réseau
Q	L'état idle
n	Le nombre maximum de retransmissions
m	L'étage maximum du backoff pour CSMA/CA
W_0	La taille minimale de la fenêtre de contention correspondant à la première tentative de transmission
W	Le nombre d'étages de backoff pour CSMA/CA avec backoff PCA
L_p	La taille du paquet
L_s	La taille du paquet reçu avec succès
L_c	La taille du paquet collisioné
L_f	La taille du paquet non reçu
L_{ack}	La taille de l'ACK

5.2.3 Les probabilités utilisées dans le modèle

Dans le tableau 5.2, nous présenterons les différentes probabilités indispensables à la réalisation de notre modèle.

TABLE 5.2 – Probabilités du modèle IEEE 802.15.4k CSMA/CA PCA non slotté

Probabilités	Description
h_p	La probabilité que le paquet soit prioritaire
α	La probabilité que le canal soit occupé dans le CCA
P_Q	La probabilité de résider dans l'état idle
τ	La probabilité qu'un nœud tente d'effectuer le CCA sur un slot de temps
P_c	La probabilité de collision
P_{te}	La probabilité d'erreur
P_e	La probabilité d'échec de transmission
$p_{i,k}$	Les probabilités des états de la chaîne de Markov associées à PCA non slotté
$b_{i,k,j}$	Les probabilités des états de la chaîne de Markov associées à CSMA/CA non slotté

5.2.4 La chaîne de Markov proposée

Notre modèle de chaîne de Markov des deux mécanismes CSMA/CA non slotté avec backoff PCA et CSMA/CA non slotté de l'amendement IEEE 802.15.4k est défini par son graphe de transition, illustré dans la figure 5.1.

Les probabilités h_p et $(1 - h_p)$ représentent les probabilités que le paquet disponible soit prioritaire ou non prioritaire, respectivement. Soit α la probabilité que le canal soit occupé dans le CCA, P_e la probabilité d'echec de transmission (collision ou soit transmis avec des erreurs). Soit Q l'état des arrivées des paquets et qui se produit à la fin des tentatives d'accès au canal dans les différents cas (succès, échec ou délai dépassé) pour les deux mécanismes. Notons par P_Q sa probabilité associée.

Les deux processus stochastiques de notre chaîne de Markov sont décrits comme suit :

- Les états de la chaîne de Markov associés aux paquets prioritaires sont guidés par un processus stochastique bidimensionnel $\Big(c(t), d(t)\Big)$, où $c(t)$ représente le compteur d'attente backoff et $d(t)$ représente le délai encouru par le paquet. Les états (i,k), $i \in [0, W-1]$, $k \in [1,d]$ représentent les périodes d'attente backoff. Les états $(0,k)$, $k \in [1,d]$ représentent le CCA. Les états allant de $(-2,0)$ à $(-2, L_s - 1)$ et de $(-3,0)$ à $(-3, L_f - 1)$ représentent une transmission réussie et non réussie, respectivement. L_s et L_f indiquent respectivement la taille des paquets transmis

avec succès ou non transmis.

- Les états de la chaîne de Markov associés aux paquets non prioritaires sont guidés par un processus stochastique tridimensionnel $\big(s(t), c(t), r(t)\big)$, où $s(t)$ représente l'étage du backoff, $c(t)$ le compteur du backoff et $r(t)$ l'état du compteur de transmission ou retransmission au temps t.

  Les états (i, k, j), $i \in [0, m]$, $k \in [0, W_i - 1]$, $j \in [0, n]$ représentent les états de backoff. Les états $(i, 0, j)$, $i \in [0, m]$, $j \in [0, n]$ représentent le CCA. Les états allant de $(-2, 0, j)$ à $(-2, L_s - 1, j)$ et de $(-1, 0, j)$ à $(-1, L_f - 1, j)$, $j \in [0, n]$ modélisent la transmission réussie et non réussie, respectivement.

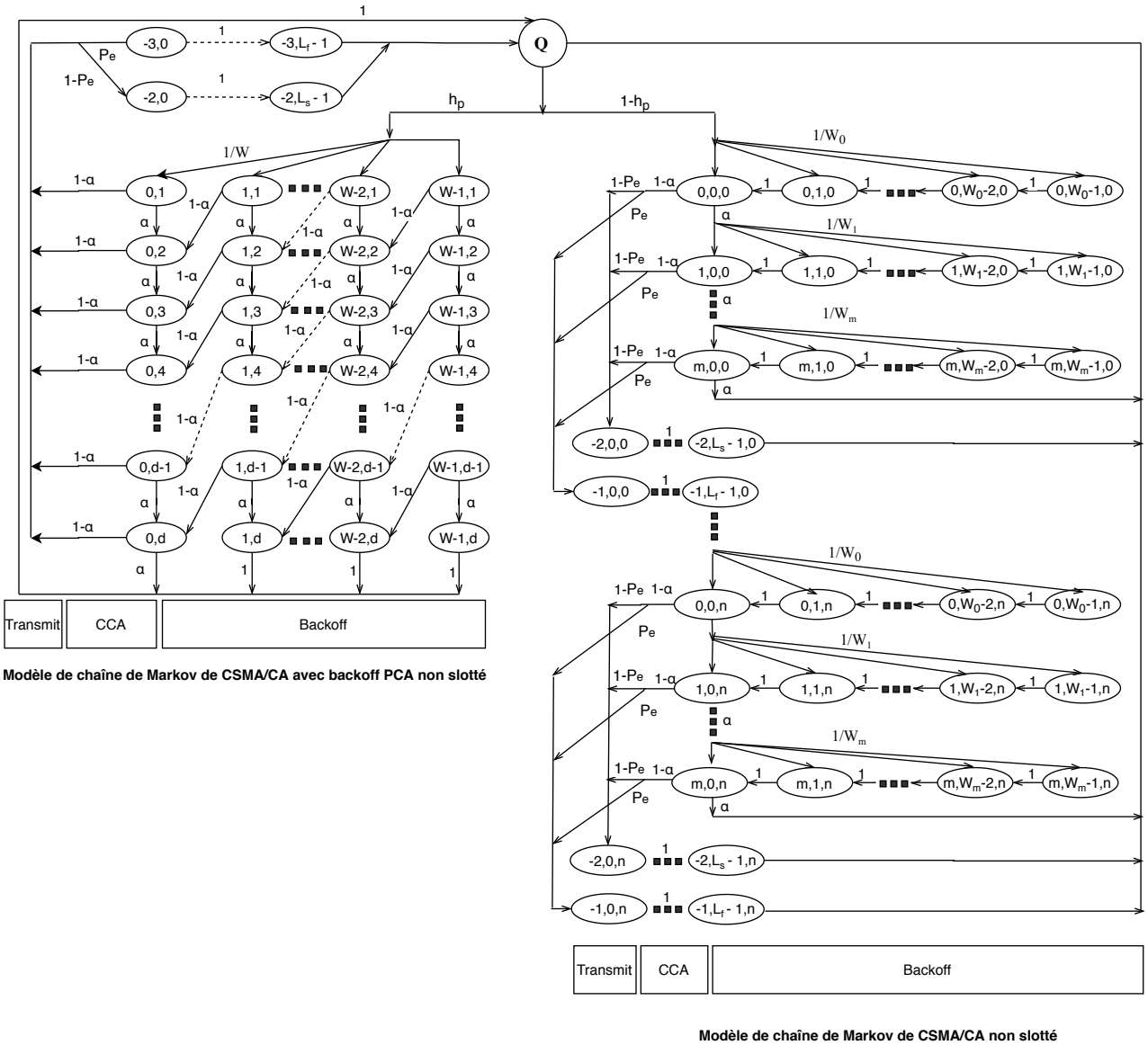


FIGURE 5.1 – Chaîne de Markov des mécanismes de IEEE 802.15.4k non slotté.

5.2.4.1 Probabilités de transition

A partir de la figure 5.1, les probabilités de transition associées à la chaîne de Markov sont décrites comme suit

$$P(-2,0|0,k) = (1-\alpha)(1-P_e), \forall\ k \in [1,d]. \tag{5.1}$$

$$P(-3,0|0,k) = (1-\alpha)\ P_e\ , \forall\ k \in [1,d]. \tag{5.2}$$

$$P(Q|i,d) = 1, \forall\ i \in [0,W-1]. \tag{5.3}$$

$$P(i,1|Q) = \frac{h_p}{W}. \tag{5.4}$$

$$P(i,k|i,k-1) = \alpha, \forall\ i \in [1,W-1], k \in [2,d]. \tag{5.5}$$

$$P(Q|0,d) = \alpha. \tag{5.6}$$

$$P(i,k,j|i,k+1,j) = 1, \forall i \in [0,m], k \in [0,W_i-1], j \in [0,n]. \tag{5.7}$$

$$P(i,k,j|i-1,0,j-1) = \frac{\alpha}{W_i}, \forall\ i \in [0,m], k \in [0,W_i-1], j \in [0,n]. \tag{5.8}$$

$$P(0,k,j|i,0,j-1) = \frac{(1-\alpha)P_e}{W_0}, \forall\ i \in [0,m], k \in [0,W_i-1]. \tag{5.9}$$

$$P(0,k,0|Q) = \frac{(1-h_p)}{W_0}. \tag{5.10}$$

$$P(Q|m,0,j) = \alpha, \forall\ i \in [0,m], j \in [0,n]. \tag{5.11}$$

$$P(-2,0,j|i,0,j) = (1-\alpha)(1-P_e), \forall\ i \in [0,m], j \in [0,n]. \tag{5.12}$$

$$P(-1,0,j|i,0,j) = (1-\alpha)\ P_e, \forall\ i \in [0,m], j \in [0,n]. \tag{5.13}$$

Les équations (5.1) et (5.2) représentent les probabilités de transition de l'état CCA de CSMA/CA avec backoff PCA au états succès et échec, respectivement. L'équation (5.3) est la probabilité d'écraser un paquet prioritaire lorsque le délai maximum est atteint. Les équations (5.4) et (5.10) modélisent la probabilité de sélectionner un état de backoff aléatoirement à partir de l'état idle pour PCA et CSMA/CA, respectivement. L'équation (5.5) représente la probabilité de trouver un canal occupé à l'étage du backoff i et réessayer d'accéder au canal en utilisant CSMA/CA avec backoff PCA. La probabilité d'écraser le paquet prioritaire en raison de délai dépassée est donnee par l'équation (5.6). Le compteur du backoff décrémente dans CSMA/CA avec la probabilité exprimée dans (5.7). L'équation (5.8) représente la probabilité de trouver le canal occupé dans l'étage de backoff i et de sélectionner un état uniformément dans le prochain étage $i+1$. La probabilité d'échec de transmission dans le dernier étage du backoff (m) après avoir trouvé le canal occupé dans CCA est exprimée dans (5.9), où le nœud sélectionne uniformément un état dans la prochaine étape de retransmission. L'équation (5.11) est la probabilité de revenir à l'état de sommeil (état idle) lorsque le maximum

compteur du backoff (i.e, m) ou lorsque la dernière tentative de retransmission n sont atteints. Les équations (5.12) et (5.13) représentent les probabilités de transition de l'état CCA de CSMA/CA aux états succès et échec, respectivement.

Nous utilisons les équations de (5.1) à (5.13) pour calculer la distribution stationnaire de la chaîne de Markov proposée.

5.2.4.2 Probabilités d'états stationnaires

Le calcul de la distribution stationnaire est essentielle pour dériver les métriques de performance des deux mécanismes, en termes de fiabilité, de consommation d'énergie et de débit. Nous représentons par $p_{i,k}$ les probabilités des états de la chaîne de Markov associée à CSMA/CA avec backoff PCA non slotté et par $b_{i,k,j}$ les probabilités des états de la chaîne de Markov associée à CSMA/CA non slotté.

a) La probabilité stationnaire associée à CSMA/CA avec backoff PCA non slotté

Pour calculer la distribution $p_{i,k}$, il faut d'abord passer par le calcul de $p_{i,1}$ et $p_{i,2}$, où le délai encouru est égal à 1 et 2, respectivement.

Selon le modèle de chaîne de Markov de CSMA/CA avec PCA backoff non slotté donné dans la figure 5.1, nous avons

- La probabilité qu'un nœud ayant un paquet prioritaire à transmettre sélectionne l'un des états de backoff aléatoires est exprimée par l'équation (5.14).

$$p_{i,1} = \frac{P_Q\, h_p}{W}\ ,\ \forall\ i \in [0, W-1]. \tag{5.14}$$

- La probabilité que le compteur aléatoire soit égal à i et que le délai encouru soit égal à 2 est donnée comme suit

$$p_{i,2} = \begin{cases} \alpha p_{i,1} + (1-\alpha)\, p_{i+1,1} & ,\ i \in [0, W-2], \\ \alpha p_{i,1} & ,\ i = W-1. \end{cases} \tag{5.15}$$

- En utilisant les équations (5.14) et (5.15) et en exploitant la récurrence, la probabilité de tout état de backoff dans CSMA/CA avec backoff PCA non slotté est

$$p_{i,k} = \sum_{j=0}^{min(W-1-i,k-1)} C_{k-1}^{j}\, (1-\alpha)^j\, \alpha^{k-j-1} \frac{P_Q\, h_p}{W}\ ,\forall\ i \in [1, W-1]\ , k \in [1, d]. \tag{5.16}$$

Où, $C_u^k = \binom{u}{k}$ représente la combinaison de u objets pris k à la fois.

- La probabilité que le nœud tente un CCA dans l'état $(0, k)$ est exprimée par

$$p_{0,k} = \sum_{j=0}^{min(W-1,k-1)} C_{k-1}^{j} \, (1-\alpha)^{j} \, \alpha^{k-j-1} \frac{P_Q \, h_p}{W}, \; k \in [1, d]. \tag{5.17}$$

- La probabilité d'état de transmission non réussie est décrite dans l'équation (5.18).

$$p_{-3,0} = (1-\alpha) \, P_e \sum_{k=1}^{d} p_{0,k}. \tag{5.18}$$

- La probabilité de l'état de transmission réussie est donnée comme suit

$$p_{-2,0} = (1-\alpha)(1-P_e) \sum_{k=1}^{d} p_{0,k}. \tag{5.19}$$

b) La probabilité stationnaire associé à CSMA/CA non slotté

Soit $b_{i,k,j} = \lim_{t \to +\infty} P(s(t) = i, c(t) = k, r(t) = j), k \in (-1, max(W_i - 1, L_s - 1, L_f - 1)), j \in [0, n], i \in [-2, m]$ la probabilité stationnaire de la chaîne de Markov associée au mécanisme CSMA/CA non slotté. Selon le modèle de chaîne de Markov de CSMA/CA non slotté donné dans la figure 5.1 et basé sur [27], mais en tenant compte des erreurs de transmission, nous obtenons les équations (5.20) - (5.26).

Pour $i \in [0, m]$, nous avons

$$b_{i,k,j} = \frac{W_i - k}{W_i} \, b_{i,0,j} \; , \; \forall \; k \in [0, W_i - 1]. \tag{5.20}$$

Où, la valeur du compteur de backoff W_i est uniformément choisie à l'étage i sur l'intervalle $[0, W_i - 1]$, comme exprimée dans l'expression (5.21).

$$W_i = \begin{cases} 2^i W_0 & i \leq m_b - m_0 \\ 2^{m_b - m_0} W_0 & i \in]m_b - m_0, m]. \end{cases} \tag{5.21}$$

Avec $W_0 = 2^{macMinBE}$, $m_b = macMaxBE$ et $m_0 = macMinBE$ (voir le tableau 5.3).

- La probabilité que le nœud tente un CCA dans l'état $(i, 0, j)$ est donnée comme suit

$$b_{i,0,j} = \alpha^i \, b_{0,0,j}, \forall \; i \in [0, m], \, j \in [0, n]. \tag{5.22}$$

- La probabilité de retransmission après m tentatives échouées d'accès au canal est donnée dans (5.23).

$$b_{0,0,j} = \left(P_e (1-\alpha) \sum_{i=0}^{m} b_{i,0,j-1} \right)^j = y_p^j \, b_{0,0,0} \; , \forall \; j \in [0, n]. \tag{5.23}$$

Où $y_p = P_e\ (1-\alpha^{m+1})$ représente la probabilité que le nœud accède au canal dans les m étages du backoff avec occurrence d'une erreur de transmission ou d'une collision.

- La probabilité de résider dans l'état $(0,0,0)$ est

$$b_{0,0,0} = \frac{(1-h_p)\ P_Q}{W_0} + \sum_{k=1}^{W_0-1} b_{0,k,0} = (1-h_p)\ P_Q. \tag{5.24}$$

- La probabilité d'un état de transmission réussie est donnée par l'équation (5.25).

$$b_{-2,0,j} = (1-P_e)(1-\alpha^{m+1})\ b_{0,0,j}\ \ ,\forall\ \ j \in [0,n]. \tag{5.25}$$

- La probabilité d'un état de transmission non réussie est

$$b_{-1,0,j} = P_e\ (1-\alpha^{m+1})\ b_{0,0,j}\ \ ,\forall\ \ j \in [0,n]. \tag{5.26}$$

c) Calcul de la probabilité de résider dans l'état Q

Toutes les probabilités tirées du graphe de transition sont données en fonction de la probabilité P_Q. Afin de dériver P_Q, nous développons la propriété de normalisation donnée par l'équation (5.27).

$$\sum_{i=0}^{W-1}\sum_{k=1}^{d} p_{i,k} + \sum_{k=0}^{L_s-1} p_{-2,k} + \sum_{k=0}^{L_f-1} p_{-3,k} + \sum_{i=0}^{m}\sum_{k=0}^{W_i-1}\sum_{j=0}^{n} b_{i,k,j} + \sum_{j=0}^{n}\left(\sum_{k=0}^{L_s-1} b_{-2,k,j} + \sum_{k=0}^{L_f-1} b_{-1,k,j}\right) = 1. \tag{5.27}$$

En utilisant les équations (5.16) et (5.17), le premier terme est obtenu comme suit

$$\sum_{i=0}^{W-1}\sum_{k=1}^{d} p_{i,k} = \sum_{k=1}^{d} p_{0,k} + \sum_{i=1}^{W-1}\sum_{k=1}^{d} p_{i,k} = \frac{h_p}{W}\Bigg[\sum_{k=1}^{d}\sum_{j=0}^{min(W-1,k-1)} C_{k-1}^{j}(1-\alpha)^j\alpha^{k-j-1} +$$

$$\sum_{i=0}^{W-1}\sum_{k=1}^{d}\sum_{j=0}^{min(W-1-i,k-1)} C_{k-1}^{j}(1-\alpha)^j\alpha^{k-j-1}\Bigg] \times P_Q = S_1 P_Q. \tag{5.28}$$

En utilisant l'expression donnée dans (5.19), le deuxième terme est

$$\sum_{k=0}^{L_s-1} p_{-2,k} = L_s\ (1-\alpha)(1-P_e)\sum_{k=1}^{d} p_{0,k} = L_s(1-\alpha)(1-P_e)\frac{P_Q\ h_p}{W} \times \sum_{k=1}^{d}\sum_{j=0}^{min(W-1,k-1)} C_j^{k-1}(1-\alpha)^j\alpha^{k-j-1} = S_2 P_Q. \tag{5.29}$$

D'après l'équation (5.18), le troisième terme est décrit dans (5.30).

$$\sum_{k=0}^{L_f-1} p_{-3,k} = L_f\ (1-\alpha)P_e\sum_{k=1}^{d} p_{0,k} = L_f(1-\alpha)P_e\frac{P_Q\ h_p}{W} \times \sum_{k=1}^{d}\sum_{j=0}^{min(W-1,k-1)} C_j^{k-1}(1-\alpha)^j\alpha^{k-j-1} = S_3 P_Q. \tag{5.30}$$

D'après les équations (5.20) et (5.21), le quatrième terme est obtenu comme suit

$$\sum_{i=0}^{m}\sum_{k=0}^{W_i-1}\sum_{j=0}^{n} b_{i,k,j} = \sum_{i=0}^{m}\sum_{j=0}^{n}\frac{W_i+1}{2}\alpha^i\ b_{0,0,j} = S_4 P_Q. \tag{5.31}$$

Où,

$$b_{i,k,j} = \begin{cases} \frac{(1-h_p)P_s}{2}\left[\frac{1-(2x)^{m+1}}{1-2x}W_0 + \frac{1-x^{m+1}}{1-x}\right]\frac{1-y_p^{n+1}}{1-y_p}, & if\ m \leq m_b - m_0 \\ \frac{(1-h_p)P_s}{2}\left[\frac{1-(2x)^{m_b-m_0+1}}{1-2x}W_0 + \frac{1-x^{m_b-m_0+1}}{1-x} + (2^{m_b}+1)x^{m_b-m_0+1}\frac{1-x^{m_b-m_0+1}}{1-x}\right]\frac{1-y_p^{n+1}}{1-y_p}, & if\ m > m_b - m_0. \end{cases} \tag{5.32}$$

En utilisant les expressions (5.22)-(5.26), le cinquième terme est donné par l'équation (5.33).

$$\sum_{j=0}^{n}\Big(\sum_{k=0}^{L_s-1} b_{-2,k,j} + \sum_{k=0}^{L_f-1} b_{-1,k,j}\Big) = P_Q\,(1-h_p)\Big[L_s\,(1-P_e)(1-\alpha^{m+1}) + L_f\,P_e\Big]\,\frac{1-y_p^{n+1}}{1-y_p} = S_5 P_Q. \tag{5.33}$$

La probabilité P_Q est alors exprimée comme suit

$$P_Q = \frac{1}{S_1 + S_2 + S_3 + S_4 + S_5}. \tag{5.34}$$

Nous pouvons, à présent, exprimer la probabilité τ qu'un nœud tente un CCA dans un intervalle de temps aléatoire. Elle est donnée par l'équation (5.35).

$$\tau^U = \tau^U_{pca} + \tau^U_{csma} = \sum_{k=1}^{d} p_{0,k} + \sum_{i=0}^{m}\sum_{j=0}^{n} b_{i,0,j}. \tag{5.35}$$

5.2.4.3 Calcul de probabilité d'échec de transmission

- Soit P_e la probabilité de transmission de données non réussie pouvant être due à une collision avec la probabilité P_c ou à des erreurs de transmission avec la probabilité P_{te}.

$$P_e = P_c + P_{te}. \tag{5.36}$$

- Soit P_c la probabilité qu'au moins une des stations restantes $(N-1)$ transmette sur le même slot de temps donné. Son expression est donnée dans (5.37).

$$P_c = 1 - (1-\tau)^{N-1}. \tag{5.37}$$

- P_{te} représente la probabilité que la transmission a échouée à cause des erreurs. Elle est exprimée comme suit

$$P_{te} = 1 - (1 - BER)^L. \tag{5.38}$$

BER (Bit Error Rate) est le taux d'erreur binaire et L la taille de la trame.

