

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université ABDERRAHMANE MIRA de Béjaïa
Faculté des Sciences Exactes
Département d'Informatique



Mémoire pour l'obtention du diplôme de Master recherche en
Informatique

Domaine : Mathématique et Informatique

Filière : Informatique

Spécialité : Réseaux et Systèmes Distribués

Thème

Modélisation et évaluation de performances des protocoles MAC
de IEEE 802.15.4 des réseaux de capteurs sans fil

Présenté par :

Lydia DJOUMI

Feriel OUADI

Soutenues devant le jury composé de :

M ^{me} Lina BACHIRI	MCA	Univ. de Bejaia	Président
M ^{me} Louiza BOUALLOUCHE-MEDJKOUNE	Professeur	Univ. de Bejaia	Rapporteur
M ^{me} Lynda ALKAMA	Docteur	Univ. de Bejaia	Co-Rapporteur
M ^r Mohand MOKTEFI	MAA	Univ. de Bejaia	Examineur

Année Universitaire : 2020/2021

Remerciements

On remercie dieu le tout puissant de nous avoir donné la santé et la volonté d'entamer et de terminer ce mémoire.

Tout d'abord, ce travail ne serait pas aussi riche et n'aurait pas pu avoir le jour sans l'aide et l'encadrement de Madame BOUALLOUCHE-MEDJKOUNE Louiza, on la remercie pour la qualité de son encadrement exceptionnel, pour sa patience, rigueur et sa disponibilité durant notre préparation de ce travail.

On tient également à exprimer notre profonde gratitude à Madame ALKAMA Lynda pour son suivi et son énorme soutien, qu'elle n'a cessé de nous prodiguer tout au long de cette période.

On adresse aussi nos vifs remerciements aux membres des jurys pour avoir bien voulu examiner et juger ce travail.

On remercie tous les membres de notre famille qui nous ont apporté leur soutien et leur aide au cours de ces années d'études, et plus spécialement à nos chers parents.

On ne laissera pas cette occasion passer, sans remercier tous nos collègues pour leur aide et leurs précieux conseils.

Enfin, nos remerciements à tous ceux qui ont contribué de près ou de loin au bon déroulement de ce projet.

Dédicaces

A ma très chère mère

Quoi que je fasse ou que je dise, je ne saurai point te remercier comme il se doit. Ton affection me couvre, ta bienveillance me guide et ta présence à mes cotés a toujours été ma source de force pour affronter les différents obstacles.

A mon très cher père

Tu as toujours été à mes cotés pour me soutenir et m'encourager. Que ce travail traduit ma gratitude et mon affection.

*A mes très chers frères **Nassim** et **Nadir**.*

*A mes très chères sœurs **Nabila**, **Amel**, **Kenza** et **Thanina**.*

Puisse dieu vous donnez santé, bonheur, courage et surtout réussite.

DJOUMI Lydia

Je dédie ce modeste travail

A mes très chers parents pour tant d'amour a mon égard, pour leur patience, et leur sacrifices tout au long de ma vie que Dieu leur apporte tous ce qu'ils souhaitent.

*A mes chers frères **Ouahid**, **Youcef** et **Mahdi**.*

A tous les moments d'enfance passés avec vous mes frères, en gage de ma profonde estime pour l'aide que vous m'avez apporté. Vous m'avez soutenu, réconforté et encouragé. Puissent nos liens fraternels se consolident et se pérennisent encore plus.

*A ma chère tante maternelle **Samia** que Dieu t'accorde une longue vie.*

A mes oncles et tantes paternelles et maternelles.

*A mes adorables neveux **Rafif** et **Mohamed**.*

*A mes belles sœurs **Sonia** et **Rosa**.*

A tous les cousins, les voisins et les amis que j'ai connu jusqu'à maintenant.

A tous les enseignants de l'université de Béjaia qui ont contribué à ma formation.

OUADI Ferial

Table des matières

Table des figures	iv
Liste des tableaux	vi
Notations et Abréviations	vii
Introduction générale	1
I État de l'art	4
1 Les réseaux de capteurs sans fil	5
1.1 Introduction	5
1.2 Les réseaux sans fil	5
1.2.1 Les réseaux personnels sans fil (WPAN)	6
1.2.2 Les réseaux locaux sans fil (WLAN)	7
1.2.3 Les réseaux métropolitains sans fil (WMAN)	7
1.2.4 Les réseaux étendus (WWAN)	7
1.3 Réseaux de capteurs sans fil (RCSFs)	8
1.3.1 Architecture d'un nœud capteur	8
1.3.2 Architecture d'un RCSF et ses caractéristiques	9
1.3.3 Avantages et inconvénients des RCSFs	12
1.3.4 Domaines d'application des RCSFs	12
1.3.5 Standarisisation	14
1.4 Conclusion	15
2 Le standard IEEE 802.15.4	16
2.1 Introduction	16
2.2 Le standard IEEE 802.15.4	16
2.2.1 Définition	16
2.2.2 Types de périphériques IEEE 802.15.4	17
2.2.3 Protocoles basés sur la norme IEEE 802.15.4	17
2.2.4 Topologies du réseau	17
2.2.5 Architecture en couche du réseau IEEE 802.15.4	18
2.2.5.1 La couche physique de IEEE 802.15.4	18
2.2.5.2 La Sous-couche MAC dans IEEE 802.15.4	19
2.2.6 Mécanismes d'accès au canal	22

2.2.6.1	Protocole CSMA/CA	22
2.2.6.2	Protocole Aloha	24
2.2.7	Introduction à l'évaluation de performances des réseaux et ses outils de modélisation	25
2.2.8	Limites de la norme IEEE 802.15.4	26
2.2.9	Évolution de la norme IEEE 802.15.4	26
2.3	Conclusion	28
 II Contributions		 29
 3 Modélisation analytique et évaluation des performances du mécanisme IEEE 802.15.4		
Aloha slotté		30
3.1	Introduction	30
3.2	Modélisation analytique du mécanisme d'accès au canal Aloha slotté	30
3.2.1	Hypothèses du modèle	30
3.2.2	Les Paramètres utilisés dans le modèle	31
3.2.3	Les probabilités utilisées dans le modèle	31
3.2.4	Proposition d'une chaîne de Markov pour le mécanisme S-Aloha	32
3.2.4.1	Probabilités de transition	32
3.2.4.2	Calcul des probabilités d'états stationnaires	34
3.2.4.3	Condition de normalisation	35
3.2.4.4	Calcul de la probabilité de collision	35
3.3	Calcul des métriques de performances	36
3.3.1	Fiabilité	36
3.3.2	Énergie consommée	36
3.3.3	Débit	37
3.3.4	Délai	37
3.4	Analyse de performances de mécanisme IEEE 802.15.4 S-Aloha	38
3.4.1	Méthode d'analyse et logiciels utilisés	38
3.4.2	Valeurs des paramètres utilisés	38
3.4.3	Résultats, analyses et comparaisons	39
 4 Modélisation analytique et évaluation des performances du mécanisme IEEE 802.15.4		
CSMA/CA slotté		44
4.1	Introduction	44
4.2	Modélisation analytique du mécanisme d'accès au canal CSMA/CA slotté	44
4.2.1	Hypothèses du modèle	44
4.2.2	Paramètres utilisés dans le modèle	45
4.2.3	Les probabilités utilisées dans le modèle	45
4.2.4	Proposition d'une chaîne de Markov pour le mécanisme CSMA/CA slotté	47
4.2.4.1	Probabilités de transition	48
4.2.4.2	Calcul des probabilités d'états stationnaires	48

4.2.4.3	Condition de normalisation	49
4.2.4.4	Calcul de la probabilité de collision	50
4.2.4.5	Calcul des probabilités que le canal soit occupé	50
4.3	Calcul des métriques de performances	51
4.3.1	Fiabilité	51
4.3.2	Énergie consommée	52
4.3.3	Débit	52
4.3.4	Délai	53
4.4	Analyse de performances des mécanismes S-CSMA	53
4.4.1	Méthode d'analyse et logiciels utilisés	53
4.4.2	Valeurs des paramètres utilisés	54
4.4.3	Résultats, analyses et comparaisons	54
4.5	Conclusion	59
	Conclusion générale	60
	Bibliographie	62

Table des figures

1.1	Classification des réseaux sans fil selon la zone de couverture.	6
1.2	Architecture d'un nœud capteur.	9
1.3	Architecture d'un réseau de capteur sans fil.	10
1.4	Les standards IEEE 802 mettant l'accent sur les normes IEEE 802.15.	14
2.1	Exemple de topologies en étoile et point à point.	18
2.2	Représentation d'une supertrame IEEE 802.15.4.	22
2.3	Fonctionnement du protocole CSMA/CA slotté.	23
2.4	Fonctionnement du protocole Aloha slotté.	25
3.1	Graphe de transition de la Chaîne de Markov du mécanisme IEEE 802.15.4 S-Aloha	33
3.2	Fiabilité Vs Taille du réseau, avec $L_p = 100$ bytes.	39
3.3	Fiabilité Vs Taille du réseau & variant la Taille des paquets L_p	39
3.4	Énergie Vs Taille du réseau, avec $L_p = 100$ bytes.	40
3.5	Énergie Vs Taille du réseau & variant la Taille des paquets L_p	40
3.6	Débit Vs Taille du réseau, avec $L_p = 100$ bytes.	41
3.7	Débit Vs Taille du réseau & variant la Taille des paquets L_p	41
3.8	Délai Vs Taille du réseau, avec $L_p = 100$ bytes.	42
3.9	Délai Vs Taille du réseau & variant la Taille des paquets L_p	42
4.1	Graphe de transition de la Chaîne de Markov du mécanisme IEEE 802.15.4 CSMA/CA	46
4.2	Fiabilité Vs Taille du réseau, avec $L_p = 100$ bytes	54
4.3	Fiabilité Vs Taille du réseau & variant la Taille des paquets L_p	55
4.4	Énergie Vs Taille du réseau, avec $L_p = 100$ bytes.	55
4.5	Énergie Vs Taille du réseau & variant la taille des paquets L_p	56
4.6	Débit Vs Taille du réseau, avec $L_p = 100$ bytes.	57
4.7	Débit Vs Taille du réseau & variant la taille du paquet L_p	57
4.8	Délai Vs Taille du réseau, avec $L_p = 100$ bytes.	58

4.9 Délai Vs Taille du réseau & variant la Taille des paquets L_p 58

Liste des tableaux

2.1	Comparaison entre les standards IEEE 802.15.4	27
3.1	Paramètres du modèle IEEE 802.15.4 Aloha slotté	31
3.2	Probabilités du modèle IEEE 802.15.4 S-ALOHA slotté	31
3.3	Paramètres utilisés pour l'évaluation des performances de IEEE 802.15.4 S-Aloha .	38
4.1	Paramètres du modèle IEEE 802.15.4 CSMA/CA slotté	45
4.2	Probabilités du modèle IEEE 802.15.4 CSMA/CA slotté	45
4.3	Paramètres utilisés pour l'évaluation des performances de CSMA/CA slotté	54

Notations et Abréviations

ACK	Acknowledgement
ASK	Amplitude Shift Keying
BE	Backoff Exponent
BI	Beacon Interval
BPSK	Binary Phase-Shift Keying
CAP	Contention Access Period
CCA	Clear Channel Assessment
CFP	Contention Free Period
CSMA/CA	Carrier Sence Multiple Access with Collision Avoidance
CW	Contention Window
DSME	Deterministic and Synchronous Multi-channel Extension
DSSS	Direct Sequence Spread Spectrum
ED	Energy Detection
FFD	Full Function Device
GMSK	Gaussian Minimum Shift Keying
GPRS	General Packet Radio Services
GTS	Guranteed Time Slot
IEEE	Institut of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IFS	Inter Frame Space
ISO	International Organization for Standardization
LAN	Local Area Network
LIFS	Long Inter Frame Space
LLC	Logical Link Control
LLDN	Low Latency Deterministic Network
LQI	Link Quality Indication
LR-WPAN	Low Rate Wireless Personal Area Network

MAC	Medium Access Control
NB	Number of Backoffs
O-QPSK	Offset Quadrature Phase-Shift Keying
OSI	Open System Interconnection
PAN	Personal Area Network
PDA	Personnal Digital Assistant
PHY	Physical Layer
PSSS	Parallel Sequence Spread Spectrum
RCSF	Réseau de Capteurs Sans Fil
RFD	Reduced Function Device
SIFS	Short Inter Frame Slot
TSCH	Time Slotted Channel Hopping
UMTS	Universal Mobile Telecommunications System
UWB	Ultra Wide Band
WBAN	Wireless Body Area Network
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WPAN	Wireless Personal Area Network
WWAN	Wireless Wide Area Network

Introduction générale

Les avancées technologiques et techniques opérées dans le domaine des réseaux sans fil, de la micro-fabrication et de l'intégration des microprocesseurs ont fait naître une nouvelle génération de réseaux de capteurs à grande échelle adaptés à une gamme d'applications très variée. Ce domaine est considéré comme l'une des technologies contemporaines les plus prometteuses, il s'est créé pour offrir des solutions économiquement intéressantes et faciles à déployer pour la surveillance à distance et au traitement des données dans les environnements complexes et distribués. Cette nouvelle technologie permet de révolutionner notre façon de vivre, de travailler et d'interagir avec l'environnement physique qui nous entoure. En terme de domaines d'applications, les réseaux de capteurs ont connu un très grand succès, car ils détiennent un potentiel qui révolutionne de nombreux secteurs de notre économie et notre vie quotidienne de la surveillance et la préservation de l'environnement, à la fabrication industrielle. Tout en passant par l'automatisation dans les secteurs de transport et de la santé, la modernisation de la médecine, de l'agriculture, de la télématique et de la logistique.

Ces dernières années, une grande diversité de standards de communication suit l'évolution technologique. Ainsi, dans le but d'être en phase à l'égard de ces progrès, l'organisme IEEE (Institute of Electrical and Electronics Engineers) a été fondé en 1980. Il a eu comme tâche de standardiser les couches basses des réseaux locaux et métropolitains par le biais de liaisons filaires ou sans fil. Ce groupe a produit des normes incontournables, telles que, la norme 802.11, la norme 802.3 et les normes 802.15.1, 802.15.3 et 802.15.4. Cette dernière représente le meilleur compromis pour les réseaux de capteurs sans fil.

Dans ce mémoire, nous nous sommes intéressées à étudier en profondeur le standard IEEE 802.15.4 et plus exactement la couche MAC (Medium Access Control) proposée dans ce dernier. D'importants efforts doivent être faits dans les couches basses du modèle OSI (Open System Interconnection), car sans une couche physique et une couche MAC fiables, toutes les optimisations proposées pour les couches supérieures resteront vaines.

La modélisation analytique par chaîne de Markov et l'analyse des performances de la norme IEEE 802.15.4 a été le sujet de recherche de plusieurs articles publiés dans la littérature. Les modèles

s'inspirent principalement des modèles de la norme IEEE 802.11. BIANCHI a proposé un modèle analytique du protocole IEEE 802.11 [1] qui est considéré comme un modèle de référence à base duquel se sont construits la plupart des modèles qui existent dans la littérature. Dans [2], les auteurs élargissent le modèle de Bianchi et calculent le débit et la consommation d'énergie dans les conditions de saturation du trafic. Les auteurs dans [3] proposent un modèle de chaîne de Markov à deux dimensions dans des conditions de trafic non saturé pour le mécanisme CSMA/CA (Carrier Sence Multiple Access with Collision Avoidance) slotté du protocole IEEE 802.15.4. En calculant la probabilité de distribution stationnaire de la chaîne de Markov, ils obtiennent des formules mathématiques pour le débit et la consommation d'énergie. Dans [4], les auteurs ont étudié la stabilité du débit, le délai moyen de la file d'attente ainsi que la problématique d'énergie de la couche MAC du protocole IEEE 802.15.4.

Il existe donc un grand nombre de modèles analytiques pour analyser les mécanismes d'accès du protocole IEEE 802.15.4. Dans ce mémoire, nous allons nous intéresser à l'analyse de performances des mécanismes MAC offerts par la norme IEEE 802.15.4, dédiés aux réseaux de capteurs sans fil. L'évaluation de performance de cette norme nous permettra d'illustrer de manière quantitative un ensemble de métriques de performances, tel que, le débit, le délai, la fiabilité et l'énergie consommée. L'évaluation de performances peut être réalisée en utilisant une modélisation analytique qui a pour avantage d'offrir un temps de calcul faible et demande moins de développement informatique. De plus, les résultats sont plus proches de la réalité. L'intérêt de l'application des méthodes analytiques est qu'elles permettent de bien comprendre quelles sont les lois internes de fonctionnement du système.

Le modèle analytique par chaîne de Markov que nous proposons pour le mécanisme ALOHA slotté de la norme IEEE 802.15.4 est le premier dans la littérature tout en considérant un mode beacon, un trafic saturé et un canal idéal. Notre 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.

Organisation du mémoire

Le manuscrit est organisé en une introduction, deux parties découpées en quatre chapitres et une conclusion. La première partie nommée "État de l'art " englobe les deux premiers chapitres à savoir " Les Réseaux de Capteurs Sans Fil (RCSFs)" et "Le standard IEEE 802.15.4", où :

- Dans le chapitre 1, nous présenterons des généralités sur les réseaux de capteurs sans fil, leurs caractéristiques et domaines d'application.
- Dans le chapitre 2, nous décrirons la norme IEEE 802.15.4, ses modes de fonctionnement et ses mécanismes d'accès. Nous discuterons par la suite ses limites et son évolution au fil de temps.

La deuxième partie de ce travail regroupe nos contributions. Elle contient les deux derniers chapitres.

- Le chapitre 3 sera consacré à la proposition d'un modèle analytique pour le mécanisme Aloha slotté de la norme IEEE 802.15.4. Nous y présentons notre modèle de chaîne de Markov à trois dimensions est capable d'estimer la fiabilité, le débit, le délai et l'énergie consommée. Par la suite, nous allons montrer la variation du nombre de nœuds et de la taille des paquets afin d'estimer leur impact sur les performances du réseau.
- Le dernier chapitre se focalisera sur la modélisation et l'évaluation des performances du protocole MAC CSMA/CA de la norme IEEE 802.15.4 dans le mode beacon. Dans cette partie, on y trouvera la chaîne de Markov correspondante au modèle, sa résolution et les résultats obtenus en termes de fiabilité, d'énergie consommée, de débit de données et de délai moyen ; suivis d'une interprétation et d'une comparaison entre les résultats des deux mécanismes Aloha et CSMA/CA.

