N° d'ORDRE : **30 / 2012-M / EL**

République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieure et de la Recherche Scientifique

Université des Sciences et de la Technologie Houari Boumediene

Faculté d'Électronique et d'Informatique

MEMOIRE

Présenté pour l'obtention du diplôme de MAGISTER

EN : ELECTRONIQUE

Spécialité : Traitement du Signal et des Images

Par : MOHAMEDATNI Yassine

Sujet

Développement d'algorithmes d'anticolisions pour les Systèmes RFID Passifs.

Soutenu publiquement le 01 /03/2012 , devant le jury composé de :

Mme TOUHAMI Rachida	Professeur, à l'USTHB	Présidente
Mr B.FERGANI	Maitre de conférences /A, à l'USTHB	Directeur de mémoire
Mr A. AMROUCHE	Maitre de conférences /A, à l'USTHB	Examinateur
Mme A. SERIR	Maitre de conférences /A, à l'USTHB	Examinatrice
Mr A.HAMZA	Maitre de conférences /B, à l'USTHB	Invité

REMERCIEMENTS

Je voudrais sincèrement exprimer mes plus vifs remerciements et ma gratitude à mon encadreur Belkacem Fergani, Maitre de conférences à l'USTHB, pour sa précieuse aide et son suivi permanent durant toute la période du projet.

Je tiens à exprimer ma profonde gratitude et mes remerciements les plus vifs à Madame Rachida TOUHAMI, Professeur à l'USTHB, pour avoir fait l'honneur d'accepter de présider le jury de cette soutenance.

Je tiens à remercie les membres de jury : M.*AMROUCHE Abderrahmane, Maitre de conférences à l'USTHB, Mme SERIR Amina, Maitre de conférences à l'USTHB qui ont bien voulu d'accepter d'examiner ce travail.*

Je remercie également Monsieur HAMZA Abdelkrim Maitre de conférences à l'USTHB d'accepter l'invitation et pour son aide et ses conseils.

J'adresse aussi mes remerciements à tous mes amis qui m'ont soutenu durant cette période.

Un merci tout spécial va également à Madame Belhadj, Professeur à l'USTHB, et à tous les enseignants qui ont contribué à ma formation et à tous mes camarades de l'USTHB.

Table des matières

Table des figures

Table des tableaux

Introduction Générale

L'identification sans contact est en pleine effervescence. Qu'il s'appuie sur une liaison optique, infrarouge, hyperfréquence ou plus fréquemment sur une liaison radiofréquence, le « sans contact » est appelé à un avenir rayonnant.

Badges d'accès, cartes bancaires, télépaiement, identification de bagages, identification de livres en bibliothèque, localisation de matériels en magasin, suivi du stock en rayon et changement de prix à distance, voilà un petit échantillon de ce que le « sans contact » permet de réaliser.

Les nouvelles technologies, de par leur plus grande souplesse, et leur grande capacité de stockage d'informations rendent l'échange d'information nettement plus rapide et efficace. Elles devraient remettre en question le processus d'identification automatique par code barre actuellement largement utilisé. En effet, le développement des systèmes d'identification automatique par RFID devrait bientôt permettre l'identification individuelle et unique des objets et mener à la création d'un « Internet des objets » : une prolongation de l'internet que nous connaissons au monde réel.

Les premiers systèmes RFID passifs qui ont vu le jour fonctionnent dans des bandes de fréquences basses et sont aujourd'hui largement employés. Ils ont ouvert la voie vers le développement d'une nouvelle technologie RFID, plus performante et faible coût, fonctionnant à des fréquences plus élevées. L'identification est réalisée par des tags (aussi appelés « étiquettes intelligentes ») qui sont associés aux objets à identifier. Ces derniers sont constitués d'une puce électronique et d'une antenne. Contrairement aux systèmes de communication classiques, ils sont alimentés à distance et ne possèdent aucune source propre d'émission radiofréquence, on les qualifie alors de systèmes passifs. Et un lecteur dont la mission de récupérer l'information portée par l'étiquette.

Les signaux d'identification reçus par le lecteur sensé identifié chacun des objets portant une étiquette RFID, se mélangent et s'interfèrent ce qui complique la tâche du lecteur quant à la discrimination des informations individuelles de chacun des objets. C'est le problème de la collision de signaux provenant des étiquettes. Pour le résoudre, le lecteur RFID doit mettre en œuvre une procédure (un algorithme) d'anticollision permettant de séparer les signaux émanant de chaque étiquette afin de récupérer leurs codes EPC respectifs.

L'objectif de ce mémoire de Magister est de faire une étude bibliographique détaillée de l'état de l'art des algorithmes d'anticollisions puis de faire étude comparative des performances de quelques uns d'entre eux. Pour ce faire, ce mémoire est organisé comme suit : Dans le premier chapitre, nous réalisons une présentation générale de la RFID et des différentes technologies de radio-identification existantes. Nous ferons un état de l'art des systèmes RFID passifs en mettant l'accent sur les procédés physiques mis en œuvre et les avantages de cette technologie. Le second chapitre se veut une étude bibliographique détaillée des algorithmes (protocoles) d'anticollision. Nous présentons aussi une taxonomie de ces protocoles selon le type d'interférences. Le troisième chapitre concerne les techniques d'accès multiple dans le contexte des systèmes RFID. Nous mettons l'accès notamment sur la technique CDMA. Nous analysons son apport à la résolution du problème de collision comparativement avec les autres algorithmes de l'état de l'art. Le quatrième chapitre est dédié à la simulation et l'évaluation des performances comparées des protocoles d'anticollision mis en œuvre.

Finalement, la conclusion résumera l'ensemble des travaux de ce mémoire et présentera les perspectives envisagées.

Chapitre 1

La technologie RFID

Introduction :

L'objectif de ce chapitre est de présenter la technologie RFID et tout particulièrement la technologie RFID passive. En premier lieu, il présente le dispositif sans contact, notamment les systèmes RFID. En second lieu, aborde l'état de l'art des systèmes RFID en présentant les protocoles de communications utilisés, l'architecture des lecteurs, et l'architecture des tags et enfin nous avons présentés une description générale de la chaine d'émission/réception.

I.1 Les briques d'un dispositif sans contact

I.1.1 Le transpondeur

Commençons tout d'abord par le transpondeur dans lequel sont conservées, d'une part dans une mémoire déportée (ROM, PROM, E2PROM, etc…) les données faisant partie de l'application considérée et, d'autre part, dans lequel est assuré le contrôle de la communication et la partie assurant la liaison RF [1].

I.1.2 L'air

L'air assure le médium de communication. Pour sa part, l'onde électromagnétique RF assure le transport des informations. L'air participe également au couplage (magnétique) entre les antennes du transpondeur et de la station de base [1].

I.1.3 La station de base

La station de base comprend une partie analogique ayant pour but d'assurer les réception et transmission des signaux RF, les circuits de gestion du protocole de communication avec le transpondeur, la gestion de la communication (gestion de possibles collisions, authentification, cryptographie, …..) et enfin, une interface assurant le dialogue avec le système hôte [1].

I.1.4 Le système hôte

Le système hôte (host) dont la fonction est d'assurer la gestion à plus haut niveau.