5.2.4.4 Calcul de la probabilité que le canal soit occupé

- α est la probabilité de trouver un canal occupé durant le CCA. Cette occupation est due soit à la transmission de données avec la probabilité α_{data} soit à la transmission d'un accusé de réception avec la probabilité α_{ack}. Son expression est donnée dans (5.39).

$$\alpha = \alpha_{data} + \alpha_{ack}. \tag{5.39}$$

- Selon le graphe de transition, α_{data} et α_{ack} sont respectivement décrites par les expressions (5.40) et (5.41).

$$\alpha_{data} = L_p\,(1-\alpha)P_e. \tag{5.40}$$

$$\alpha_{ack} = L_{ack}\,\frac{N\tau(1-\tau)^{N-1}}{1-(1-\tau)^N}(1-\alpha)P_e. \tag{5.41}$$

L_{ack} est la taille de l'acquittement.

5.3 Calcul des métriques de performances

Dans cette section, les expressions mathématiques de la fiabilité, de l'énergie consommée et du débit offerts par le standard IEEE 802.15.4k pour les mécanismes CSMA/CA avec backoff PCA non slotté et CSMA/CA non slotté seront dérivées en utilisant la chaîne de Markov précédemment définie dans la figure 5.1, ainsi que les formules développées dans la section précédente.

5.3.1 Fiabilité

Dans notre modélisation, le calcul de cette métrique de performance dépend des probabilités τ^U, P_e et α déjà dérivées dans les équations (5.35), (5.36) et (5.39), respectivement.

5.3.1.1 Fiabilité de CSMA/CA avec backoff PCA non slotté

Dans CSMA/CA avec backoff PCA non slotté, un paquet est rejeté en raison du délai dépassé (i.e, d est atteint) ou perdu à cause d'une collision ou d'une erreur de transmission. Son expression est donnée par l'équation (5.42).

$$F^U_{PCA} = 1 - P^U_{de} - (P^U_{lc} + P^U_{lte})(1 - P^U_{de}). \tag{5.42}$$

Où,

– P_{de}^{U} indique la probabilité qu'un paquet prioritaire soit rejeté en raison d'un délai dépassé, donnée par l'équation (5.42). Les événements A_d et A_c représentent, respectivement, la probabilité que le paquet soit écrasé en raison d'un délai dépassé et la probabilité que le paquet à envoyer soit prioritaire.

$$P_{de}^{U} = P(A_d|A_c) = \frac{\alpha p_{0,d} + \sum_{i=1}^{W-1} p_{i,d}}{h_p}. \tag{5.43}$$

– P_{lc}^{U} indique la probabilité de perte de paquet à cause d'une collision. Son expression est donnée par

$$P_{lc}^{U} = 1 - (1 - \tau^{U})^{N-1}. \tag{5.44}$$

– P_{lte}^{U} indique la probabilité de perte de paquet à cause d'une erreur de transmission. Elle est donnée par l'équation (5.45).

$$P_{lte}^{U} = 1 - (1 - BER)^{L}. \tag{5.45}$$

5.3.1.2 Fiabilité de CSMA/CA non slotté

Les paquets non prioritaires utilisant le mécanisme d'accès au canal CSMA/CA non slotté sont écrasés en raison d'un échec d'accès au canal ou du nombre limite de tentatives de retransmission atteint, comme l'exprime l'équation (5.46).

$$F_{CSMA} = 1 - P_{fca}^{U} - P_{fer}^{U}. \tag{5.46}$$

Où

– P_{fca}^{U} indique la probabilité de perte de paquet à cause un échec d'accès au canal dans les $(m+1)$ étages du backoff. Elle est donnée par

$$P_{fca}^{U} = \frac{x^{m+1}(1 - y_p^{n+1})}{1 - y_p}. \tag{5.47}$$

– P_{fer}^{U} indique la probabilité que le paquet soit perdu du fait que le nombre de retransmissions est dépassé (i.e, que le nombre maximal de retransmissions n est atteint). Son expression est la suivante

$$P_{fer}^{U} = y_p^{n+1}. \tag{5.48}$$

5.3.2 Énergie consommée

Soit P_i ; P_{cca} ; P_{trans} et P_{rec}, l'énergie moyenne consommée par un nœud pendant les états : idle, écoute, transmission et réception, respectivement. La consommation moyenne d'énergie des deux mécanismes est donnée par les équations (5.49) et (5.50).

5.3.2.1 Énergie consommée par le CSMA/CA avec PCA non slotté

En utilisant les équations (5.28)-(5.30), l'énergie consommée E^{U}_{PCA} peut être dérivée comme suit

$$E^{U}_{PCA} = P_{cca}\Big(\sum_{i=0}^{W-1}\sum_{k=1}^{d} p_{i,k}\Big)+P_{trans}\sum_{k=0}^{L_p-1}\Big(p_{-2,k}+p_{-3,k}\Big)+P_i\Big(p_{-2,L_p}+p_{-3,L_p}\Big)+\sum_{k=L_p+1}^{L_p+L_{ack}+1}\Big(P_{rec}\ p_{-2,k}+P_i\ p_{-3,k}\Big). \tag{5.49}$$

5.3.2.2 Énergie consommée par le CSMA/CA non slotté

A partir des équations (5.23), (5.24), (5.32) et (5.33), E^{U}_{CSMA} est donnée par

$$E^{U}_{CSMA} = P_i\sum_{i=0}^{m}\sum_{k=1}^{W_i-1}\sum_{j=0}^{n} b_{i,k,j} + P_{cca}\sum_{i=0}^{m}\sum_{j=0}^{n} b_{i,0,j} + P_{trans}\sum_{k=0}^{L_p-1}\sum_{j=0}^{n}\Big(b_{-1,k,j}+b_{-2,k,j}\Big)$$

$$+P_i\sum_{j=0}^{n}\Big(b_{-1,L_p,j}+b_{-2,L_p,j}\Big)+\sum_{j=0}^{n}\sum_{k=L_p+1}^{L_p+L_{ack}+1}\Big(P_{rec}\ b_{-2,k,j}+P_i\ b_{-1,k,j}\Big). \tag{5.50}$$

5.3.3 Débit

La durée pendant laquelle le canal est évalué libre ou occupé est prise en compte pour calculer le débit offert.

5.3.3.1 Débit de CSMA/CA avec backoff PCA non slotté

Soit P^{Upca}_{busy} la probabilité que le canal soit occupé, exprimée comme suit

$$P^{Upca}_{busy} = 1-(1-\tau^{U}_{pca})^{N}. \tag{5.51}$$

Soit P^{Upca}_{succes} la probabilité de réussite de transmission donnée dans (5.52).

$$P^{Upca}_{succes} = \frac{N\tau^{U}_{pca}(1-\tau^{U}_{pca})^{N-1}}{P^{Upca}_{busy}}. \tag{5.52}$$

Soit T_s la durée d'une transmission réussie d'un paquet de données exprimée comme suit

$$T_s = L_p + T_{PHY} + T_{MAC} + T_{CCA} + T_{LIFS} + t_{ack-wait} + t_{ack}. \tag{5.53}$$

Soit T_e la durée d'une transmission échouée d'un paquet de données (due à une collision ou une erreur de transmission) donnée par l'équation (5.54).

$$T_e = L_p + T_{PHY} + T_{MAC} + T_{CCA} + T_{LIFS} + t_{ack-wait}. \tag{5.54}$$

Le débit associé pour CSMA/CA avec backoff PCA non slotté est donné par l'expression (5.55).

$$Db^{U}_{PCA} = \frac{L_p\, P^{Upca}_{busy}\, P^{Upca}_{succes}}{\sigma\left(1 - P^{Upca}_{busy}\right) + T_s\, P^{Upca}_{busy}\, P^{Upca}_{succes} + T_e\, P^{Upca}_{busy}\left(1 - P^{Upca}_{succes}\right)}. \tag{5.55}$$

Où σ est la durée totale d'un slot de temps, t_{ack} est la taille d'un ACK et $t_{ack-wait}$ est le temps d'attente avant de commencer la transmission de l'ACK.

5.3.3.2 Débit de CSMA/CA non slotté

Soit P^{Ucsma}_{busy} la probabilité que le canal soit occupé donnée comme suit

$$P^{Ucsma}_{busy} = 1 - (1 - \tau^{U}_{csma})^{N}. \tag{5.56}$$

Soit P^{Ucsma}_{succes} la probabilité de réussite de transmission. Son expression est la suivante

$$P^{Ucsma}_{succes} = \frac{N\tau^{U}_{csma}(1 - \tau^{U}_{csma})^{N-1}}{P^{Ucsma}_{busy}}. \tag{5.57}$$

Le débit de CSMA/CA non slotté est donné par l'expression (5.58).

$$Db^{U}_{CSMA} = \frac{L_p\, P^{Ucsma}_{busy}\, P^{Ucsma}_{succes}}{\sigma\left(1 - P^{Ucsma}_{busy}\right) + T_s\, P^{Ucsma}_{busy}\, P^{Ucsma}_{succes} + T_e\, P^{Ucsma}_{busy}\left(1 - P^{Ucsma}_{succes}\right)}. \tag{5.58}$$

5.4 Analyse de performances des mécanismes IEEE 802.15.4k PCA et CSMA/CA non slotté

5.4.1 Méthode d'analyse et logiciels utilisés

Pour l'analyse des performances du IEEE 802.15.4k CSMA/CA avec backoff PCA non slotté et IEEE 802.15.4k CSMA/CA non slotté, nous allons résoudre le système d'équations non linéaire formé par les expressions de S_1, S_2, S_3, S_4, S_5, P_Q, P_e, τ^U et α, données dans la section précédente. Ensuite, nous calculons les expressions des métriques de performance (fiabilité, débit et consommation d'énergie) citées précédemment sous trafic saturé et dans des conditions de canal idéal ($BER = 0$) et non idéal ($BER = 10^{-3}$ et $BER = 5 * 10^{-4}$) et comparer les performances des deux mécanismes d'accès au médium. Après cela, nous analysons l'impact de la variation de la probabilité que le paquet soit prioritaire h_p, de la taille des paquets L_p et de taux d'erreur binaire BER sur les performances du réseau.

5.4.2 Valeurs des paramètres utilisés

Le tableau 5.3 nous donne les différents paramètres utilisés pour l'analyse des performances.

TABLE 5.3 – Paramètres utilisés pour IEEE 802.15.4k CSMA/CA PCA non slotté

Paramètre	Valeur	Paramètre	Valeur
N, L_p, h_p, BER	Variants	L_s, L_f	7 bytes
$n, W, macMinBE$	3	L_{ack}	1 byte
m	5	L	20 bytes
$W_0, macMaxBE$	8	d	5 ms
MAC header length	16 bytes	t_{ack}	1 ms
PHY header length	6 bytes	$t_{ack-wait}$	$[1 - 1.32]$ *ms*
P_{cca}	40 mW	T_{LIFS}	0.32 ms
P_i	0.8 mW	T_{CCA}	0.128 ms
P_{trans}	30 mW	T_b	0.32 ms
P_{rec}	40 mW	σ	0.96 ms

5.4.3 Résultats, analyses et comparaisons

La figure 5.2 représente la variation de la fiabilité en fonction de la taille du réseau, dans des conditions de canal idéal ($BER = 0$) et non idéal ($BER = 10^{-3}$ et $BER = 5 * 10^{-4}$). Nous notons

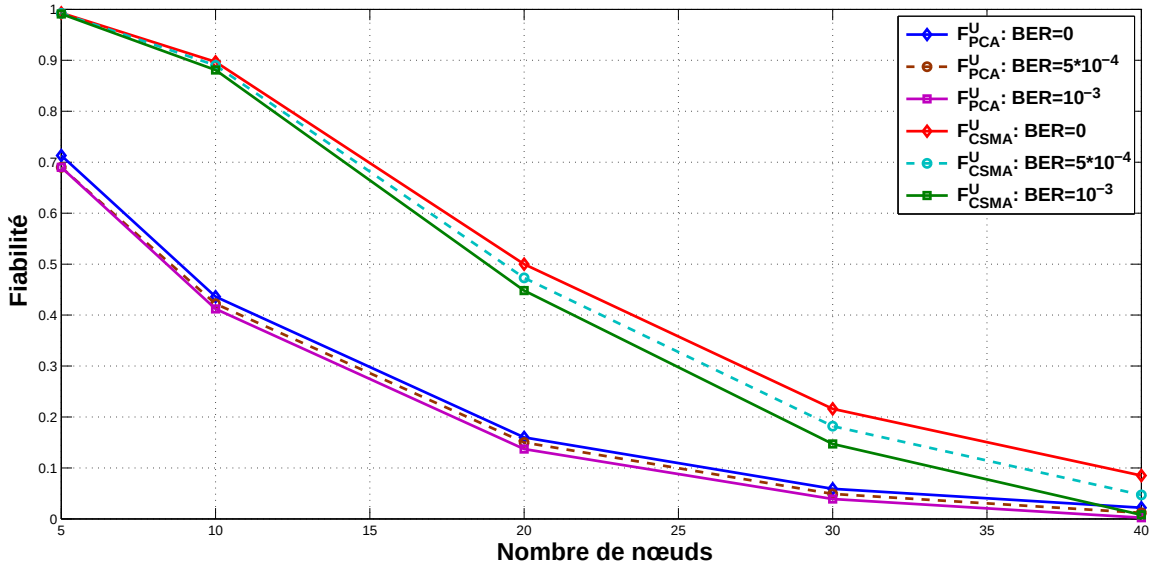


FIGURE 5.2 – Fiabilité Vs Taille du réseau & variant BER, avec $h_p = 0.5$ et $L_p = 8$ bytes.

que la fiabilité diminue avec l'augmentation de la taille du réseau en raison du nombre important de nœuds qui tentent de transmettre. Par conséquent, la probabilité de défaillance (collisions ou erreurs de transmission) augmente. De plus, nous rapportons que CSMA/CA offre une meilleure fiabilité par rapport à CSMA/CA avec backoff PCA, car la retransmission est autorisée dans le mécanisme

CSMA/CA. Tandis que dans PCA, le paquet est détruit s'il n'est pas transmis dans le délai d. La figure illustre également que lorsque nous augmentons la valeur de BER, la fiabilité diminue, car la probabilité d'erreurs de transmissions augmente.

La figure 5.3 représente la variation de la fiabilité en fonction de la taille du réseau, dans des conditions de canal idéal et non idéal (BER= 10^{-3}) et pour deux valeurs de la probabilité que le paquet soit prioritaire ($h_p = 0.3$ et $h_p = 0.8$). Nous notons que lorsque la taille du réseau augmente, la fiabilité diminue pour les deux mécanismes, car le risque de l'échec de transmission augmente avec l'augmentation des collisions. CSMA/CA offre une bonne fiabilité par rapport à PCA, car les paquets prioritaires doivent être transmis dans un délai limité, sinon ils seront perdus.

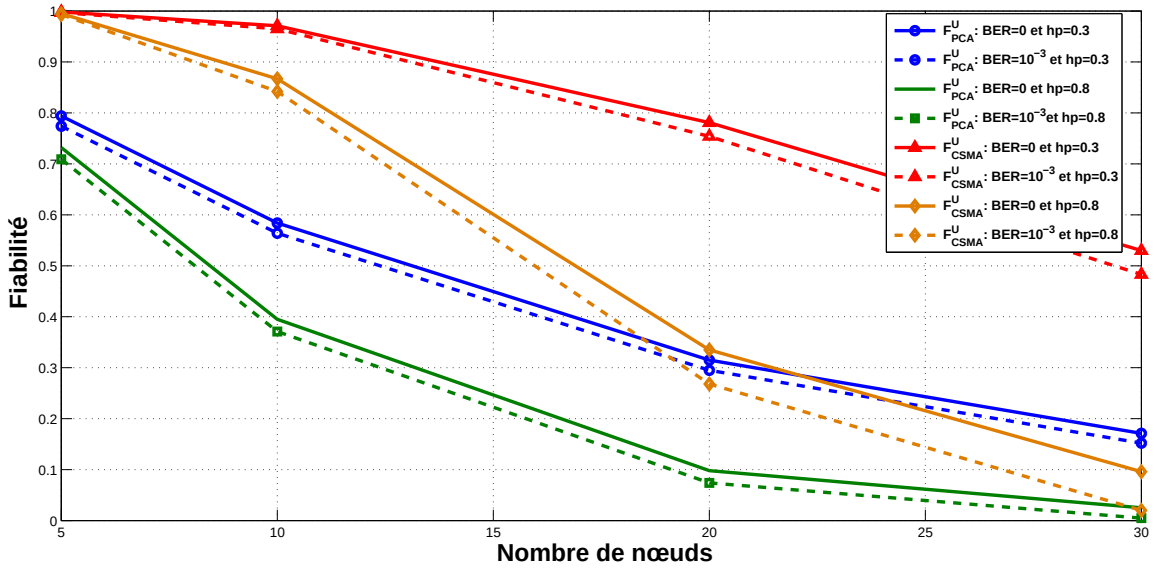


FIGURE 5.3 – Fiabilité Vs Taille du réseau & variant la probabilité h_p, avec $L_p = 8$ bytes.

Tandis que les paquets non prioritaires, si ils n'arrivent pas à être transmis dans les $(m + 1)$ étages du backoff, d'autres tentatives de transmission sont offertes. Lorsque $h_p = 0.8$, le nombre de paquets prioritaires est plus grand que lorsque $h_p = 0.3$. Par conséquent, les collisions augmentent et la fiabilité sera inférieure à celle relative à $h_p = 0.3$. Les résultats obtenus sous un canal idéal sont légèrement meilleurs que ceux sous un canal bruité.

La figure 5.4 représente la variation de la fiabilité en fonction de la taille du réseau pour les tailles de paquets ($L_p = 8$ bytes et $L_p = 28$ bytes), sous un canal idéal et non idéal ($BER = 10^{-3}$). Nous notons que la fiabilité diminue lorsque le nombre de nœuds augmente, car la probabilité de collision augmente. La fiabilité des paquets non prioritaires est plus élevée que celle des paquets

prioritaires. Cela est dû au fait que les retransmissions favorisent d'autres chances d'atteindre l'accès au canal et de transmettre. En augmentant la taille des paquets, la fiabilité augmente. Les résultats obtenus dans le canal idéal sont meilleurs que ceux dans un canal non idéal.

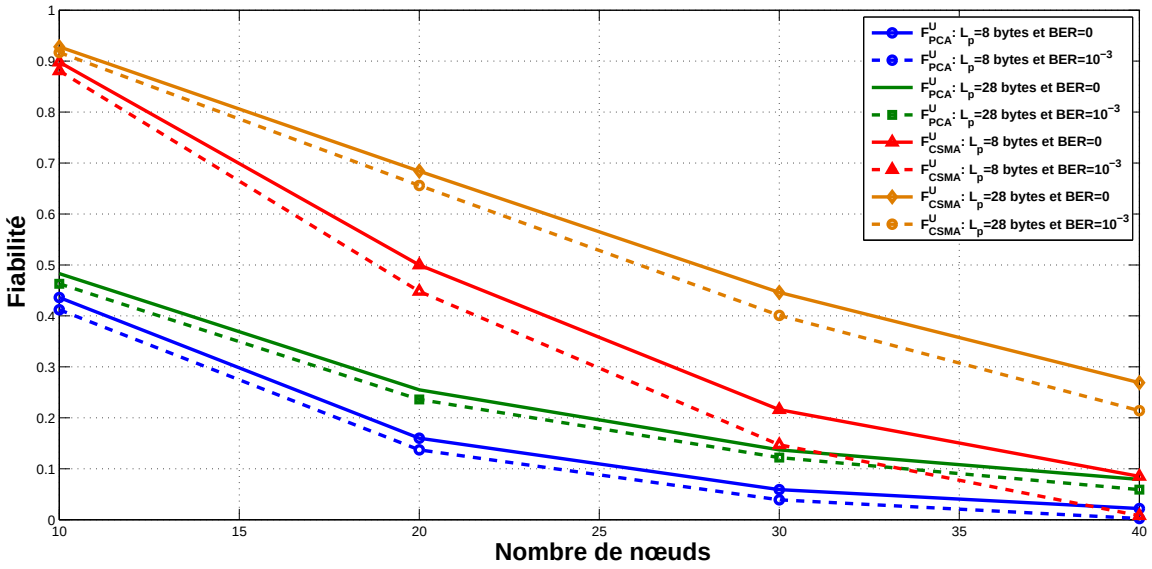


FIGURE 5.4 – Fiabilité Vs Taille du réseau & variant la Taille des paquets L_p, avec $h_p = 0.5$.

La figure 5.5 représente la variation de l'énergie en fonction de la taille du réseau pour différents BER (0, $5 * 10^{-4}$ et 10^{-3}). Lorsque la taille du réseau devient de plus en plus importante, l'énergie consommée diminue. Cette diminution est dû au fait que les nœuds consomment moins d'énergie à l'état de repos (inactif) lorsque le canal est détecté occupé. L'énergie E^U_{CSMA} est nettement plus élevé que E^U_{PCA} en raison de la retransmission autorisée pour le mécanisme CSMA/CA ($n = 3$) qui provoque une énergie consommée de plus, quelles que soient les conditions du canal. Une légère diminution de l'énergie consommée est observée lorsque des erreurs de transmission sont présentes. Cela s'explique par le fait que la probabilité d'échec augmente, ainsi les nœuds se mettent en mode inactif ; par conséquent, la consommation d'énergie diminue.