Enfin, notre rapport 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

1.1 Introduction

Avec les progrès récents des technologies de communication sans fil et de l'électronique numérique, la conception et le développement d'un nœud capteur multifonction à faible coût de petite taille et à faible consommation d'énergie, est devenu faisable. Sur la base des efforts conjoints d'un grand nombre de nœuds de capteurs, ces minuscules nœuds capteurs offrent de multiples fonctions notamment la détection, le traitement de données et la communication pour permettre la réalisation d'un Réseau de Capteurs Sans Fil (RCSF). Les RCSFs ont un large éventail d'applications et deviennent progressivement un élément indispensable de nos vies. Dans ce chapitre, nous présenterons dans un premier temps les réseaux sans fil ainsi que leurs catégories. Par la suite, nous enchaînerons par une présentation détaillée des RCSFs, leur architecture, leurs caractéristiques ainsi que leurs domaines d'application.

1.2 Les réseaux sans fil

Un réseau sans fil permet la communication à distance et l'accès aux applications ou aux informations sans avoir besoin d'une connexion filaire. Par conséquent, les utilisateurs bénéficient d'une véritable mobilité et d'un meilleur accès aux services et applications du réseau [5]. La communication sans fil n'est pas une idée nouvelle. Dans les temps anciens, les peuples autochtones qui utilisaient des signaux de fumée et des navires qui communiquaient via le code Morse et des signaux lumineux avaient déjà pratiqué cette opération. Cependant, en raison de l'avancement de la technologie des télécommunications, l'enthousiasme pour ce mode de communication n'a atteint cette proportion que ces dernières années. Les réseaux sans fil se déclinent en plusieurs catégories selon la distance qu'ils couvrent [6] (voir la figure 1.1).

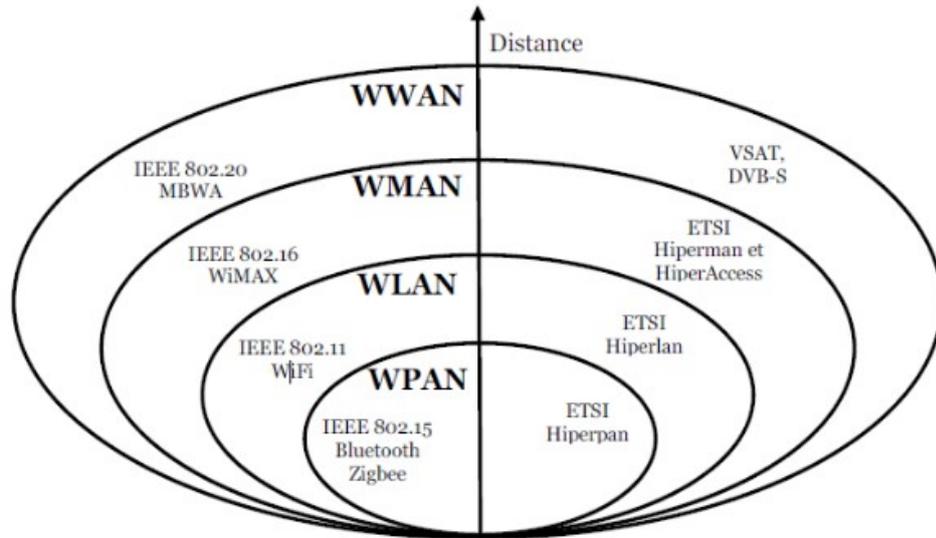


FIGURE 1.1 – Classification des réseaux sans fil selon la zone de couverture.

1.2.1 Les réseaux personnels sans fil (WPAN)

Le réseau personnel sans fil (appelé également réseau individuel sans fil ou réseau domestique sans fil), noté WPAN (Wireless Personal Area Network) concerne les réseaux sans fil d'une faible portée (de l'ordre de quelques dizaines mètres). Ce type de réseau sert généralement à relier des périphériques (imprimante, téléphone portable, appareils domestiques, ...) ou un assistant personnel (PDA) à un ordinateur sans liaison filaire ou bien à permettre la liaison sans fil entre deux machines très peu distantes. Il existe plusieurs technologies utilisées pour les WPAN :

- **HomeRF** (Home Radio Frequency), lancée en 1998 par le HomeRF Working Group (formé notamment par les constructeurs Compaq, HP, Intel, Siemens, Motorola et Microsoft) propose un débit théorique de 10 *Mbps* avec une portée d'environ 50 à 100 mètres sans amplificateur. La norme HomeRF soutenue notamment par Intel, a été abandonnée en Janvier 2003, notamment car les fondeurs de processeurs misent désormais sur les technologies WiFi (Wireless Fidelity) embarquée (via la technologie Centrino, embarquant au sein d'un même composant un microprocesseur et un adaptateur Wi-Fi) [6].
- **ZIGBEE**. La technologie ZigBee (aussi connue sous le nom IEEE 802.15.4) permet d'obtenir des liaisons sans fil à très bas prix et avec une très faible consommation d'énergie, ce qui la rend particulièrement adaptée pour être directement intégrée dans de petits appareils électroniques (appareils électroménagers, hifi, jouets, ...). La technologie Zigbee, opérant sur la bande de fréquences des 2,4 *GHz* et sur 16 canaux, permet d'obtenir des débits pouvant

atteindre 250 *Kb/s* avec une portée maximale de 100 mètres environ [6].

1.2.2 Les réseaux locaux sans fil (WLAN)

Le réseau local sans fil, noté WLAN (Wireless Local Area Network) est un réseau permettant de couvrir l'équivalent d'un réseau local d'entreprise, soit une portée d'environ une centaine de mètres. Il permet de relier entre-eux les terminaux présents dans la zone de couverture. Il existe plusieurs technologies concurrentes :

- **Wi-Fi** (Wireless Fidelity), soutenu par l'alliance WECA (Wireless Ethernet Compatibility Alliance) offre des débits allant jusqu'à 54 *Mbps* sur une distance de plusieurs centaines de mètres [6].
- **HiperLAN2** (HIGH PERFORMANCE Radio LAN 2.0) est une norme européenne élaborée par l'ETSI (European Telecommunications Standards Institute). HiperLAN 2 permet d'obtenir un débit théorique de 54 *Mbps* sur une zone d'une centaine de mètres dans la gamme de fréquence comprise entre 5150 et 5300 *Mhz* [6].

1.2.3 Les réseaux métropolitains sans fil (WMAN)

Le réseau métropolitain sans fil WMAN (Wireless Metropolitan Area Network) est connu sous le nom de Boucle Locale Radio (BLR). Les WMANs sont basés sur la norme IEEE 802.16. La boucle locale radio offre un débit utile de 1 à 10 *Mb/s* pour une portée de 4 à 10 kilomètres, ce qui destine principalement cette technologie aux opérateurs de télécommunication [6].

1.2.4 Les réseaux étendus (WWAN)

Le réseau étendu sans fil WWAN (Wireless Wide Area Network) est également connu sous le nom de réseau cellulaire mobile. Il s'agit des réseaux sans fil les plus répandus puisque tous les téléphones mobiles sont connectés à un réseau étendu sans fil. Les principales technologies permettant la mise en œuvre des réseaux WWANs sont les suivantes :

- **GSM (Global System for Mobile Communication)** ou en français Groupe Spécial Mobile,
- **GPRS (General Packet Radio Service),**
- **UMTS (Universal Mobile Telecommunication System).**

1.3 Réseaux de capteurs sans fil (RCSFs)

Un réseau de capteurs sans fil est un type spécial de réseaux ad hoc avec un grand nombre de nœuds qui sont des micro-capteurs capables de recevoir et de transmettre des données environnementales d'une manière autonome sans intervention humaine. La position de ces nœuds n'est pas obligatoirement prédéterminée, ils peuvent être aléatoirement dispersés dans une zone géographique appelée « champ de captage » correspondant au terrain d'intérêt pour le phénomène capté. Par exemple : lâchée de capteurs sur un volcan pour étudier les phénomènes volcanologiques et leurs évolutions.

Le réseau possède en général un nœud particulier, la station de base (ou sink), connectée avec les autres nœuds par un réseau filaire et est reliée à une alimentation électrique [7].

1.3.1 Architecture d'un nœud capteur

Un nœud capteur est principalement composé de quatre unités de base : l'unité de détection (ou la sonde), l'unité de traitement, l'unité de transmission et l'unité de contrôle d'énergie. Il peut contenir également, suivant son domaine d'application, des modules supplémentaires tels qu'un système de localisation (GPS ou un autre système de localisation qui donne au capteur sa position), un système générateur d'énergie (cellule solaire ou photovoltaïque), ou bien un système de mesure de distance ou d'angle avec un nœud capteur voisin. On rencontre aussi des capteurs plus volumineux, dotés d'un système mobilisateur chargé de déplacer le capteur en cas de nécessité. Le rôle de chaque unité est présenté ci-dessous [7] :

- **Unité de détection** : est un dispositif transformant l'état d'une grandeur physique observée (exemple une intensité lumineuse ou encore une température) en une grandeur utilisable. Elle se distingue de l'instrument de mesure par le fait qu'il ne s'agit que d'une simple interface entre un processus physique et une information manipulable.
- **Unité de traitement** : elle comprend un microcontrôleur assurant le traitement des données et son stockage et une mémoire flash. Ce microcontrôleur contrôle les procédures permettant au nœud de collaborer avec les autres nœuds pour effectuer les tâches d'acquisition attribuées.
- **Unité de transmission** : elle permet de connecter le nœud au réseau. Elle est chargée d'effectuer toutes les émissions et réceptions des données sur un médium sans fil.
- **Unité de contrôle d'énergie** : 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.

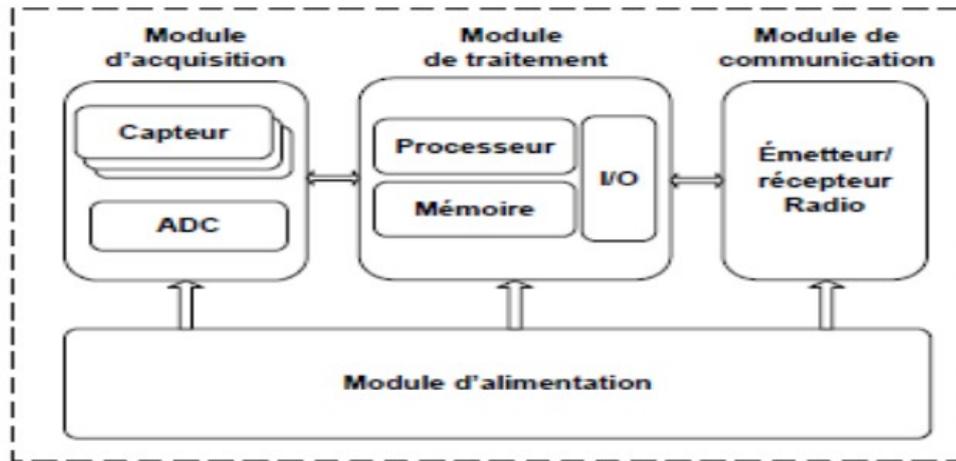


FIGURE 1.2 – Architecture d'un nœud capteur.

1.3.2 Architecture d'un RCSF et ses caractéristiques

Un réseau de capteurs est constitué essentiellement de plusieurs nœuds capteurs, un nœud sink (ou station de base) et un centre de traitement des données [8].

- **Les nœuds capteurs.** Les nœuds sont des capteurs, leur type, leur architecture et leur disposition géographique dépendent de l'exigence de l'application en question. Leur énergie est souvent limitée puisqu'ils sont alimentés par des piles.
- **Le sink :** est un nœud particulier du réseau. Il est chargé de la collecte des données issues des différents nœuds du réseau. Il doit être toujours actif puisque l'arrivée des informations est aléatoire. C'est pourquoi son énergie doit être illimitée. Dans un réseau de capteur sans fil plus ou moins large et à charge un peu élevée, on peut trouver deux sinks ou plus pour alléger la charge.
- **Centre de traitement des données :** est le centre vers lequel les données collectées par le sink sont envoyées. Ce centre a pour rôle de regrouper les données issues des nœuds et de les traiter de façon à en extraire l'information utile exploitable. Le centre de traitement peut être éloigné du sink [8], de sorte que les données doivent être transférées à travers un autre réseau. D'où la nécessité d'introduire une passerelle entre le sink et le réseau de transfert afin d'adapter le type de données au type du canal.

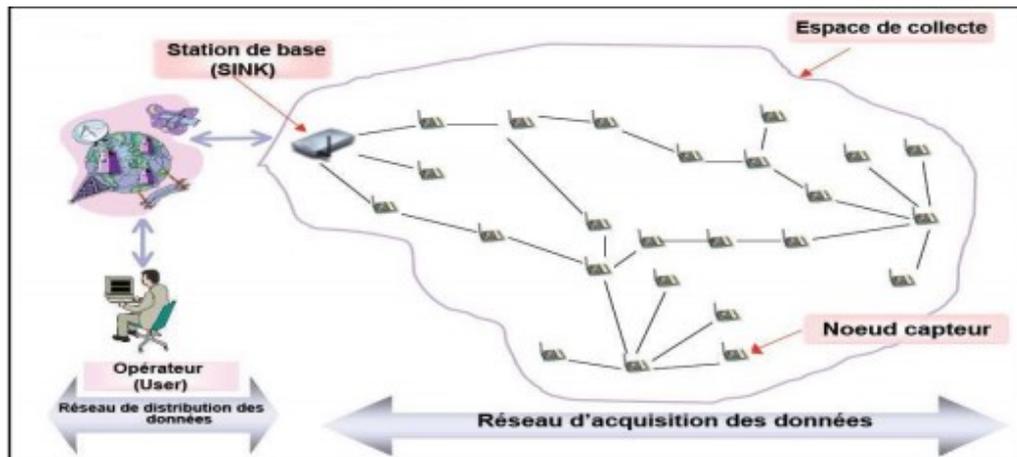


FIGURE 1.3 – Architecture d'un réseau de capteur sans fil.

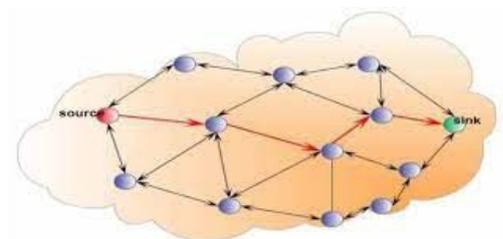
Comme le montre la figure 1.3, un RCSF est composé d'un grand nombre de nœuds capteurs éparpillés sur le champ de captage. Quand le sink diffuse une requête, les nœuds collaborent entre eux pour lui envoyer les informations captées à travers une architecture multi-sauts. Le sink transmet ensuite ces données par Internet ou par satellite au gestionnaire de tâches pour les analyser et prendre des décisions. A un niveau plus élevé, un RCSF peut être vu comme étant une combinaison de deux entités de réseau :

- **Le réseau d'acquisition des données** : représente l'union des nœuds capteurs et du sink. Son rôle consiste à collecter les données à partir de l'environnement et de les rassembler au sink.
- **Le réseau de distribution des données** : son rôle est de connecter le réseau d'acquisition des données à un utilisateur.

Il existe deux types d'architecture des RCSFs [9] :

✧ **Les réseaux de capteurs sans fil plats.**

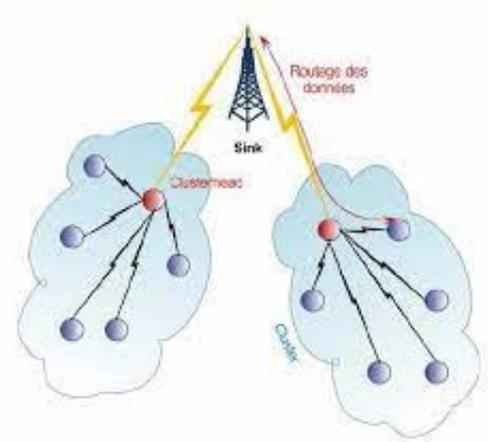
Un réseau de capteurs sans fil plat est un réseau homogène, où tous les nœuds disposent des mêmes capacités et fonctionnalités concernant le captage, la communication et la complexité du matériel. Seul le sink échappe à cette règle vu qu'il joue le rôle d'une passerelle chargée de la collecte des données issues des différents nœuds capteurs pour les transmettre à l'utilisateur [9].



Architecture plate.

❖ **Les réseaux de capteurs hiérarchiques.**

Un réseau de capteur hiérarchique est un réseau hétérogène où les nœuds ont des capacités différentes, par exemple certains nœuds peuvent disposer d'une source d'énergie plus importante, une plus longue portée de communication et/ou une plus grande puissance de calcul. Ceci permet de décharger la majorité des nœuds simples à faible coût de plusieurs fonctions du réseau [9].



Architecture hiérarchique.

- **La consommation réduite d'énergie.** Les nœuds capteurs utilisent des batteries de taille minuscule comme ressources en énergie, ce qui limite leur durée de vie. La spécificité des applications des RCSFs (militaires, sismiques et autres) fait que la recharge ou le remplacement de ces batteries est une tâche difficile ou presque impossible, ce qui nous permet de déduire que la durée de vie d'un nœud est essentiellement dépendante de la durée de vie de la batterie. Ainsi, la méthode de gestion de consommation d'énergie constitue une contrainte majeure dans ce type de réseau [10].
- **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 [7].
- **Scalabilité ou passage à l'échelle.** Contrairement aux réseaux sans fil traditionnels (personnels, locaux ou étendus), un RCSF peut contenir un très grand nombre de nœuds capteurs (des centaines, des milliers,...). Un réseau de capteur est scalable parce qu'il a la faculté d'accepter un très grand nombre de nœuds qui collaborent ensemble afin d'atteindre un objectif commun [7].
- **La tolérance aux pannes :** 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 d'interférences environnementales, ce qui conduira à la défaillance du nœud capteur [7].
- **Dynamique du réseau.** La mobilité des nœuds de capteurs ou de la station de base est im-

portante dans un réseau. Les nœuds capteurs étant dynamiques, c'est à dire itinérants, de nombreuse se pose quant à la stabilité du l'acheminement de l'énergie et de la bande passante, etc.

1.3.3 Avantages et inconvénients des RCSFs

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

1.3.4 Domaines d'application des RCSFs

La diminution de taille et de coût des micro-capteurs, l'élargissement de la gamme des types de capteurs disponibles (thermique, optique, vibrations. . .) et l'évolution des supports de communication sans fil, ont élargi le champ d'application des réseaux de capteurs. Ils s'insèrent notamment dans d'autres systèmes tels que le contrôle et l'automatisation des chaînes de montage. Ils permettent de collecter et de traiter des informations complexes provenant de l'environnement (météorologie,

étude des courants, de l'acidification des océans, de la dispersion de polluants, de propagules, etc) [11].

Dans le domaine militaire, les RCSFs sont par exemple utilisés pour détecter les intrusions ou les attaques et pour surveiller les champs de bataille [11].