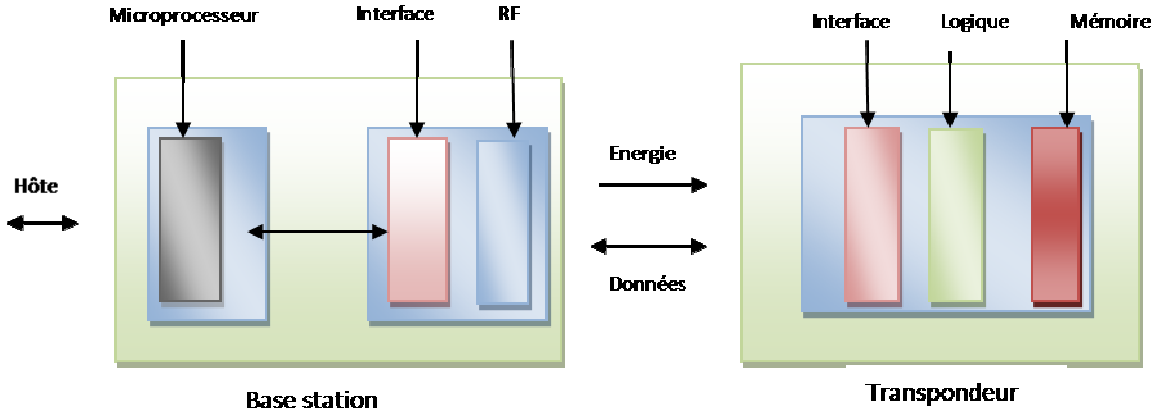


Figure I.1 Bloc diagramme d'un système « sans contact »

I.2 Principes généraux de fonctionnement du couple « station de base-transpondeur »

Dans le cadre des applications dans lesquelles l'élément déporté-le transpondeur-ne comporte pas de source locale d'alimentation à son bord et fonctionne donc par télé-alimentation [1].

I.2.1 Transfert, fourniture d'énergie et téléalimentation

A l'aide d'un signal électrique alternatif radiofréquence baptisé « porteuse », on crée, via l'enroulement que constitue l'antenne de la station de base, un champ magnétique permettant d'induire à distance une tension dans l'antenne du transpondeur qui, une fois redressée, servira d'alimentation locale à celui-ci [1].

I.2.2 Transfert de données de la station de base au transpondeur, « liaison montante »

Grace à la modulation de la porteuse effectuée à l'aide d'un flot binaire basé sur des codages bit spécifiques. On réussit à transmettre des ordres/commandes et des données au transpondeur [1].

I.2.3 Transfert de données du transpondeur à la station de base, « liaison descendante »

A l'aide d'une modulation réalisée par variation de la charge qu'il représente dans le champ, le transpondeur réussit à se faire comprendre de la station de base [1].

I.2.4 Transfert d'énergie

Pour que le transpondeur fonctionne, il est nécessaire qu'il soit alimenté, ce qui, dans le cas nous intéresse, sera à l'aide du principe de téléalimentation . le transfert d'énergie peut être effectué à l'aide d'un champ magnétique alternatif H(t) produit par la circulation d'un courant alternatif I(t) dans l'antenne de la station de base, selon la relation de la forme générale $H = NI$, formule dans laquelle N représente le nombre de spires par métre de l'antenne parcourue par le courant I. La valeur du champ magnétique est exprimée en ampères par mètre (A/m).

A ce champ magnétique correspond, dans le milieu dans lequel il se développe, une induction B(t) associée de forme générale $B(t) = \mu H(t)$, formule dans laquelle μ représente la perméabilité magnétique du milieu traversé [1].

Les lois de Biot-Laplace et Biot-Savart établissent la relation existant entre le courant I circulant dans un élément dl de circuit électrique de longueur l et l'intensité de l'induction magnétique B en fonction de la distance x existant entre le point de mesure et l'élément dl produisent le champ selon la formule :

$$\overrightarrow{dH} = \frac{(I.\vec{dl})\wedge\vec{u}}{4\pi x^2} \qquad (I.1)$$

Soit $\vec{B} = \frac{(\mu I)}{4\pi}\oint \frac{\vec{dl}\wedge\vec{u}}{x^2}$

I.2.5 Téléalimentaion

L'induction magnétique B entraine l'appariation d'un flux magnétiqueφ. A une distance d, dans un conducteur de section totale $S = N.s$ (N étant le nombre de spires), ce flux est égal à $\varphi = B(d).S$.

La variation instantanée de flux magnétique produit l'apparition d'une différence de potentiel induite, u(t), aux bornes de l'élément conducteur servant d'antenne de réception soumis à la variation du flux selon la relation bien connue $u(t) = -\frac{d\varphi}{dt}$. Voici pour l'essentiel de l'apparition d'une ddp aux bornes de l'antenne du transpondeur, ce qui correspond donc à une induction B présente aux abords du transpondeur généralement de l'ordre de quelques dizaines de nano teslas (nT) à quelques centaines de micro teslas (μT).

La qualité /quantité du transfert d'énergie dépend des fréquences sur lesquelles sont accordés les deux circuits d'antennes (base station et transpondeurs), de leurs précisions, tolérances, dérives, etc., du coefficient de couplage et les facteurs de qualité des circuits accordés de la base station et du transpondeur [1] .

I.3 L'identification par radio fréquence(RFID)

I.3.1 Historique de la RFID

La RFID est une technologie d'identification développée dans les années 1980. Bien qu'étant apparue dans les années 1950, elle ne connaît un essor que depuis les années 1990.

I.3.2 Le principe de fonctionnement des systèmes RFID

Le système RFID est composé de :

- Une étiquette ou tag intelligent (aussi appelé transpondeur), attaché à l'élément à identifier.
- Un lecteur ou station de base qui a pour but d'identifier le tag. Le lecteur envoie une onde électromagnétique en direction de l'élément à identifier. En retour, il reçoit l'information renvoyée par le tag.

Le fonctionnement général d'un système RFID est présenté dans la Figure .I.3 . Si le tag est dans la zone de lecture du lecteur, ce dernier l'active en lui envoyant une onde électromagnétique [3]. Le lecteur récupère l'information pour la traiter. Le tag est constitué d'une antenne et d'une puce électronique.

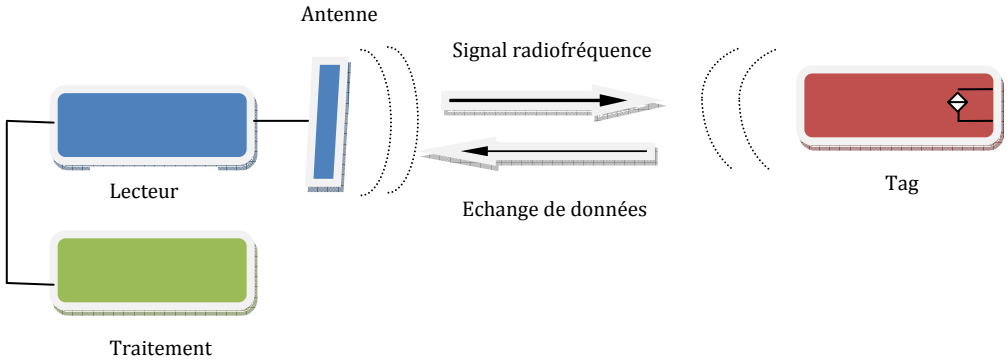


Figure I.2 Fonctionnement d'un système RFID

La différence entre les familles de systèmes RFID est la fréquence de fonctionnement. Les systèmes RFID utilisent des bandes de fréquences situées à : 125 kHz (bande BF, Basses Fréquences), 13,56 MHz (bande HF, Hautes Fréquences), 860-960 MHz (bande UHF, Ultra Hautes Fréquences), 2,45 GHz (bande micro-ondes) et 3,1-10,6 GHz (bande ULB, Ultra Large Bande, ou UWB, pour Ultra Wide Band).

I.4 Les systèmes RFID passifs

Nous allons présenter les types de communication et les architectures relatives à cette technologie.