Dans la figure 5.6, la variation de l'énergie en fonction de la taille du réseau et de la probabilité que le paquet disponible soit prioritaire h_p est représentée. Avec l'augmentation de la probabilité h_p ($h_p = 0.8$), beaucoup de nœuds ayant des messages prioritaires à transmettre tentent d'accéder au canal, donc une grande énergie est consommée par ces nœuds. Par conséquent, le peu de nœuds ayant des paquets non prioritaires consomment moins d'énergie, en les comparant aux prioritaires. Tandis que, lorsque $h_p = 0.3$, beaucoup de paquets non prioritaires tentent de transmettre consommant

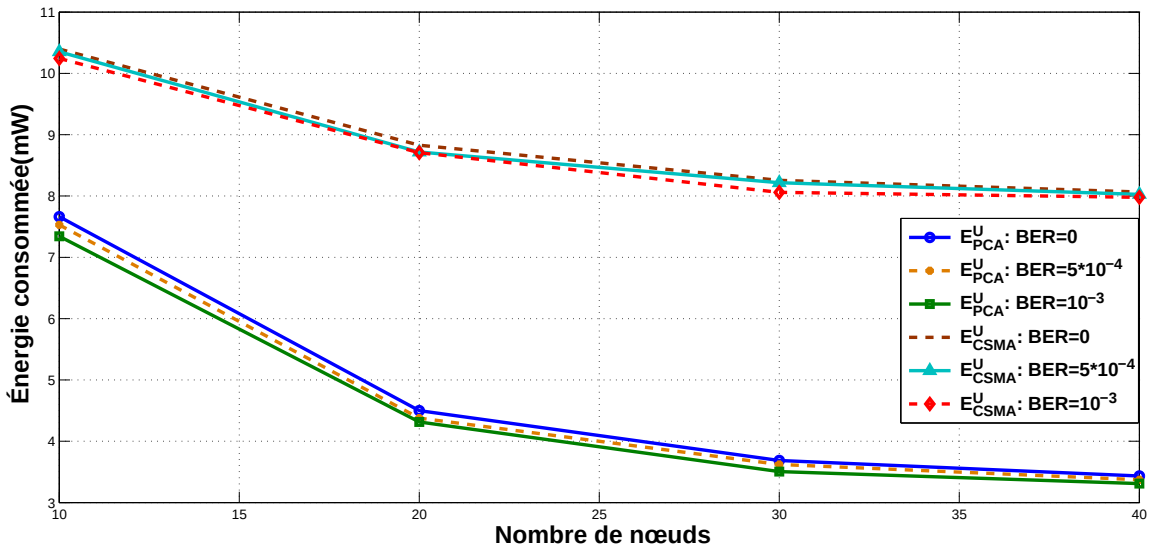


FIGURE 5.5 – Énergie Vs Taille du réseau & variant *BER*, avec $h_p = 0.5$ et $L_p = 8$ bytes.

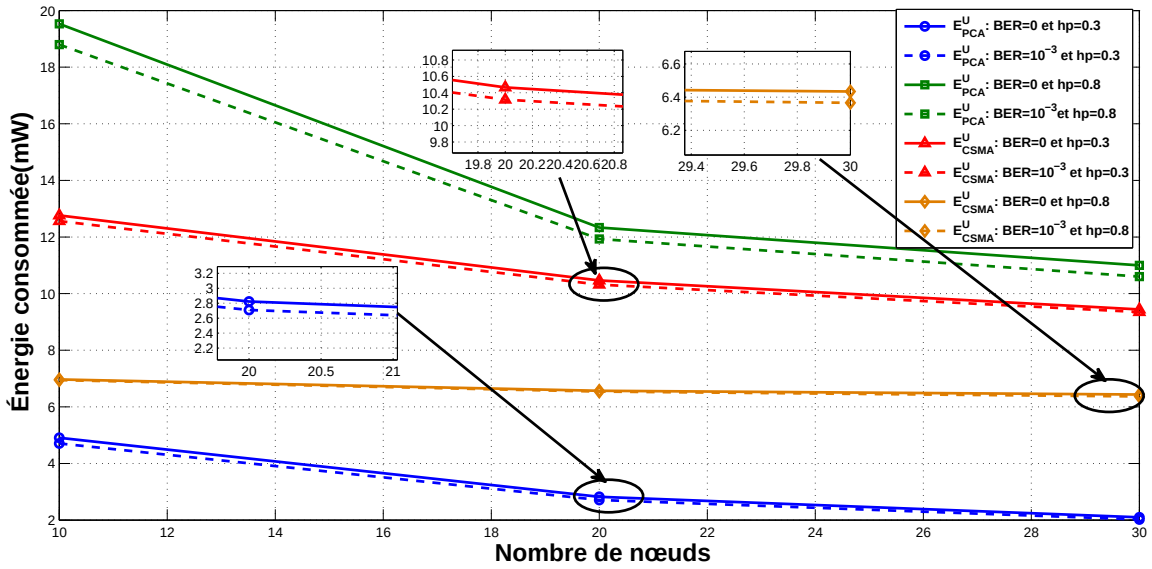


FIGURE 5.6 – Énergie Vs Taille du réseau & variant la probabilité h_p, avec $L_p = 8$ bytes.

plus d'énergie. et ainsi, les nœuds prioritaires consomment moins d'énergie vu leur petit nombre. En d'autres termes, PCA donne de bons résultats par rapport à CSMA/CA lorsque h_p est petite et donne de mauvais résultats quand $h_p = 0.8$. La figure montre également que, lorsque les erreurs de transmission existent, une diminution de l'énergie consommée est observée car les nœuds se mettent en mode repos.

La figure 5.7 trace l'énergie en fonction de la taille du réseau pour différentes tailles de paquets ($L_p = 8$ bytes et $L_p = 28$ bytes). Une grande consommation d'énergie est observée dans CSMA/CA par rapport au PCA, car lors des retransmissions, une énergie de plus est consommée. Pour de petites tailles de paquets, une grande énergie est consommée. Lorsque la taille du paquet est grande, le nœud ayant un paquet non prioritaire diffère sa transmission à un autre instant et se met à l'état inactif consommant ainsi une faible énergie (i.e. retransmission) donnant la chance aux autres nœuds. De plus, une diminution de l'énergie est également observée lors d'un canal non idéal.

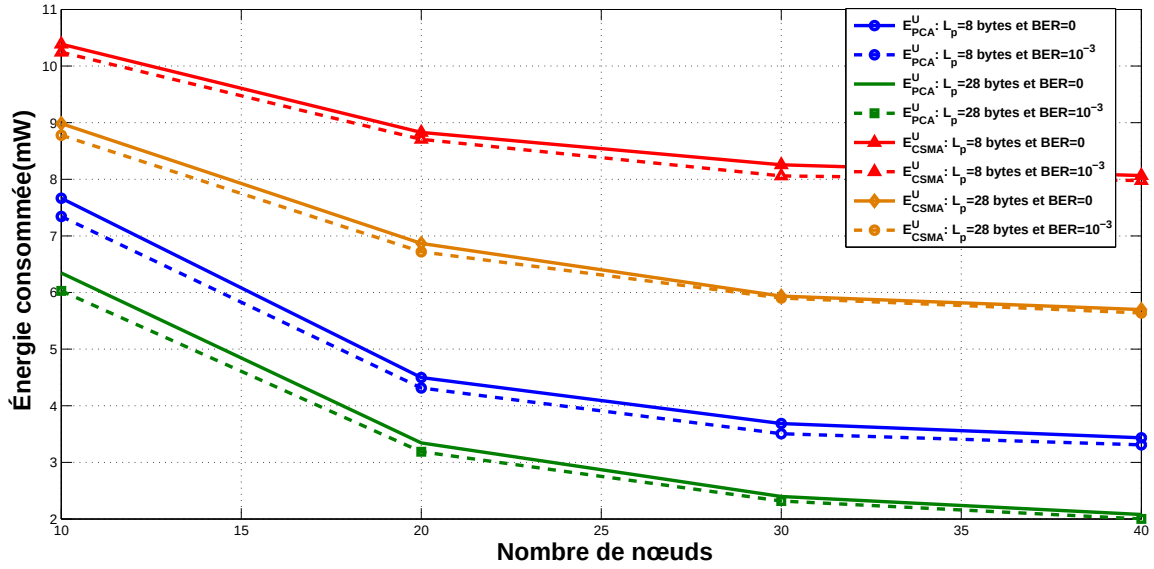


FIGURE 5.7 – Énergie Vs Taille du réseau & variant la Taille des paquets L_p, avec $h_p = 0.5$.

Avec l'augmentation du nombre de nœuds dans le réseau, la probabilité de collision augmente ; par conséquent, le débit diminue, comme illustré dans la figure 5.8. Étant donné que le débit est affecté par la probabilité de défaillance, le débit est plus élevé lorsque la probabilité de défaillance est plus faible. Par conséquent, le débit obtenu sous un canal idéal est meilleur que celui sous un canal non idéal. La figure montre également que PCA offre un débit élevé par rapport à CSMA/CA.

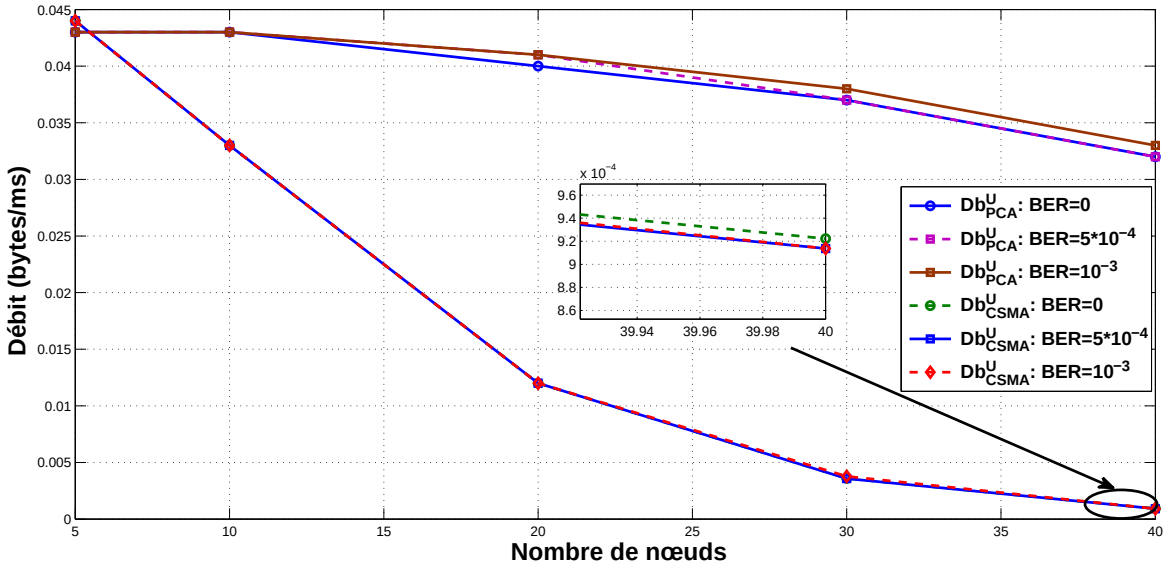


FIGURE 5.8 – Débit Vs Taille du réseau & variant *BER*, avec $h_p = 0.5$ et $L_p = 8$ bytes.

Dans la figure 5.9, la variation du débit en fonction de la taille du réseau et de la probabilité que le paquet soit prioritaire h_p est représentée. Pour $h_p = 0.3$, le débit associé à CSMA/CA diminue, car beaucoup de nœuds ayant des paquets non prioritaires essaient d'accéder au canal, engendrant ainsi des collisions et une diminution du débit. En revanche, le débit de PCA augmente, car peu de paquets tentent de transmettre, il y a un moindre risque de collision. Pour $h_p = 0.8$, nous observons l'événement contraire, le débit associé à PCA diminue et celui de CSMA/CA augmente, car il y a plusieurs paquets prioritaires dans la file d'attente. En d'autres termes, lorsque le nombre de paquets prioritaires est très important, le débit offert par PCA est faible et, en revanche, celui des paquets non prioritaires utilisant CSMA est important. Alors que lorsque h_p est petit, le débit offert par PCA sera grand et celui offert par CSMA sera petit. Avec la présence des erreurs de transmission, le débit de PCA et CSMA diminue lorsque le nombre de paquets prioritaire ou non prioritaire est petit, respectivement . En d'autres terme, lorsque $h_p = 0.3$ et $h_p = 0.8$, respectivement.

La figure 5.10 trace le débit en fonction de la taille du réseau avec différentes tailles de paquets ($L_p = 8$ bytes et $L_p = 28$ bytes). Nous notons une diminution du débit avec l'augmentation de la taille du réseau. Ceci est dû au risque élevé de collisions qui augmente à son tour la probabilité d'échec. Avec l'augmentation de la taille du paquet, nous remarquons une augmentation du débit de données pour les deux mécanismes. Car la quantité d'informations transmise sera grande. Les erreurs de transmission influent sur le débit de CSMA/CA, où le débit offert dans le canal idéal est

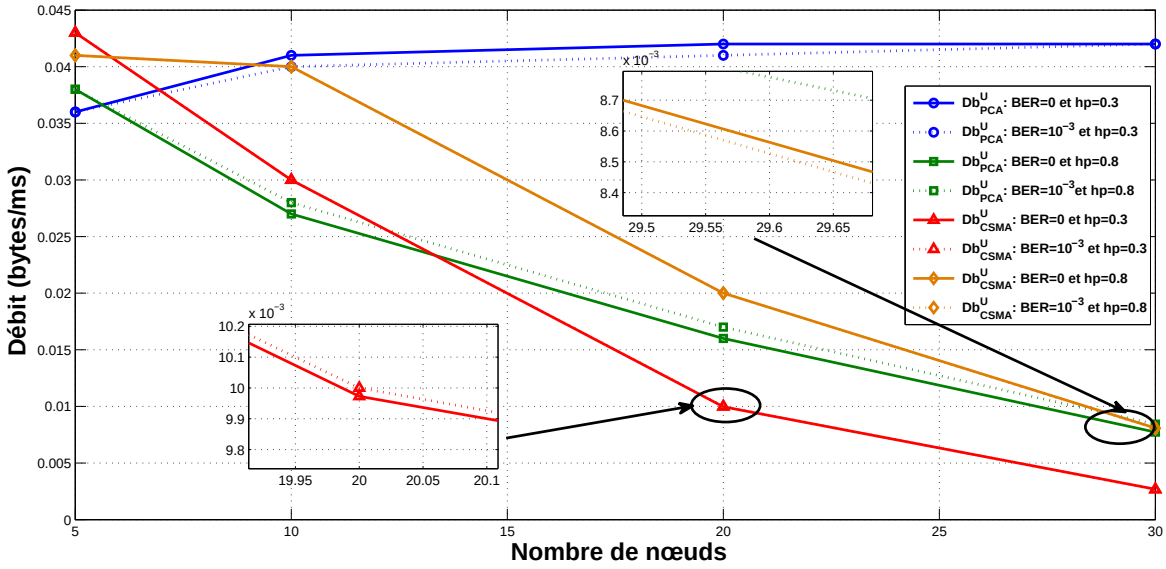


FIGURE 5.9 – Débit Vs Taille du réseau & variant la probabilité h_p, avec $L_p = 8$ bytes.

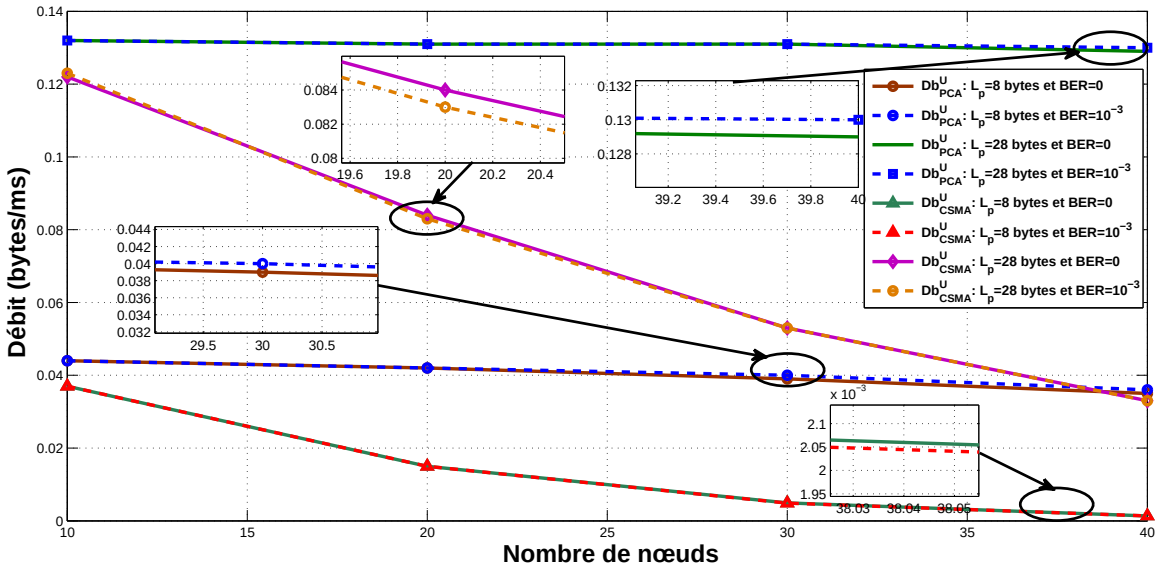


FIGURE 5.10 – Débit Vs Taille du réseau & variant la Taille des paquets L_p, avec $h_p = 0.5$.

nettement supérieur à celui dans le canal bruité. De plus, dans PCA le débit offert dans un canal bruité est meilleur que celui dans un canal idéal. Car, lors de la présence de ces erreurs, les paquets non prioritaires diffèrent leurs transmission, ce qui donne la chance aux nœuds prioritaires pour avoir l'accès au canal. D'où l'augmentation du débit de PCA dans le canal bruité.

La probabilité d'échec augmente en fonction du nombre de nœuds dans le réseau, comme le montre la figure 5.11. La raison est que lorsque le nombre de nœuds essayant de transmettre devient important, les risques de collisions ou d'erreurs de transmission augmentent. La probabilité d'échec P_e obtenue lors d'un canal idéal est inférieure à celles du canal non idéal. Aussi, chaque fois que nous augmentons le BER, la probabilité d'erreur de transmission augmente. Par conséquent, la probabilité d'échec augmente.

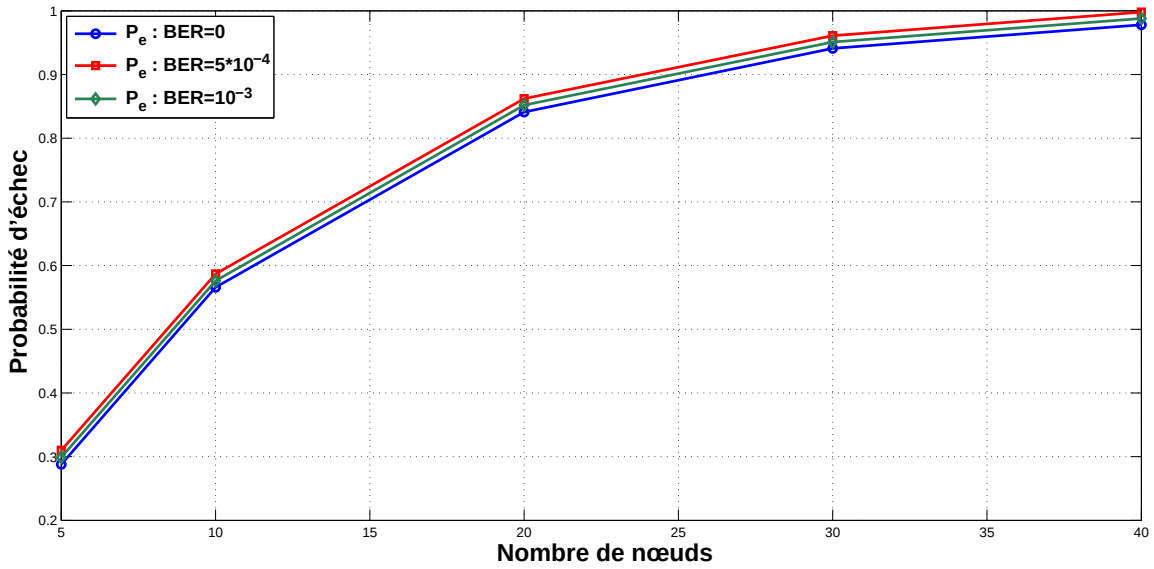


FIGURE 5.11 – Probabilité d'échec Vs Taille du réseau & variant BER, avec $h_p = 0.5$ et $L_p = 8$ bytes.

Avec l'augmentation de la taille du réseau, la probabilité d'échec augmente, en raison des risques élevés de collisions, comme illustré dans la figure 5.12. Nous constatons que lorsque nous augmentons la probabilité que le paquet soit prioritaire ($h_p = 0.8$), la probabilité d'échec augmente. Car ces paquets doivent être transmis dans un délai précis d, et vu que leur nombre est grand, les collisions et erreurs de transmissions sont grandes, d'où l'augmentation de la probabilité d'échec de transmission. Aussi, avec l'augmentation de BER, la probabilité d'échec augmente, car les erreurs de transmissions seront présentes.

En augmentant la taille du paquet ($L_p = 28$) bytes, nous notons sur la figure 5.13, une diminution

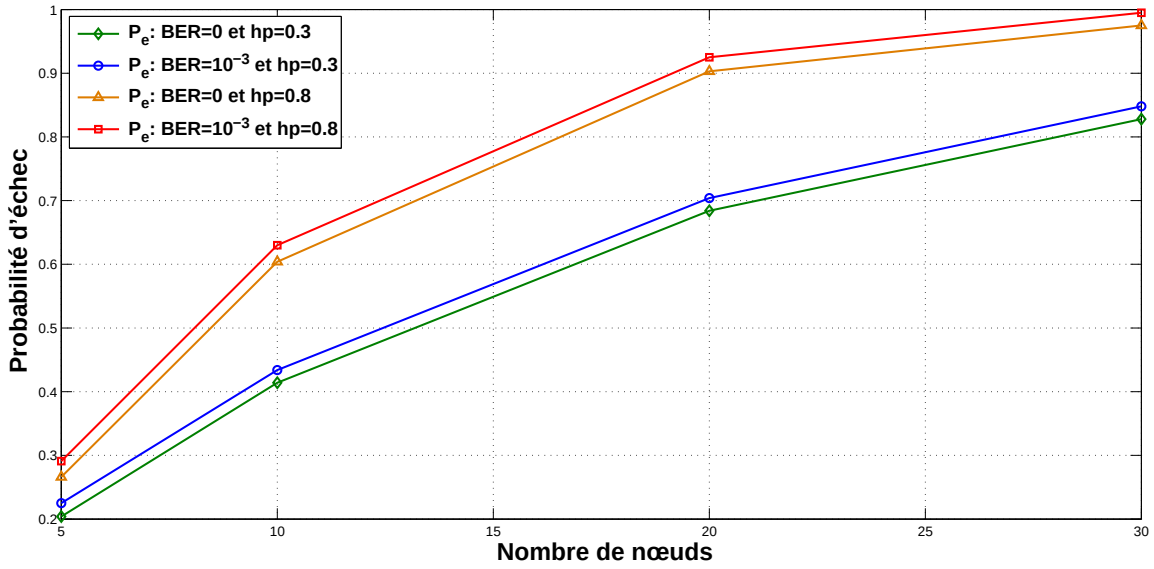


FIGURE 5.12 – Probabilité d'échec Vs Taille du réseau & variant la probabilité h_p,avec $L_p = 8$ bytes.