Dans le domaine agricole, les réseaux de capteurs surveillent des données liées à la météo, à la surveillance des cultures, notamment les maladies, l'humidité, la pollution, etc [11].

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 [11].

Dans le domaine de transport, notamment le transport routier, les réseaux de capteurs pourraient diffuser des informations de portée locale sur les conditions de circulation, les alertes, et permettre d'améliorer la sécurité [12].

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.

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.

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.

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

1.3.5 Standardisation

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 [11].

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 LLC (Logical Link Control) et MAC (Media Access Control). La figure 1.4 illustre les six groupes du comité travaillant sur différents thèmes pour différents types de réseaux [13].

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 supérieures du modèle OSI.

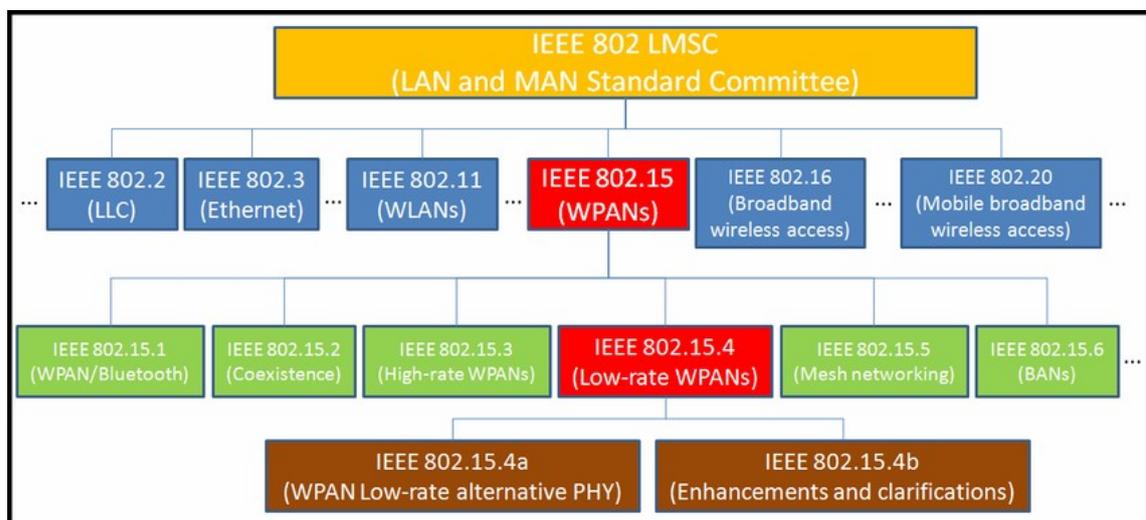


FIGURE 1.4 – Les standards IEEE 802 mettant l'accent sur les normes IEEE 802.15.

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 Conclusion

Dans ce premier chapitre, nous avons tout d'abord présenté les réseaux sans fil en général et les réseaux de capteurs sans fil en particulier. Dans un second lieu, nous avons dressé les caractéristiques des réseaux de capteurs sans fil, son architecture et ses domaines d'applications. Nous avons, par la suite, spécifié les avantages et les inconvénients de ce type de réseau. Finalement, nous avons présenté la technologie IEE 802.15.4 qui est une solution idéale pour la mise en œuvre des RCSFs avec une faible consommation d'énergie et une faible latence.

Le chapitre suivant sera consacré à la présentation détaillée de cette technologie sans fil, tout en considérant son architecture, son principe de fonctionnement et enfin son évolution au fil du temps.

Chapitre 2

Le standard IEEE 802.15.4

2.1 Introduction

Le monde des réseaux et de l'internet compte deux organismes de standardisations très influents : L'IEEE et L'IETF (Internet Engineering Task Force). Ces deux organismes ont tous deux comme objectif de standardiser les couches basses du modèle OSI pour l'IEEE (physique et MAC) et les couches hautes pour l'IETF (réseau, transport, etc.). Avec l'apparition des réseaux personnels WPAN, les contraintes et les besoins sont changés, le principal but n'est plus d'atteindre des débits toujours plus élevés mais de maximiser la durée de vie des réseaux. De ce fait, les standards 802.15.1 et 802.15.3 ne peuvent pas être utilisées pour les réseaux LR-WPANs (Low Rate Wireless Personal Area Networks). Le standard IEEE 802.15.4 a été proposé pour cette raison. Cette norme ne traite que des deux premières couches du modèle OSI dans les réseaux LR-WPANs. Ces réseaux sont caractérisés par un faible débit et une faible consommation énergétique [14]. Dans ce chapitre, nous présentons en détail le standard IEEE 802.15.4, où nous aborderons les spécificités des deux couches : physique et MAC, ainsi que les concepts relatifs aux fonctionnements de ces derniers. Par la suite, nous discuterons sur les limites de ce standard ainsi que son évolution au fil du temps.

2.2 Le standard IEEE 802.15.4

2.2.1 Définition

La technologie sans fil IEEE 802.15.4 initiale a été créée en 2003. Elle représente un système de communication à courte portée destiné aux applications de réseaux personnels sans fil (WPAN) à bas débit. Cette norme convient très bien aux besoins des réseaux de capteurs sans fil en termes de bas débit, de faible consommation énergétique et de faible coût des entités du réseau.

2.2.2 Types de périphériques IEEE 802.15.4

Il existe deux types de périphériques (appelés aussi dispositifs ou appareils) dans un réseau IEEE 802.15.4 : les appareils à fonctions complètes FFD (Full-Function Device) et les appareils à fonctions réduites RFD (Reduced-Function Device) [7] :

- Un appareil FFD est capable d'exécuter toutes les tâches décrites dans la norme IEEE 802.15.4. Il peut accepter n'importe quel rôle dans le réseau et peut assumer trois rôles différents dans un réseau de capteurs sans fil, à savoir : coordinateur PAN, routeur ou simple capteur.
- Un appareil RFD a des capacités limitées. Sa puissance de traitement et la taille de sa mémoire sont inférieures à celle des appareils FFD. En revanche, ils sont destinés à des applications très simples.

2.2.3 Protocoles basés sur la norme IEEE 802.15.4

- ZigBee : est un protocole de haut niveau, de faible coût et à faible consommation d'énergie destiné pour les réseaux de capteurs sans fil. Cette technologie a pour but la communication à courtes distances [15].
- Wireless HART : est un protocole de communication développé par la Fondation des communications HART, utilisé en contrôle industriel pour communiquer numériquement avec des capteurs. Ce standard utilise les couches inférieures de la norme IEEE 802.15.4 et assure la synchronisation, la sécurité et la confidentialité des communications grâce au chiffrement et à l'authentification [11].

2.2.4 Topologies du réseau

Le standard IEEE 802.15.4 supporte deux types de topologies : la topologie en étoile et la topologie point à point (peer-to-peer) [16].

- 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.

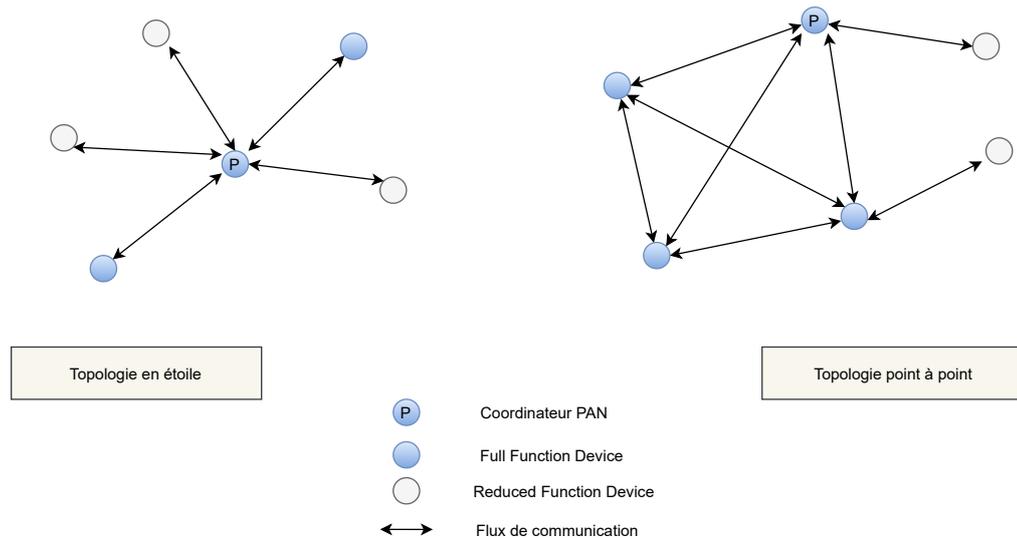


FIGURE 2.1 – Exemple de topologies en étoile et point à point.

2.2.5 Architecture en couche du réseau IEEE 802.15.4

L'architecture de la norme IEEE 802.15.4 est définie en termes d'un certain nombre de couches du modèle à sept couches de l'OSI (Open System Interconnection). 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.

2.2.5.1 La couche physique de IEEE 802.15.4

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 [17] :

- ✧ **Gestion de l'activation et désactivation du module radio.** La radio pourra prendre trois états différents : 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.** Le ED (Energy Detection) mesure l'énergie dans le canal.
- ✧ **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 médium.** 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 parmi les différents canaux disponible.** 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. Le standard IEEE 802.15.4 propose quatre différentes couches physiques exploitant chacune des techniques de modulation, comme présenté ci-dessous :
- ✧ 868/915 MHz utilisant DSSS (Direct Sequence Spread Spectrum).
- ✧ 868/915 MHz utilisant aussi la technique d'étalement de spectre DSSS mais combinée avec une modulation O-QPSK (Offset Quadrature Phase-Shift Keying).
- ✧ 868/915 MHz utilisant la technique de l'étalement de spectre PSSS (Parallel Sequence Spread Spectrum) et combinant les deux techniques de modulation BPSK et ASK (Amplitude Shift Keying).
- ✧ 2450 MHz utilisant DSSS pour l'étalement de spectre et la O-QPSK comme modulation.

Le standard offre 27 canaux de communication selon le choix de la bande de fréquence et de la couche physique.

2.2.5.2 La Sous-couche MAC dans IEEE 802.15.4

La sous-couche MAC (Medium Acces Control) 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 [17] :

- **La synchronisation avec le coordinateur** : le coordinateur PAN envoie périodiquement des trames balises pour synchroniser les membres de son réseau.
- **La création du réseau** : la couche supérieure envoie une requête à la couche MAC afin 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 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.

- **La génération des trames balises** : 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.

a) 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 [14] :

- Les trames Beacon : sont envoyées uniquement par les nœuds coordinateurs, afin d'administrer le réseau.
- Les trames de données : servent à transférer des données utiles entre les nœuds du réseau.
- Les trames d'acquiescement : servent à confirmer la bonne réception des trames de données.
- Les trames de contrôle : servent à effectuer des demandes spécifiques.

b) Les Modes de fonctionnement dans IEEE 802.15.4

Le standard IEEE 802.15.4 offre deux modes de fonctionnement [14] :

- **Le mode non balisé.** Dans ce mode il y a absence de synchronisation entre les nœuds du réseau. Afin 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. Dans ce mode, les mécanismes utilisés pour se protéger des collisions sont le CSMA/CA non slotté et le Aloha non slotté.
- **Le mode balisé.** Dans ce mode les mécanismes utilisés sont le CSMA/CA slotté et le Aloha slotté, il est le mode le plus important dans le standard vu qu'il est performant en terme de débit, de consommation énergétique et de fiabilité. Ce mode est un mode dit synchronisé. Les nœuds doivent suivre une structure périodique appelée supertrame. Cette structure périodique commence toujours par l'envoi d'une trame par le coordinateur appelée trame Beacon. Cette trame Beacon a pour rôle de synchroniser les nœuds avec leur coordinateur, et fournir toutes les informations sur le fonctionnement du réseau.

c) Le transfert de données dans IEEE 802.15.4

Le standard définit trois modes de transfert de données à savoir [14] :

- Transmission de données des fils vers le coordinateur (transmission directe) : les données sont envoyées de la part des fils vers leur coordinateur. Ce mode est utilisé dans la topologie en étoile ;
- Transmission de données du coordinateur vers ses fils (transmission indirecte) : les données sont envoyées par le coordinateur vers ses fils. Ce mode de transmission est aussi utilisé dans la topologie en étoile ;
- Transmission de données : si le réseau est un réseau de type point-à-point les nœuds communiquent entre eux en utilisant le CSMA/CA et Aloha.

d) La structure de la supertrame

La supertrame est une structure temporelle périodique, divisée en unités de temps élémentaires de 20 *symboles* appelées périodes backoff notés *aUnitbackoff period* . La taille de la supertrame est modifiable, en d'autre terme la taille de la supertrame n'est pas fixée à l'avance et selon le choix de certains paramètres on pourra modifier sa taille. Quelque soit sa longueur, elle est divisée en 16 slots de taille identique. Ces slots temporels sont composés d'un certain nombre de périodes backoff. La supertrame revient périodiquement pour fournir un mécanisme de synchronisation aux nœuds qui doivent rendre la radio éteinte pour réduire le coût de consommation d'énergie. La supertrame se compose des trois parties suivantes (voir la figure 2.2) :

- Une trame Beacon (Balise).
- Une partie active où les nœuds peuvent avoir la radio allumée. La partie active de la supertrame est divisée en deux sous-parties :
 - ✧ La partie CAP (Contention Access Period) où les nœuds communiquent avec leur coordinateur en utilisant les protocoles CSMA/CA slotté et Aloha slotté.
 - ✧ La partie CFP (Contention Free Period) est une partie optionnelle de la supertrame où un nœud peut demander l'attribution exclusive des slots appelés GTS (Guranteed Time Slot).
- Une partie inactive où les nœuds devront éteindre leur radio pour faire des économies d'énergie. A chaque réception d'une balise, tous les nœuds sont informés de la durée de la supertrame. La transmission régulière des balises permet d'informer l'ensemble des dispositifs sur les changements pouvant se produire dans la supertrame.

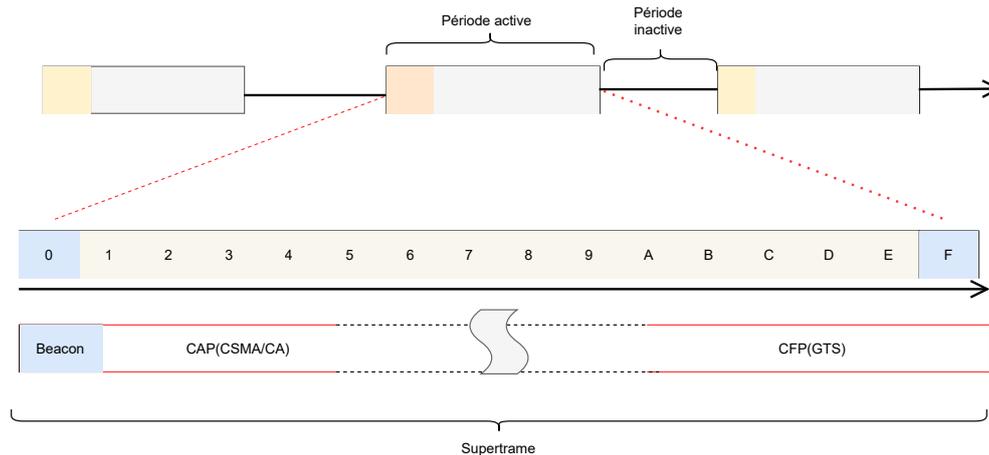


FIGURE 2.2 – Représentation d'une supertrame IEEE 802.15.4.

2.2.6 Mécanismes d'accès au canal

2.2.6.1 Protocole CSMA/CA

Le protocole CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) a pour principe de désynchroniser le temps d'envoi des trames des différents nœuds en utilisant un tirage d'un temps aléatoire dans un intervalle conditionné par le BE (Backoff Exponent). Après ce temps d'attente, les nœuds doivent vérifier l'état du canal avant de transmettre. Avant d'entamer la description du fonctionnement du CSMA/CA nous devons tout d'abord définir la terminologie utilisée dans le standard IEEE 802.15.4 [16] :

- *aUnitBackoffPeriod* : unité de temps égale à 20 *symboles*.
- *BE* (Backoff Exponent) : initialisé à $MacMinBE = 3$.
- *Backoff* : temps d'attente aléatoire tiré dans l'intervalle $[0, 2^{BE} - 1]$.
- *CW* (Contention Window) : représente le nombre d'unités de temps après le temps Backoff où le canal doit être libre avant la transmission.
- *macMaxCSMABackoffs* : le nombre de fois où le canal est trouvé occupé avant d'abandonner l'émission de la trame, initialisé à 3.
- *macMaxFrameRetries* : le nombre de retransmissions maximum autorisé pour chaque trame, initialisé à 4.