I.4.1 Les types de communication

La communication du lecteur vers le tag est appelée liaison montante (uplink) et la réponse du tag vers le lecteur est appelée liaison descendante (downlink). La Figure. I.4 montre le principe d'une communication RFID.

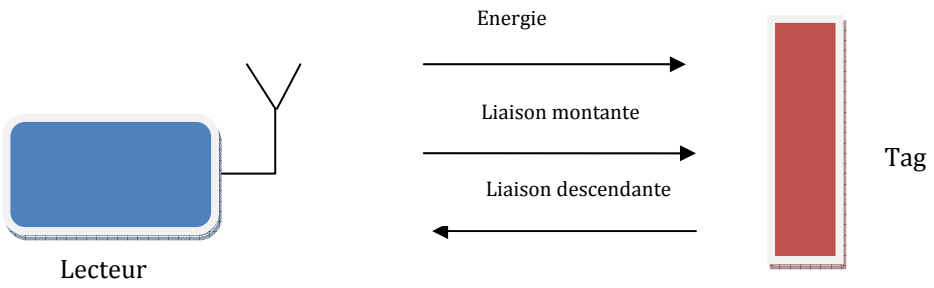


Figure I.3 Représentation schématique d'une communication RFID

Les deux principaux protocoles de communication entre un tag et un lecteur RFID sont : le protocole TTO (Tag Talk Only, signifiant que seul le tag transmet des données) et le protocole RTF (Reader Talk First, signifiant que le lecteur est maître dans la communication) . Le choix d'un protocole plutôt qu'un autre dépend de l'application visée. Dans le protocole TTO, il n'existe pas de liaison montante [7]. Un tag utilisant cette procédure transmet ses données de façon régulière lorsqu'il est alimenté. Cette procédure est particulièrement rapide. Elle permet de lire un grand nombre de tags RFID [17].

Lorsqu'un tag RTF entre dans la zone de lecture d'un lecteur, il attend une demande (requête) avant de transmettre son identifiant. On distingue également deux types de procédures de communication entre le lecteur et le tag : celles qui utilisent un transfert continu d'énergie et celles qui le font de manière séquentielle [17].

La communication est contrôlée au niveau du lecteur et du tag par une partie numérique qui reçoit et transmet les données par une interface radiofréquence.

I.4.2 Architecture des tags RFID passifs

I.4.2.1 Description de l'architecture d'un tag RFID passif

Un tag RFID passif est composé d'une antenne et d'une puce électronique. On peut distinguer dans cette dernière une partie radiofréquence (Front-end radio), et une partie numérique [10].

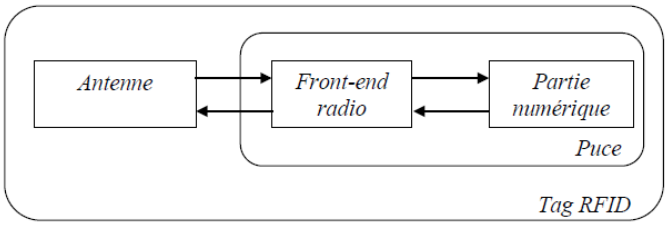


Figure I.4 Schéma fonctionnel d'une puce RFID

La partie numérique a pour rôle d'analyser les instructions reçues, de coder/décoder les informations et de répondre en envoyant ces données au front-end radio. La partie numérique est réveillée par le front end radio lorsque le niveau d'énergie recueillie par l'antenne est suffisant [17].

I.4.2.2 Description du front-end radio d'une puce RFID

Les fonctions principales du front-end radio sont: la récupération d'énergie, la réception du signal et la rétro-modulation (Fig. I.6)

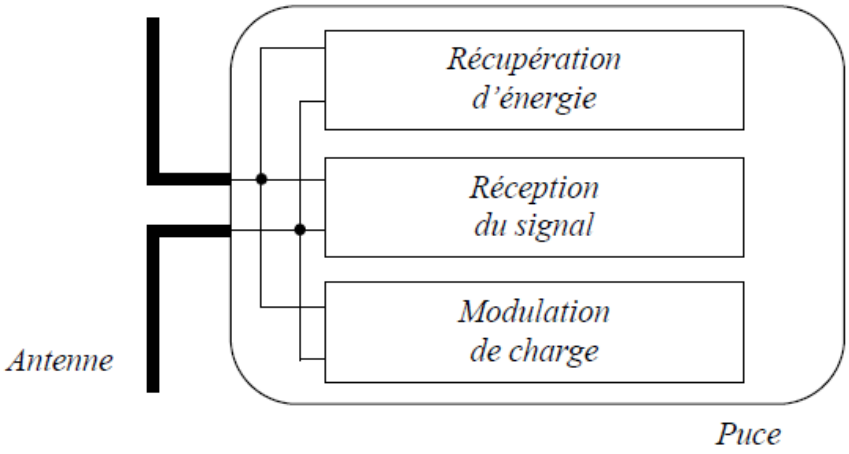


Figure I.5 Schéma bloc fonctionnel du front end radio d'un tag RFID UHF

I.4.2.2.1 Récupération d'énergie

La récupération d'énergie est assurée par un redresseur qui permet de récupérer une tension continue à partir de la porteuse radiofréquence reçue par l'antenne. C'est cette tension qui permet la téléalimentation du tag. Le redresseur est suivi d'un régulateur ou d'un limiteur de tension afin de stabiliser la tension et de protéger la puce des risques de surtension. Une capacité réservoir en sortie du redresseur assure l'alimentation de la puce durant la phase de rétro-modulation [9].

I.4.2.2.2 Récupération des données

La fonction de récupération des données transmises par le lecteur, est assurée par une chaîne de réception classique comprenant un démodulateur, un filtre en bande de base et un convertisseur analogique/numérique. Le décodage et le traitement de l'information sont réalisés par la partie numérique. [17].

I.4.2.2.3 Transmission des données par rétro-modulation

La rétro-modulation est assurée par un système de modulation de la charge à l'entrée de l'antenne. Cette dernière est commandée par la partie numérique du tag. La modulation de charge entraine une variation du coefficient de réflexion au niveau de l'interface entre l'antenne du tag et la puce. En d'autres termes, elle consiste en une variation de l'impédance d'entrée de la puce. Il est possible de faire varier la partie réelle et/ou la partie imaginaire de cette impédance. Ainsi, en fonction du signal binaire qui commande la modulation de charge et en fonction du type de modulation, le signal incident est plus ou moins réfléchi comme indiqué sur la Fig. I.6. Sur cette figure, l'impédance Zc représente une charge adaptée à l'impédance de l'antenne. En modulant la partie réelle de la charge (Figure I.7(a)), on réalise une modulation de type ASK. En modulant la partie imaginaire (Figure I.7(b)), on réalise une modulation de type PSK (Phase Shift Keying) [7] .