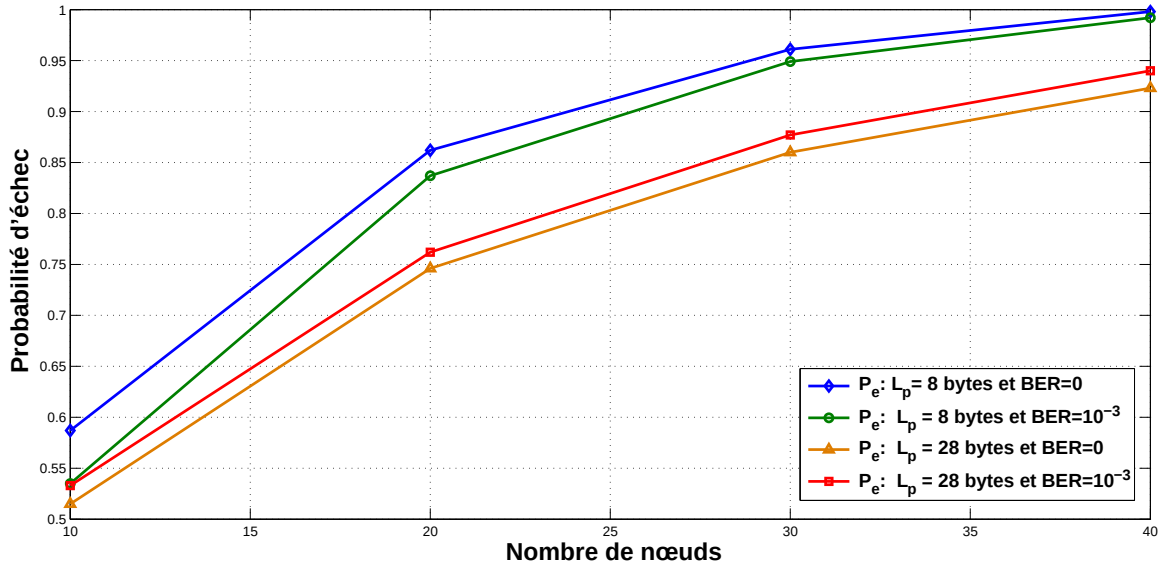


FIGURE 5.13 – Probabilité d'échec Vs Taille du réseau & variant la Taille des paquets L_p, avec $h_p = 0.5$.

de la probabilité d'échec, car le temps de transmission d'un long paquet sera plus grand. Dans un canal non idéal, la probabilité P_e est supérieure à celle calculée dans le canal idéal.

5.5 Conclusion

Dans ce chapitre, nous nous sommes intéressés à l'analyse des performances du réseau IEEE 802.15.4k, dans des conditions de saturation du trafic et sous un canal idéal et non idéal, dans le mode non beacon. Dans notre modèle analytique, nous avons proposé une nouvelle chaîne de Markov à temps discret bidimensionnel qui modélise, pour la première fois dans la littérature, le mécanisme de transmission des paquets prioritaires, et une chaîne de Markov à temps discret tridimensionnel qui modélise le mécanisme de transmission de paquets non prioritaires. Le modèle proposé prend en compte un nombre fixe de nœuds disposés en topologie en étoile dans le cas de saturation de trafic et sous un canal bruité, tout en tenant compte du mécanisme d'accusé de réception et des limites de retransmission. La résolution du modèle de chaîne de Markov proposé nous a permis de calculer la probabilité que le paquet tente un CCA, ainsi que la probabilité de défaillance. Nous avons utilisé ces probabilités pour dériver les expressions théoriques de certaines métriques de performance à savoir : la fiabilité, la consommation d'énergie et le débit, puis comparer les performances des deux mécanismes. Ensuite, nous avons analysé l'impact de la variation du taux d'erreur binaire, de la probabilité que le paquet soit prioritaire et de la longueur des paquets, tout en variant la taille du réseau, pour tester l'efficacité du modèle sur la probabilité de défaillance et les métriques étudiées.

Nous observons que le PCA non slotté permet une réduction de la consommation d'énergie, offre un débit élevé mais une fiabilité inférieure à celle de CSMA/CA non slotté. En effet, à mesure que l'on augmente le nombre de dispositifs, IEEE 802.15.4k offre une fiabilité réduite, une énergie réduite et un débit réduit. Pour des paquets de grandes tailles, le protocole donne une bonne fiabilité, une très faible consommation d'énergie, une faible probabilité d'échec et un débit plus élevé.

Chapitre6

Modélisation analytique et évaluation des performances du mécanisme IEEE 802.15.4k LECIM ALOHA PCA slotté

Sommaire

6.1 Introduction

Dans ce chapitre, nous proposons un modèle de chaîne de Markov à trois dimensions de ALOHA PCA slotté (S-aloha PCA) pour la transmission des paquets prioritaires et une chaîne de Markov à trois dimensions de ALOHA slotté (S-aloha) pour la transmission des paquets non prioritaires dans le standard IEEE 802.15.4k. Ce modèle est le premier travail, dans la littérature, servant à modéliser les deux mécanismes ALOHA de IEEE 802.15.4k à travers une chaîne de Markov. Sur la base de notre modèle proposé, nous calculons la fiabilité, la consommation d'énergie, le débit et le délai moyen pour les deux mécanismes dans des conditions de saturation de trafic sous un canal idéal. Enfin, nous évaluons les effets de la variation du nombre de nœuds N, de la probabilité que le paquet disponible soit prioritaire h_p et de la taille des paquets L_p sur les performances de nos métriques.

6.2 Modélisation analytique des mécanismes d'accès au canal ALOHA PCA et ALOHA non slotté

Dans cette section, nous présentons le modèle analytique proposé pour S-aloha PCA et S-aloha de IEEE 802.15.4k dans des conditions de saturation du trafic sous un canal idéal.

6.2.1 Hypothèses du modèle

Nous supposons les hypothèses suivantes dans lequel notre modèle de CM est applicable.

1. Un nombre fixe de dispositifs (N) disposés en topologie en étoile ;
2. Considération des conditions de saturation du trafic ;
3. Considération d'un canal idéal ;
4. Prise en charge des accusés de réception.

6.2.2 Paramètres et notations utilisés dans le modèle

Les paramètres utilisés dans notre modèle sont représentés dans le tableau 6.1.

TABLE 6.1 – Paramètres du modèle IEEE 802.15.4k ALOHA PCA slotté

Paramètre	Description
N	La taille du réseau
Q	L'état idle
n	Le nombre maximum de retransmissions
m	L'étage du backoff maximum
W_0	La taille minimale de la fenêtre de contention qui correspond à la première tentative de transmission
L_p	La taille du paquet
L_s	La taille du paquet reçu avec succès
L_c	La taille du paquet collisioné
L_{ack}	La taille de l'ACK
σ	La durée d'un intervalle de temps
t_{ack}	La durée de la trame ACK
$t_{ack-zait}$	Le temps d'attente avant de transmettre l'ACK

6.2.3 Les probabilités utilisées dans le modèle

Le tableau 6.2 présente les différentes probabilités indispensables à la réalisation du modèle.

Table 6.2 – Probabilités du modèle IEEE 802.15.4k ALOHA PCA slotté

Probabilités	Description
h_p	La probabilité que le paquet soit prioritaire
P_Q	La probabilité de résider dans l'état idle
P_s	La probabilité de transmission réussie
τ	La probabilité de transmettre dans n'importe quel intervalle de temps aléatoire
P_c	La probabilité de collision
P_d	La probabilité de rejet du paquet dans S-aloha PCA
P_e	La probabilité de rejet du paquet dans S-aloha dû à un échec de transmission
P_r	La probabilité de rejet du paquet dans S-aloha en raison de retransmissions dépassées
$P_{i,k,j}$	Les probabilités des états de la chaîne de Markov associée à S-aloha PCA
$b_{i,k,j}$	Les probabilités des états de la chaîne de Markov associée à S-aloha

6.2.4 La chaîne de Markov proposée

Notre modèle de chaîne de Markov est composé de deux parties : un modèle pour S-aloha PCA et un autre pour S-aloha, comme illustré dans son graphe de transition dans la figure 6.1. Soit h_p la probabilité qu'un paquet soit prioritaire et $(1 - h_p)$ la probabilité que le paquet soit non prioritaire. P_Q représente la probabilité que le nœud réside dans l'état inactif (idle) Q et qui se produit à la fin de chaque état du paquet (transmis, non transmis, perdu ou écrasé).

Soit $s(t)$, $c(t)$ et $d(t)$ les processus stochastiques modélisant la transmission d'un paquet prioritaire en utilisant le mécanisme S-aloha PCA, où $s(t)$ représente l'étage du backoff, $c(t)$ représente le compteur d'attente backoff et $d(t)$ représente le délai encouru par le paquet. Le triple $(s(t), c(t), d(t))$ est le modèle de chaîne de Markov à 3D proposé pour S-aloha PCA, où nous utilisons (i, k, j) pour désigner un état particulier. Les états (i, k, j), $i \in [0, m]$, $k \in [0, W_i - 1]$, $j \in [1, d]$ représentent les périodes d'attente backoff. Les états $(i, 0, j)$, $i \in [0, m]$, $j \in [1, d]$ représentent les états de transmission. Les états de $(-2, 0, 0)$ à $(-2, L_s - 1, 0)$ et de $(-1, 0, 0)$ à $(-1, L_c - 1, 0)$ représentent respectivement les états de transmission réussie et non réussie (en raison de collisions). L_s et L_c indiquent respectivement la longueur des paquets transmis avec succès et non transmis.

Soit $s(t)$, $c(t)$ et $r(t)$ les processus stochastiques représentant l'étage de backoff, l'état du compteur de backoff et l'état du compteur de retransmission au temps t, respectivement. Le triplet $(s(t), c(t), r(t))$ est le modèle de chaîne de Markov à 3D proposé pour S-aloha. Les états (i, k, j) $i \in [0, m]$, $k \in [0, W_i - 1]$, $j \in [0, n]$ représentent les états de périodes d'attente backoff. Les états $(i, 0, j)$ $i \in [0, m]$, $j \in [0, n]$ représentent les états de transmission. Les états allant de $(-2, 0, j)$ à $(-2, L_s - 1, j)$ et de $(-1, 0, j)$ à $(-1, L_c - 1, j)$, $j \in [0, n]$ modélisent, respectivement, les états de

transmission réussie et non réussie. Soit P_s la probabilité que le paquet soit transmis avec succès pour les deux mécanismes.

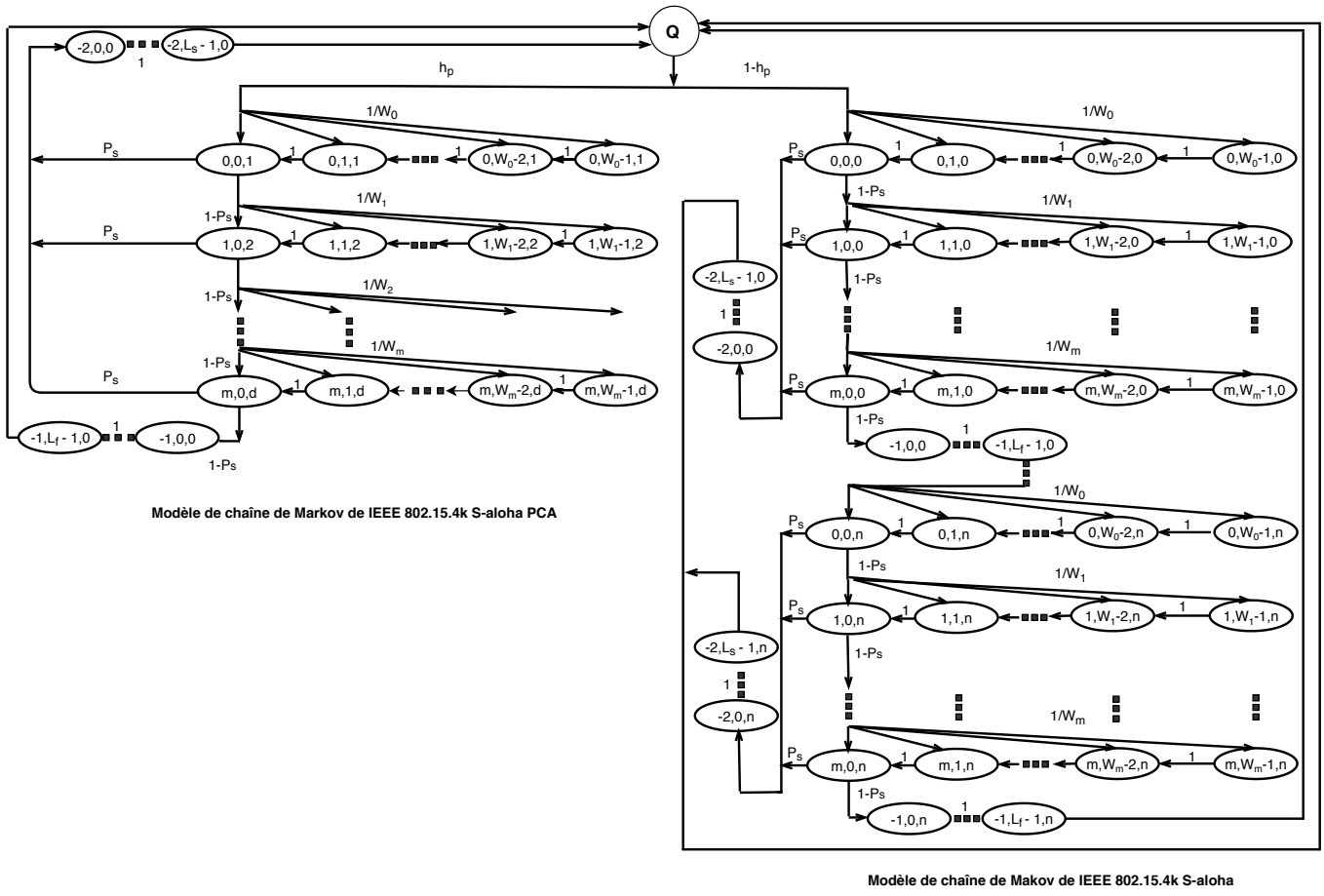


FIGURE 6.1 – Chaîne de Markov des mécanismes IEEE 802.15.4k ALOHA PCA slotté

Un paquet prioritaire est rejeté pour deux raisons : **(i)** le délai est dépassé, **(ii)** la transmission échouée durant les $(m+1)$ étages de backoff. Tandis qu'un paquet non prioritaire est rejeté en raison : **(i)** d'une transmission échouée durant les $(m+1)$ étages de backoff, **(ii)** du nombre maximum de tentatives de retransmission atteint. Dans le reste de ce chapitre, nous considérons que les paquets prioritaires ne sont rejetés qu'en raison d'un échec de transmission durant les $(m+1)$ étages de backoff, ce qui signifie que $m < d$.

6.2.4.1 Probabilités de transition

Les probabilités de transition associées à la chaîne de Markov sont décrites dans les équations (6.1)-(6.10).

$$P(i,k,j|i,k+1,j) = 1, \forall\ i \in [0,m], k \in [0,W_i-1], j \in [1,d]. \tag{6.1}$$

$$P(i,k,j|i-1,0,j-1) = \frac{1-P_s}{W_i}, \forall\ i \in [0,m], k \in [0,W_i-1], j \in [1,d]. \tag{6.2}$$

$$P(0,k,1|Q) = \frac{h_p}{W_0}, \forall k \in [0,W_i-1]. \tag{6.3}$$

$$P(-2,0,0|i,0,j) = P_s\ , \forall\ i \in [0,m], j \in [1,d]. \tag{6.4}$$

$$P(-1,0,0|i,0,j) = (1-P_s), \forall\ i \in [0,m], j \in [1,d]. \tag{6.5}$$

$$P(i,k,j|i,k+1,j) = 1, \forall\ i \in [0,m], k \in [0,W_i-1], j \in [0,n]. \tag{6.6}$$

$$P(i,k,j|i-1,0,j-1) = \frac{1-P_s}{W_i}, \forall\ i \in [0,m], k \in [0,W_i-1], j \in [0,n]. \tag{6.7}$$

$$P(0,k,0|Q) = \frac{(1-h_p)}{W_0}, k \in [0,W_i-1]. \tag{6.8}$$

$$P(-2,0,j|i,0,j) = P_s\ , \forall\ i \in [0,m], j \in [0,n]. \tag{6.9}$$

$$P(-1,0,j|i,0,j) = (1-P_s), \forall\ i \in [0,m], j \in [0,n]. \tag{6.10}$$

Le compteur du backoff décrémente avec la probabilité exprimée dans (6.1) pour S-aloha PCA et dans (6.6) pour S-aloha. La probabilité de transmission échouée et de sélection d'un état uniformément lors du prochain étage de backoff est donnée dans les équations (6.2) et (6.7) pour le S-aloha PCA et S-aloha, respectivement. Les équations (6.3) et (6.8) donnent les probabilités de passer au premier étage de backoff à partir de l'état idle pour les paquets prioritaires et non prioritaires, respectivement. Les équations (6.4) et (6.5) représentent la probabilité de transition à l'état succès et échec dans S-aloha PCA, respectivement. Les équations (6.9) et (6.10) représentent la probabilité de transition à l'état succès et échec dans S-aloha, respectivement

6.2.4.2 Probabilités d'états stationnaires

Nous utilisons les équations (6.1) - (6.10) pour calculer la distribution stationnaire de notre chaîne de Markov. Nous représentons par $p_{i,k,j}$ et $b_{i,k,j}$ les probabilités des états de la chaîne de Markov associées à S-aloha PCA et les probabilités des états de la chaîne de Markov associées à S-aloha, respectivement.

a) La probabilité stationnaire du modèle associé à S-aloha PCA

Soit $p_{i,k,j} = \lim_{t\to+\infty} P\Big(s(t) = i, c(t) = k, d(t) = j\Big)$, $i \in [-2, m]$, $k \in \Big(-1, max(W_i - 1, L_s - 1, L_c - 1)\Big)$, $j \in [1, d]$ la probabilité stationnaire de S-aloha PCA, où L_s et L_c sont les périodes de temps pour une transmission réussie du paquet et une transmission échouée (à cause de collision), respectivement.

Nous avons

$$p_{i,k,j} = \frac{W_i - k}{W_i}\, p_{i,0,j},\ \forall\ k \in [0, W_i - 1]. \tag{6.11}$$

- La valeur du compteur de backoff W_i est uniformément choisie à l'étage i de l'intervalle $[0, W_i - 1]$

$$W_i = 2^i W_0,\ \forall i \in [0, m]. \tag{6.12}$$

- La probabilité que le nœud tente de transmettre un paquet prioritaire est donnée par

$$p_{i,0,j} = (1 - P_s)^i\, p_{0,0,1} = x^i\, p_{0,0,1},\ \forall\ i \in [0, m]. \tag{6.13}$$

Où $x = (1 - P_s)$ représente la probabilité d'échec de transmission à n'importe quel étage du backoff.

- La probabilité de résider dans l'état $(0, 0, 1)$ est donnée par l'équation (6.14).

$$p_{0,0,1} = \sum_{k=0}^{W_0-1} p_{0,k,1} = h_p\, P_Q. \tag{6.14}$$

- La probabilité de l'état de réussite est

$$p_{-2,0,0} = P_s \sum_{i=0}^{m} p_{i,0,j} = (1 - x^{m+1})\, p_{0,0,1},\ \forall\ j \in [1, d]. \tag{6.15}$$

- La probabilité de l'état d'échec est donnée par

$$p_{-1,0,0} = (1 - P_s) \sum_{i=0}^{m} p_{i,0,j} = x\, \frac{(1 - x^{m+1})}{1 - x} = y\, p_{0,0,1},\ \forall\ j \in [1, d]. \tag{6.16}$$

Où $y = \frac{x\,(1-x^{m+1})}{1-x}$ représente la probabilité d'échec de transmissions au cours des $(m + 1)$ étages de backoff.

b) La probabilité stationnaire associée à S-aloha

Soit $b_{i,k,j} = \lim_{t\to+\infty} P\Big(s(t) = i, c(t) = k, r(t) = j\Big), i \in [-2, m], k \in \Big(-1, max(W_i - 1, L_s - 1, L_c - 1)\Big)$, $j \in [0, n]$ la probabilité stationnaire de S-aloha de notre chaîne de Markov.

Nous avons

$$b_{i,k,j} = \frac{W_i - k}{W_i}\, b_{i,0,j},\ \forall\ k \in [0, W_i - 1]. \tag{6.17}$$

La valeur du compteur de backoff W_i est uniformément choisie à l'étage i dans l'intervalle $[0, W_i - 1]$ donnée par l'équation (6.12).