Avant tout essai de transmission d'une nouvelle trame en utilisant le mécanisme CSMA/CA slotté, les nœuds doivent passer par ces étapes :

1. Initialisation des paramètres (*CW*, *NB*, *BE*) à leur valeur par défaut.

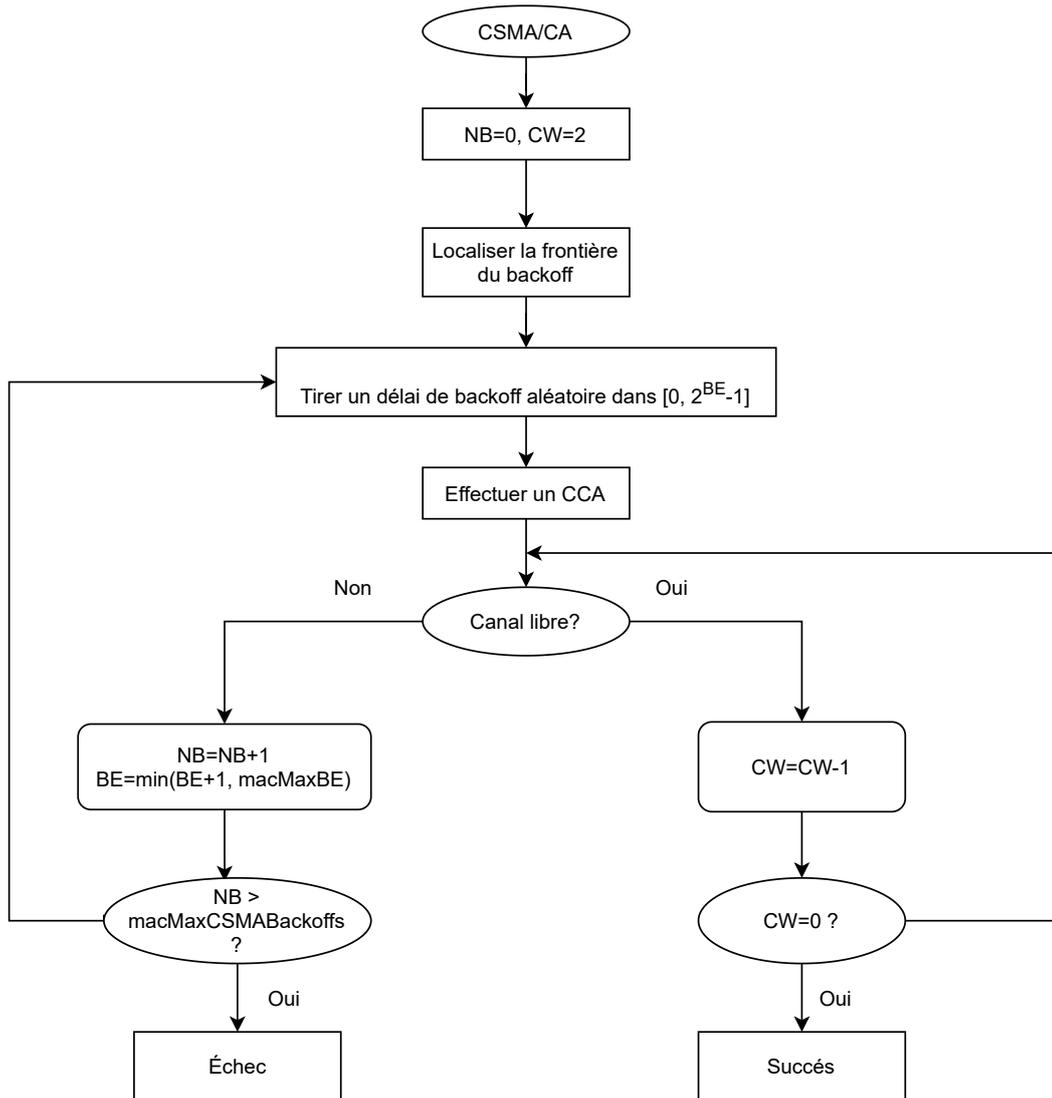


FIGURE 2.3 – Fonctionnement du protocole CSMA/CA slotté.

2. Tirage d'un temps aléatoire (*Backoff*) pour désynchroniser les transmissions.
3. Tous les nœuds doivent s'assurer qu'il reste assez de temps avant la fin de la supertrame pour le Backoff, les deux CW , l'envoi de la trame, et l'acquittement (si ce dernier est demandé).
4. A la fin du temps d'attente aléatoire (*Backoff*) les nœuds doivent tester l'état du canal en effectuant un *CCA* (Clear Channel Assessment) qui dure 8 *Symboles* de temps :
 - Si le canal est occupé, le nœud incrémente les paramètres CW , NB , BE comme suit : $NB = NB + 1$, $BE = \min(BE + 1, macMaxBE)$ et $CW = 2$.
 - Si $NB > macMaxCSMABackoffs$ (ie, le nombre maximum pour transmettre une trame est dépassé), le nœud abandonne l'envoi de la trame en cours. Dans le cas contraire le nœud tire un nouveau Backoff pour renvoyer la trame (retourner à l'étape2).

- Si au contraire le canal est détecté libre, le nœud décrémente la valeur de CW ($CW = CW - 1$). Si $CW = 0$, la trame est envoyée au début du prochain $aUnitBackoffPeriod$, sinon le nœud exécute un nouveau CCA après un $aUnitBackoffPeriod$.

2.2.6.2 Protocole Aloha

Aloha slotté et Aloha non slotté sont utilisés pour la compréhension et l'analyse des systèmes de transmission sans fil. Ces méthodes d'accès sont implémentées dans les réseaux satellitaires et la téléphonie mobile. Dans Aloha, l'envoi simultané des paquets par plus d'un mobile cause une collision. Après avoir transmis un paquet, l'émetteur reçoit l'accusé de réception sur l'état de la transmission. Tous les paquets non reçus seront retransmis après un temps aléatoire. Dans la suite de ce travail, nous nous intéressons à Aloha slotté, dans lequel le temps est divisé en unités égales appelées slots. La transmission a toujours lieu au début du slot (les transmissions sont synchronisées avec l'horloge du système, et l'accusé de réception sera reçu à la fin du slot courant). Les paquets entrés en collision sont mis en attente jusqu'à leurs retransmissions planifiées après un nombre aléatoire de slots. Chaque nœud capteur qui utilise ce protocole et voulant accéder au canal de communication suit la démarche suivante [17] :

1. La sous-couche MAC initialise la fenêtre de contention à une période de temps, BE à $macMinBE$ et NB à 0,
2. Le capteur choisit un temps d'attente aléatoire dans la plage $[0, 2^{BE} - 1]$ unités et puis le décrémente jusqu'à arriver à zéro. Après il passe à l'étape suivante,
3. Si $CW = 0$, aller à l'étape 7. Sinon passer 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 passer à l'étape suivante,
5. Si NB est inférieur à la valeur de $macMaxCSMABackoffs$, le nœud tire un autre $backoff$ pour renvoyer 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 est prête à être envoyée à la frontière du prochain $backoff$.

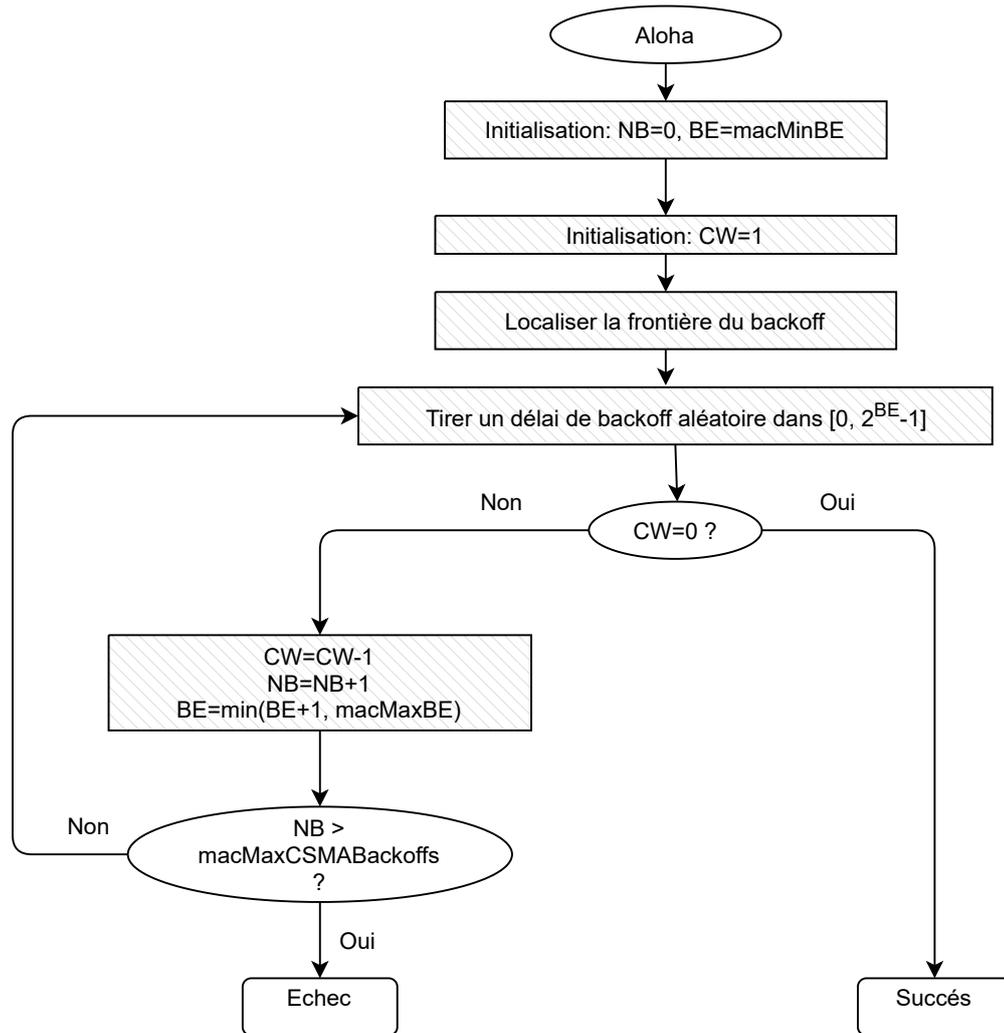


FIGURE 2.4 – Fonctionnement du protocole Aloha slotté.

2.2.7 Introduction à l'évaluation de performances des réseaux et ses outils de modélisation

Les performances du réseau sont des grandeurs qualitatives et quantitatives pour caractériser le fonctionnement d'un réseau. Le but d'une évaluation de performances est de trouver des indicateurs représentant le comportement du réseau [18].

La modélisation analytique et la simulation sont des outils adéquats pour réaliser l'évaluation de performance d'un système. La modélisation analytique est une manière de faire un modèle abstrait du système en proposant une représentation du système et de ses paramètres d'entrée. Plusieurs approches de modélisations analytiques (chaîne de Markov, Réseaux de Petri stochastiques..) existent dans la littérature dépendant de la nature du système à étudier ainsi que des grandeurs de performance à évaluer.

Les chaînes de Markov sont un formalisme mathématique simple pour analyser un phénomène stochastique. Un modèle est basé sur des états et des transitions ou probabilité. Sa simple structure permet de modéliser une large classe de systèmes. Les chaînes de Markov sont des outils bien connus où les nombreux résultats théoriques permettent d'analyser le système modélisé. Les chaînes de Markov 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 évaluation de performances, les chaînes de Markov présentent une simplicité et une efficacité incontournable. Dans la littérature, la plupart des modélisations du standard 802.15.4 utilisent les chaînes de Markov comme outil de modélisation. Notre travail sera également réalisée à l'aide de cet outil.

2.2.8 Limites de la norme IEEE 802.15.4

Les performances des protocoles MAC du standard IEEE 802.15.4, dans les deux modes balisé et non balisé, ont été étudiés dans le passé. Les auteurs ont identifié les principales limites de la norme IEEE 802.15.4 qui la rendent inadapté aux scénarios d'application à temps critique comme les applications industrielles et médicales [18] :

- Délai non borné : les protocoles MAC du 802.15.4-2003 sont basés sur l'algorithme CSMA/CA, et ça ne permet de garantir aucune borne de délai maximale expérimentée sur des données pour atteindre la destination finale ;
- Fiabilité de communication limitée. La norme offre un très faible taux de délivrance de paquet, même lorsque le nombre de nœuds n'est pas important, ceci la rend inadapté pour les applications critiques ;
- Non protection contre les interférences et l'évanouissement du signal : qui sont des phénomènes très fréquents, en particulier lorsque les réseaux de capteurs/actionneurs sont utilisées. Contrairement aux autres technologies sans fil, le 802.15.4 utilise un seul canal et n'intègre pas le mécanisme du saut de canal contre les interférences et l'évanouissement du signal.

2.2.9 Évolution de la norme IEEE 802.15.4

La norme initiale IEEE 802.15.4-2003 a été créée en 2003 pour définir les techniques spécifiques de cette norme. Elle a été amendée par une nouvelle norme publiée le 7 juin 2006 en proposant une sous-couche MAC et quatre couches PHYs. L'IEEE 802.15.4-2006, amendée par la suite à trois reprises, reste actuellement la seule base en cours de validité sur laquelle s'appuient les amendements. Le tableau (2.1) représente les améliorations proposées par cet ensemble normatif [17].

TABLE 2.1 – Comparaison entre les standards IEEE 802.15.4

Version	Date	Débit (kb/s)	Protocole MAC	Caractéristiques
802.15.4	2003	250	CSMA/CA	Consommation d'énergie ultra-faible Faible consommation de données
802.15.4	2006	250	CSMA/CA	Amélioration de la sécurité La synchronisation des messages diffusés
802.15.4a	2007	1000	ALOHA	Possibilité d'utiliser simultanément un même canal Prise en charge des liaisons de longue portée
802.15.4c	2009	250	/	/
802.15.4d	2009	100	CSMA/CA	L'écoute avant de parler Le contrôle de transmission
802.15.4	2011	1000	CSMA/CA ALOHA	Révision de la version de 2006
802.15.4e	2012	/	DSME LLDN TSCH	Minimisation des collisions Haute fiabilité du système
802.15.4f	2012	250	Aloha	Communications fiables
802.15.4g	2012	800	CSMA/CA	Évitement des interférences Sécurité
802.15.4j	2013	250	/	Canalisation flexible est gardée
802.15.4k	2013	/	CSMA/CA PCA ALOHA PCA	Priorité
802.15.4m	2014	1638	/	Basse énergie Amélioration des performances
802.15.4p	2014	36	CSMA/CA CSMA/CA PCA	Prise en charge de : fixe à fixe, fixe vers mobile et mobile à mobile
802.15.4	2015	1000	TSCH CSMA/CA	Révision de la norme de 2011
802.15.4n	2016	500	/	Transmission d'informations médicales
802.15.4q	2016	jusqu'à 1000	/	Consommation réduite d'énergie Débits de données plus élevés
802.15.4u	2016	150	/	Utilisé pour des niveaux de puissance plus larges sans licence
802.15.4t	2017	2000	/	Débit de données élevé
802.15.4v	2017	300	/	Activation des bandes régionales sous-GHz
802.15.4s	2018	/	/	Spectre radio efficace Sélection du meilleur PAN disponible
802.15.4x	2019	jusqu'à 2400	/	Débits de données plus élevés
802.15.4z	2020	2000	/	Révision de la version de 2015

2.3 Conclusion

Dans ce chapitre, nous avons tout d'abord introduit la norme IEEE 802.15.4 en présentant ses modes de fonctionnements et les couches utilisées dans cette version. Par la suite, nous avons expliqué les mécanismes d'accès au canal puis présenté les limites de la norme IEEE 802.15.4 et son évolution au fil du temps. La norme IEEE 802.15.4 a été évoluée et amendée à plusieurs reprises et a donné naissance à plusieurs versions. Notre objectif est d'évaluer les performances de cette version et de réaliser une étude comparative entre les deux protocoles Aloha et CSMA/CA. Pour atteindre notre objectif, nous choisissons de mener notre étude à l'aide de la modélisation analytique stochastique (en utilisant la chaîne de Markov). Cette approche nous permettra d'analyser le comportement de cette version et d'obtenir des résultats exacts. Ceci fera l'objet des chapitres suivants.

Deuxième partie

Contributions

Chapitre 3

Modélisation analytique et évaluation des performances du mécanisme IEEE 802.15.4 Aloha slotté

3.1 Introduction

Dans ce chapitre, nous allons nous intéresser à un modèle analytique capable d'estimer les métriques de performances du mécanisme Aloha slotté (S-Aloha) pour la transmission des paquets dans le standard IEEE 802.15.4. Notre modélisation repose sur une chaîne de Markov à trois dimensions. En se basant sur le modèle proposé, et en utilisant les hypothèses ainsi qu'une méthodologie bien définie, les expressions des mesures de performances tels que la fiabilité, l'énergie consommée, le débit et le délai moyen ont pu être développées. Et comme dernière partie du chapitre, une évaluation des performances du réseau IEEE 802.15.4 S-Aloha en fonction du nombre de nœuds N ainsi que l'effet de la variation du nombre de nœuds et de la taille des paquets L_p sur les performances du réseau a été effectuée.

3.2 Modélisation analytique du mécanisme d'accès au canal Aloha slotté

Dans cette partie, nous allons présenter le modèle analytique proposé pour S-Aloha de IEEE 802.15.4 dans des conditions de saturation du trafic sous un canal idéal.

3.2.1 Hypothèses du modèle

Les propositions suivantes sont appliquées dans notre modèle de chaîne de Markov :

- Un nombre fixe de nœuds (N).

- Considération des conditions de saturation du trafic.
- Considération d'un canal idéal.
- Prise en charge des accusés de réception.

3.2.2 Les Paramètres utilisés dans le modèle

Les notations utilisés dans notre modèle sont représentés dans le tableau 3.1.

TABLE 3.1 – Paramètres du modèle IEEE 802.15.4 Aloha slotté

Paramètre	Description
N	La taille du réseau
S	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 collisionné
L_{ack}	La taille de l'ACK
σ	La durée d'un intervalle de temps

3.2.3 Les probabilités utilisées dans le modèle

Les probabilités indispensables à la réalisation de notre modèle sont données par le tableau 3.2.

TABLE 3.2 – Probabilités du modèle IEEE 802.15.4 S-ALOHA slotté

Probabilités	Description
τ	La probabilité de transmettre dans n'importe quel intervalle de temps aléatoire
P_c	La probabilité de collision
P_e	La probabilité de rejet du paquet dû à un échec de transmission
P_r	La probabilité de rejet du paquet en raison de retransmissions dépassées
$b_{i,k,j}$	Les probabilités des états de la chaîne de Markov

3.2.4 Proposition d'une chaîne de Markov pour le mécanisme S-Aloha

Dans cette section, nous présentons notre modèle de chaîne de Markov proposé pour S-aloha qui est illustré par son graphe de transition dans la figure 3.1.

Dans cette chaîne, nous définissons un sous ensemble d'états E composé de trois processus stochastiques, $E = \{s(t), c(t), r(t)\}$ où :

- $s(t)$: est le processus stochastique qui représente l'étage du backoff à l'instant t .
- $c(t)$: est le processus stochastique qui représente la valeur du compteur de backoff
- $r(t)$: est le processus stochastique qui représente la transmission ou la retransmission à l'instant t .

Dans notre modèle :

- ✧ 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 $(-2, L_s - 1, j)$, $j \in [0, n]$ modélisent les états de transmission réussie.
- ✧ Les états allant de $(-1, 0, j)$ à $(-1, L_c - 1, j)$, $j \in [0, n]$ modélisent les états de transmission non réussie (collisionnée).
- ✧ la probabilité P_c représente la probabilité que le paquet transmis rencontre une collision.

3.2.4.1 Probabilités de transition

Les probabilités de transition associées à la chaîne de Markov sont données dans les équations suivantes (3.1)-(3.5).

$$P(i, k, j | i, k + 1, j) = 1, \forall i \in [0, m], k \in [0, W_i - 1], j \in [0, n]. \quad (3.1)$$

$$P(i, k, j | i - 1, 0, j - 1) = \frac{P_c}{W_i}, \forall i \in [0, m], k \in [0, W_i - 1], j \in [0, n]. \quad (3.2)$$

$$P(0, k, 0 | S) = \frac{(1 - \lambda)}{W_0}, k \in [0, W_i - 1]. \quad (3.3)$$

$$P(-2, 0, j | i, 0, j) = 1 - P_c, \forall i \in [0, m], j \in [0, n]. \quad (3.4)$$

$$P(-1, 0, j | i, 0, j) = P_c, \forall i \in [0, m], j \in [0, n]. \quad (3.5)$$

- Le compteur du backoff décroît avec la probabilité exprimée par l'équation (3.1).