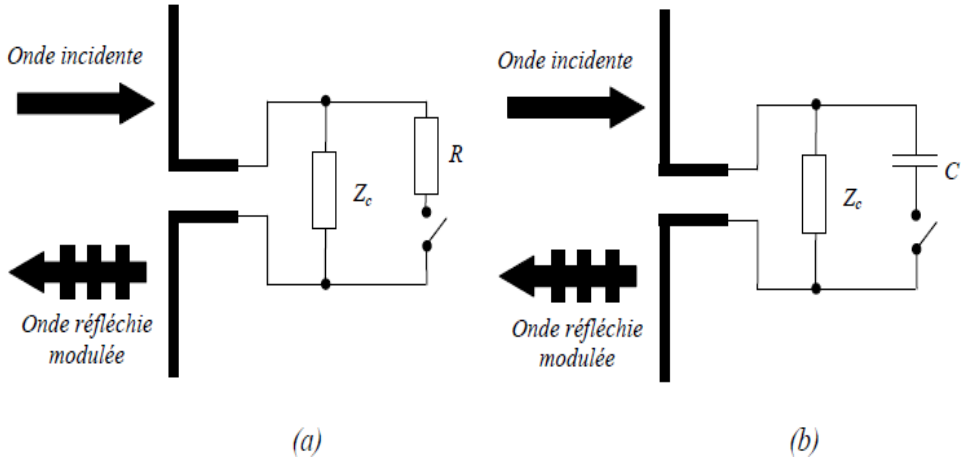


Figure I.6 Réflexion de l'onde incidente grâce à la technique de modulation de charge. (a) Modulation de la partie réelle. (b) Modulation de la partie imaginaire

I.4.3 Architecture des lecteurs RFID

Un lecteur RFID a pour rôle de gérer la communication avec les tags RFID. Un lecteur est composé de différentes fonctions illustrées sur la Figure. I.8 :

- Une unité de contrôle numérique. cette unité génère et met en forme le signal numérique contenant l'information à transmettre aux tags et traite en retour, la réponse de celui-ci [8].
- Un front-end radio constitué d'un émetteur et d'un récepteur radiofréquence. Cette partie est en charge de la génération d'une porteuse

radiofréquence, de sa modulation avec un signal numérique généré par l'unité de contrôle et de la démodulation de la réponse des tags [17].

- D'une ou plusieurs antennes permettant de transmettre et de recevoir les données, et de propager l'énergie radiofréquence télé-alimentant les tags [8,17].

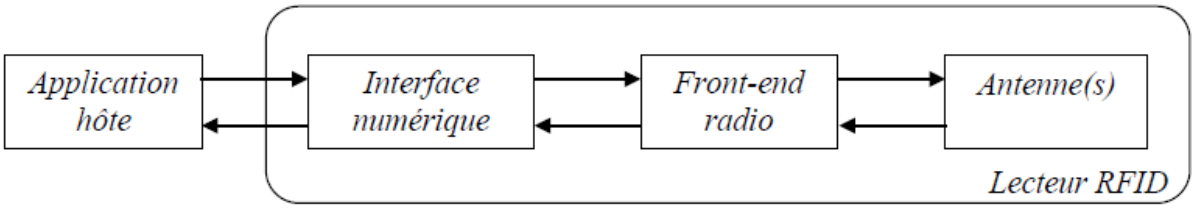


Figure I.7 Schéma fonctionnel d'un lecteur RFID

I.4.3.1 Description de la chaîne d'émission

La Figure. I.9 nous montre le schéma simplifié d'une chaîne d'émission d'un lecteur RFID. Les données arrivent codées de la partie numérique, elles sont modulées grâce à une porteuse générée par une PLL (Phase Locked Loop). Le signal modulé est ensuite amplifié puis filtré avant d'être transmis.

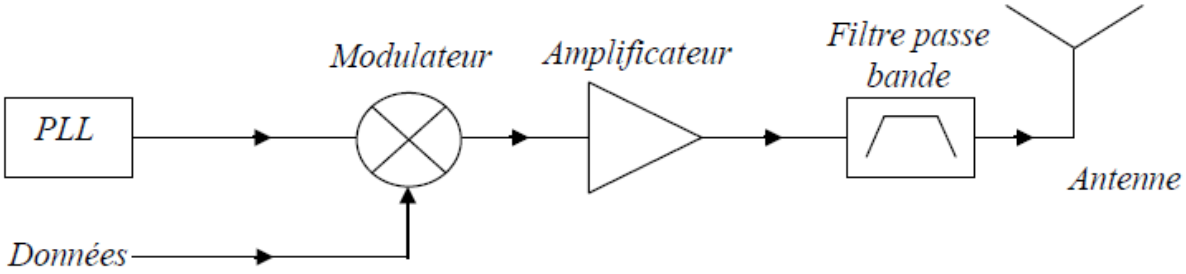


Figure I.8 Chaîne d'émission simplifiée d'un module UHF

I.4.3.2 Description de la chaîne de réception

La Fig. I.10 nous montre le schéma simplifié de l'architecture d'un récepteur. Le signal reçu est d'abord amplifié à l'aide d'un amplificateur faible bruit (LNA - Low Noise Amplifier), filtré, démodulé (souvent par un démodulateur I/Q) et numérisé par un convertisseur analogique / numérique.

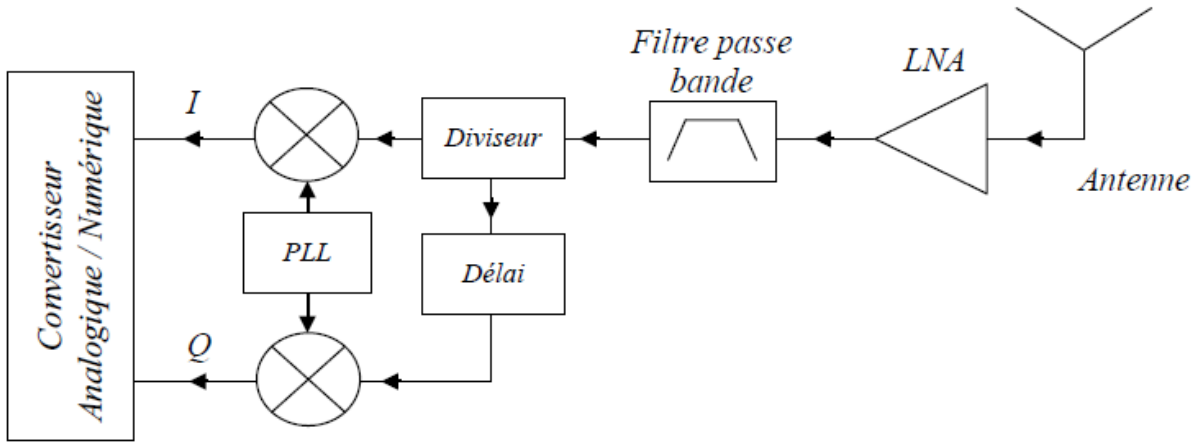


Figure I.9 Chaîne de réception simplifiée

I.4.4 Conclusion

Dans ce chapitre, après une présentation du dispositif sans contact, nous avons aborder la technologie RFID, où nous avons présenter un état de l'art des systèmes RFID passive. Où Nous avons présenté les architectures des lecteurs RFID et des tags. En suite nous avons présenté une description générale de la chaine d'émission/réception et de du système RFID.

Chapitre 2

LES ALGORITHMES D'ANTICOLLISION DANS LE SYSTEME RFID

Introduction

Dans l'identification par radiofréquence (RFID), les étiquettes (les Tags) mémorisent des identifications uniques et sont attachés à des objets, un lecteur effectue la procédure d'interrogation pour reconnaître un objet en émettant des signaux radio. Comme d'autres systèmes de communication sans fil, les systèmes RFID souffrent aussi du problème de brouillage du signal. Il existe deux types d'interférences. L'une est appelée collision lecteur, l'autre est appelée la collision tag. Les collisions ralentissent la procédure d'interrogation du tag. Par conséquent, les protocoles d'anticollision lecteur et d'anticollision tag sont tenus respectivement à réduire les collisions tags et les collisions lecteur pour améliorer les performances de la procédure d'interrogation. Dans ce chapitre, nous introduisons les protocoles d'anticollision lecteur et d'anticollision tag existants [14].