- La probabilité que le nœud tente de transmettre un paquet non prioritaire est donnée par

$$b_{i,0,j} = (1 - P_s)^i \, b_{0,0,j} = x^i \, b_{0,0,j}, \ \forall \, i \in [0, m], \, j \in [0, n]. \tag{6.18}$$

- La probabilité de retransmission après m tentatives d'échec de transmission est donnée par l'équation (6.19).

$$b_{0,0,j} = \left(x \sum_{i=0}^{m} b_{i,0,j-1} \right)^j = \left(x \, \frac{1 - x^{m+1}}{1 - x} \right)^j b_{0,0,0} = y^j \, b_{0,0,0}, \ \forall j \in [0, n]. \tag{6.19}$$

- La probabilité de résider dans l'état $(0, 0, 0)$ se calcule comme suit

$$b_{0,0,0} = \frac{(1 - h_p) \, P_Q}{W_0} + \sum_{k=1}^{W_0 - 1} b_{0,k,0} = (1 - h_p) \, P_Q. \tag{6.20}$$

- La probabilité de l'état succès est donnée par l'équation (6.21).

$$b_{-2,0,j} = P_s \sum_{i=0}^{m} b_{i,0,j} = (1 - x^{m+1}) \, b_{0,0,j}, \ \forall \ j \in [0, n]. \tag{6.21}$$

- La probabilité d'état échec est

$$b_{-1,0,j} = (1 - P_s) \sum_{i=0}^{m} b_{i,0,j} = y \, b_{0,0,j}, \ \forall \ j \in [0, n]. \tag{6.22}$$

c) Calcul de la probabilité de résider dans l'état Q

A partir du graphe de transition, chaque état dépend de la probabilité P_Q. Pour la dériver, nous utilisons la condition de normalisation exprimée par l'équation (6.23). Nous dérivons ensuite l'expression de chaque terme de cette équation dans les équations (6.24)-(6.28).

$$\sum_{i=0}^{m} \sum_{k=0}^{W_i - 1} p_{i,k,i+1} + \sum_{k=0}^{L_c - 1} p_{-1,k,0} + \sum_{k=0}^{L_s - 1} p_{-2,k,0} + \sum_{i=0}^{m} \sum_{k=0}^{W_i - 1} \sum_{j=0}^{n} b_{i,k,j} +$$

$$\sum_{j=0}^{n} \left(\sum_{k=0}^{L_s - 1} b_{-2,k,j} + \sum_{k=0}^{L_c - 1} b_{-1,k,j} \right) = 1. \tag{6.23}$$

En utilisant les équations (6.11), (6.12), (6.13) et (6.14), nous obtenons le premier terme comme suit

$$\sum_{i=0}^{m} \sum_{k=0}^{W_i - 1} \sum_{j=1}^{d} p_{i,k,j} = \sum_{i=0}^{m} \sum_{j=1}^{d} \frac{W_i + 1}{2} x^i \, p_{0,0,1} = \frac{h_p}{2} \left[\frac{1 - (2x)^{m+1}}{1 - 2x} W_0 + \frac{1 - x^{m+1}}{1 - x} \right] \times P_Q = S_1 P_Q. \tag{6.24}$$

À partir des équations (6.14) et (6.16), le deuxième terme s'exprime par

$$\sum_{k=0}^{L_c - 1} p_{-1,k,j} = \sum_{k=0}^{L_c - 1} \frac{x \, (1 - x^{m+1})}{1 - x} \, h_p \, P_Q = L_c \, \frac{x \, (1 - x^{m+1})}{1 - x} \, h_p \, P_Q = S_2 P_Q. \tag{6.25}$$

D'après les équations (6.14) et (6.15), nous obtenons le troisième terme donné dans (6.26).

$$\sum_{k=0}^{L_s-1} p_{-2,k,j} = \sum_{k=0}^{L_s-1}(1-x^{m+1})\, h_p\, P_Q = L_s\,(1-x^{m+1})\, h_p\, P_Q = S_3 P_Q. \tag{6.26}$$

Le quatrième terme est obtenu grâce aux équations (6.12) et (6.17)-(6.20).

$$\sum_{i=0}^{m}\sum_{k=0}^{W_i-1}\sum_{j=0}^{n} b_{i,k,j} = \sum_{i=0}^{m}\sum_{j=0}^{n}\frac{W_i+1}{2}x^i\, b_{0,0,j} = P_Q\frac{(1-h_p)}{2}\left[\frac{1-(2x)^{m+1}}{1-2x}W_0+\frac{1-x^{m+1}}{1-x}\right]\frac{1-y^{n+1}}{1-y} = S_4 P_Q. \tag{6.27}$$

D'après les équations (6.19)-(6.22), le dernier terme est

$$\sum_{j=0}^{n}\left(\sum_{k=0}^{L_s-1} b_{-2,k,j}+\sum_{k=0}^{L_c-1} b_{-1,k,j}\right) = P_Q\,(1-h_p)\,(1-x^{m+1})\left[L_s+\frac{L_c\,x}{1-x}\right]\frac{1-y^{n+1}}{1-y} = S_5 P_Q. \tag{6.28}$$

Finalement, P_Q s'exprime comme suit

$$P_Q = \frac{1}{S_1+S_2+S_3+S_4+S_5}. \tag{6.29}$$

Nous pouvons, à présent, exprimer la probabilité τ qu'un nœud transmette dans n'importe quel intervalle de temps aléatoire, donnée par l'équation (6.30).

$$\tau = \sum_{i=0}^{m}\sum_{j=1}^{d} p_{i,0,j} + \sum_{i=0}^{m}\sum_{j=0}^{n} b_{i,0,j} = P_Q\,\frac{1-x^{m+1}}{1-x}\left[h_p+(1-h_p)\,\frac{1-y^{n+1}}{1-y}\right]. \tag{6.30}$$

6.2.4.3 Calcul de la probabilité de succès

La probabilité que le paquet soit transmis avec succès pour les deux mécanismes est

$$P_s = (1-\tau)^{N-1}. \tag{6.31}$$

6.3 Calcul des métriques de performances

Dans cette section, nous dérivons les expressions mathématiques de la fiabilité, de délai moyen, de l'énergie consommée, et de débit offert par le standard IEEE 802.15.4k pour les mécanismes S-aloha PCA et S-aloha en utilisant la chaîne de Markov précédemment définie dans la figure 6.1 et les formules développées dans la section précédente.

6.3.1 Fiabilité

Dans ce modèle, la fiabilité dépend des probabilités P_s et τ.

6.3.1.1 Fiabilité de S-aloha PCA

Les paquets de données prioritaires sont rejetés en raison d'un échec de transmission dans les $(m+1)$ étages de backoff avec la probabilité P_d exprimée comme suit

$$P_d = x\, p_{m,0,d} = x^{m+1}. \tag{6.32}$$

La fiabilité est alors donnée par

$$R_{aloha}^{PCA} = 1 - P_d. \tag{6.33}$$

6.3.1.2 Fiabilité de S-aloha

Les paquets de données non prioritaires sont rejetés en raison d'un échec de transmission dans les $(m+1)$ étages de backoff ou en raison de retransmissions dépassées (c'est-à-dire que le nombre maximum de retransmissions n est atteint), comme décrit dans les équations (6.34) et (6.35), respectivement.

$$P_e = \sum_{j=0}^{n} x\, b_{m,0,j} = \frac{x^{m+1}(1-y^{n+1})}{1-y}. \tag{6.34}$$

$$P_r = \sum_{i=0}^{m} x\, b_{i,0,n} = y^{n+1}. \tag{6.35}$$

La fiabilité est alors donnée, comme suit

$$R_{aloha} = 1 - P_e - P_r. \tag{6.36}$$

6.3.2 Énergie consommée

Dans ce modèle, nous calculons uniquement l'énergie consommée pour une transmission de données réussie. Définissons la consommation énergétique du nœud en mode veille par P_i, la consommation en mode transmission par P_{tm} et la consommation en mode réception par P_{rm}. La consommation moyenne d'énergie des deux mécanismes est donnée par les équations (6.37) et (6.38).

6.3.2.1 Énergie consommée par S-aloha PCA

En utilisant les équations (6.24)-(6.26), E_{PCA} peut être dérivé comme suit

$$E_{aloha}^{PCA} = P_i \sum_{i=0}^{m} \sum_{k=1}^{W_i-1} p_{i,k,i+1} + +P_{tm} \sum_{k=0}^{L-1} (p_{-1,k,0} + p_{-2,k,0}) + P_i(p_{-1,L,0} + p_{-2,L,0})$$

$$+ \sum_{k=L+1}^{L+L_{ack}+1} (P_{rm}\, p_{-2,k,0} + P_i\, p_{-1,k,0}). \tag{6.37}$$

6.3.2.2 Énergie consommée par S-aloha

A partir des équations (6.27) et (6.28), E_{aloha} est donnée par l'équation (6.38).

$$E_{aloha} = P_i \sum_{i=0}^{m} \sum_{k=1}^{W_i-1} \sum_{j=0}^{n} b_{i,k,j} + P_{tm} \sum_{k=0}^{L-1} \sum_{j=0}^{n} (b_{-1,k,j} + b_{-2,k,j}) + P_i \sum_{j=0}^{n} (b_{-1,L,j} + b_{-2,L,j}) + \sum_{j=0}^{n} \sum_{k=L+1}^{L+L_{ack}+1} (P_{rm}\, b_{-2,k,j} + P_i\, b_{-1,k,j}). \tag{6.38}$$

6.3.3 Débit

Le débit définit le nombre moyen de paquets de données transmis avec succès par unité de temps.

6.3.3.1 Débit de S-aloha PCA

Soit P_c^{pca} la probabilité d'une transmission qui rencontre des collisions donnée par

$$P_c^{pca} = 1 - (1 - \tau_{aloha}^{pca})^{N-1}. \tag{6.39}$$

Soit $P_{success}^{pca}$ la probabilité d'une transmission réussie, exprimée par l'équation (6.40).

$$P_{success}^{pca} = \frac{N\tau_{aloha}^{pca}(1 - \tau_{aloha}^{pca})^{N-1}}{P_c^{pca}}. \tag{6.40}$$

Soit T_s la durée de transmission réussie d'un paquet de données. Son expression est la suivante

$$T_s = L_p + T_{PHY} + T_{MAC} + T_{LIFS} + t_{ack-wait} + t_{ack}. \tag{6.41}$$

Soit T_c la durée de transmission non réussie (à cause des collisions), donnée par

$$T_c = L_p + T_{PHY} + T_{MAC} + T_{LIFS} + t_{ack-wait}. \tag{6.42}$$

Le débit associé pour S-aloha PCA est alors donné par

$$Db_{aloha}^{PCA} = \frac{L_p\, P_c^{pca}\, P_{success}^{pca}}{\sigma(1 - P_c^{pca}) + T_s\, P_c^{pca}\, P_{success}^{pca} + T_c\, P_c^{pca}(1 - P_{success}^{pca})}. \tag{6.43}$$

Où, σ est la durée d'un intervalle de temps, t_{ack} est la durée de la trame d'accusé de réception et $t_{ack-wait}$ est le temps d'attente avant de commencer la transmission de l'ACK .

6.3.3.2 Débit de S-aloha

Soit P_c^{aloha} la probabilité d'une transmission avec collision. Son expression est la suivante

$$P_c^{aloha} = 1 - (1 - \tau_{aloha})^{N-1}. \tag{6.44}$$

Soit $P_{success}^{aloha}$ la probabilité d'une transmission réussie donnée par l'équation (6.45).

$$P_{success}^{aloha} = \frac{N\tau_{aloha}(1 - \tau_{aloha})^{N-1}}{P_c^{aloha}}. \tag{6.45}$$

Alors, le débit de S-aloha est obtenu par l'équation (6.46).

$$Db_{aloha} = \frac{L_p P_c^{aloha} P_{success}^{aloha}}{\sigma(1 - P_c^{aloha}) + T_s P_c^{aloha} P_{success}^{aloha} + T_c P_c^{aloha}(1 - P_{success}^{aloha})}. \tag{6.46}$$

Où T_s et T_c sont les mêmes que ceux définis dans les équations (6.41) et (6.42), respectivement.

6.3.4 Délai

Le délai moyen $E[D]$ d'un paquet de données transmis avec succès représente l'intervalle de temps entre l'instant où le paquet de données est prêt à être transmis et l'instant de la réception de sa trame ACK correspondante. En revanche, nous ne considérons que le délai des transmissions réussies.

6.3.4.1 Délai de S-aloha PCA

Le délai de transmission associé au paquet prioritaire est exprimé comme suit

$$E[D_{aloha}^{PCA}] = \sum_{i=0}^{m} P(A_i|A_t)E[D_i]. \tag{6.47}$$

Où

- L'événement A_i indique l'occurrence d'une transmission réussie du paquet à l'instant $i + 1$ étant donné i transmissions échouées, alors que l'événement A_t indique l'occurrence d'une transmission de paquet réussie dans les m tentatives de transmission.

$$P(A_i|A_t) = \frac{(1 - P_s)^i}{\sum_{k=0}^{m}(1 - P_s)^k} = x^i \frac{1 - x}{1 - x^{m+1}}. \tag{6.48}$$

- D_i est l'événement où un nœud envoie un paquet prioritaire avec succès au i^{ieme} instant.

$$E[D_i] = T_s + i\,T_c + T_b \sum_{h=0}^{i} E[D_h^{pca}]. \tag{6.49}$$

– $E[D_h^{pca}]$ est le délai de l'étage du backoff. T_s et T_c sont les périodes de temps pour une transmission réussie et non réussie des paquets données précédemment par les équations (6.41) et (6.42), respectivement.

$$\sum_{h=0}^{i} E[D_h^{pca}] = \sum_{h=0}^{i} \frac{W_h - 1}{2} = \sum_{h=0}^{i} \frac{2^h W_0 - 1}{2} = \frac{-1}{2}\Big[(1 - 2^{i+1})W_0 + (i + 1)\Big]. \tag{6.50}$$

En utilisant les équations (6.47), (6.48), (6.49) et (6.50), le délai moyen de S-aloha PCA est donné par

$$E[D_{aloha}^{PCA}] = \sum_{i=0}^{m} \left[\left(x^i \frac{1 - x}{1 - x^{m+1}} \right) \left[T_s + i\, T_c - \frac{T_b}{2}\Big[(1 - 2^{i+1})W_0 + (i + 1)\Big] \right] \right]. \tag{6.51}$$

6.3.4.2 Délai de S-aloha

Le délai de transmission associé au paquet non prioritaire est donné par l'équation (6.52).

$$E[D_{aloha}] = \sum_{j=0}^{n} P(B_j|B_t)E[D_j]. \tag{6.52}$$

Où

– L'événement B_j indique l'occurrence d'une transmission réussie du paquet à l'instant $j + 1$ étant donné j transmissions échouées, alors que l'événement B_t indique l'occurrence d'une transmission réussie du paquet dans les m tentatives de transmission.

$$P(B_j|B_t) = \frac{y^j}{\sum_{k=0}^{n} y^k} = y^j \frac{1 - y}{1 - y^{n+1}}. \tag{6.53}$$

– D_j est l'événement où un nœud envoie avec succès un paquet non prioritaire au j^{ieme} instant, donné par

$$E[D_j] = T_s + j\, T_c + T_b \sum_{h=0}^{j} E[D_h^{aloha}]. \tag{6.54}$$

– $E[D_h^{aloha}]$ est le délai de l'étage backoff, exprimé comme suit :

$$E[D_h^{aloha}] = \sum_{h=0}^{i} \frac{W_h - 1}{2} = \sum_{h=0}^{i} \frac{2^h W_0 - 1}{2} = \frac{-1}{2}\Big[(1 - 2^{i+1})W_0 + (j + 1)\Big]. \tag{6.55}$$

En utilisant les équations (6.53)-(6.55), le délai moyen de S-aloha est donné par l'équation (6.56).

$$E[D_{aloha}] = \sum_{j=0}^{n} \left[\left(y^j \frac{1 - y}{1 - y^{n+1}} \right) \left(T_s + i\, T_c - \sum_{i=0}^{m} \frac{T_b}{2}\Big[(1 - 2^{i+1})W_0 + (i + 1)\Big] \right) \right]. \tag{6.56}$$

6.4 Analyse de performances des mécanismes IEEE 802.15.4k S-aloha PCA et S-aloha

6.4.1 Méthode d'analyse et logiciels utilisés

A partir du modèle analytique proposé dans la section précédente (voir section 6.2.4), nous avons résolu le système d'équations non linéaire formé par les expressions de S_1, S_2, S_3, S_4, S_5, P_s, P_c et τ en utilisant des méthodes numériques. Pour obtenir des résultats numériques à la fois du S-aloha PCA et du S-aloha de IEEE 802.15.4k, nous utilisons le logiciel mathématique Mathcad. Les résultats obtenus sont utilisés pour calculer les expressions de fiabilité, de délai, de débit et de la consommation d'énergie décrites dans la section 6.3, et comparer les performances des deux mécanismes d'accès au médium. Enfin, nous évaluons les effets de la variation du nombre de nœuds N, de la probabilité h_p, de la taille des paquets L_p et de l'étage de backoff m sur les performances de nos métriques en utilisant Matlab.

6.4.2 Valeurs des paramètres utilisés

Le tableau 6.3 nous donne les différents paramètres utilisés pour l'analyse des performances.

Table 6.3 – Paramètres utilisés pour l'évaluation des performances de IEEE 802.15.4k ALOHA PCA slotté

Paramètre	Valeur	Paramètre	Valeur
n	3	$aMaxSIFSFrameSize$	18 bytes
m	4	$aMaxSIFSPeriod$	12 symbols
L_p, h_p, N	Variants	t_{ack}	1 ms
W_0	8	$t_{ack-wait}$	$[1 - 1.32]\ ms$
$macMinBE$	3	T_{LIFS}	0.32 ms
d	6 ms	T_b	1.92 ms
$L_s = L_c$	80 bytes	P_i	0.8 mW
L_{ack}	20 byte	P_{tm}	30 mW
MAC header length	16 bytes	P_{rm}	40 mW
PHY header length	6 bytes	σ	0.96 ms

6.4.3 Résultats, analyses et comparaisons

La figure 6.2 représente la variation de la fiabilité en fonction de la taille du réseau, pour deux valeurs différentes de la probabilité h_p que le paquet soit prioritaire ($h_p = 0.3$ et $h_p = 0.8$). Nous

notons que lorsque la taille de réseau devient de plus en plus grande, la fiabilité diminue. Ceci est dû au fait que la probabilité de collision augmente lorsque un grand nombre de nœuds tente de transmettre. Dans S-aloha, la fiabilité lorsque $h_p = 0.8$ est légèrement meilleure que lorsque $h_p = 0.3$, car il y a moins de nœuds ayant des paquets non prioritaires à transmettre, par conséquent la fiabilité est légèrement grande. En revanche, dans S-aloha PCA, la fiabilité n'est pas influencée par l'augmentation de la probabilité h_p. La figure montre également que S-aloha PCA offre une bonne fiabilité par rapport S-aloha.

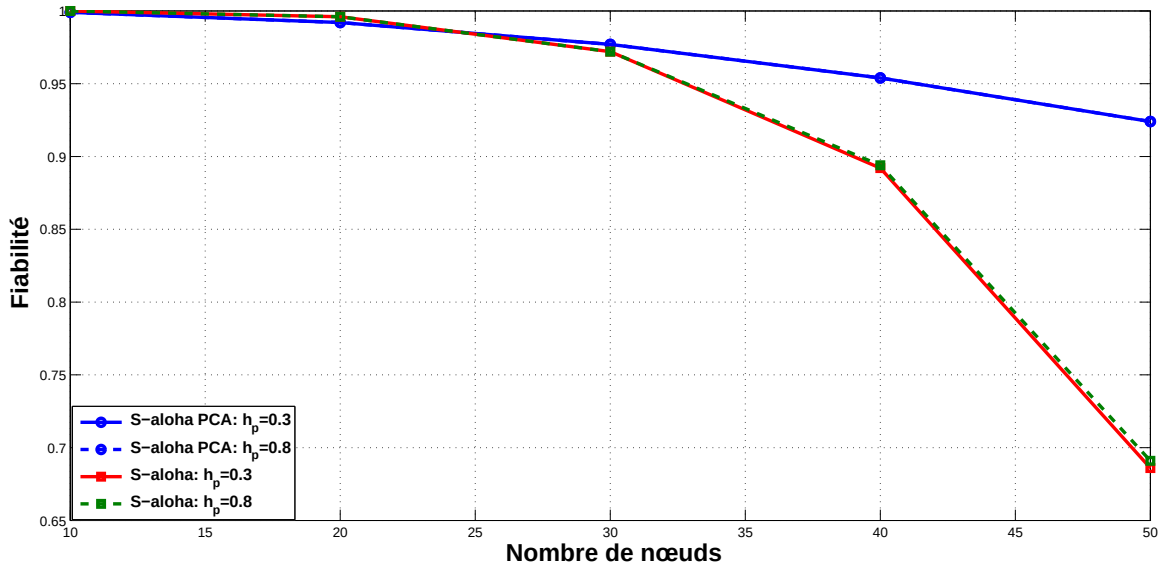


FIGURE 6.2 – Fiabilité Vs Taille du réseau & variant la probabilité que le paquet est prioritaire h_p, avec $L_p = 100$ bytes.

La variation de la fiabilité en fonction de la taille du réseau pour différentes tailles de paquets ($L_p = 20$ bytes et $L_p = 100$ bytes) est illustrée dans la figure 6.3. Nous reportons que la fiabilité diminue lorsque le nombre de stations augmente, car la probabilité de collision augmente. En augmentant la taille des paquets, la fiabilité reste la même. En d'autres termes, peu importe la taille du paquet, la probabilité de sa transmission avec succès reste constante. La fiabilité offerte par PCA est meilleure que celle de aloha quelque soit la taille du réseau et la taille des paquets.

La figure 6.4 trace la variation de l'énergie consommée en fonction de la taille du réseau et de la probabilité que le paquet soit prioritaire ($h_p = 0.3$ et $h_p = 0.8$). Avec l'augmentation de la probabilité h_p ($h_p = 0.8$), beaucoup de nœuds ayant des paquets prioritaires à transmettre tentent de transmettre, ainsi une grande énergie est consommée par ces nœuds. Par conséquent, le peu de nœuds ayant de paquets non prioritaires à transmettre, consomment moins d'énergie. Tandis que, lorsque

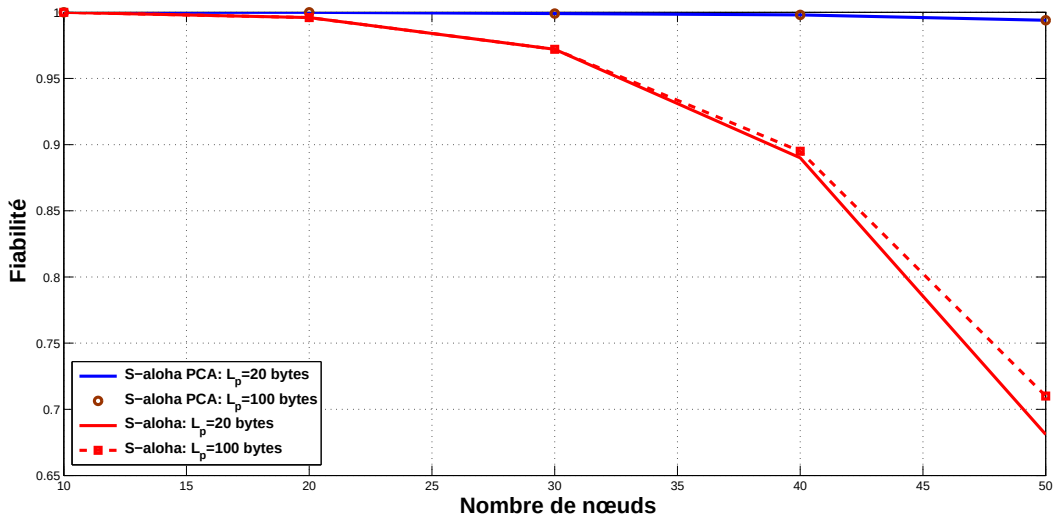


FIGURE 6.3 – Fiabilité Vs Taille du réseau & variant la Taille des paquets L_p, avec $h_p = 0.5$.