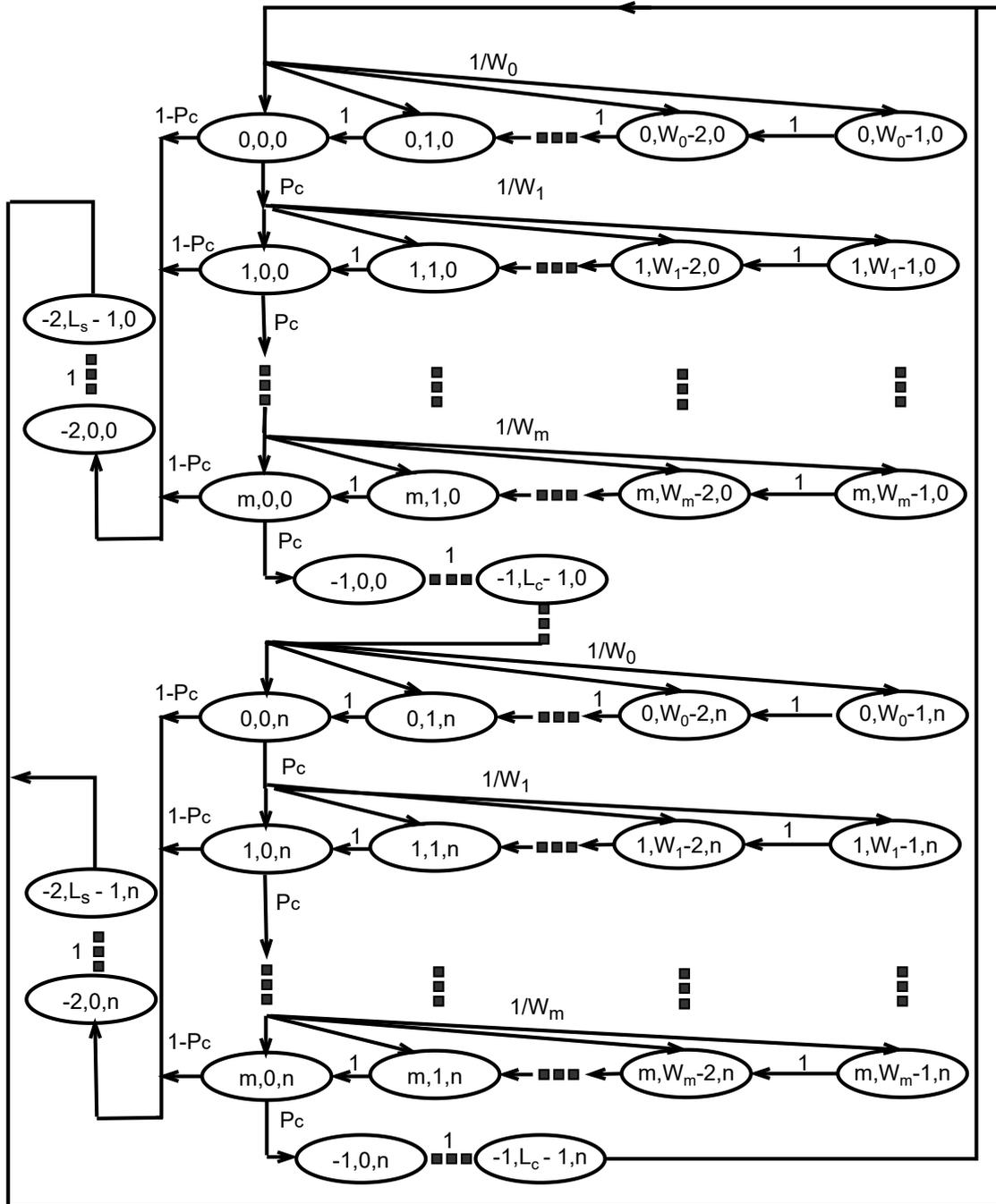


FIGURE 3.1 – Graphe de transition de la Chaîne de Markov du mécanisme IEEE 802.15.4 S-Aloha

- L'équation (3.2) représente la probabilité de transmission échouée et sélection d'un état lors du prochain étage de backoff.
- L'équation (3.3) donne la probabilité de passer au premier étage de backoff à partir de l'état idle (inactif).
- Les probabilités de transition à l'état succès et à l'état échec sont données dans les équations (3.4) et (3.5), respectivement.

3.2.4.2 Calcul des probabilités d'états stationnaires

Pour calculer la distribution stationnaire de notre chaîne de Markov nous utilisons les équations (3.1) - (3.5). Nous représentons par $b_{i,k,j}$ les probabilités des états de la chaîne de Markov.

Soit $b_{i,k,j} = \lim_{t \rightarrow +\infty} P(s(t) = i, c(t) = k, r(t) = j), i \in [-2, m], k \in (-1, \max(W_i - 1, L_s - 1, L_c - 1)), j \in [0, n]$ la probabilité stationnaire de notre chaîne de Markov.

Nous avons :

$$b_{i,k,j} = \frac{W_i - k}{W_i} b_{i,0,j}, \quad \forall k \in [0, W_i - 1]. \quad (3.6)$$

- 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 (3.7).

$$W_i = 2^i W_0, \quad \forall i \in [0, m]. \quad (3.7)$$

- La probabilité que le nœud tente de transmettre un paquet est donnée par

$$b_{i,0,j} = P_c^i b_{0,0,j} = x^i b_{0,0,j}, \quad \forall i \in [0, m], j \in [0, n]. \quad (3.8)$$

Où $x = P_c$ représente la probabilité d'échec de transmission à n'importe quel étage du backoff due à une collision

- La probabilité de retransmission après m tentatives d'échec de transmission est donnée par l'équation (3.9).

$$b_{0,0,j} = \left(x \sum_{i=0}^m b_{i,0,j-1} \right)^j = \left(x \frac{1 - x^{m+1}}{1 - x} \right)^j b_{0,0,0} = y^j b_{0,0,0}, \quad \forall j \in [0, n]. \quad (3.9)$$

Où $y = x \frac{(1 - x^{m+1})}{1 - x}$ représente la probabilité d'échec de transmission au cours des $(m + 1)$ étages du backoff.

- La probabilité de l'état succès est donnée par l'équation (3.10).

$$b_{-2,0,j} = (1 - P_c) \sum_{i=0}^m b_{i,0,j} = (1 - x^{m+1}) b_{0,0,j}, \quad \forall j \in [0, n]. \quad (3.10)$$

– La probabilité de l'état échec est

$$b_{-1,0,j} = P_c \sum_{i=0}^m b_{i,0,j} = y b_{0,0,j}, \quad \forall j \in [0, n]. \quad (3.11)$$

3.2.4.3 Condition de normalisation

Comme nous avons déjà vu dans le graphe de transition, chaque état dépend de la probabilité $b_{0,0,0}$. Nous utilisons la condition de normalisation donnée par l'équation (3.12) pour la dériver. Ensuite, on déduit l'expression de ses termes dans les équations (3.13), (3.14).

$$\sum_{i=0}^m \sum_{k=0}^{W_i-1} \sum_{j=0}^n b_{i,k,j} + \sum_{j=0}^n \left(\sum_{k=0}^{L_s-1} b_{-2,k,j} + \sum_{k=0}^{L_c-1} b_{-1,k,j} \right) = 1. \quad (3.12)$$

Le terme $\sum_{i=0}^m \sum_{k=0}^{W_i-1} \sum_{j=0}^n b_{i,k,j}$ est obtenu grâce aux équations (3.6)-(3.9).

$$\sum_{i=0}^m \sum_{k=0}^{W_i-1} \sum_{j=0}^n b_{i,k,j} = \sum_{i=0}^m \sum_{j=0}^n \frac{W_i + 1}{2} x^j b_{0,0,j} = b_{0,0,0} \left[\frac{1 - (2x)^{m+1}}{1 - 2x} W_0 + \frac{1 - x^{m+1}}{1 - x} \right] \frac{1 - y^{n+1}}{1 - y} = S_1 b_{0,0,0}. \quad (3.13)$$

D'après les équations (3.9)-(3.11), le dernier terme se calcule comme suit :

$$\sum_{j=0}^n \left(\sum_{k=0}^{L_s-1} b_{-2,k,j} + \sum_{k=0}^{L_c-1} b_{-1,k,j} \right) = b_{0,0,0} (1 - x^{m+1}) \left[L_s + \frac{L_c x}{1 - x} \right] \frac{1 - y^{n+1}}{1 - y} = S_2 b_{0,0,0}. \quad (3.14)$$

Finalement, $b_{0,0,0}$ s'exprime comme suit :

$$b_{0,0,0} = \frac{1}{S_1 + S_2}. \quad (3.15)$$

Nous pouvons à présent exprimer la probabilité τ qu'un nœud transmette dans n'importe quel intervalle de temps aléatoire donnée par l'équation (3.16).

$$\tau = \sum_{i=0}^m \sum_{j=0}^n b_{i,0,j} = \frac{1 - x^{m+1}}{1 - x} \frac{1 - y^{n+1}}{1 - y} b_{0,0,0}. \quad (3.16)$$

3.2.4.4 Calcul de la probabilité de collision

La probabilité que le paquet transmis rencontre une collision est :

$$P_c = 1 - (1 - \tau)^{N-1}. \quad (3.17)$$

3.3 Calcul des métriques de performances

En utilisant la chaîne de Markov déjà définie dans la figure 3.1 et les formules développées dans la partie précédente, nous dérivons les expressions mathématiques de la fiabilité, de délai moyen, de l'énergie consommée, et de débit.

3.3.1 Fiabilité

La fiabilité est la probabilité d'une transmission réussie des paquets. Elle est liée aux probabilités P_c et τ . Les paquets de données sont rejetés en raison d'un échec de transmission dans les $(m + 1)$ étages de backoff comme décrit dans l'équation (3.18) ou en raison de retransmissions dépassées comme décrit dans l'équation (3.19).

$$P_e = \sum_{j=0}^n x b_{m,0,j} = \frac{x^{m+1}(1 - y^{n+1})}{1 - y}. \quad (3.18)$$

$$P_r = \sum_{i=0}^m x b_{i,0,n} = y^{n+1}. \quad (3.19)$$

La fiabilité est alors donnée, comme suit

$$R = 1 - P_e - P_r. \quad (3.20)$$

3.3.2 Énergie consommée

Dans ce modèle, nous nous intéressons à l'énergie consommée dans le cas d'une transmission réussie. Soient P_i la consommation énergétique du nœud en mode veille, P_{tm} en mode transmission et P_{rm} en mode réception.

A partir des équations (3.13) et (3.14), la consommation moyenne d'énergie est donnée par l'équation (3.21).

$$E = P_i \sum_{i=0}^m \sum_{k=1}^{W_i-1} \sum_{j=0}^n b_{i,k,j} + P_{tm} \sum_{k=0}^{L-1} \sum_{j=0}^n (b_{-1,k,j} + b_{-2,k,j}) + P_i \sum_{j=0}^n (b_{-1,L,j} + b_{-2,L,j}) + \sum_{j=0}^n \sum_{k=L+1}^{L+L_{ack}+1} (P_{rm} b_{-2,k,j} + P_i b_{-1,k,j}). \quad (3.21)$$

3.3.3 Débit

Le débit est la quantité de données transmise avec succès par unité de temps.

- Soit P_c la probabilité d'une transmission avec collision. Elle est donnée par :

$$P_c = 1 - (1 - \tau)^{N-1}. \quad (3.22)$$

- Soit P_s la probabilité d'une transmission réussie donnée par l'équation (3.23).

$$P_s = \frac{N\tau(1 - \tau)^{N-1}}{P_c}. \quad (3.23)$$

Alors, le débit est obtenu par l'équation (3.24).

$$Db = \frac{L_p P_c P_s}{\sigma(1 - P_c) + T_s P_c P_s + T_c P_c (1 - P_s)}. \quad (3.24)$$

où

$$T_s = L_p + T_{PHY} + T_{MAC} + T_{LIFS} + t_{ack-wait} + t_{ack}. \quad (3.25)$$

et

$$T_c = L_p + T_{PHY} + T_{MAC} + T_{LIFS} + t_{ack-wait}. \quad (3.26)$$

représentent les durées de transmission réussie et non réussie, respectivement.

3.3.4 Délai

Le délai $E[D]$ d'une transmission de données réussie est l'intervalle du temps à partir duquel le paquet est dans l'entête MAC prêt à être transmis, jusqu'à ce qu'un ACK soit reçu. On prend en considération que le délai d'une transmission réussie. Le délai de transmission associé au paquet est donné par l'équation (3.27).

$$E[D] = \sum_{j=0}^n P(B_j|B_t)E[D_j]. \quad (3.27)$$

- L'événement B_j représente une transmission d'un paquet avec succès à l'instant $j + 1$ après j transmissions échouées.
- L'événement B_t indique une transmission réussie du paquet dans les m tentatives de transmissions.

$$P(B_j|B_t) = \frac{y^j}{\sum_{k=0}^n y^k} = y^j \frac{1 - y}{1 - y^{n+1}}. \quad (3.28)$$

- D_j est l'événement où un nœud envoie avec succès un paquet au j^{ieme} instant, donné par

$$E[D_j] = T_s + j T_c + T_b \sum_{h=0}^j E[D_h]. \quad (3.29)$$

– $E[D_h]$ est le délai de l'étage backoff, exprimé comme suit :

$$E[D_h] = \sum_{h=0}^i \frac{W_h - 1}{2} = \sum_{h=0}^i \frac{2^h W_0 - 1}{2} = \frac{-1}{2} \left[(1 - 2^{i+1}) W_0 + (j + 1) \right]. \quad (3.30)$$

En utilisant les équations (3.28)-(3.30), le délai moyen est donné par l'équation (3.31).

$$E[D] = \sum_{j=0}^n \left[\left(y^j \frac{1-y}{1-y^{n+1}} \right) \left(T_s + i T_c - \sum_{i=0}^m \frac{T_b}{2} \left[(1 - 2^{i+1}) W_0 + (i + 1) \right] \right) \right]. \quad (3.31)$$

3.4 Analyse de performances de mécanisme IEEE 802.15.4 S-Aloha

3.4.1 Méthode d'analyse et logiciels utilisés

Afin de réaliser notre étude analytique et évaluer les performances du mécanisme S-Aloha du 802.15.4, nous avons utilisé deux logiciels mathématiques. A l'aide du logiciel Mathcad, nous avons résolu un système d'équations non linéaire formé par les expressions de S_1 , S_2 , P_c et τ pour d'obtenir les valeurs numériques. Par la suite nous avons développé un programme mathématique sous Matlab pour implémenter les expressions des métriques de performance telles que la fiabilité, l'énergie consommée, le débit et le délai. Cette implémentation nous a permis de générer des graphes en fonction du nombre de nœuds N et de la taille du paquet L_p .

3.4.2 Valeurs des paramètres utilisés

La table 3.3 indique les différents paramètres utilisés pour l'analyse des performances.

TABLE 3.3 – Paramètres utilisés pour l'évaluation des performances de IEEE 802.15.4 S-Aloha

Paramètre	Valeur	Paramètre	Valeur	Paramètre	Valeur
n	3	T_b	1.92 ms	σ	0.96 ms
m	4	P_r	40 mW	T_{LIFS}	0.32 ms
L_p, N	Variants	P_i	0.8 mW	<i>MAC header length</i>	16 bytes
W_0	8	P_t	30 mW	<i>PHY header length</i>	6 bytes
$L_s = L_c$	80 bytes	t_{ack}	1 ms		
L_{ack}	20 bytes	$t_{ack-wait}$	[1 – 1.32] ms		

3.4.3 Résultats, analyses et comparaisons

La figure 3.2 représente la variation de la fiabilité en fonction de la taille du réseau, pour une taille du paquet ($L_p = 100 \text{ bytes}$). 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.

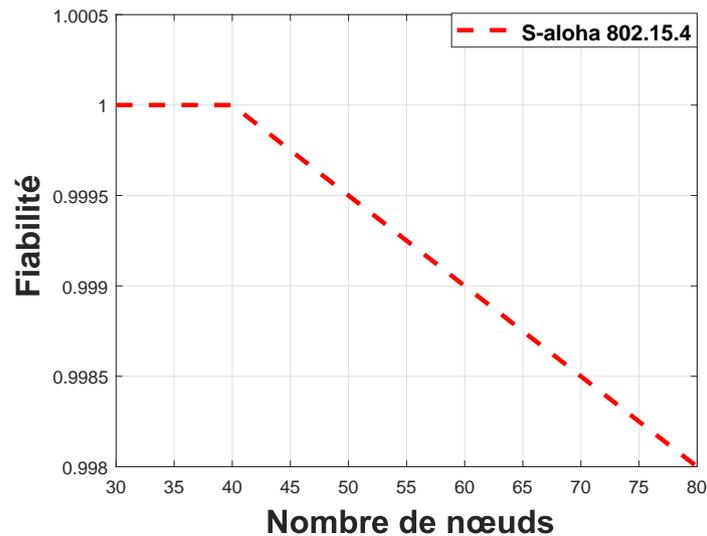


FIGURE 3.2 – Fiabilité Vs Taille du réseau, avec $L_p = 100 \text{ bytes}$.

La figure 3.3 illustre la variation de la fiabilité en fonction de la taille du réseau pour différentes tailles de paquets ($L_p = 20 \text{ bytes}$ et $L_p = 100 \text{ bytes}$). Nous reportons que plus le nombre de stations

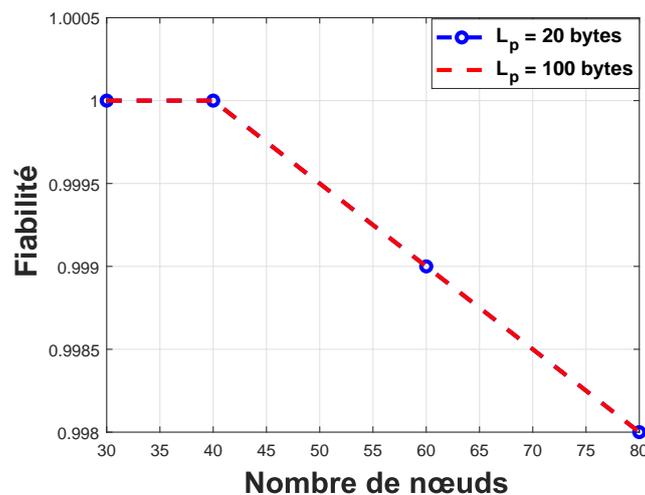


FIGURE 3.3 – Fiabilité Vs Taille du réseau & variant la Taille des paquets L_p .

augmente, plus la probabilité de collision augmente, plus la fiabilité diminue. En augmentant la

taille du paquet de données, la fiabilité reste la même. En d'autres termes, quelle que soit la taille du paquet de données, la probabilité de sa transmission avec succès reste constante.