Quand un lecteur (ou interrogateur) transmet une requête à un tag, il fournit également de l'énergie pour alimenter un tag passif. Si le lecteur et le tag passif sont suffisamment proches, le lecteur peut recevoir le signal réfléchi par le tag. Pour une telle situation, nous disons que le tag se trouve dans la zone d'interrogation du lecteur.

Lorsque deux ou plusieurs lecteurs sont trop rapprochés ou bien plusieurs tags apparaissent dans la zone d'interrogation d'un même lecteur, il se produit des interférences, qui sont principalement classés comme le problème de collision lecteur et le problème de collision tag. Ci dessous, nous décrivons ces deux types de problèmes.

- **Le problème de collision lecteur (ou l'interférence lecteur):**

Le tag est excité par le lecteur dans la zone de réponse du tag (par exemple, la zone d'interrogation) est beaucoup moins large que la zone de transmission du lecteur (également appelé zone d'interférence). Quand un tag est dans la zone d'interrogation d'un lecteur A et dans la zone d'interférence d'un autre lecteur B, et en raison de l'interférence des lecteurs, ce tag ne peut pas recevoir la commande de

demande du lecteur A correctement ou le lecteur A ne peut pas interpréter la réponse correctement. C'est ce qu'on appelle le problème de collision lecteur. Par exemple, la figure II.1, le **tag T** se trouve dans la zone d'interrogation du lecteur A et dans la zone d'interférence du lecteur B. Le problème de collision lecteur se produit lors d'une telle situation [14].

- **problème de collision Tag:**

Pour identifier les tags au sein de la zone d'interrogation, un lecteur envoie une requête pour demander les tags de renvoyer leurs (IDs) identifiants. Lorsque plusieurs tags dans la zone d'interrogation du lecteur répondent à la demande simultanément, une collision se produit et le lecteur ne peut identifier aucun tag correctement. C'est ce qu'on appelle le problème de collision tag. Par exemple, la figure II.1, les tags **S** et **T** sont dans la zone d'interrogation du lecteur **A**. Si les tags **S** et **T** envoient leurs identifiants pour répondre à la demande de lecteur **A** en même temps, le problème de collision se produit et aucun tag ne peut être reconnu par le lecteur **A** [14].

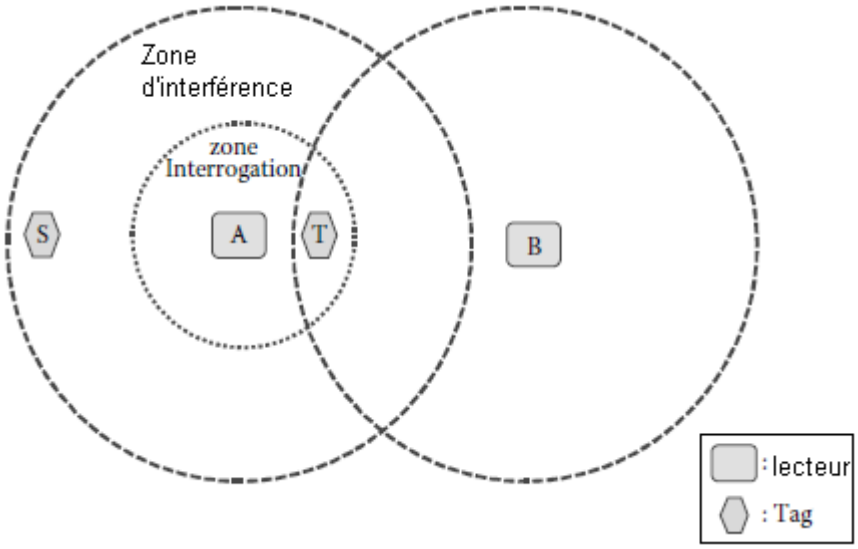


Figure II.1 la relation entre la zone d'interrogation et la zone d'interférence

Plusieurs protocoles d'anticollisions tag sont proposés pour réduire les collisions tag. Ils peuvent être classés principalement en trois catégories: Protocoles à base d'ALOHA, Protocoles à base d'arbre, et des protocoles à base de compteur.

En résumé, les protocoles d'anticollision lecteurs sont classés comme TDMA, FDMA, et les protocoles CSMA, tandis que les protocoles anticollisions tag sont classés comme suit : Les protocoles à base d'ALOHA, à base d'arbres et des protocoles à base de compteur.

Notre objectif est de proposer une étude comparative d'algorithmes d'anticollisions de signaux RFID passifs et de montrer l'intérêt apporté par l'application des techniques

d'étalement du spectre associés aux méthodes conventionnelles comme la technique ALOHA et ses différentes variantes.

Tableau II.1 les différents protocoles d'anticollision

Type de collision	Catégorie	Protocoles
COLLISION LECTEUR	TDMA	DCS
		Colorwave
	FDMA	HiQ
		EPCglobal Gen2
	CSMA	ETSI 302 208 Standard
COLLISION TAG	A BASE D'ALOHA	ALOHA
		Slotted ALOHA
		Frame Slotted ALOHA
		ISO/IEC 18000-6A
	A BASE D'ARBRE	QT
		Bit-by-bit binary tree
		EPCglobal Class0
		TSA
		BSQTA
		BSCTTA
		AQS (Adaptive Query spilitting)
	A BASE DE COMPTEUR	ISO/IEC 18000-6B
		ABS

II.1 Les approches d'anticollision dans les systèmes RFID

Les problèmes de collision lecteur sont subdivisés en problèmes de collision lecteur-tag et problèmes de collision lecteur-lecteur.

La collision lecteur-tag se produit lorsque le signal d'un lecteur voisin interfère avec les réponses des tags réservés à un autre lecteur.

La collision lecteur-lecteur se produit quand un tag entend plusieurs lecteurs en même temps. Dans cette situation, le tag peut être incapable de répondre à tous les lecteurs.

Les problèmes de collision dans les systèmes RFID se résument comme suit dans Figure. II.3:

- collision tag-tag dans la figure II.3 (a).
- collision lecteur-tag dans la figure II.3 (b).
- les collisions lecteur-lecteur dans la figure II.3 (c).

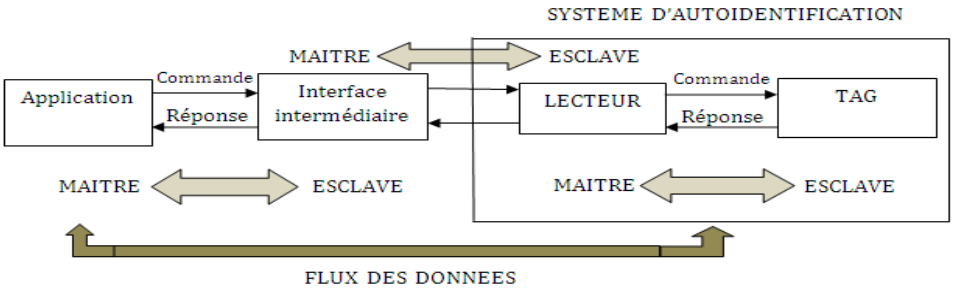


Figure II.2 Diagramme principale d'un système RFID

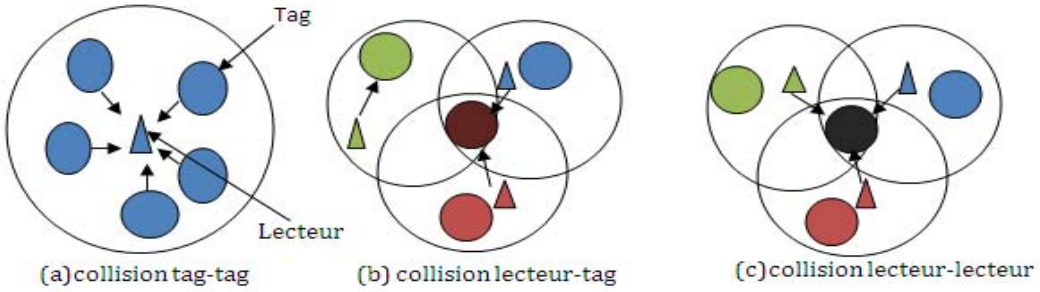


Figure II.3 les problèmes de Collisions dans le système RFID

De nombreuses procédures multi-accès d'anticollision ont été développées avec l'objectif de séparer les signaux de chaque Tag. Fondamentalement, il existe quatre procédures différentes : SDMA, FDMA, CDMA et TDMA.