$h_p = 0.3$, beaucoup de paquets non prioritaires tentent de transmettre consommant plus d'énergie. En revanche, les nœuds non prioritaires consomment moins d'énergie vu leur petit nombre. Dans

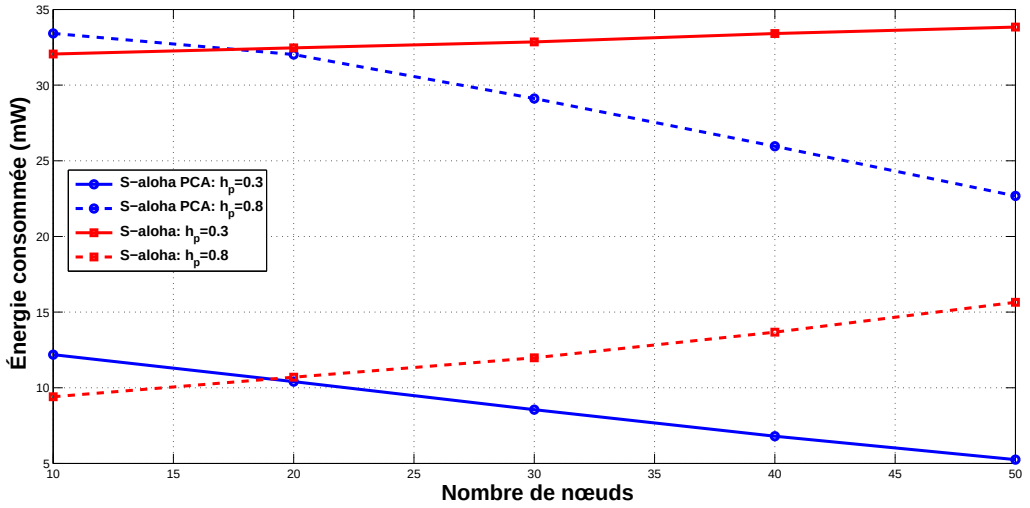


FIGURE 6.4 – Énergie Vs Taille du réseau & variant la probabilité que le paquet est prioritaire h_p, avec $L_p = 100$ bytes.

S-aloha, l'énergie consommée est très grande par rapport à PCA lorsque la taille du réseau est très importante, cela est dù aux retransmissions offertes pour les paquets non prioritaires lors de l'échec de transmission dans les $m + 1$ étages du backoff. Dans ces retransmissions, une énergie de plus va être consommée. En d'autres termes, PCA donne de bons résultats par rapport à aloha peu importe la valeur de la probabilité h_p.

Dans la figure 6.5, l'énergie en fonction de la taille du réseau pour différentes tailles des paquets (L_p = 20 bytes et L_p = 100 bytes) est représentée. Avec l'augmentation de la taille du réseau, nous constatons une diminution de l'énergie des nœuds ayant des paquets prioritaires à transmettre. En revanche, une augmentation de l'énergie consommée par les nœuds ayant des paquet non prioritaires est observée. Lors d'une grande taille des paquets, l'énergie consommée devient plus importante, pour les deux mécanismes, car le paquet prend plus de temps dans l'état réception. L'énergie consommée dans S-aloha PCA est inférieure à celle dans S-aloha, car les paquets prioritaires doivent être transmis dans un délai prédéfini, sinon ils seront écrasés. Mais, les paquets non prioritaires ont d'autres tentatives de transmission dans le cas de l'échec de transmission.

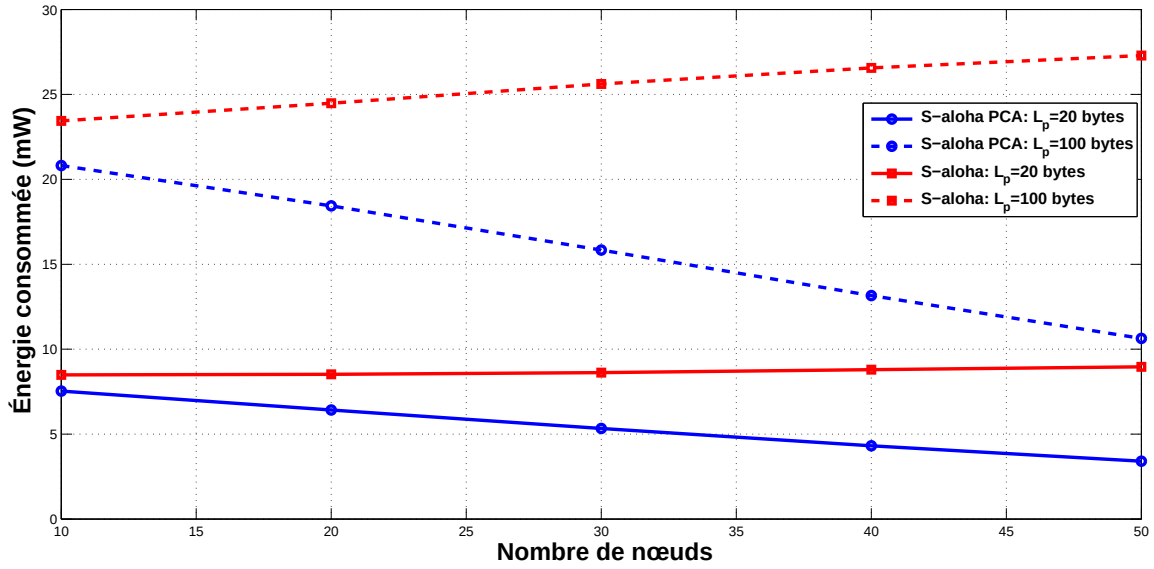


FIGURE 6.5 – Énergie Vs Taille du réseau & variant la Taille des paquets L_p, avec h_p = 0.5.

La figure 6.6 illustre la variation du débit en fonction de la taille du réseau avec variation de la probabilité h_p (h_p = 0.3 et h_p = 0.8). Le débit augmente au fur et à mesure que le nombre de nœuds dans le réseau augmente. Cela s'explique par le fait que la bande passante est de plus en plus utilisée. Lorsque h_p = 0.3, le nombre de paquets non prioritaires est très grand et celui des prioritaires est petit, ainsi la quantité d'informations transmise est grande, c'est pour cela que le débit associé à aloha est supérieur à celui associé à PCA. Nous remarquons l'inverse lorsque h_p = 0.8, ce qui veut dire que le débit qu'offrent les paquets non prioritaires est inférieur à celui des paquets prioritaires. La figure montre également que lorsque le nombre de nœuds dépasse 50, S-aloha offre un débit plus élevé que celui de S-aloha PCA, peu importe la valeur de la probabilité h_p. La raison est que

dans aloha les nœuds disposent de plusieurs tentatives de transmissions pour avoir une transmission réussie de la quantité de données désirée. Contrairement au PCA où les paquets seront perdus s'ils

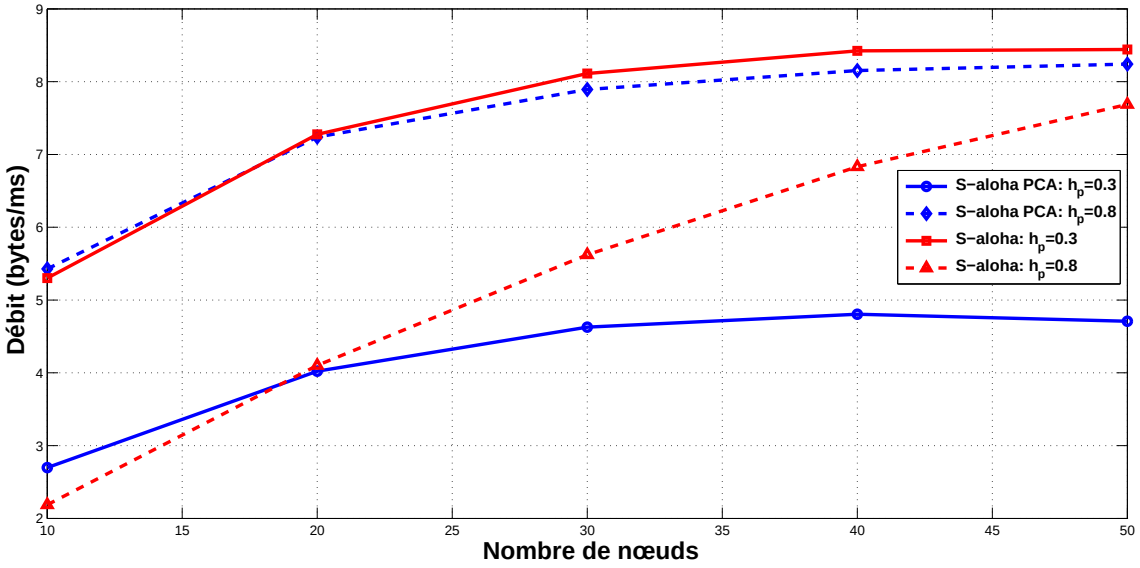


FIGURE 6.6 – Débit Vs Taille du réseau & variant la probabilité que le paquet est prioritaire h_p, avec $L_p = 100$ bytes.

ne sont pas transmis durant les $(m + 1)$ étages du backoff.

Avec l'augmentation de la taille des paquets ($L_p = 100$ bytes), une augmentation du débit est observée dans la figure 6.7, car la quantité de données transmise est importante. La bande passante est de plus en plus utilisée lorsque le nombre de nœuds est grand, d'où l'augmentation du débit avec l'augmentation de la taille du réseau. Nous constatons aussi que le débit offert par les paquets non prioritaires est supérieur à celui des paquets prioritaires, en raison de la retransmission qui donne d'autres tentatives de transmission aux nœuds non prioritaires.

La figure 6.8 montre que le délai augmente avec l'augmentation de la taille du réseau, ce qui s'explique par le fait que les nœuds passent beaucoup de temps dans l'état de transmission, car la probabilité de collision augmente. S-aloha dépense un délai plus élevé par rapport à S-aloha PCA, car la transmission d'un paquet prioritaire sera rapide (avant que le délai d s'achève). Tandis que, pour les nœuds ayant des paquets non prioritaires, un délai de plus est dépensé dans les retransmissions. Le délai est plus grand quand $h_p = 0.3$ que quand $h_p = 0.8$, car le nombre de paquets non prioritaires est plus grand, et ce type de nœuds passe beaucoup de temps dans les retransmissions.

Dans la figure 6.9, le délai en fonction de la taille de réseau pour les tailles des paquets ($L_p = 20$ bytes et $L_p = 100$ bytes) est présenté. La figure montre que pour une grande taille de paquets, le délai

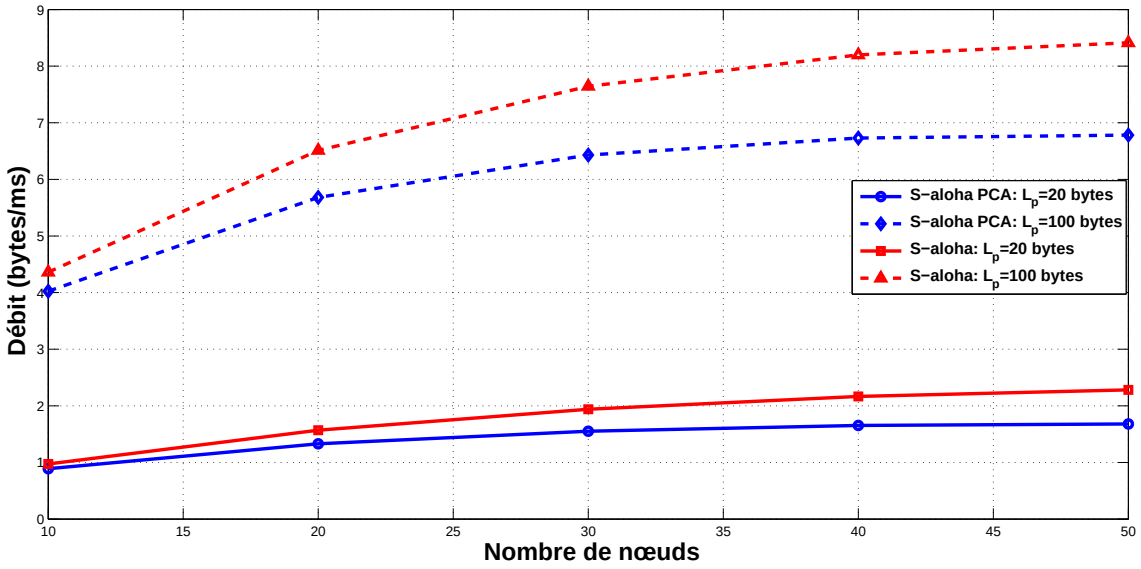


FIGURE 6.7 – Débit Vs Taille du réseau & variant la Taille des paquets L_p, avec $h_p = 0.5$.

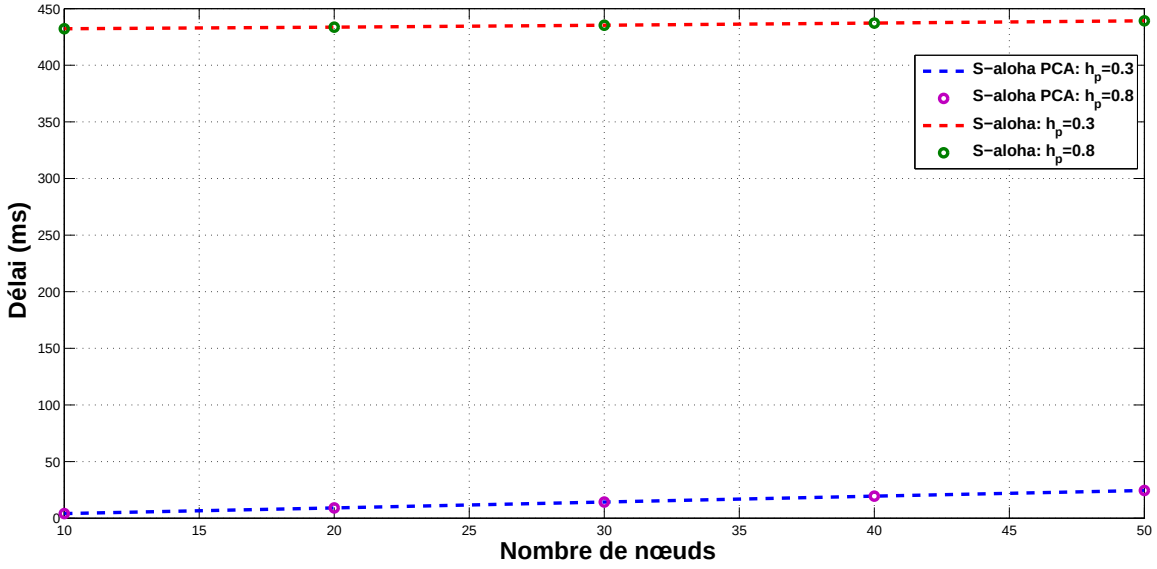


FIGURE 6.8 – Délai Vs Taille du réseau & variant la probabilité que le paquet est prioritaire h_p, avec $L_p = 100$ bytes.

augmente, car la durée de transmission de ces paquets devient grande. Les nœuds ayant des paquets non prioritaires dépensent un temps de plus par rapport aux autres nœuds, car la retransmission prends du temps supplémentaire.

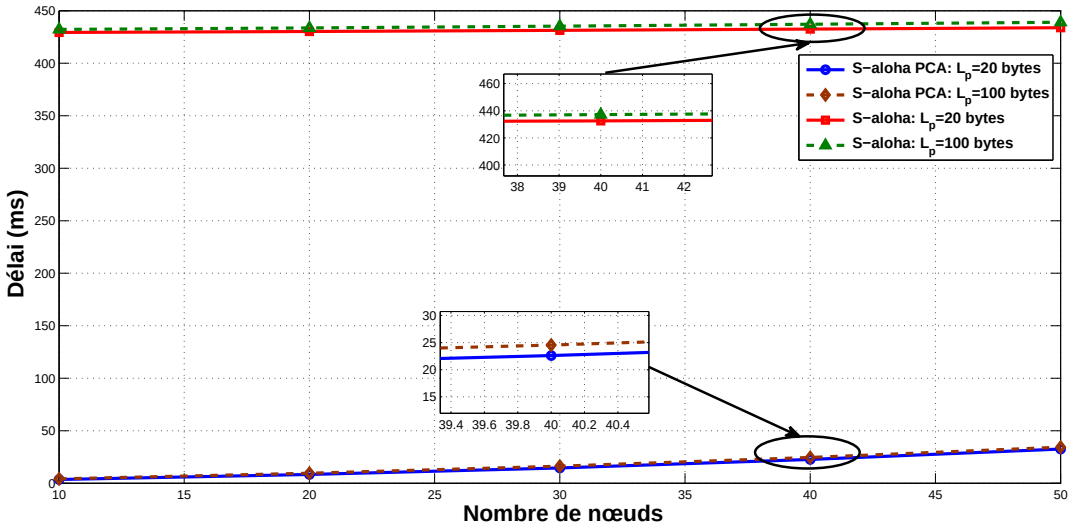


FIGURE 6.9 – Délai Vs Taille du réseau & variant la Taille des paquets L_p, avec $h_p = 0.5$.

La figure 6.10 montre qu'avec l'augmentation du nombre de nœuds dans le réseau, la probabilité de succès diminue, à cause des risques élevés des collisions. Nous constatons que lorsque nous augmentons la probabilité que le paquet soit prioritaire, la probabilité de succès est légèrement plus grande.

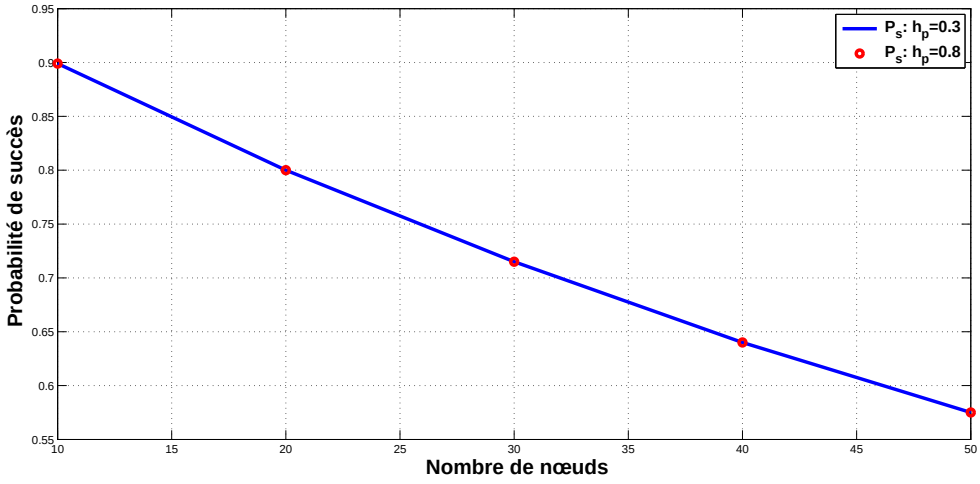


FIGURE 6.10 – Probabilité de succès Vs Taille du réseau & variant la probabilité que le paquet est prioritaire h_p, avec $L_p = 100$ bytes.

En augmentant la taille des paquets dans 6.11, la probabilité de succès reste constante. Ce qui veut dire que la probabilité P_s n'est pas affectée par la taille des paquets. La figure montre aussi que la probabilité de succès diminue avec l'augmentations du nombre de nœuds.

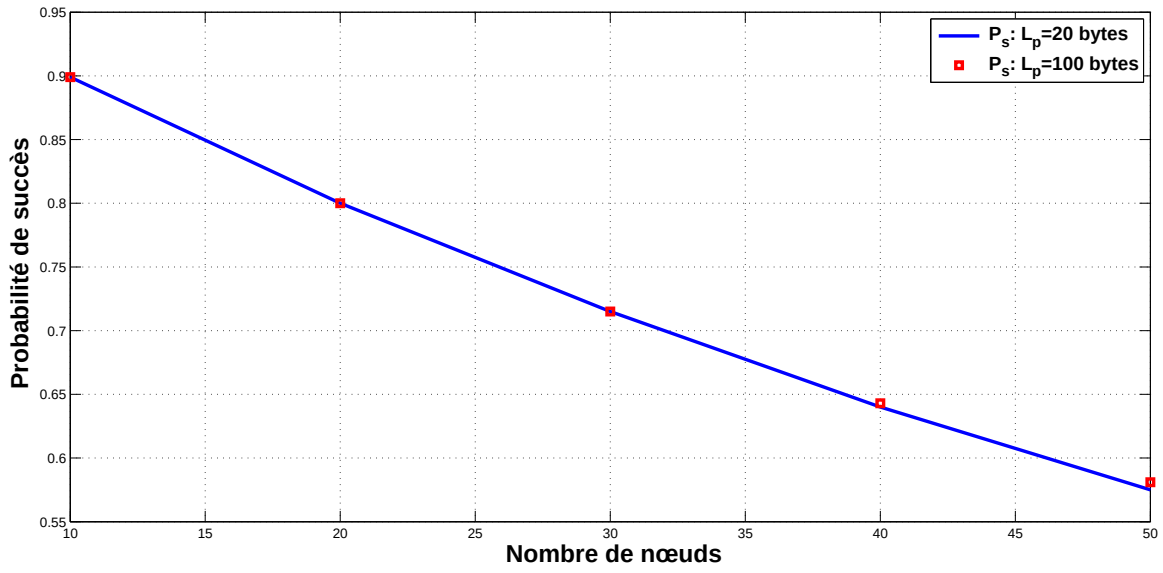


FIGURE 6.11 – Probabilité de succès Vs Taille du réseau & variant la Taille des paquets L_p, avec $h_p = 0.5$.