La figure 3.4 représente la consommation d'énergie en fonction de la taille du réseau. Nous notons que lorsque le nombre de nœud augmente, l'énergie consommée diminue. Un nœud consomme de l'énergie lors de la transmission du paquet et lors de la réception de son ACK. Dans le cas où

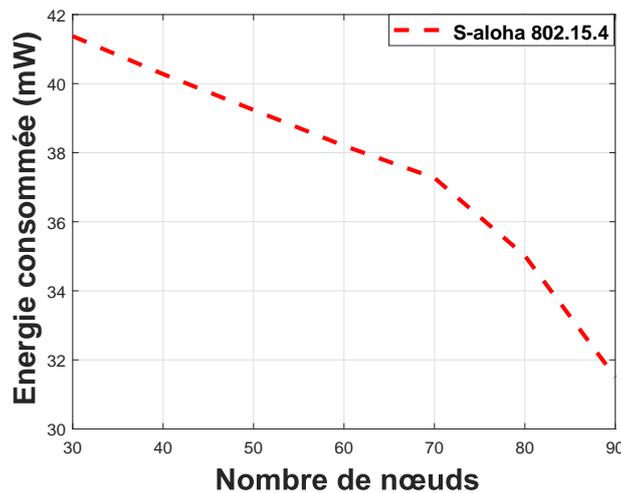


FIGURE 3.4 – Énergie Vs Taille du réseau, avec $L_p = 100$ bytes.

un très grand nombre de nœuds tentent de transmettre un message, une collision se produira. Par conséquent, les nœuds se mettent en mode sommeil et donc ils ne consomment pas de l'énergie.

La figure 3.5 représente la consommation d'énergie en fonction de la taille du réseau pour différentes tailles de paquets ($L_p = 20$ bytes et $L_p = 100$ bytes). L'énergie consommée dans le cas

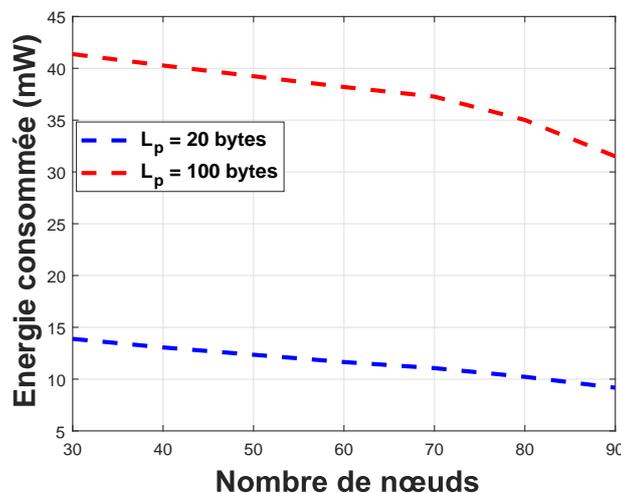


FIGURE 3.5 – Énergie Vs Taille du réseau & variant la Taille des paquets L_p .

d'un paquet de grande taille ($L_p = 100$ bytes) est plus grande que celle consommée par un paquet

de petite taille ($L_p = 20 \text{ bytes}$). Ceci est dû au fait que le délai de la transmission et de la réception de l'ACK est grand, par conséquent l'énergie consommée sera plus grande.

La figure 3.6 trace le débit en fonction de la taille du réseau, pour une taille du paquet ($L_p = 100 \text{ bytes}$). Nous notons une diminution du débit avec l'augmentation de la taille du réseau. Cela s'ex-

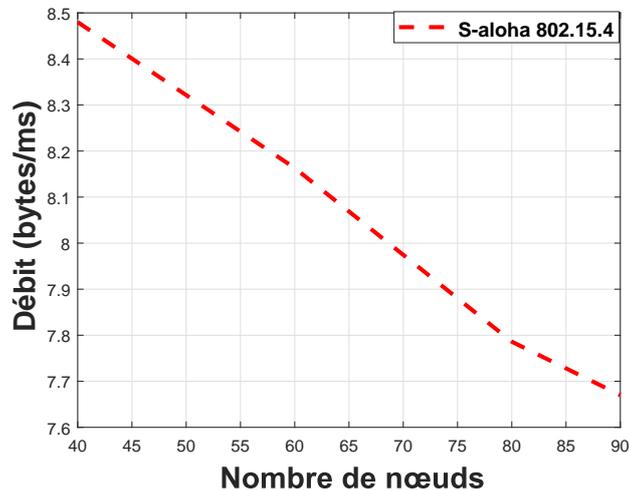


FIGURE 3.6 – Débit Vs Taille du réseau, avec $L_p = 100 \text{ bytes}$.

plique par le fait que lorsque un grand nombre de nœuds tentent de transmettre, un risque élevé de collisions est observé qui augmente à son tour la probabilité d'échec. Par conséquent, une faible quantité de données sera transmises avec succès.

La figure 3.7 illustre la variation du débit en fonction de la taille du réseau pour différentes tailles de paquets ($L_p = 20 \text{ bytes}$ et $L_p = 100 \text{ bytes}$). Nous reportons que plus le nombre de stations

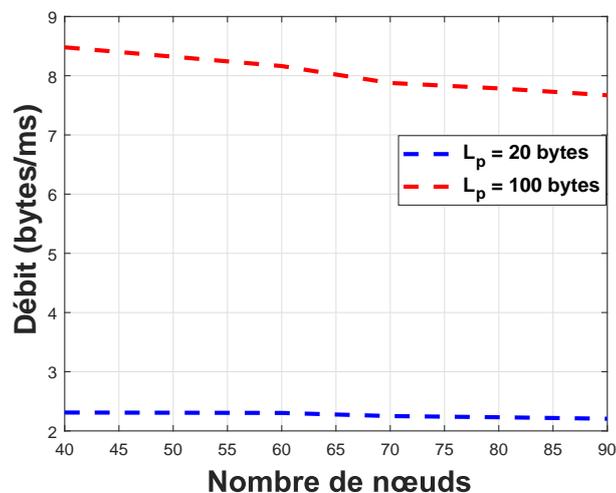


FIGURE 3.7 – Débit Vs Taille du réseau & variant la Taille des paquets L_p .

augmente, plus la probabilité de collision augmente, plus le débit diminue. Nous constatons aussi

que le débit offert par les nœuds ayant une taille importante ($L_p = 100 \text{ bytes}$) est supérieur à celui offert par les paquets ayant une taille faible ($L_p = 20 \text{ bytes}$) car la quantité de données transmises est importante.

La figure 3.8 représente la variation du délai en fonction de la taille du réseau, pour une taille de paquet ($L_p = 100 \text{ bytes}$). Comme le montre la figure, le délai augmente au fur et à mesure

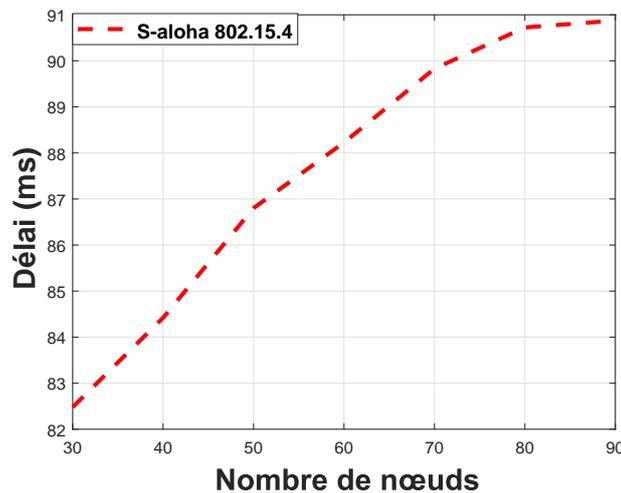


FIGURE 3.8 – Délai Vs Taille du réseau, avec $L_p = 100 \text{ bytes}$.

que le nombre de nœuds dans le réseau augmente. Lorsque un grand nombre de nœuds tente de transmettre, la probabilité de collision augmente. Par conséquent, le nœud passe beaucoup de temps dans la période backoff, d'où le délai élevé.

La figure 3.9 représente la variation du délai en fonction de la taille du réseau pour différents

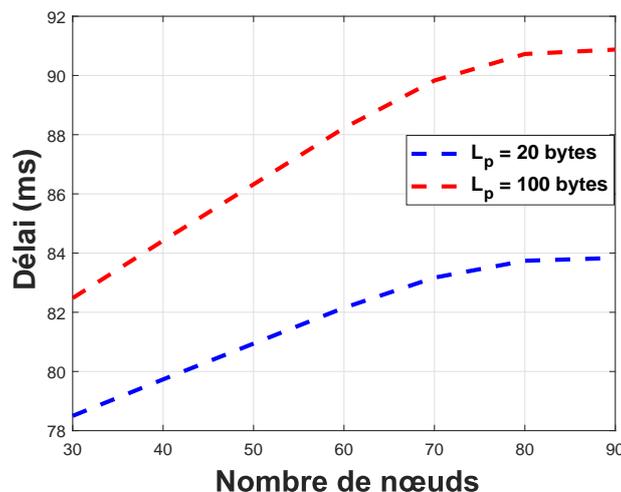


FIGURE 3.9 – Délai Vs Taille du réseau & variant la Taille des paquets L_p .

tailles de paquets ($L_p = 20 \text{ bytes}$ et $L_p = 100 \text{ bytes}$). Nous notons que plus la taille du paquet est

grande plus le délai devient grand. La raison est que les nœuds ayant des paquets de grande taille à transmettre ($L_p = 100 \text{ bytes}$) dépensent beaucoup plus de temps pour la transmission de ses derniers en les comparant nœuds ayant des paquets ayant de petite taille ($L_p = 20 \text{ bytes}$).

Conclusion

Tout au long de ce chapitre, nous avons présenté un modèle analytique basé sur une chaîne de Markov pour analyser les performances du mécanisme Aloha slotté (S-aloha) de la norme IEEE 802.15.4. Nous avons dérivé les expressions mathématiques de fiabilité, de l'énergie consommée, de délai pour une transmission réussie et de débit offerts par la norme IEEE 802.15.4. Nous avons analysé l'impact de la variation de la taille du réseau et de la taille des paquets sur les métriques étudiées. A l'issue de cette étude, nous avons constaté qu'à mesure que nous augmentons la taille des paquets, le débit augmente en parallèle. En augmentant la taille du réseau, une fiabilité plus basse, un délai plus élevé, une consommation d'énergie plus faible, et un débit faible sont observés.

Chapitre 4

Modélisation analytique et évaluation des performances du mécanisme IEEE 802.15.4 CSMA/CA slotté

4.1 Introduction

Dans ce chapitre, nous présentons un modèle du protocole MAC IEEE 802.15.4 CSMA/CA slotté et une analyse des performances du réseau en termes de fiabilité, de débit, de délai et de consommation d'énergie. Le modèle proposé se base sur une chaîne de Markov à trois dimensions du modèle de Park [2]. L'analyse des performances du réseau IEEE 802.15.4 en fonction du nombre de nœuds N et de la taille des paquets L_p a été effectuée. Et à la fin du chapitre, nous faisons une comparaison entre les deux protocoles utilisés dans la contribution en étudiant les résultats d'analyse de performances des deux mécanismes : ALOHA slotté et CSMA/CA slotté.

4.2 Modélisation analytique du mécanisme d'accès au canal CSMA/CA slotté

Dans cette section, nous proposons un modèle analytique généralisé du mécanisme CSMA/CA slotté de IEEE 802.15.4 dans des conditions de saturation du trafic sous un canal idéal.

4.2.1 Hypothèses du modèle

Nous supposons les hypothèses suivantes dans lesquelles notre modèle de chaîne de Markov (CM) est applicable :

- Un nombre fixe de nœuds (N).

- Tous les nœuds tentent d'envoyer des données au coordinateur PAN (trafic saturé).
- Considération d'un canal idéal.
- Prise en charge des accusés de réception.

4.2.2 Paramètres utilisés dans le modèle

Les notations utilisés dans notre modèle sont représentées dans le tableau 4.1.

TABLE 4.1 – Paramètres du modèle IEEE 802.15.4 CSMA/CA slotté

Paramètre	Description
N	La taille du réseau
S	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 collisionné
L_{ack}	La taille de l'ACK
σ	La durée d'un intervalle de temps

4.2.3 Les probabilités utilisées dans le modèle

Les probabilités indispensables à la réalisation de notre modèle sont données par le tableau 4.2.

TABLE 4.2 – Probabilités du modèle IEEE 802.15.4 CSMA/CA slotté

Probabilités	Description
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_c	La probabilité de collision
P_e	La probabilité d'échec
P_r	La probabilité de rejet du paquet en raison de retransmissions dépassées
$b_{i,k,j}$	Les probabilités des états de la chaîne de Markov

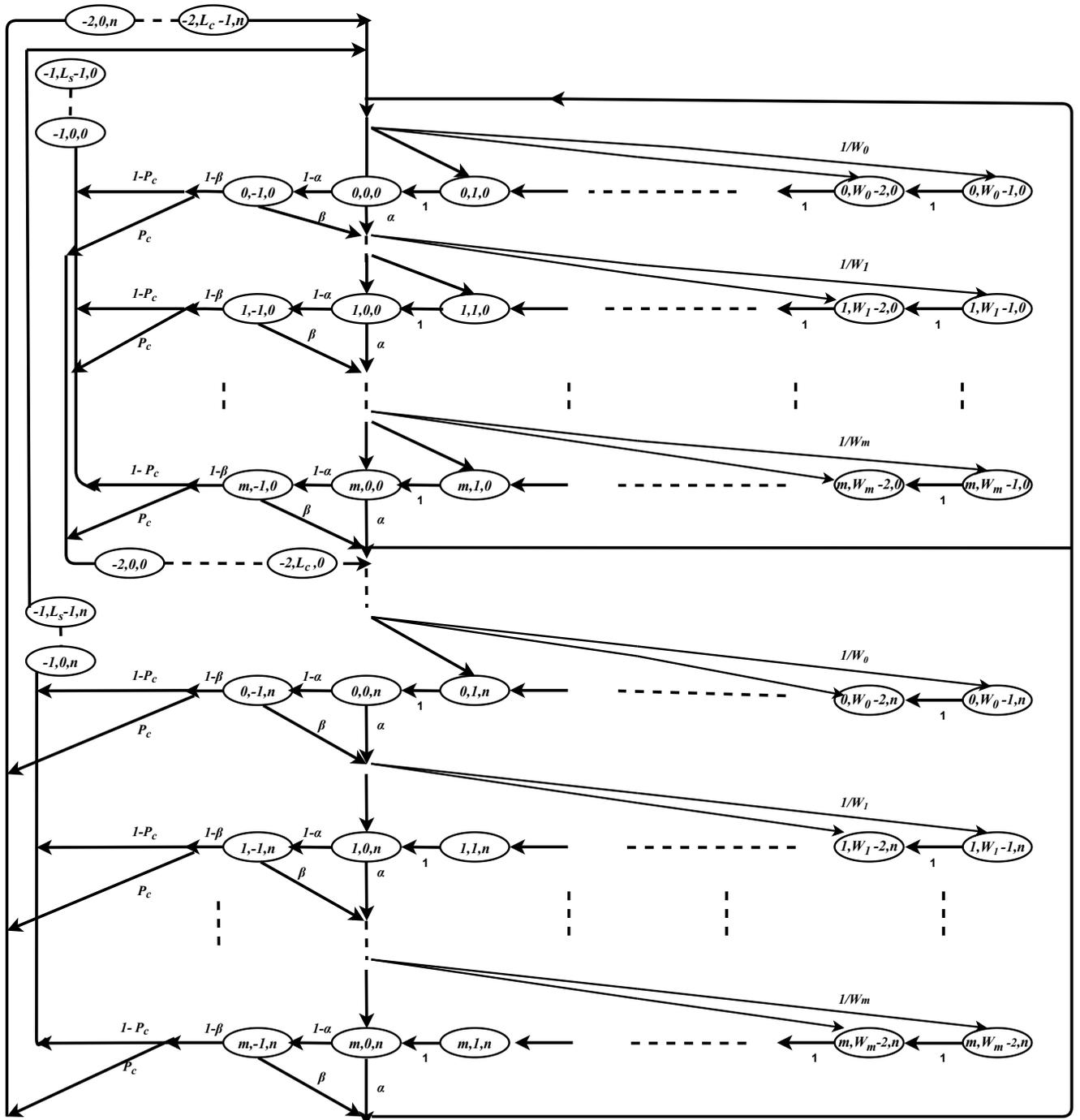


FIGURE 4.1 – Graphe de transition de la Chaîne de Markov du mécanisme IEEE 802.15.4 CSMA/CA

4.2.4 Proposition d'une chaîne de Markov pour le mécanisme CSMA/CA slotté

Dans cette section, nous présentons le modèle de chaîne de Markov proposé par Park [2] pour le protocole CSMA/CA qui est illustré par son graphe de transition dans la figure 4.1. Dans cette chaîne, nous définissons un sous ensemble d'états E composé de trois processus stochastiques, $E = \{s(t), c(t), r(t)\}$ où :

- $s(t)$: est le processus stochastique qui représente l'étage du backoff à l'instant t .
- $c(t)$: est le processus stochastique qui représente la valeur du CCA1/CCA2 à l'instant t .
- $r(t)$: est le processus stochastique qui représente la transmission et retransmission à l'instant t .

Dans ce modèle :

- ✧ 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 $(i, 0, j)$ 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 $(-2, L_s - 1, j)$, $j \in [0, n]$ modélisent les états de transmission réussie.
- ✧ Les états allant de $(-1, 0, j)$ à $(-1, L_c - 1, j)$, $j \in [0, n]$ modélisent les états de transmission non réussie (collisionné).
- ✧ Le paramètre α représente la probabilité que le canal soit occupé dans le CCA1.
- ✧ Le paramètre β représente la probabilité que le canal soit occupé dans le CCA2.
- ✧ Le paramètre P_c représente la probabilité que le paquet transmis rencontre une collision.