La technique SDMA (Space Division Multiple Access) consiste à partager l'accès au canal de transmission selon des zones de l'espace. Ainsi une antenne (du lecteur) directionnelle rotative qui pointe vers différentes régions de l'espace permet de réaliser une SDMA. Il est vrai que la porté du lecteur est limitée dans l'espace mais permet d'atteindre un grand nombre de lecteurs séquentiellement.

La technique FDMA (Frequency Division Multiple Access) consiste à allouer une bande de fréquence à chaque utilisateur, l'inconvénient de cette technique est le coût élevé du lecteur ; Cette technique d'anticollision reste également limitée à quelques applications spécialisées.

La technique CDMA (Code Division Multiple Access).utilise la modulation d'étalement du spectre basé sur des codes d'étalement pseudo-aléatoires dans la bande complète des fréquences. Bien que le CDMA serait idéal pour l'anticollision, mais elle ajoute beaucoup de complexité des calculs.

La technique TDMA (Time Division Multiple Acces) est basée sur la répartition des ressources dans le temps. Les utilisateurs partagent la même bande passante et émettent les données dans différents intervalles de temps ou *time slot* qui leurs sont

alloués. Dans les systèmes RFID, le plus grand groupe des algorithmes d'anticollision sont basés sur la technique TDMA [15].

II.2 Les protocoles d'anticollision des Tags :

Plusieurs protocoles d'anticollision des tags sont proposés pour réduire les collisions des tags. Ils peuvent être classés en trois catégories: les protocoles à base d'ALOHA, les protocoles à base d'arbres et les protocoles à base de compteur. Ci-dessous, nous présentons quelques protocoles classe par classe.

II.2.1 Les protocoles à base d'ALOHA

Le canal de transmission se caractérise par sa " largeur de bande ", qui s'exprime dans le cas d'un signal numérique par un débit en bits ou en octets par seconde.

La durée d'émission de la trame (paquet de données) est fonction inverse du débit sur le réseau. Le " débit utile " est égal au nombre de bits que le réseau peut transmettre par seconde sans collision : c'est une fraction du débit total. Pour calculer la durée d'un transfert de fichier il faut soustraire à ce débit utile l'" overhead " provoqué par le découpage du fichier en trames (paquets) ainsi que par l'adjonction au contenu utile des adresses et contrôles. De tout cela découle que le débit utilisable pour transporter du contenu n'est qu'une fraction du débit physique offert par le réseau. Cette fraction sera d'autant plus élevée que le protocole est plus performant [31].

On peut représenter mathématiquement les performances de chaque protocole en partant des lois probabilistes des files d'attente. Appelons " durée de trame " la durée (fonction inverse du débit) de l'émission d'une trame par un ordinateur, et notons G le nombre moyen de trames émises pendant une durée de trame. Supposons que le nombre des trames émises pendant une durée de trames obéit à la loi de Poisson, qui rend compte des processus d'arrivée dans une file d'attente. La probabilité que le nombre des trames émises pendant une durée de trames soit égal à k est alors :

$$P(k) = G^k e^{-k}/k! \qquad \text{(II.1)}$$

Nous présenterons ci-dessous les deux protocoles de transmission sur réseau local qui ont été historiquement les premiers : " Aloha " et " Slotted ALOHA ". Etant simples, ils ont l'avantage de se représenter facilement sous forme mathématique ; la démarche qui a permis de passer du premier au second est un bon exemple du type de raisonnement que font les concepteurs de protocoles.

II.2.1.1 Le protocole ALOHA :

II.2.1.1.1 Le principe du protocole ALOHA

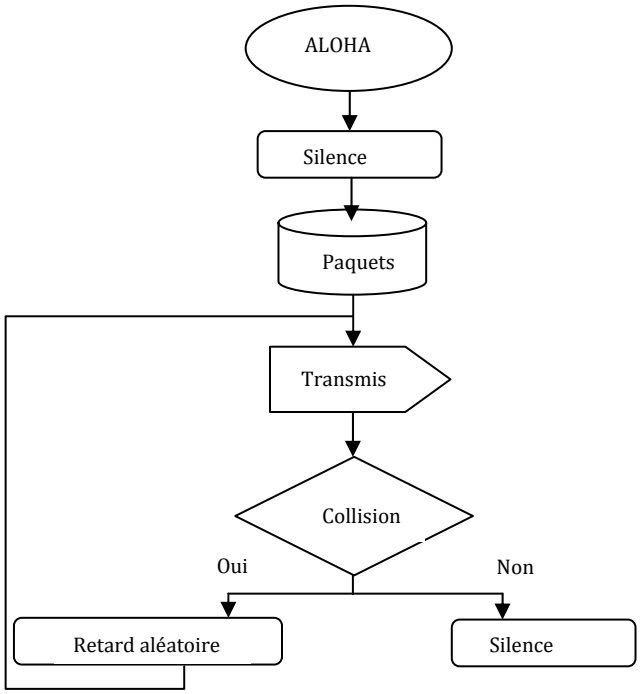


Figure II.4 le principe de base du protocole ALOHA

Le premier protocole de réseau local, nommé " Aloha ", a été mis au point en 1970 par Abramson à l'université d'Hawaï. Il voulait assurer la communication entre des établissements de l'université situés sur des îles éloignées les unes des autres.

Le principe de ce protocole est que tous les ordinateurs émettent en même temps, reçoivent en même temps, donc communiquent en même temps sur la même bande de fréquence. Il s'agit donc d'une conversation à plusieurs, principe opposé à celui de la commutation qui procède en allouant à chaque conversation des ressources cloisonnées les unes par rapport aux autres [31].

L'émetteur découpe le message en trames comportant l'adresse du récepteur et un numéro d'ordre. Les ordinateurs reçoivent toutes les trames émises sur le réseau et trient celles qui leur sont destinées en lisant les adresses. Le destinataire reconstitue le message en ouvrant ces trames pour en extraire le contenu et le ranger dans l'ordre après celui des trames précédentes.

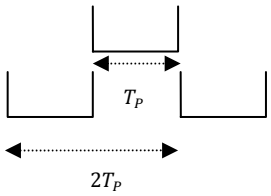
Cependant si deux ordinateurs émettent une trame en même temps, il y a collision : le signal émis dans la bande de fréquence est incompréhensible. Il faut alors réémettre.

On considère un ensemble de sources de trafic générant λ paquets par secondes et on note $T_p$la durée moyenne d'un paquet en secondes. On introduit alors le trafic normalisé (ou offered channel traffic) :

$G = \lambda T_p$ Qui représente le nombre moyen de tentatives de transmission de paquets pendant la durée d'un paquet.

On considère alors que la probabilité que k paquets soient générés pendant la durée d'un paquet suit une distribution de Poisson et s'écrit comme dans l'équation (II.1).