6.5 Conclusion

Dans ce dernier chapitre, nous avons présenté un nouveau modèle analytique basé sur une chaîne de Markov pour analyser les performances des mécanismes ALOHA PCA slotté (S-aloha PCA) et ALOHA (S-aloha) slotté de la norme IEEE 802.15.4k. Le modèle de chaîne de Markov proposé est à trois dimensions pour les deux mécanismes. Le modèle considère un nombre fixe de nœuds disposés en une topologie en étoile, un trafic saturé, un canal idéal, un mécanisme d'accusé de réception et des limites de retransmissions. Nous avons dérivé les expressions mathématiques de la fiabilité, de la consommation d'énergie, du débit et du délai moyen pour une transmission de paquets réussie, de la norme IEEE 802.15.4k utilisant les mécanismes S-aloha PCA et S-aloha pour les paquets prioritaires et non prioritaires, respectivement. Nous avons analysé l'impact de la variation de la taille du réseau, la probabilité que le paquet disponible soit prioritaire et la taille des paquets sur la probabilité de succès de transmission et les métriques étudiées.

Nous observons que S-aloha PCA permet de réduire la consommation d'énergie, le débit et le

délai moyen par rapport au S-aloha. Tandis qu'une importe fiabilité est observée. En effet, au fur et à mesure que l'on augmente le nombre de nœuds, S-aloha PCA offre une fiabilité élevée par rapport à aloha, une énergie réduite, un débit élevé et un délai moyen élevé. Aussi pour une grande taille de paquet, il offre une fiabilité maximale égale à 1, un délai moyen faible, un débit élevé et une consommation d'énergie élevée. La probabilité de réussite de la transmission reste constante lorsque la taille du paquet devient de plus en plus importante. Tous ces résultats sont des exigences importantes dans les applications industrielles, en particulier pour les systèmes d'infrastructures prioritaires.

Conclusion générale et perspectives

Récemment, le concept d'infrastructure critique est apparu dans le domaine de la mise en réseau de capteurs sans fil. Les infrastructures critiques sont des installations physiques, des actifs et des services qui, s'ils étaient interrompus ou détruits, auraient un impact sérieux sur la santé, la sûreté, la sécurité ou l'économie d'une société ou d'une nation. Par conséquent, la surveillance de ces infrastructures est essentielle pour leur sécurité, leur fiabilité, leur maintenance préventive et leur réduction des coûts grâce à des opérations et une efficacité améliorées.

Avec la mise en œuvre réussie de nombreuses applications des RCSFs, il y avait une tendance à développer et à utiliser une application sans fil pour surveiller les infrastructures critiques. C'est ainsi qu'est né le concept de réseaux de surveillance des infrastructures critiques à faible consommation d'énergie (LECIM). Une grande zone de couverture, une infrastructure minimale, un réseau mis en service, une faible consommation d'énergie, un faible débit de données, un faible coût et un flux de données asymétrique sont quelques-unes des principales caractéristiques/exigences d'un réseau LECIM. Cependant, de nombreux protocoles MAC destinés aux RCSFs, des standards de la famille IEEE 802 et d'autres technologies sans fil ne conviennent pas aux réseaux LECIM pour une ou plusieurs des raisons suivantes : consommation d'énergie élevée, coût élevé, complexité de l'infrastructure, exigence élevée de QoS, petit nombre d'utilisateurs pris en charge, exigence de débit de données élevé, faible marge de liaison pour les environnements difficiles, besoins de maintenance, charge utile importante et topologie du réseau. Après avoir réalisé ce problème, l'organisme IEEE a proposé l'amendement IEEE 802.15.4k en 2013 pour faciliter la communication dans les dispositifs des réseaux LECIM.

La norme IEEE 802.15.4k utilise une topologie de réseau en étoile composée d'un coordinateur PAN et de nœuds de capteurs. La norme a des spécifications de sous-couche MAC et de couche PHY qui permettent la collecte des messages de haute priorité à partir d'un grand nombre de nœuds de capteurs qui sont largement dispersés ou se trouvent dans des environnements difficiles. La sous-couche MAC définit les algorithmes d'accès au canal prioritaire, chacun avec des versions slotté

et non slotté, et la couche PHY définit deux alternatives physique, à savoir LECIM DSSS PHY et LECIM FSK PHY. La couche MAC prend en charge de nouvelles fonctionnalités, telles que la fragmentation MPDU et le schéma d'accès au canal prioritaire. La norme "k" propose dans sa sous-couche MAC deux mécanismes d'accès prioritaire au canal à savoir le CSMA-CA avec backoff PCA et le ALOHA PCA, dédiés uniquement aux messages hautement prioritaires afin de les transmettre en un délai minimal. Dans le mode beacon, les versions slotté de ces mécanismes sont utilisées. Tandis que les versions non slotté sont utilisées dans le mode non beacon.

L'objectif de cette thèse été de proposer des modèles analytiques pour les mécanismes MAC de l'amendement IEEE 802.15.4k dédiés aux applications de surveillance des infrastructures critiques. Avant d'entamer le développement de ces modèles, nous avons réalisé une synthèse critique sur les versions existantes de la norme IEEE 802.15.4 qui constitue la norme de base de l'amendement "k". Les mécanismes MAC proposés permettent un accès prioritaire au canal afin de transmettre un message prioritaire qui représente une situation critique qui devra être réparée. Ce message prioritaire pourrait être, par exemple, une température très élevée mesurée par le nœud capteur qui signifie qu'un incendie est déclenché. Pour la surveillance des ponts, les capteurs sont installés sur les parties critiques du pont et sont utilisés pour surveiller les dommages et fractures pouvant survenir. Dans le cas de détection d'un dommage ou d'une fracture, tous les capteurs qui ont détecté l'incident envoient simultanément des messages d'urgence au système de contrôle afin de les réparer.

Les modèles mathématiques proposés permettent d'évaluer les performances de cet amendement et de voir l'impact de quelques paramètres sur les performances du réseau. Le premier modèle proposé est un modèle de chaîne de Markov pour les mécanismes IEEE 802.15.4k CSMA/CA avec backoff PCA slotté et IEEE 802.15.4k CSMA/CA slotté dans un mode beacon, un trafic saturé, un mécanisme d'accusé de réception, des limites de retransmission et des conditions de canal bruité. La résolution du système induit par notre modèle nous a permis de calculer les métriques de performances suivantes : la fiabilité, l'énergie consommée, le débit et le délai. L'impact de la variation du nombre de nœuds, de la taille du paquet, de la probabilité que le paquet soit prioritaire et du taux d'erreur binaire sur les performances du réseau est analysé. Par la suite, nous avons fait une analyse comparative entre CSMA/CA de IEEE 802.15.4k avec le CSMA/CA de IEEE 802.15.4. En augmentant la taille des paquets, la probabilité de réussite de transmission des paquets prioritaires augmente en parallèle. Avec l'augmentation de la taille du réseau, une fiabilité plus élevée, un délai

plus faible, une consommation d'énergie négligeable et un débit plus faible sont observés pour la transmission de paquets prioritaires par rapport aux paquets non prioritaires.

La deuxième contribution présentée est un modèle de chaîne de Markov modélisant le IEEE 802.15.4k CSMA/CA avec backoff PCA et IEEE 802.15.4k CSMA/CA dans un mode non beacon. Sur la base de notre modèle proposé, nous avons calculé la fiabilité, l'énergie et le débit pour les deux mécanismes dans des conditions de saturation du trafic, sous un canal bruité, tout en tenant compte du mécanisme d'accusé de réception et des limites de retransmission. Par la suite, nous avons évalué les effets de la variation du nombre de nœuds, de la probabilité que le paquet soit prioritaire et de la taille des paquets sur les performances du réseau. Nous observons que PCA non slotté permet une réduction de l'énergie consommée, offre un débit élevé mais une fiabilité inférieure à celle de CSMA/CA non slotté. En effet, à mesure que l'on augmente le nombre de dispositifs, IEEE 802.15.4k offre une fiabilité réduite, une énergie réduite et un débit plus élevé. Aussi, pour une grande taille de paquet, cela donne une fiabilité élevée, une très faible consommation d'énergie, une faible probabilité d'échec et un débit plus élevé.

Le troisième modèle de chaîne de Markov proposé est un modèle pour le IEEE 802.15.4k ALOHA PCA et IEEE 802.15.4k ALOHA dans un mode beacon, un trafic saturé, sous un canal idéal, tenant compte du mécanisme d'accusé de réception et des limites de retransmission. Pour prouver l'efficacité de notre modèle, nous avons analysé l'impact de la variation du nombre de nœuds, de la probabilité que le paquet soit prioritaire, et de la longueur des paquets sur la fiabilité, la consommation d'énergie, le débit, le délai moyen et la probabilité de succès de transmission afin de comparer les performances des deux mécanismes. Nous observons que S-aloha PCA permet de réduire la consommation d'énergie, le débit et le délai moyen par rapport au S-aloha. Mais, il offre une fiabilité plus élevée. En effet, pour un réseau dense, S-aloha PCA offre une fiabilité élevée, une énergie réduite, un débit élevé et un retard moyen élevé. Aussi pour une grande taille de paquets, S-aloha PCA offre un délai moyen élevé, un débit élevé, une consommation d'énergie élevée, et une fiabilité élevée et constante peu importe la taille des paquets. La probabilité de réussite de transmission dans le réseau reste presque constante lorsque la taille du paquet devient de plus en plus importante. Tous les résultats obtenus sont les exigences importantes des applications industrielles, en particulier pour les systèmes d'infrastructures critiques.

Les résultats obtenus dans nos trois contributions sont satisfaisants car la taille des paquets de données et la taille du réseau sont les paramètres les plus importants dans les applications industrielles notamment dans les systèmes de surveillance des infrastructures critiques. Et en les variant, de très bons résultats sont observés.

Comme perspectives de recherche, nous proposons les points suivants :

- Extension de nos modèles proposés dans le cas du trafic non saturé ;
- Analyse comparative entre les mécanismes CSMA/CA avec backoff PCA slotté et non slotté ;
- Modélisation et évaluation de performances du mécanisme ALOHA PCA non slotté ;
- Comparaison entre les mécanismes CSMA/CA avec backoff PCA et ALOHA PCA ;
- Rédaction d'une synthèse sur tous les mécanismes d'accès au canal proposés par le standard IEEE 802.15.4 et réalisation d'une comparaison entre eux ;
- Effectuer une simulation Monte carlo pour les trois contributions et une simulation sous un simulateur réseau ;
- Modélisation et évaluation des performances d'autres amendements de IEEE 802.15.4, comme le IEEE 802.15.4s-2018.

Publications issues de cette thèse

Les résultats des travaux réalisés dans le cadre de cette thèse ont été synthétisés et ont fait l'objet de plusieurs publications parues et d'autres à paraître à court ou à long termes dans des revues internationales de renommée et de plusieurs actes de proceeding de conférence et de doctoriales nationales et internationales parues entre 2017 et 2019. Vu leur importance, ces résultats ont reçu de l'intérêt des chercheurs du domaine et ont eu un impact positif.

Articles de journaux internationaux avec facteur d'impact

1. L. Alkama, L. Bouallouche- Medjkoune et L. Bachiri. "Modeling and Performance Evaluation of the IEEE 802.15.4K CSMA/CA with Priority Channel Access Mechanism Under Fading Channel ". Wireless Personal Communications (WPC), Springer, 2020, accepted. DOI : 10.1007/s11277-020-07584-9.
2. L. Alkama et L. Bouallouche- Medjkoune. "IEEE 802.15.4 historical revolution versions, a survey ". Computing, Springer, 2020, accepted. DOI : 10.1007/s00607-020-00844-3.
3. L. Alkama, L. Bouallouche- Medjkoune et L. Bachiri. "Modeling and performance evaluation of IEEE 802.15.4k slotted ALOHA with PCA mechanism designed for critical infrastructure monitoring systems ". Submitted.
4. L. Alkama, L. Bouallouche- Medjkoune, M.Atmani et L. Bachiri. "Performance analysis of the unslotted IEEE 802.15.4k MAC protocols under saturated traffic and fading channel conditions ". Submitted.

Conférences nationales et internationales

1. L. Alkama and L. Bouallouche- Medjkoune. The IEEE 802.15.4 standard in wireless sensor networks with low power consumption. The 5th Global Congress on Renewable Energy and Environment (ESWAE). Lara Convention Center, Antalya Turkey, 9-11 November 2017.
2. L. Alkama, L. Bouallouche- Medjkoune et L.Bachiri. Modélisation analytique de la norme IEEE 802.15.4k des réseaux LECIM. Journées doctoriales de la recherche opérationnelle, université de Bejaia, Algérie, 12-13 Décembre 2018.
3. L. Alkama, L. Bouallouche- Medjkoune et L.Bachiri. Transmission des messages prioritaires dans les réseaux d'infrastructures critiques. Journées doctoriales sur l'innovation et le transfert technologique, université de Bejaia, Algérie, 15-16 Juillet 2019.

Bibliographie

[1] "Stratégie nationale sur les infrastructures essentielles". https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-fra.pdf, 2009.

[2] "IEEE 802.15.4 Standard, Part 15.4 : Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (LR WPANs)", pp 1–670, IEEE, 2003.

[3] "IEEE Std 802.15.4k, Part 15.4 : Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 5 : Physical Layer Specifications for Low Energy, Critical Infrastructure Monitoring Networks", pp 1–149, IEEE, 2013.

[4] L. Alkama, L. Bouallouche-Medjkoune and L. Bachiri, "Modeling and performance evaluation of the IEEE 802.15.4K CSMA/CA with Priority Channel Access mechanism under fading channel", Wireless Personnal Communication, vol 115, pp 527—-556,, Springer, 2020.

[5] L. Alkama and L. Bouallouche-Medjkoune, "IEEE 802.15.4 historical revolution versions : A survey", Computing, pp 1–33, Springer, 2020.

[6] J. Geier, "Wireless Networks First-step". https://books.google.dz/books?id=kMSpNG2HHPsC&pg=PA3&hl=fr&source=gbs_toc_r&cad=3#v=onepage&q&f=false, 2004.

[7] C. Ouanteur, "Evaluation de performances des Réseaux de capteurs sans fil IEEE 802.15.4", Thèse de Doctorat, Université de Bejaia, Algérie, 2017.

[8] A. Bourai, "La localisation dans les réseaux de capteurs cas étudié", Thèse de Doctorat, Université de Tlemcen, Algérie, 2014.

[9] B. Benmammar, "La technologie agent et les réseaux sans fil", Thèse de Doctorat, Laboratoire d'Informatique de Paris-Nord, France, 2004.

[10] M. Kocakulak and I. Butun, "An overview of wireless sensor networks towards internet of things". *In IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)*, pp 1–6. IEEE, 2017.

[11] H. M. A. Fahmy, "Wireless Sensor Networks : Energy Harvesting and Management for Research and Industry", pp 12–23, Springer International Publishing, 2020.

[12] M. Atmani, "Proposition et Validation Formelle d'un Mécanisme d'accès au Medium pour les réseaux decapteurs sans fil", Thèse de Doctorat, Université de Bejaia, Algérie, 2015.

[13] T. L. Dickey, C. L. McCrank, J. I. Masters, D. M. Markuson and M. S. Evans, "ZigBee, Thread and BLE co-existence with 2.4 GHz WiFi". https://patents.google.com/patent/US10667285B2/en, 2020.

[14] T. Duc Chung, I. Rosdiazli and B. Kishore, "Battery's Life-Time Estimation of Industrial WirelessHART Sensor Actuator Node", Arabian Journal for Science and Engineering, vol 45, pp 6287–6295, Springer, 2020.

[15] Z. Padrah, C. Pop, E. Jecan, A. Pastrav, T. Palade, O. Ratiu and E. Puschita, "An ISA 100.11a Model Implementation for Accurate Industrial WSN Simulation in ns-3". *In International Workshop on Antenna Technology (IWAT)*, pp 1–4. IEEE, 2020.

[16] J. Ben Slimane, "Allocation conjointe des canaux de fréquence et des créneaux de temps et routage avec QdS dans les réseaux de capteurs sans fil denses et étendus", Thèse de Doctorat, Ecole supérieure des communications de Tunis et l'université de Lorraine, 2013.

[17] M. N. Abdeddaim, "Analyse des performances d'un réseau de capteurs exploitant le standard ieee 802.15.4", Thèse de Doctorat, Université de Grenoble, France, 2012.

[18] K. Chen, "Performance evaluation by simulation and analysis with applications to computer networks", pp 1–316, John Wiley & Sons, 2015.

[19] C. Rovetta, "Simulation parfaite de réseaux fermés de files d'attente et génération aléatoire de structures combinatoires", Thèse de Doctorat, Paris Sciences et Lettres, France, 2017.

[20] M. Mehraei, "Mood States Prediction by Stochastic Petri Nets". *In International Psychological Applications Conference and Trends (INPACT2017)*, pp 258–262. Budapest, Hungary, 2017.

[21] G. Wang, Y. Zhang, S. J. Shepherd, C. B. Beggs and N. Rao, "Application of stochastic petri nets for modelling the transmission of airborne infection in indoor environment", International Scientific Journal of Clinical Medicine, vol 32, pp 587–592, Acta Medica Mediterranea, 2016.

[22] E. M. Clarke, T. A. Henzinger, H. Veith and R. Bloem, "Handbook of model checking. chapter 32 : Process algebra and model checking", vol 10, pp 1149–1195, Springer, 2018.

[23] A. W. Tekulu, "Process algebra for performance evaluation", Thèse de Doctorat, School of Industrial and Information Engineering, Milano, 2020.

[24] J. Misic, V. B. Misic and S. Shafi, "Performance of IEEE 802.15.4 beacon enabled PAN with uplink transmissions in non-saturation mode-access delay for finite buffers". *In Proceedings*

of the First International Conference on Broadband Networks, pp 416–425. Washington, United States, IEEE, 2004.

[25] P. K. Sahoo and J.-P. Sheu, "Modeling IEEE 802.15.4 based wireless sensor network with packet retry limits". *In Proceedings of the 5th ACM symposium on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks*, pp 63–70. Canada, 2008.

[26] S. Pollin, M. Ergen, S. C. Ergen, B. Bougard, L. Van der Perre, I. Moerman, A. Bahai, P. Varaiya and F. Catthoor, "Performance analysis of slotted carrier sense IEEE 802.15.4 medium access layer", IEEE Transactions on wireless communications, vol 7, pp 3359–3371, IEEE, 2008.

[27] P. Park, P. Di Marco, P. Soldati, C. Fischione and K. H. Johansson, "A generalized Markov chain model for effective analysis of slotted IEEE 802.15.4". *In IEEE 6th International Conference on Mobile Adhoc and Sensor Systems*, pp 130–139. IEEE, 2009.

[28] Y. Chen, Z.-Y. Wang and L. Huang, "Performance analysis of a non-beacon enabled IEEE 802.15.4 network with retransmission and ACK mode", arXiv preprint arXiv :1609.01101, pp 1–48, 2016.

[29] I. El Korbi and L. A. Saïdane, "Performance Evaluation of Unslotted CSMA/CA for Wireless Sensor Networks : Energy Consumption Analysis and Cross Layer Routing", International Journal of Computer Network and Information Security, vol 9, pp 1–12, Modern Education and Computer Science Press, 2017.

[30] M. Šnipas, V. Radziukynas and E. Valakevičius, "Numerical solution of reliability models described by stochastic automata networks", Reliability Engineering & System Safety, vol 169, pp 570–578, Elsevier, 2018.

[31] M. Šnipas, V. Radziukynas and E. Valakevičius, "Modeling reliability of power systems substations by using stochastic automata networks", Reliability Engineering & System Safety, vol 157, pp 13–22, Elsevier, 2017.

[32] G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function", IEEE Journal on selected areas in communications, vol 18, pp 535–547, IEEE, 2000.

[33] T. Park, T. Kim, J. Choi, S. Choi and W. Kwon, "Throughput and energy consumption analysis of IEEE 802.15.4 slotted CSMA/CA", Electronics Letters, vol 41, pp 1017–1019, IET, 2005.

[34] P. Park, P. Di Marco, C. Fischione and K. H. Johansson, "Modeling and optimization of the IEEE 802.15.4 protocol for reliable and timely communications", IEEE Transactions on Parallel and Distributed Systems, vol 24, pp 550–564, IEEE, 2012.

[35] H. Tavakoli, J. Mišić, M. Naderi and V. B. Mišić, "Adaptive low-energy clustering in slotted beacon-enabled IEEE 802.15.4 networks", Wireless Communications and Mobile Computing, vol 16, pp 393–407, Wiley Online Library, 2016.

[36] V.-C. Phan, "Performance Analysis of IEEE 802.15.4 MAC Protocol Under Light Traffic Condition in IoT Environment", Journal on Electronics and Communications, vol 7, pp 94–99, REV, 2018.

[37] E. Feo and G. A. Di Caro, "An analytical model for IEEE 802.15.4 non-beacon enabled CSMA/CA in multihop wireless sensor networks", Istituto Dalle Molle di Studi sull'Intelligenza Artificiale (IDSIA), pp 1–10, Lugano, Switzerland, 2011.

[38] P. Di Marco, P. Park, C. Fischione and K. H. Johansson, "Analytical modeling of multi-hop IEEE 802.15.4 networks", IEEE Transactions on Vehicular Technology, vol 61, pp 3191–3208, IEEE, 2012.

[39] M. Gamal, N. Sadek, M. R. Rizk and M. A. E. Ahmed, "Optimization and modeling of modified unslotted CSMA/CA for wireless sensor networks", Alexandria Engineering Journal, vol 59, pp 681–691, Elsevier, 2020.

[40] "IEEE 802.15.4 standard, part 15.4 : Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications for Low-Rate Wireless Personal Area Networks (WPANs)", pp 1–320, IEEE, 2006.

[41] "IEEE Standard 802.15.4a, Part 15.4 : Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs) : Amendment 1 : Add Alternate PHYs", pp 1–203, IEEE, 2007.

[42] E. Karapistoli, F.-N. Pavlidou, I. Gragopoulos and I. Tsetsinas, "An overview of the IEEE 802.15.4a standard", IEEE Communications Magazine, vol 48, pp 47–53, IEEE, 2010.

[43] L. De Nardis and M.-G. Di Benedetto, "Overview of the IEEE 802.15.4/4a standards for low data rate Wireless Personal Data Networks". *In 4th Workshop on Positioning, Navigation and Communication*, pp 285–289. Hannover, Germany, IEEE, 2007.

[44] H. W. Pflug, D. Neirynck, J. Romme, K. Philips and H. de Groot, "UWB pulse amplitude estimation method for IEEE 802.15.4a". *In IEEE International Conference on Ultra-Wideband*, vol 1, pp 1–4. Nanjing, China, IEEE, 2010.

[45] Z. Ahmadian and L. Lampe, "Performance analysis of the IEEE 802.15.4a UWB system", IEEE Transactions on Communications, vol 57, pp 1474–1485, IEEE, 2009.