4.2.4.1 Probabilités de transition

Les probabilités de transition associées à la chaîne de Markov sont données dans les équations suivantes (4.1)-(4.5).

$$P(i, k, j|i, k + 1, j) = 1, \forall i \in [0, m], k \in [0, W_i - 1], j \in [0, n]. \quad (4.1)$$

$$P(-2, 0, j|i, 0, j) = (1 - \alpha)(1 - \beta)(1 - P_c), \forall i \in [0, m], j \in [0, n]. \quad (4.2)$$

$$P(-1, 0, j|i, 0, j) = (1 - \alpha)(1 - \beta) P_c, \forall i \in [0, m], j \in [0, n]. \quad (4.3)$$

$$P(i, k, j|i - 1, 0, j) = \frac{\alpha + (1 - \alpha)\beta}{W_i}, \forall i \in [0, m], k \in [0, W_i - 1], j \in [0, n]. \quad (4.4)$$

$$P(0, k, 0|S) = \frac{(1 - \lambda)}{W_0}, k \in [0, W_i - 1]. \quad (4.5)$$

- Le compteur du backoff décrémente à chaque slot de temps avec la probabilité donnée par l'équation (4.1).
- L'équation (4.2) représente La probabilité de transition de l'état CCA1 de CSMA/CA au slot succès.
- L'équation (4.3) représente la probabilité de transition de l'état CCA1 de CSMA/CA au slot échec.
- La probabilité de trouver canal occupé soit dans CCA1 ou CCA2 et de sélectionner un état dans l'étage du backoff est donnée par l'équation (4.4).
- L'équation (4.5) modélise la probabilité de revenir au premier étage de backoff à partir de l'étape de repos (inactif), respectivement.

4.2.4.2 Calcul des probabilités d'états stationnaires

Pour calculer la distribution stationnaire de notre chaîne de Markov nous utilisons les équations (4.1) - (4.5).

Nous représentons par $b_{i,k,j}$ les probabilités des états de la chaîne de Markov.

Soit $b_{i,k,j} = \lim_{t \rightarrow +\infty} P(s(t) = i, c(t) = k, r(t) = j), i \in [-2, m], k \in (-1, \max(W_i - 1, L_s - 1, L_c - 1)), j \in [0, n]$ la probabilité stationnaire de notre chaîne de Markov.

Nous avons :

$$b_{i,k,j} = \frac{W_i - k}{W_i} b_{i,0,j}, \forall k \in [0, W_i - 1]. \quad (4.6)$$

- La valeur du compteur de backoff W_i est uniformément choisie à l'étage i dans l'intervalle

$[0, W_i - 1]$ est donnée par l'équation (4.7).

$$W_i = \begin{cases} 2^i W_0, & \forall i \leq m_b - m_0. \\ 2^{m_b - m_0} W_0, & \forall i > m_b - m_0. \end{cases} \quad (4.7)$$

Avec $m_b = \text{macMaxBE}$ et $m_0 = \text{macMinBE}$.

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

$$b_{i,0,j} = (\alpha + (1 - \alpha)\beta)^i b_{0,0,j} = x^i b_{0,0,j}, \quad \forall i \in [0, m], j \in [0, n]. \quad (4.8)$$

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 (4.9).

$$b_{0,0,j} = (1 - \alpha)(1 - \beta) P_c \sum_{i=0}^m b_{i,0,j-1} = \left(1 - x\right) P_c \sum_{i=0}^m x^i)^j b_{0,0,0} = y^j b_{0,0,0}, \quad \forall j \in [0, n]. \quad (4.9)$$

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

– La probabilité que le nœud tente un CCA2 dans l'état $(i, -1, j)$ est donné par l'équation (4.10).

$$b_{i,-1,j} = (1 - \alpha) x^i y^j, \quad \forall i \in [0, m], j \in [0, n]. \quad (4.10)$$

– La probabilité de l'état succès est donnée par l'équation (4.11).

$$b_{-2,0,j} = (1 - P_c)(1 - x^{m+1}) b_{0,0,j}, \quad \forall j \in [0, n]. \quad (4.11)$$

– La probabilité de l'état échec est

$$b_{-1,0,j} = P_c (1 - x^{m+1}) b_{0,0,j}, \quad \forall j \in [0, n]. \quad (4.12)$$

4.2.4.3 Condition de normalisation

Comme le montre le graphe de transition, chaque état dépend de la probabilité $b_{0,0,0}$. Nous utilisons la condition de normalisation donnée par l'équation (4.13) pour la dériver. Ensuite, on déduit l'expression de ses termes dans les équations (4.14)-(4.16).

$$\sum_{i=0}^m \sum_{k=0}^{W_i-1} \sum_{j=0}^n b_{i,k,j} + \sum_{i=0}^m \sum_{j=0}^n b_{i,-1,j} + \sum_{j=0}^n \left(\sum_{k=0}^{L_s-1} b_{-1,k,j} + \sum_{k=0}^{L_c-1} b_{-2,k,j} \right) = 1. \quad (4.13)$$

Le premier terme est obtenu grâce aux équations (4.6)-(4.9).

$$\sum_{i=0}^m \sum_{k=0}^{W_i-1} \sum_{j=0}^n b_{i,k,j} = \sum_{i=0}^m \sum_{j=0}^n \frac{W_i + 1}{2} x^i b_{0,0,j} = S_1 b_{0,0,0} \quad (4.14)$$

Avec

$$b_{i,k,j} = \begin{cases} \frac{b_{0,0,0}}{2} \left[\frac{1-(2x)^{m+1}}{1-2x} W_0 + \frac{1-x^{m+1}}{1-x} \right] \frac{1-y^{n+1}}{1-y}, & \text{si } m \leq m_b - m_0, \\ \frac{b_{0,0,0}}{2} \left[\frac{1-(2x)^{m_b-m_0+1}}{1-2x} W_0 + \frac{1-x^{m_b-m_0+1}}{1-x} + (2^{m_b} + 1)x^{m_b-m_0} \frac{1-x^{m_b-m_0+1}}{1-x} \right] \frac{1-y^{n+1}}{1-y}, & \text{si } m > m_b - m_0. \end{cases}$$

Le deuxième terme est donné dans (4.15) :

$$\begin{aligned} \sum_{i=0}^m \sum_{j=0}^n b_{i,-1,j} &= \sum_{i=0}^m \sum_{j=0}^n (1-\alpha) (\alpha + (1-\alpha)\beta)^i b_{0,0,j} \\ &= (1-\alpha) \frac{1-x^{m+1}}{1-x} \frac{1-y^{n+1}}{1-y} b_{0,0,0} = S_2 b_{0,0,0}. \end{aligned} \quad (4.15)$$

D'après les équations (4.9)-(4.12), le dernier terme se calcule comme suit :

$$\sum_{j=0}^n \left(\sum_{k=0}^{L_s-1} b_{-1,k,j} + \sum_{k=0}^{L_c-1} b_{-2,k,j} \right) = (L_s(1-P_c) + L_c P_c) (1-x^{m+1}) \frac{1-y^{n+1}}{1-y} b_{0,0,0} = S_3 b_{0,0,0}. \quad (4.16)$$

Finalement, $b_{0,0,0}$ s'exprime comme suit :

$$b_{0,0,0} = \frac{1}{S_1 + S_2 + S_3}. \quad (4.17)$$

Nous pouvons à présent exprimer la probabilité τ qu'un noeud tente le CCA1 dans un slot de temps choisi aléatoirement donnée par l'équation (4.18).

$$\tau = \sum_{i=0}^m \sum_{j=0}^n b_{i,0,j} = \frac{1-x^{m+1}}{1-x} \frac{1-y^{n+1}}{1-y} b_{0,0,0}. \quad (4.18)$$

4.2.4.4 Calcul de la probabilité de collision

La probabilité que le paquet transmis rencontre une collision est :

$$P_c = 1 - (1-\tau)^{N-1}. \quad (4.19)$$

4.2.4.5 Calcul des probabilités que le canal soit occupé

– La probabilité α que le canal soit occupé pendant le CCA1 est donnée par l'expression (4.20).

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 .

$$\alpha = \alpha_1 + \alpha_2 \quad (4.20)$$

A partir du graphe de transition de la figure 4.1, les expressions de α_1 et α_2 sont données dans les équations (4.21) et (4.22), respectivement.

$$\alpha_1 = L_p (1 - \alpha)(1 - \beta) P_c \quad (4.21)$$

$$\alpha_2 = L_{ack} \frac{N \tau (1 - \tau)^{N-1}}{1 - (1 - \tau)^N} (1 - (1 - \tau)^{N-1}) (1 - \alpha) (1 - \beta). \quad (4.22)$$

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

– La probabilité β que le canal soit occupé pendant le CCA2 est donnée par l'équation (4.23).

$$\beta = \frac{1 - (1 - \tau)^{N-1} + N\tau(1 - \tau)^{N-1}}{2 - (1 - \tau)^N + N\tau(1 - \tau)^{N-1}}. \quad (4.23)$$

4.3 Calcul des métriques de performances

En utilisant la chaîne de Markov déjà définie dans la figure 4.1 et les formules développées dans la partie précédente, nous dérivons les expressions mathématiques de la fiabilité, de délai moyen, de l'énergie consommée et de débit.

4.3.1 Fiabilité

Les paquets de données sont rejetés en raison d'un échec d'accès au canal comme décrit dans l'équation (4.24) ou du nombre limite de tentatives de retransmission atteint comme décrit dans l'équation (4.25).

$$P_{fe} = \sum_{j=0}^n P_c (1 - \beta) b_{i,-1,n} = \frac{x^{n+1}(1 - y^{n+1})}{1 - y}. \quad (4.24)$$

$$P_{fr} = \sum_{j=0}^n x b_{m,0,j} = y^{n+1}. \quad (4.25)$$

L'expression de la fiabilité associée à CSMA/CA slotté est donnée par l'équation (4.26)

$$F = 1 - P_{fe} - P_{fr}. \quad (4.26)$$

4.3.2 Énergie consommée

Dans ce modèle, nous nous intéressons à l'énergie consommée dans le cas d'une transmission réussie. Soient :

- 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,
- P_{rec} l'énergie consommée pendant l'état de réception.

A partir des équations (4.14) et (4.16), la consommation moyenne d'énergie est donnée par l'équation (4.27).

$$E = P_i \sum_{i=0}^m \sum_{k=1}^{W_i-1} \sum_{j=0}^n b_{i,k,j} + P_{cca} \sum_{i=0}^m \sum_{j=0}^n (b_{i,0,j} + b_{i,-1,j}) + P_i \sum_{j=0}^n (b_{-1,L_p,j} + b_{-2,L_p,j}) + \quad (4.27)$$

$$P_{tm} \sum_{k=0}^{L_p-1} \sum_{j=0}^n (b_{-1,k,j} + b_{-2,k,j}) + \sum_{j=0}^n \sum_{k=L_p+1}^{L_p+L_{ack}+1} (P_{rec} b_{-2,k,j} + P_i b_{-1,k,j}).$$

4.3.3 Débit

Le débit 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.

- Soit P_b la probabilité que le canal soit occupé donnée par l'expression (4.28).

$$P_b = 1 - (1 - \tau)^N. \quad (4.28)$$

- Soit P_s la probabilité d'une transmission réussie donnée par l'expression (4.29).

$$P_s = \frac{N\tau(1 - \tau)^{N-1}}{P_b}. \quad (4.29)$$

Alors, le débit est obtenu par l'équation (4.30).

$$Db = \frac{L_p P_b P_s}{\sigma(1 - P_b) + T_s P_b P_s + T_c P_b (1 - P_s)}. \quad (4.30)$$

où

- T_s est la durée d'une transmission réussie qui est donné comme suit :

$$T_s = L_p + T_{PHY} + T_{MAC} + 2T_{CCA} + T_{LIFS} + t_{ack-wait} + t_{ack}. \quad (4.31)$$

- T_c la durée d'une transmission non réussie qui est donné comme suit :

$$T_c = L_p + T_{PHY} + T_{MAC} + 2T_{CCA} + T_{LIFS} + t_{ack-wait}. \quad (4.32)$$

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

4.3.4 Délai

Le délai est défini comme l'intervalle de temps à partir de l'instant d'arrivée du paquet jusqu'à la réception de son ACK. Il est donné par l'équation (4.33) :

$$D = T_{ds} + E[T_h] + \left(\frac{y}{1-y} - \frac{(n+1)y^{n+1}}{1-y^{n+1}} \right) (T_{df} + E[T_h]). \quad (4.33)$$

$E[T_h]$ indique le délai approximatif du backoff défini comme suit :

$$E[T_h] = 2T_b \left[1 + \frac{1}{4} \left(\frac{1-\gamma}{1-\gamma^{m+1}} \left(2W_0 \frac{1-(2\gamma)^{m+1}}{1-2\gamma} - \frac{3(m+1)\gamma}{1-\gamma} \right) + \frac{3\gamma}{1-\gamma} - (W_0 + 1) \right) \right]. \quad (4.34)$$

Où

- T_{ds} est le temps nécessaire pour une transmission réussie.
- T_{df} indique le temps pris pour une transmission non réussie.
- T_b est la durée d'une unité backoff.
- $\gamma = \max(\alpha, \beta(1-\alpha))$.

4.4 Analyse de performances des mécanismes S-CSMA

4.4.1 Méthode d'analyse et logiciels utilisés

A partir du modèle analytique proposé dans la section précédente (voir section 4.2), nous allons dans un premier lieu résoudre le système d'équations non linéaire formé par les expressions S_1 , S_2 , S_3 , P_c et τ en utilisant les deux logiciels Mathcad et Matlab pour obtenir les résultats numériques de CSMA/CA slotté (S-CSMA). Dans un second lieu, nous calculons les expressions de la fiabilité, de délai, de débit et de l'énergie consommée dans un trafic saturé et dans des conditions de canal idéal. Par la suite, nous faisons une comparaison avec le mécanisme IEEE 802.15.4 S-aloha en termes de fiabilité, de consommation énergétique, de débit et de délai moyen.

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 l'évaluation des performances de CSMA/CA slotté

Paramètre	Valeur	Paramètre	Valeur	Paramètre	Valeur
n	3	$aMaxSIFS FrameSize$	18 bytes	$t_{ack-wait}$	[1 – 1.32] ms
m	4	$aMaxSIFS Period$	12 symbols	P_{trans}	30 mW
L_p, N	Variants	$MAC header length$	16 bytes	P_i	0.8 mW
W_0	8	$PHY header length$	6 bytes	P_{rec}	40 mW
$macMinBE$	3	T_{LIFS}	0.32 ms	P_{cca}	40 mW
$L_s = L_c$	80 bytes	T_b	0.32 ms	σ	0.96 ms
L_{ack}	20 bytes	t_{ack}	1 ms		

4.4.3 Résultats, analyses et comparaisons

La figure 4.2 trace la fiabilité en fonction du nombre de nœuds dans le réseau, pour les deux protocoles, IEEE 802.15.4 S-aloha et IEEE 802.15.4 S-CSMA. Lorsque le nombre de nœuds augmente, la fiabilité associée à S-aloha diminue. Ceci est dû au fait que beaucoup de nœuds transmettent sans vérifier l'état du canal. Par contre la fiabilité associée à S-CSMA reste stable en augmentant la

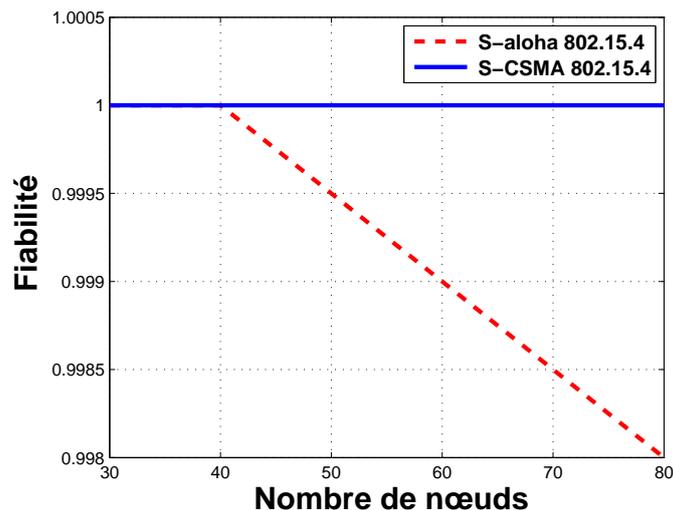


FIGURE 4.2 – Fiabilité Vs Taille du réseau, avec $L_p = 100$ bytes

taille du réseau car ce mécanisme procède à minimiser les collisions. Nous notons que la fiabilité de S-CSMA est meilleure que celle de S-aloha car les nœuds ayant des paquets à transmettre en

utilisant le mécanisme CSMA/CA écoute le canal avant de transmettre, et une fois le canal est libre il n'y aurait plus de collision donc on aura une fiabilité élevée.

La variation de la fiabilité en fonction de la taille du réseau pour différentes tailles de paquets ($L_p = 20 \text{ bytes}$ et $L_p = 100 \text{ bytes}$) est illustrée dans la figure 4.3. Lorsque la longueur des paquets

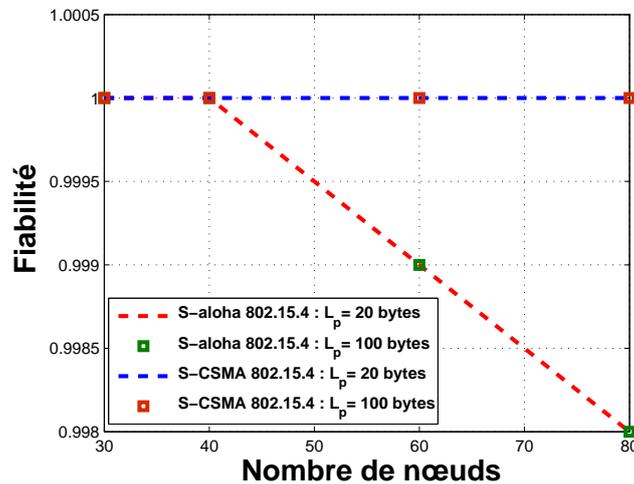


FIGURE 4.3 – Fiabilité Vs Taille du réseau & variant la Taille des paquets L_p .

devient de plus en plus importante, 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 le S-CSMA est meilleure que celle de S-aloha quelque soit la taille du réseau et la taille des paquets car en raison de la technique d'écoute du canal.

La figure 4.4 illustre la variation de l'énergie en fonction du nombre de nœuds dans le réseau. Lorsque la taille du réseau devient de plus en plus importante, l'énergie consommée diminue. Cette

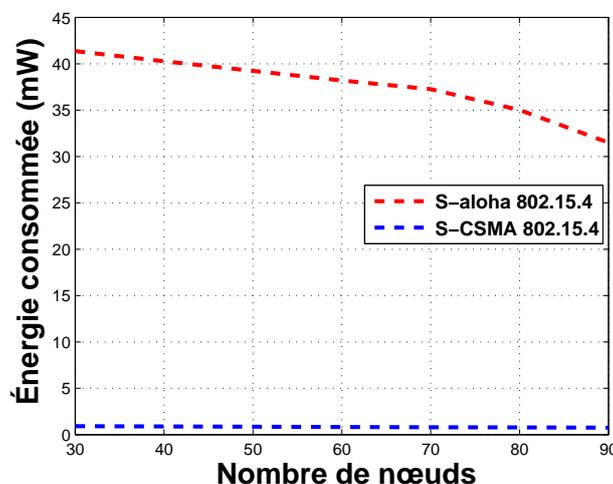


FIGURE 4.4 – Énergie Vs Taille du réseau, avec $L_p = 100 \text{ bytes}$.

diminution est dû au fait que les nœuds consomment moins d'énergie lorsque le canal est détecté occupé. L'énergie associée à S-aloha est clairement plus élevée que celle associée à S-CSMA car dans Aloha le nœud transmet sans écouter l'état du canal ce qui provoque une haute consommation d'énergie.