Si on identifie alors un paquet particulier on peut dire que la transmission sera effectuée avec succès si aucun paquet n'a été émis dans une "fenêtre temporelle" de T_p avant l'émission de ce paquet identifié et que ce dernier a été le seul à être émis durant son temps d'émission T_p .



La probabilité de succès que l'on note S s'écrit donc :$S = \Pr[k = 0] \Pr[k = 1]$

$$S = Ge^{-2G} \qquad \text{(II.2)}$$

Cette probabilité est la probabilité qu'un paquet soit émis et qu'il passe, c'est donc aussi le nombre moyen de paquets qui passent avec succès durant la durée d'un paquet et bien entendu ce nombre ne peut pas être plus grand que 1 [34]. Pour remonter au débit effectif en bits/sec, il faut regarder la taille du paquet en nombre de bits : N_p et on obtient alors :

$$Débit = \left(\frac{N_p}{T_p}\right) Ge^{-2G} \qquad \text{(II.3)}$$

Soit, en remplaçant G par sa valeur :

$$Débit = \lambda N_p e^{-2\lambda T_p} \qquad \text{(II.4)}$$

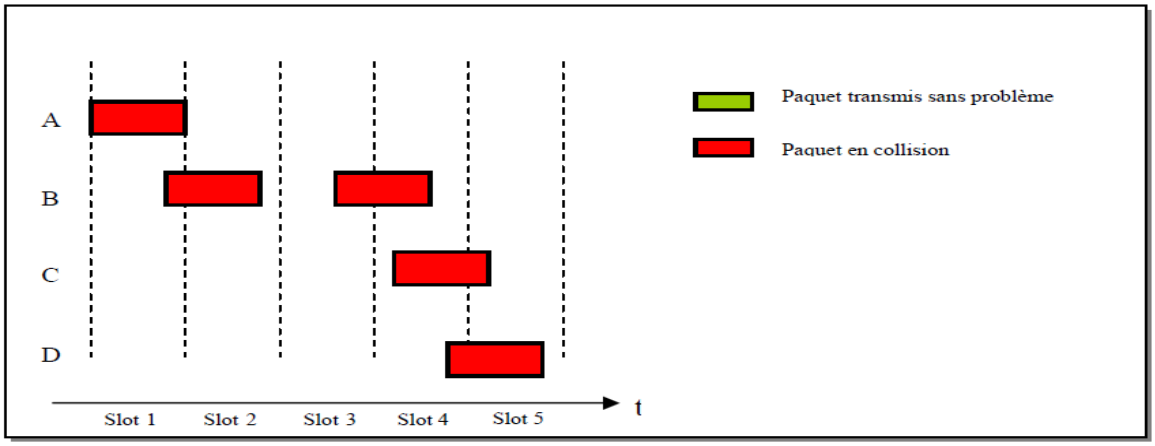


Figure II.5 Le processus de collision du protocole ALOHA

Le fonctionnement :

ALOHA est indépendant des slots : donc il est plus simple et sans synchronisation.

- Laisser les utilisateurs transmettre en toute liberté
- S'il y a une collision, l'émetteur attend de manière aléatoire avant de renvoyer la trame
- Le temps d'attente aléatoire permet d'éviter une situation de blocage

⇒ La collision est constatée même si le premier bit d'une trame recouvre le dernier bit d'une autre

⇒ Les trames sont alors détruites et devront être retransmises ultérieurement

- la probabilité des collisions croit : en effet la trame envoyée à t0 entre en collision avec les autres trames envoyées dans l'intervalle [t0-1, t0+1].

l'efficacité :

L'efficacité est donnée par le pourcentage de trames parvenant à échapper aux collisions.

Supposons N tags avec beaucoup de trames à émettre, chacun transmet pendant un slot avec une probabilité *p.*

P(succès par un tag donné) = P(tag transmet) . P (pas d'autres tag qui transmettent dans [t0-1,t0]) . P(pas d'autres tags qui transmettent dans [t0, t0+1])

$$= p(1-p)^{N-1}(1-p)^{N-1} \qquad \text{(II.5)}$$

$$= p(1-p)^{2(N-1)} \qquad \text{(II.6)}$$

✓ p est optimum pour N -> infini ..., elle est égale à $1/2e = 0.18$

Le prix à payer pour un protocole ALOHA est qu'il est complètement non synchronisé.

Il peut y avoir des retards importants en raison des collisions successives entre les paquets transmis et la retransmission de ces derniers. Si la distance entre le tag et le lecteur est d, le temps de propagation, est :

$$T_d = {}^{d}/_{c} \qquad \text{(II.7)}$$

Où d est la distance et $c = 3\times10^8\, m/s$ est la vitesse de la lumière. Figure II.6 Illustre le cas où une collision se produit. Notez que si un paquet est transmis, et il est reçue après un tempsT_d. Après avoir examiné l'intégralité de donnée, une erreur a été détectée et un message erreur d'une durée T_n retourné à chaque tag. Le système bloque la retransmission de chaque tag sur une durée aléatoire et indépendante dont le temps estT_w. L'intervalle de temps entre la deuxième et la première réception d'un paquet I, est :

$$\Delta = T_P + T_n + T_w + 2T_d \qquad \text{(II.8)}$$

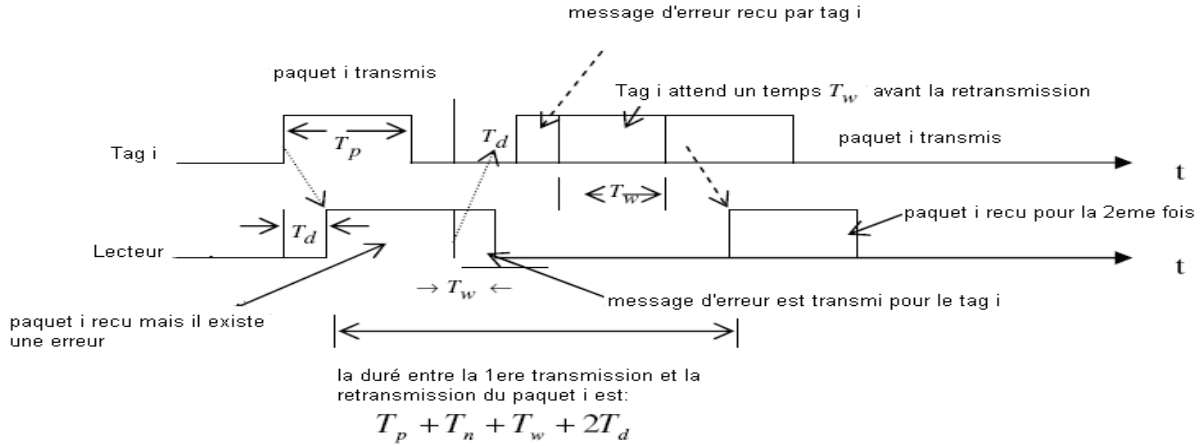


Figure II.6 le principe de fonctionnement du protocole ALOHA

Le temps de réponse moyen est donné par D

$$D = T_d P_0 + (T_d + \Delta)(1-P_0)P_0 + (T_d + 2\Delta)(1-P_0)^2 P_0 + \ldots\ldots + (T_d + q\Delta)(1-P_0)^q P_0 + \ldots. \qquad \text{(II.9)}$$

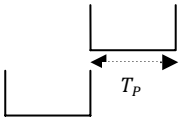
à l'aide de : $\begin{cases} 1 + x + x^2 + \ldots. = \dfrac{1}{1-x} \\ 1 + 2x + 3x^2 + \ldots. = \dfrac{1}{(1-x)^2} \end{cases}$

Et d'effectuer les manipulations mathématiques appropriés, (II.9) devient :

$$D = T_d + \frac{\Delta}{P_0}(1-P_0) = T_d + \Delta\left(e^{2G} - 1\right) \qquad \text{(II.9)}$$

II.2.1.2 Le Protocole Slotted ALOHA

En 1972, Roberts mit au point une version perfectionnée du protocole Aloha : une horloge installée sur le réseau émet un signal à la fin de chaque durée de trame. Un ordinateur n'a le droit d'émettre qu'au reçu du signal de l'horloge : au lieu d'émettre une trame dès qu'il en a envie, il doit donc attendre le prochain signal d'horloge. Une collision se produira si deux ordinateurs ont eu envie d'émettre pendant une même durée de trame, car ils émettront ensemble au reçu du signal d'horloge.