[46] "IEEE Standard 802.15.4c, Part 15.4 : Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs) Amendment 2 : Alternative Physical Layer Extension to support one or more of the Chinese 314-316 MHz, 430-434 MHz, and 779-787 MHz bands", pp 1–21, IEEE, 2009.

[47] B. Xia, Q. Fu, D. Li and L. Zhang, "Performance evaluation and channel modeling of IEEE 802.15.4c in urban scenarios". *In 16th Asia-Pacific Conference on Communications (APCC)*, pp 497–502. Auckland, New Zealand, IEEE, 2010.

[48] "IEEE Standard 802.15.4d, Part 15.4 : Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs) Amendment 3 : Alternative Physical Layer Extension to support the Japanese 950 MHz bands", pp 1–27, IEEE, 2009.

[49] "IEEE Std 802.15.4, part 15.4 : Low-rate wireless personal area networks (LR-WPANs)", pp 1–314, IEEE, 2011.

[50] W. Du, D. Navarro and F. Mieyeville, "Performance evaluation of IEEE 802.15.4 sensor networks in industrial applications", International Journal of Communication Systems, vol 28, pp 1657–1674, Wiley Online Library, 2015.

[51] Z. Abbas, N. Javaid, M. A. Khan, S. Ahmed, U. Qasim and Z. A. Khan, "Simulation analysis of IEEE 802.15.4 non-beacon mode at varying data rates". *In Seventh International Conference on Broadband, Wireless Computing, Communication and Applications*, pp 46–52. IEEE, 2012.

[52] D. Striccoli, G. Boggia and L. A. Grieco, "A Markov model for characterizing IEEE 802.15.4 MAC layer in noisy environments", IEEE Transactions on Industrial Electronics, vol 62, pp 5133–5142, IEEE, 2015.

[53] M. Atmani, D. Aïssani and Y. Hadjadj-Aoul, "Towards bandwidth and energy optimization in IEEE 802.15.4 wireless sensor networks", Computing, vol 100, pp 597–620, Springer, 2018.

[54] "IEEE Std 802.15.4e, Part 15.4 : Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 1 : MAC sublayer", pp 1–225, IEEE, 2012.

[55] D. De Guglielmo, S. Brienza and G. Anastasi, "IEEE 802.15.4e : A survey", Computer Communications, vol 88, pp 153–152, Elsevier, 2016.

[56] F. Chen, R. German and F. Dressler, "Towards IEEE 802.15.4e : A study of performance aspects". *In 8th IEEE International Conference On Pervasive Computing and Communications Workshops (PERCOM Workshops)*, pp 68–73. Mannheim, Germany, IEEE, 2010.

[57] D. De Guglielmo, G. Anastasi and A. Seghetti, "From IEEE 802.15.4 to IEEE 802.15.4e : A step towards the internet of things". *In Advances onto the Internet of Things*, vol 260, pp 135–152. Springer International Publishing Switzerland, 2014.

[58] S. Touloum, L. Bouallouche-Medjkoune, D. Aissani and C. Ouanteur, "Performance analysis of the ieee 802.15. 4e tsch-ca algorithm under a non-ideal channel", International Journal of Wireless and Mobile Computing, vol 18, pp 1–15, Inderscience Publishers (IEL), 2020.

[59] G. Z. Papadopoulos, X. Fafoutis and P. Thubert, "Multi-Source Time Synchronization in IEEE Std 802.15.4-2015 TSCH Networks", Internet Technology Letters, vol 3, pp 1–6, Wiley Online Library, 2020.

[60] N. Choudhury, R. Matam, M. Mukherjee and J. Lloret, "A Performance-to-Cost Analysis of IEEE 802.15.4 MAC With 802.15.4e MAC Modes", IEEE Access, vol 8, pp 41936–41950, IEEE, 2020.

[61] "IEEE Std 802.15.4f, Part 15.4 : Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 2 : Active Radio Frequency Identification (RFID) System Physical Layer (PHY)", pp 1–72, IEEE, 2012.

[62] "IEEE Std 802.15.4g, Part 15.4 : Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 3 : Physical Layer (PHY) Specifications for Low-Data-Rate, Wireless, Smart Metering Utility Networks", pp 1–252, IEEE, 2012.

[63] K.-H. Chang and B. Mason, "The IEEE 802.15.4g standard for smart metering utility networks". *In IEEE Third international conference on smart grid communications (SmartGridComm)*, pp 476–480. Tainan, Taiwan, IEEE, 2012.

[64] F. Righetti, C. Vallati, D. Comola and G. Anastasi, "Performance Measurements of IEEE 802.15.4g Wireless Networks". *In IEEE 20th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM)*, pp 1–6. Washington, USA, IEEE, 2019.

[65] H. Harada, K. Mizutani, J. Fujiwara, K. Mochizuki, K. Obata and R. Okumura, "IEEE 802.15.4g based Wi-SUN communication systems", IEICE Transactions on Communications, vol 100, pp 1032–1043, The Institute of Electronics, Information and Communication Engineers, 2017.

[66] C.-S. Sum, M.-T. Zhou, F. Kojima and H. Harada, "Experimental Performance Evaluation of Multihop IEEE 802.15.4/4g/4e Smart Utility Networks in Outdoor Environment", Wireless Communications and Mobile Computing, vol 2017, pp 1–13, Hindawi, 2017.

[67] C.-S. Sum, F. Kojima and H. Harada, "Performance analysis of a multi-hop IEEE 802.15.4g OFDM system in multi-PHY layer network". *In IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pp 1538–1542. London, UK, IEEE, 2013.

[68] K. Mochizuki, K. Obata, K. Mizutani and H. Harada, "Development and field experiment of wide area Wi-SUN system based on IEEE 802.15.4g". *In IEEE 3rd World Forum on Internet of Things (WF-IoT)*, pp 76–81. Reston, USA, IEEE, 2016.

[69] J. Muñoz, T. Chang, X. Vilajosana and T. Watteyne, "Evaluation of IEEE 802.15.4g for environmental observations", Sensors, vol 18, pp 3468, Multidisciplinary Digital Publishing Institute, 2018.

[70] "IEEE Std 802.15.4j, Part 15.4 : Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 4 : Alternative Physical Layer Extension to Support Medical Body Area Network (MBAN) Services Operating in the 2360 MHz-2400 MHz Band", pp 1–24, IEEE, 2013.

[71] D. Wang, D. Evans and R. Krasinski, "IEEE 802.15.4j : extend ieee 802.15.4 radio into the mban spectrum [industry perspectives]", IEEE Wireless Communications, vol 19, pp 4–5, IEEE, 2012.

[72] M. A. B. Abbasi, S. Nikolaou and M. A. Antoniades, "A high gain EBG backed monopole for MBAN off-body communication". *In IEEE International Symposium on Antennas and Propagation (APSURSI)*, pp 1907–1908. Victoria, BC, Canada, IEEE, 2016.

[73] S. Wang, K. Mimis, M. Z. Bocus, G. T. Watkins and J. P. Coon, "Cognitive antenna selection relay for green heterogeneous healthcare networks", IEEE wireless communications, vol 20, pp 44–52, IEEE, 2013.

[74] "IEEE Std 802.15.4m, Part 15.4 : Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 6 : TV White Space Between 54 MHz and 862 MHz Physical Layer", pp 1–118, IEEE, 2014.

[75] C.-S. Sum, L. Lu, M.-T. Zhou, F. Kojima and H. Harada, "Design considerations of IEEE 802.15.4m low-rate WPAN in TV white space", IEEE Communications Magazine, vol 51, pp 74–82, IEEE, 2013.

[76] C.-S. Sum, M.-T. Zhou, L. Lu, R. Funada, F. Kojima and H. Harada, "IEEE 802.15.4m : The first low rate wireless personal area networks operating in TV white space". *In 18th IEEE International Conference on Networks (ICON)*, pp 326–332. Singapore, IEEE, 2012.

[77] J. Kim, J. Han, Z. H. Mir and Y.-B. Ko, "Efficient topology construction and routing for IEEE 802.15.4m-based smart grid networks", Wireless Networks, vol 23, pp 533–551, Springer, 2017.

[78] J. Kim, J. Han, Y.-B. Ko and F. Filali, "Interleaving-based orphan channel scanning for the IEEE 802.15.4m in TVWS Smart Grid Networks". *In Seventh International Conference on Ubiquitous and Future Networks*, pp 89–94. Sapporo, Japan, IEEE, 2015.

[79] L. Bedogni, A. Achtzehn, M. Petrova, P. Mähönen and L. Bononi, "Performance assessment and feasibility analysis of IEEE 802.15.4m wireless sensor networks in TV grayspaces", ACM Transactions on Sensor Networks (TOSN), vol 13, pp 1–27, ACM New York, USA, 2017.

[80] F. Chiti, R. Fantacci, F. Nizzi, L. Pierucci and T. Pecorella, "A cooperative spectrum sensing protocol for IEEE 802.15.4m wide-area WSNs". *In IEEE International Conference on Communications (ICC)*, pp 1–6. Paris, France, IEEE, 2017.

[81] "IEEE Std 802.15.4p, Part 15.4 : Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 7 : Physical Layer for Rail Communications and Control (RCC)", pp 1–45, IEEE, 2014.

[82] "IEEE Std 802.15.4, IEEE Standard for Low-Rate Wireless Personal Area Networks (WPANs)", pp 1–709, IEEE, 2015.

[83] "IEEE Std 802.15.4n, IEEE Standard for Low-Rate Wireless Networks Amendment 1 : Physical Layer Utilizing China Medical Bands", pp 1–27, IEEE, 2016.

[84] "IEEE Std 802.15.4q, IEEE Standard for Low-Rate Wireless Networks Amendment 2 : Ultra-Low Power Physical Layer", pp 1–52, IEEE, 2016.

[85] "IEEE Std 802.15.4u, IEEE Standard for Low-Rate Wireless Networks Amendment 3 : Use of the 865 MHz to 867 MHz Band in India", pp 1–18, IEEE, 2016.

[86] "IEEE Std 802.15.4t, IEEE Standard for Low-Rate Wireless Networks Amendment 4 : Higher Rate (2 Mb/s) Physical (PHY) Layer", pp 1–25, IEEE, 2017.

[87] "IEEE Std 802.15.4v, IEEE Standard for Low-Rate Wireless Networks Amendment 5 : Enabling/Updating the Use of Regional Sub-GHz Bands", pp 1–35, IEEE, 2017.

[88] "IEEE Std 802.15.4s, IEEE Standard for Low-Rate Wireless Networks Amendment 6 : Enabling Spectrum Resource Measurement Capability", pp 1–51, IEEE, 2018.

[89] "IEEE Std 802.15.4x, IEEE Standard for Low-Rate Wireless Networks Amendment 7 : Defining Enhancements to the Smart Utility Network (SUN) Physical Layers (PHYs) Supporting up to 2.4 Mb/s Data Rates", pp 1–28, IEEE, 2019.

[90] "802.15.4-2015/cor 1 IEEE standard for low-rate wireless networks corrigendum 1", pp 1–12, IEEE, 2018.

[91] B. Rozel, "La sécurisation des infrastructures critiques : recherche d'une méthodologie d'identification des vulnérabilités et modélisation des interdépendances", Thèse de Doctorat, Laboratoire de Génie Electrique de Grenoble, France, 2009.

[92] C. F. P. A. Infrastructures, "The Report of the President's Commission on Critical Infrastructure Protection", Washington, DC, 1997.

[93] A. Vidács and R. Vida, "Wireless sensor network based technologies for critical infrastructure systems". *In Intelligent monitoring, control, and security of critical infrastructure systems*, pp 301–316. Springer Berlin Heidelberg, 2015.

[94] A. Tabassum, S. Chinthavali, L. Chen and A. Prakash, "Data Mining Critical Infrastructure Systems : Models and Tools", IEEE Intelligent Informatics Bulletin, vol 19, pp 1–8, IEEE, 2018.

[95] B. Gebremedhin, J. Haapola and J. Iinatti, "Implementation and evaluation of ieee 802.15. 4k priority channel access", Thèse de Doctorat, University of Oulu, Finland, 2013.

[96] B. Johan, C. Mike and H. David, "Low Energy Critical Infrastructure Monitoring". https://mentor.ieee.org/802.15/dcn/10/15-10-0528-00-leci-low-energy-critical-infrastructure-monitoring.pptx, 2010.

[97] M. Zhang and S. She, "Wastewater Monitoring System in Industrial Workshop Based on Wireless Sensor Network", International Journal of Online and Biomedical Engineering (iJOE), vol 13, pp 63–74, Germany, SCImago Institutions Ranking, 2017.

[98] D. Miljković, "Fault detection methods : A literature survey". *In Proceedings of the 34th international convention MIPRO*, pp 750–755. Opatija, Croatia, IEEE, 2011.

[99] J. Oza, Z. Narmawala, S. Tanwar and P. K. Singh, "Public Transport Tracking and its Issues", International Journal of Computer Sciences and Engineering, vol 5, pp 192–197, 2017.

[100] R. White, A. Gadaev, I. Nuzhnov, I. Kirsanov-Belov and D. Boiko, "Container tracking systems and methods". https://patentimages.storage.googleapis.com/77/b7/98/accad3fca8b8e2/US20190147398A1.pdf, 2019.

[101] L. Chia, B. Bhardwaj, P. Lu and R. Bridgelall, "Railroad track condition monitoring using inertial sensors and digital signal processing : A review", IEEE Sensors Journal, vol 19, pp 25–33, IEEE, 2018.

[102] N. K. Jain, R. Saini and P. Mittal, "A review on traffic monitoring system techniques". *In Soft Computing : Theories and Applications*, pp 569–577. Springer, 2019.

[103] S. K. Swain, S. Barik and R. Das, "Nanomaterials as sensor for hazardous gas detection", Handbook of Ecomaterials, pp 1247–1266, Springer Nature Switzerland, 2019.

[104] G. Xiaohua, R. Pengfei, W. Tian, S. Hongfei, L. Fei and L. Renjie, "A. GMM-Based intrusion detection for perimeter security system". *In 14th IEEE International Conference on Electronic Measurement & Instruments (ICEMI)*, pp 1794–1800. Changsha, China, IEEE, 2019.

[105] N. Bhadwal, V. Madaan, P. Agrawal, A. Shukla and A. Kakran, "Smart Border Surveillance System using Wireless Sensor Network and Computer Vision". *In International Conference on Automation, Computational and Technology Management (ICACTM)*, pp 183–190. London, United Kingdom, IEEE, 2019.

[106] A. Dhekne, A. Chakraborty, K. Sundaresan and S. Rangarajan, "TrackIO : tracking first responders inside-out". *In 16th Symposium on Networked Systems Design and Implementation)*, pp 751–764. Boston, USA, USENIX Association, 2019.

[107] N. Ullah, M. S. Chowdhury, M. Al Ameen and K. S. Kwak, "Energy efficient MAC protocol for low-energy critical infrastructure monitoring networks using wakeup radio", International Journal of Distributed Sensor Networks, vol 8, pp 1–15, Hindawi, 2012.

[108] X. Xiong, T. Wu, H. Long and K. Zheng, "Implementation and performance evaluation of LECIM for 5G M2M applications with SDR". *In IEEE Globecom Workshops (GC Wkshps)*, pp 612–617. IEEE, 2014.

[109] L. Leonardi, G. Patti, F. Battaglia and L. L. Bello, "Simulative assessments of the IEEE 802.15.4 CSMA/CA with priority channel access in structural health monitoring scenarios". *In IEEE 15th International Conference on Industrial Informatics (INDIN)*, pp 375–380. Emden, Germany, IEEE, 2017.

[110] M. Sanaullah Chowdhury, N. Ullah, M. A. Ameen and K. S. Kwak, "Framed slotted aloha based MAC protocol for low energy critical infrastructure monitoring networks", International Journal of Communication Systems, vol 27, pp 1783–1797, Wiley Online Library, 2014.

[111] B. G. Gebremedhin, J. Haapola and J. Iinatti, "Performance evaluation of IEEE 802.15.4k priority channel access with DSSS PHY". *In Proceedings of European Wireless 2015 ; 21th European Wireless Conference*, pp 1–6. Budapest, Hungary, VDE, 2015.

[112] M. S. Kiran and P. Rajalakshmi, "Performance analysis of CSMA/CA and PCA for time critical industrial IoT applications", IEEE Transactions on Industrial Informatics, vol 14, pp 2281–2293, IEEE, 2018.

[113] L. Bachiri, D. Aïssani and L. Bouallouche-Medjkoune, "Saturation throughput analysis of the IEEE 802.11e EDCA network with contention free burst under fading channel", Wireless personal communications, vol 79, pp 545–564, Springer, 2014.

[114] M. Yazid, L. Bouallouche-Medjkoune, D. Aïssani, N. Amrouche and K. Bakli, "Analytical analysis of applying packet fragmentation mechanism on both basic and RTS/CTS access methods of the IEEE 802.11b DCF network under imperfect channel and finite load conditions", Wireless personal communications, vol 77, pp 477–506, Springer, 2014.

[115] C. Ouanteur, D. Aïssani, L. Bouallouche-Medjkoune, M. Yazid and H. Castel-Taleb, "Modeling and performance evaluation of the IEEE 802.15.4e LLDN mechanism designed for industrial applications in WSNs", Wireless Netw, vol 96, pp 1355–1376, Springer, 2017.

Résume

Dans les réseaux de capteurs sans fil, chaque dispositif est capable de surveiller son environnement et d'envoyer les informations collectées via une connexion sans fil. Néanmoins, pour la surveillance des infrastructures critiques, des messages critiques doivent être transmis dans un délai minimal pour faire face aux pannes qui peuvent se produire. Afin de permettre cette surveillance, l'utilisation de la norme 802.15.4 devient limitée. Ainsi, en 2013, l'organisme IEEE a proposé une nouvelle version nommée IEEE 802.15.4k. Cet amendement propose de nouveaux mécanismes d'accès au canal prioritaire à savoir le Carrier Sense Mutiple Access with Collision Avoidance avec backoff Priority Channel Access (CSMA/CA avec backoff PCA) et ALOHA PCA. Afin d'évaluer les performances de l'amendement "k", dans les modes beacon et non beacon, nous avons modélisé ses deux mécanismes par une chaîne de Markov. La résolution des systèmes induits par nos modèles de CSMA/CA avec backoff PCA et de ALOHA PCA, nous a permis de calculer quelques métriques de performance, telles que la fiabilité, l'énergie consommée, le débit et le délai. Des conditions de canal bruité comportant des erreurs de transmission et non bruité et des conditions de trafic saturé et non saturé sont considérées dans cette thèse. De plus, l'effet de la variations de quelques paramètres sur nos métriques de performances est proposé. Les résultats obtenus dans nos contributions sont satisfaisants, car la taille des paquets de données et la taille du réseau sont les paramètres les plus importants dans les applications industrielles notamment dans les systèmes de surveillance des infrastructures critiques. Et en les variant, de très bons résultats sont observés.

Mots clés: Réseaux d'infrastructures critiques, LECIM, PCA, ALOHA PCA, IEEE 802.15.4k, chaînes de Markov, évaluation de performances.

Abstract

In wireless sensor networks, each device is able to monitor its environment and send the collected information via a wireless connection. However, for the monitoring of critical infrastructure, critical messages must be transmitted with minimal delay to deal with failures that may occur. In order to allow this monitoring, the use of the 802.15.4 standard becomes limited. Thus, in 2013, the IEEE organization proposed a new version called IEEE 802.15.4k. This amendment proposes new priority channel access mechanisms, namely Carrier Sense Mutiple Access with Collision Avoidance with Priority Channel Access backoff (CSMA/CA with PCA backoff) and ALOHA PCA. In order to evaluate the performance of the "k" amendment, in beacon and non-beacon modes, we have modeled its two mechanisms by a Markov chain. The resolution of the systems induced by our models of CSMA/CA with backoff PCA and ALOHA PCA, allowed us to calculate some performance metrics, such as reliability, energy consumed, throughput and delay. Noisy channel conditions including transmission errors and not noisy and saturated and unsaturated traffic conditions are considered in this thesis. In addition, the effect of varying some parameters on our performance metrics is proposed. The results obtained in our contributions are satisfactory, because the size of the data packets and the size of the network are the most important parameters in industrial applications, especially in critical infrastructure monitoring systems. And by varying them, very good results are observed.

Keywords: Critical infrastructure networks, LECIM, PCA, ALOHA PCA, IEEE 802.15.4k, Markov chains, performance evaluation.

الملخص

في شبكات الاستشعار اللاسلكية ، يستطيع كل جهاز مراقبة بيئته وإرسال المعلومات المجمعة عبر اتصال لاسلكي. ومع ذلك ، من أجل مراقبة البنية التحتية الحرجة ، يجب إرسال الرسائل الحرجة بأقل تأخير ممكن للتعامل مع الإخفاقات التي قد تحدث. للسماح بهذه المراقبة ، يصبح استخدام معيار 802.15.4 محدودًا. وهكذا ، في عام 2013 ، اقترحت منظمة IEEE إصدارًا جديدًا يسمى IEEE 802.15.4k. يقترح هذا التعديل آليات وصول جديدة للقنوات ذات الأولوية ، وهي الوصول المتعدد بحساس الناقل مع تجنب الاصطدام مع أولوية الوصول إلى القنوات التراجعية (CSMA / CA مع تراجع PCA) و ALOHA PCA. من أجل تقييم أداء تعديل "k" ، في أوضاع المنارة وغير المنارة ، قمنا بنمذجة آليتيها بواسطة سلسلة ماركوف. سمحت لنا دقة الأنظمة الناتجة عن نماذجنا من CSMA / CA مع التراجع PCA و ALOHA PCA بحساب بعض مقاييس الأداء ،مثل الموثوقية والطاقة المستهلكة والإنتاجية والتأخير. وتأخذ هذه الأطروحة في الاعتبار ظروف القناة المشوشة بما في ذلك أخطاء الإرسال وظروف الحركة الصاخبة والمشبعة وغير المشبعة. بالإضافة إلى ذلك ، تم اقتراح تأثير تغيير بعض المعلمات على مقاييس أدائنا. النتائج التي تم الحصول عليها من مساهماتنا مُرضية ، لأن حجم حزم البيانات وحجم الشبكة هما أهم المعايير في التطبيقات الصناعية ، ولا سيما في أنظمة مراقبة البنية التحتية الحيوية. ومن خلال تغييرها ، يتم ملاحظة نتائج جيدة جدًا.

المفاتيح : شبكات البنية التحتية الحرجة، IEEE 802.15.4k, ALOHA PCA, PCA, LECIM ,سلاسل ماركوف ، تقييم الفعاليات.