L'énergie consommée en fonction du nombre de nœuds pour différentes tailles des paquets ($L_p = 20 \text{ bytes}$ et $L_p = 100 \text{ bytes}$) est représentée dans la figure 4.5. Avec l'augmentation du nombre

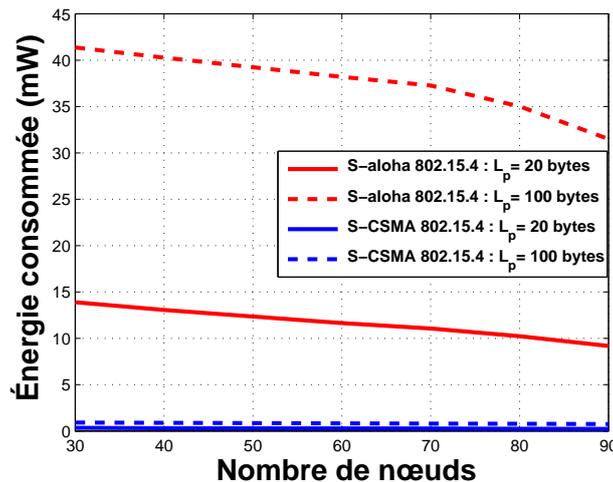
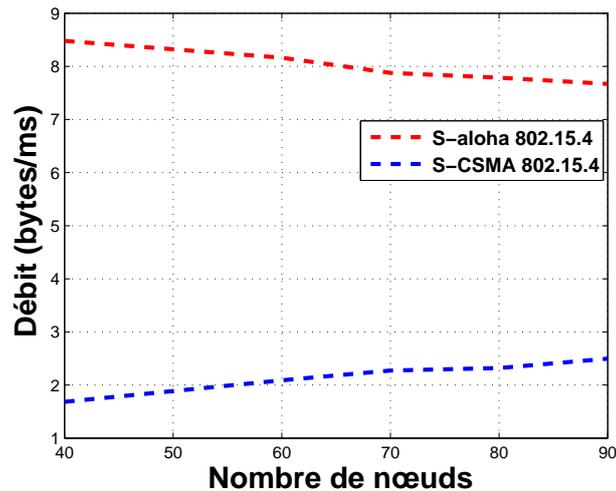


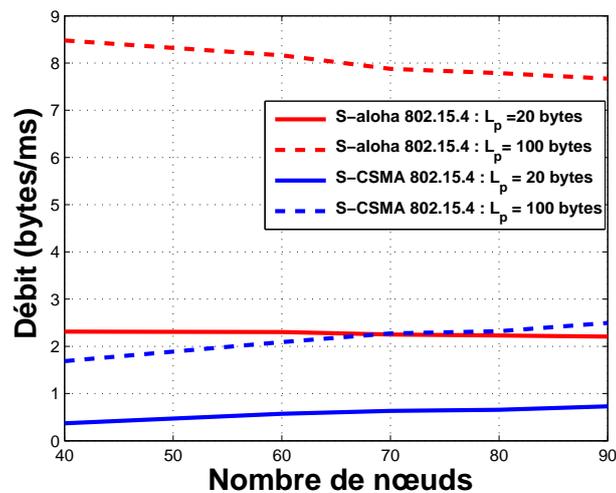
FIGURE 4.5 – Énergie Vs Taille du réseau & variant la taille des paquets L_p .

de nœuds, nous remarquons une diminution de l'énergie pour les deux mécanismes. Lors d'une grande taille des paquets, l'énergie consommée devient plus importante, également pour les deux mécanismes, car le paquet prend beaucoup de temps dans l'état transmission et réception. L'énergie consommée dans S-CSMA est inférieure à celle dans S-aloha, car le mécanisme S-CSMA fait en sorte de minimiser l'énergie consommée en utilisant la technique d'écoute du canal qui permet d'éviter les collisions.

La figure 4.6 montre la variation de débit en fonction de la taille du réseau pour une taille des paquets ($L_p = 100 \text{ bytes}$). Nous remarquons que le débit augmente lorsque le nombre de nœuds augmente dans le réseau pour le mécanisme S-CSMA/CA car la bande passante est utilisée d'avantage. Par contre, pour le S-Aloha nous constatons que le débit diminue en augmentant la taille du réseau, ceci est dû au fait que la probabilité de collisions augmente en raison de l'absence de la technique d'écoute du canal. Ce qui conduit à une transmission non réussie des paquets. Le débit obtenu par le mécanisme IEEE 802.15.4 S-Aloha est plus grand que celui de 802.15.4 S-CSMA pour un réseau de grande taille.

FIGURE 4.6 – Débit Vs Taille du réseau, avec $L_p = 100$ bytes.

La figure 4.7 trace le débit en fonction du nombre de nœuds pour différentes tailles des paquets ($L_p = 20$ bytes et $L_p = 100$ bytes). Avec l'augmentation de la taille du réseau, une augmentation du débit est observée pour le mécanisme S-CSMA car la bande passante est de plus en plus utilisée lorsque le nombre de nœuds est grand. Nous constatons aussi que le débit offert par les nœuds ayant une taille ($L_p = 100$ bytes) est supérieur à celui des paquets ayant une taille ($L_p = 20$ bytes) pour les deux mécanismes, car la quantité de données transmise est importante. Le débit augmente au fur et à mesure que le nombre de nœuds dans le réseau augmente pour le S-CSMA/CA donc il offre un débit plus élevé. Mais malgré que le débit offert par le S-Aloha diminue mais il reste comme même meilleur que celui offert par le S-CSMA.

FIGURE 4.7 – Débit Vs Taille du réseau & variant la taille du paquet L_p .

Avec l'augmentation de la taille du réseau, le délai augmente pour les deux mécanismes, comme le montre la figure 4.8. La raison est qu'un nombre de nœuds élevé engendre des collisions qui conduisent à des retransmissions. Sans oublier que le nœud va d'abord doubler la fenêtre de backoff

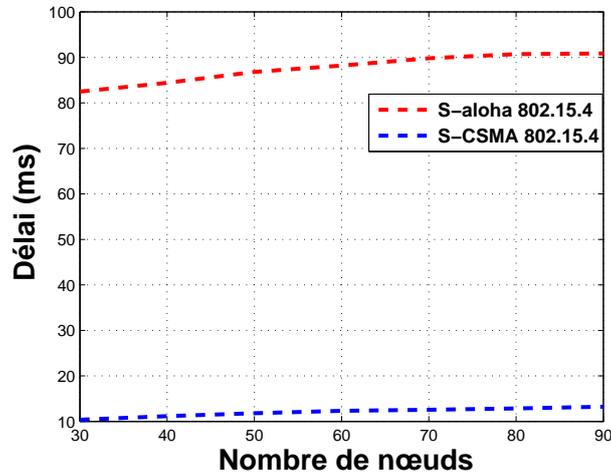


FIGURE 4.8 – Délai Vs Taille du réseau, avec $L_p = 100$ bytes.

puis retransmettre. Tous ceci fait que le nœud prend plus de temps à transmettre son paquet lorsque la taille du réseau augmente. Le délai pris par S-aloha est beaucoup plus élevé par rapport à celui de S-CSMA car en utilisant le mécanisme Aloha les nœuds transmettent à plusieurs reprises sans détecter l'état du canal, et par conséquent beaucoup de collisions se produisent ce qui conduit à une retransmission et donc un délai en plus.

Dans la figure 4.9, 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

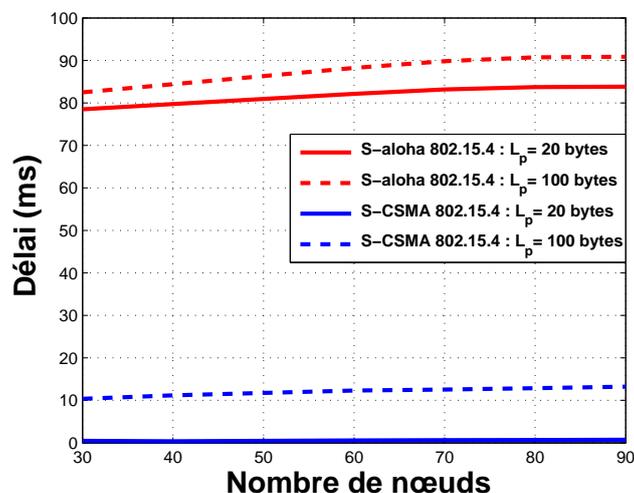


FIGURE 4.9 – Délai Vs Taille du réseau & variant la Taille des paquets L_p .

délai augmente, car la durée de transmission de ces paquets devient grande. S-aloha offre un délai plus élevé par rapport à S-CSMA en raison d'absence de la technique d'écoute du canal.

4.5 Conclusion

Dans ce dernier chapitre, nous avons présenté un modèle analytique basé sur une chaîne de Markov pour analyser les performances du mécanisme CSMA slotté de IEEE 802.15.4. Le modèle de chaîne de Markov proposé est à trois dimensions, il prend en compte un nombre fixe de nœuds, 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 pour les nœuds utilisant le mécanisme S-CSMA de la norme IEEE 802.15.4 pour l'accès au médium. Ensuite, nous avons analysé l'impact de la variation de la fiabilité, de l'énergie, du débit et du délai, tout en variant la taille du réseau ainsi que la taille des paquets, pour tester l'efficacité du modèle sur les métriques étudiées.

Nous observons que S-CSMA permet de réduire la consommation d'énergie, le débit et le délai moyen par rapport au S-aloha. Tandis qu'une importante fiabilité est observée. En effet, à mesure que l'on augmente le nombre de nœuds, S-CSMA offre une fiabilité élevée par rapport à S-aloha, une énergie réduite, un débit réduit et un délai moyen réduit. Aussi pour une grande taille de paquet, il offre une fiabilité maximale égale à 1, un délai moyen élevé, et une consommation d'énergie importante.

Conclusion générale

Les réseaux de capteurs sans fil (RCSFs) sont une nouvelle technologie qui a surgi après les grands progrès technologiques concernant le développement des capteurs intelligents, des processeurs puissants et des protocoles de communications sans fil. Ce type de réseau composé de certains ou de milliers d'éléments, a pour but la collecte de données de l'environnement, leur traitement et leur dissémination vers le monde extérieur. Le standard IEEE 802.15.4 est un protocole de communication défini par l'IEEE. Il est destiné aux réseaux sans fil de la famille des LR-WPANs (Low Rate Wireless Personal Area Networks) du fait de leur faible consommation énergétique, de leur faible portée et du faible débit des dispositifs utilisant ce protocole. Le standard IEEE 802.15.4 fournit les spécificités et les protocoles des couches basses physique et MAC du modèle OSI.

L'objectif de ce travail été de proposer des modèles analytiques pour les mécanismes MAC de la norme IEEE 802.15.4 dédiés aux applications des réseaux de capteurs sans fil, d'évaluer leurs performances et de faire une comparaison entre les performances des deux protocoles MAC proposés.

Le premier modèle proposé est un modèle de chaîne de Markov pour le mécanisme IEEE 802.15.4 Aloha élaboré un trafic saturé, sous un canal idéal, tenant compte du mécanisme d'accusé de réception et des limites de retransmission. 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. Les résultats montrent que S-aloha 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. Le deuxième modèle présenté est un modèle de chaîne de Markov modélisant le IEEE802.15.4 CSMA/CA slotté dans un trafic saturé, sous un canal idéal, tenant compte du mécanisme d'accusé de réception et des limites de retransmission. Le modèle proposé a permis de dériver les expressions des métriques de performance à savoir : le délai moyen de transmission avec succès, l'énergie consommée, la fiabilité et le débit. Pour prouver l'efficacité de notre modèle, nous avons analysé l'impact de la variation du nombre de nœuds, et de la longueur des paquets sur les métriques étudiées. Nous observons que S-CSMA offre, une énergie réduite, un débit faible, un délai moyen faible

ainsi qu'une fiabilité élevée en le comparant à S-aloha.

Comme perspectives de recherche, nous proposons les points suivants :

- Extension de nos modèles proposés dans le cas du trafic non saturé ;
- Modélisation et évaluation des performances des mécanisme Aloha et CSMACA dans le mode non beacon (version non slotté) ;
- Analyse comparative entre les mécanismes CSMA/CA non slotté et ALOHA non slotté ;
- Étude d'autres amendements de la norme IEEE 802.15.4 concernant le niveau physique et MAC.

Bibliographie

- [1] 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.
- [2] 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.
- [3] H. Wen, C. Lin, Z.-J. Chen, H. Yin, T. He and E. Dutkiewicz, “An improved markov model for ieee 802.15. 4 slotted csma/ca mechanism”, Journal of computer science and technology, vol 24, pp 495–504, Springer, 2009.
- [4] D. Yin and T. T. Lee, “Performance analysis of markov modulated ieee 802.15. 4 beaconable mode”, Wireless networks, vol 19, pp 1709–1724, Springer, 2013.
- [5] 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.
- [6] “Chapitre 1 : Présentation générale des réseaux sans fil”. <https://zenodo.org/record/1038504/files/Chapitre%201%20les%20technologies%20sans%20fils.pdf>.
- [7] S. Touloum, “Modelisation et optimisation dans les Reseaux de Capteurs sans fil”, Thèse de Doctorat, Université de Bejaia, Algérie, 2020.
- [8] A. I.F, S. Weilian, S. Y and C. E, “A survey on sensor networks”. In *IEEE Communications Magazine*, pp 102–114, 2002.
- [9] I. Mohammad and M. Imad, “Handbook of sensor networks. chapter 15 : Compact wireless and wired sensing systems”, vol 10, pp 1–860, CRC Press, 2005.
- [10] S. Athmani, “Protocole de sécurité Pour les Réseaux de capteurs Sans Fil”, Thèse de Doctorat, Université Hadj Lakhder - Batna, Algérie, 2010.

- [11] 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 Personal Communication*, vol 115, pp 527—556., Springer, 2020.
- [12] 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.
- [13] H. M. A. Fahmy, “Wireless Sensor Networks : Energy Harvesting and Management for Research and Industry”, pp 12–23, Springer International Publishing, 2020.
- [14] 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.
- [15] “Zigbee specification.”. <http://www.zigbee.org.ZigBee>, 2004.
- [16] “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.
- [17] L. Alkama, “Evaluation et optimisation des performances des réseaux de capteurs d’infrastructures critiques IEEE 802.15.4k”, Thèse de Doctorat, Université de Bejaia, Algerie, 2020.
- [18] C. Ouanteur, “Evaluation de performances des Réseaux de capteurs sans fil IEEE 802.15.4”, Thèse de Doctorat, Université de Bejaia, Algérie, 2017.

Résumé

Le domaine des réseaux de capteurs sans fils est considéré comme l'une des technologies contemporaines les plus prometteuses. Il s'est créé pour offrir des solutions économiquement intéressantes et faciles à déployer pour la surveillance à distance et au traitement des données dans les environnements complexes et distribués. Un réseau de capteurs sans fil est constitué d'un ensemble de nœuds qui ont des capacités de mesures, de stockage, de traitement des données et de communication sans fil. De nombreuses applications telles que les applications militaires, la surveillance de l'environnement et le suivi de biens ou de personnes,... présentent le besoin commun d'être constituées de réseaux composés de nœuds à faible débit, à faible coût et à faible consommation énergétique. D'où l'apparition des RCSFs. Le standard IEEE 802.15.4 représente le meilleur compromis pour les réseaux de capteurs sans fil. Dans ce travail, Nous allons nous baser sur l'analyse de performances des mécanismes MAC proposés par la norme IEEE 802.15.4, à savoir Aloha slotté et CSMA/CA slotté. L'analyse des résultats nous permettra de définir les paramètres ayant un impact sur les performances du réseau. Pour ce faire, nous proposons une modélisation analytique par chaîne de Markov pour le mécanisme ALOHA slotté de la norme IEEE 802.15.4 qui est le premier dans la littérature considérant un mode beacon, un trafic saturé et un canal idéal. Notre modèle est capable d'estimer la fiabilité, l'énergie consommée, le débit et le délai. Par la suite, une évaluation de l'effet de quelques paramètres sur les performances du réseau est effectuée. Enfin, nous constatons que CSMA/CA offre par rapport à ALOHA, une meilleure fiabilité, une énergie consommée minimale, un délai très petit et un débit de données élevé. Avec l'augmentation de la taille du réseau et de la taille des paquets, de très bons résultats sont obtenus, à partir duquel on constate que CSMA/CA est le plus adapté.

Mots clés: Réseaux de capteurs sans fils, IEEE 802.15.4, Aloha slotté, CSMA/CA slotté, Chaîne de Markov, Evaluation de performances.

Abstract

The field of wireless sensor networks is considered to be one of the most promising contemporary technologies. It was created to offer economically attractive and easy to deploy solutions for remote monitoring and data processing in complex and distributed environments. A wireless sensor network is made up of a set of nodes that have wireless measurement, storage, data processing and communication capabilities. Many applications such as military applications, environmental monitoring and tracking of goods or people, ... have the common need to be constituted of networks composed of low speed, low cost and low nodes. energy consumption. Hence the appearance of WSNs. The IEEE 802.15.4 standard represents the best compromise for wireless sensor networks. In this work, we will be based on the performance analysis of MAC mechanisms proposed by the IEEE 802.15.4 standard, namely slotted Aloha and slotted CSMA/CA. Analysis of the results will allow us to define the parameters that have an impact on the performance of the network. To do this, we propose an analytical Markov chain modeling for the slotted ALOHA mechanism of the IEEE 802.15.4 standard which is the first in the literature considering a beacon mode, a saturated traffic and an ideal channel. Our model is able to estimate reliability, energy consumed, throughput and delay. Subsequently, an evaluation of the effect of some parameters on the performance of the network is carried out. Finally, we find that CSMA/CA offers compared to ALOHA, better reliability, minimal power consumption, very small delay and high data throughput. With the increase in network size and packet size, very good results are obtained, from which CSMA/CA is found to be the most suitable.

Keywords: Wireless sensor networks, IEEE 802.15.4, Slotted Aloha, Slotted CSMA/CA, Markov chain, performance evaluation.