L'astuce de ce protocole, c'est de diminuer la durée du silence nécessaire pour éviter la collision. Cette durée était de $2T_P$ avec Aloha, elle devient de T_P seulement avec Slotted Aloha . Ce perfectionnement a un coût : il faut installer une horloge sur le réseau, et mettre sur chaque ordinateur le dispositif lui interdisant d'émettre si ce n'est au reçu du signal de l'horloge [31]. Si on se place dans le cadre d'un système de communications utilisant une structure de trame temporelle avec des times slots définis, la probabilité de collision par chevauchement d'un paquet émis dans une fenêtre temporelle de taille T_P est impossible. La probabilité de transmission avec succès est alors simplement égale à la probabilité d'émettre un paquet pendant la durée d'un paquet [34]. On a alors : $S = \Pr[k = 1]$

$$S = Ge^{-G} \qquad \text{(II.10)}$$

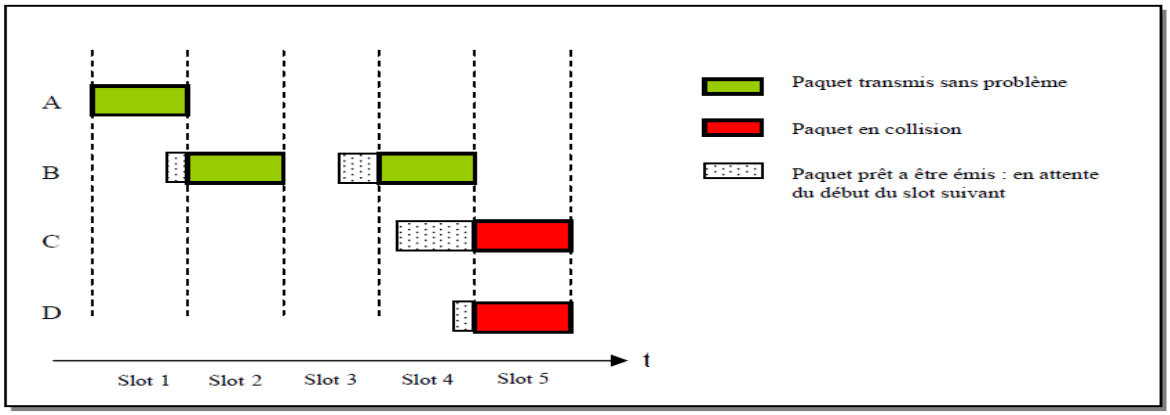


Figure II.7 Le processus de collision du protocole Slotted ALOHA

- **Les suppositions :**
  - Toutes les trames ont la même taille.
  - Le temps divisé en slots identiques (le temps de transmettre 1 trame).
  - Les tags commencent l'émission des trames seulement au début des slots.
  - Les tags sont synchronisés.
  - Si plusieurs tags transmettent dans un slot, tous les tags détectent la collision.
- **Le fonctionnement :**
  - Quand un tag reçoit une nouvelle trame, il la transmet pendant le slot suivant.
  - Si pas de collision, le tag envoi la nouvelle trame pendant le slot suivant.
  - Si collision, le tag retransmet la trame pendant un slot ultérieur avec une probabilité *p* jusqu'au succès.

- **Les avantages :**
  - Un seul tag actif peut émettre continuellement au taux maximum du canal.
  - Très décentralisé : la synchronisation n'est faite que pour les slots à l'intérieur des tags.
  - Très simple.

- **Les inconvénients :**
  - Les collisions font perdre des slots.
  - Possibilité de plusieurs slots vides.

- **L'efficacité**

Supposons N tags avec beaucoup de trames à émettre, chacun transmet pendant un slot avec une probabilité *p.*

- La probabilité avec laquelle le 1er tag réussi à émettre avec succès dans un slot, égale à :

$$p(1-p)^{N-1} \qquad \text{(II.10)}$$

- La probabilité avec laquelle tous les tags réussissent, égale à :

$$Np(1-p)^{N-1} \qquad \text{(II.11)}$$

- Pour un max d'efficacité avec N tags, trouver p* qui maximise $\mathrm{Np}(1-\mathrm{p})^{\mathrm{N}-1}$ quand N devient très grand
- Pour plusieurs tags, prendre la limite de $Np^*(1-p^*)^{N-1}$ quand N tend vers l'infini : donc $p^*= 1/e = 0.37$

Le canal est utilisé pour des transmissions utiles pendant 37% du temps.

Avec un calcul similaire au cas du protocole ALOHA, Le temps de réponse moyen est donné par D :

$$D = T_d + \Delta\left(e^G - 1\right) \quad \text{(II.12)}$$

II.2.1.3 Le Protocole Frame Slotted ALOHA

Dans le protocole frame Slotted Aloha la procédure d'interrogation est divisée en un ensemble de trame (ensemble des slots), chaqu'une ayant plusieurs intervalle temporelle (time slot). En réception de la commande « REQUEST » du lecteur, chaque tag peut répondre simplement dans un intervalle (slot) choisie au hasard au cours d'une période d'une trame (contient plusieurs slots) . S'il n'ya qu'une seule réponse du tag dans un intervalle temporelle (time slot), le lecteur peut identifier ce tag avec succès. Un Tag non identifié avec succès sera résélectionner dans un intervalle de temps (slot) de la trame suivante pour retransmettre leur ID (identifiant). Au moment où aucun tag ne répond pas, tous les tags sont alors identifiés avec succès.

Dans le Tableau II.2, nous montrons un exemple de protocole frame slotted ALOHA dans lequel chaque frame comporte quatre slots temporels. Supposons qu'il y a six tags avec des identifiants uniques 5-bit dans la zone d'interrogation d'un lecteur. La procédure d'exécution du protocole est décrite comme suit:

1. Le lecteur envoie la commande REQUEST en premier temps pour synchroniser le début d'une trame.
2. Chaque tag choisit au hasard une des quatre slots disponibles dans la trame 0 et répond par son ID après avoir reçu la commande REQUEST. Dans notre exemple, dans la trame 0, seulement l'ID du tag dans le slot n°1 peut être identifié avec succès. Les collisions se produisent dans les slots 2 et 4, et aucun tag ne répond dans slot 3.
3. Les tags identifiés peuvent être sélectionnés par la commande SELECT pour lire ou écrire des données. Elles cesseront de répondre aux commandes REQUEST dans les trames suivantes.
4. Le lecteur envoie une requête REQUEST jusqu'à ce que tous les tags soient identifiés avec succès.

Un inconvénient du protocole frame slotted ALOHA est que ses performances se dégradent lorsque le nombre de slots de temps dans la trame ne correspond pas correctement au nombre de tags dans la zone d'interrogation. Le protocole dynamique frame slotted ALOHA essaye d'éliminer l'inconvénient en ajustant dynamiquement la taille de la trame en fonction de l'estimation du nombre de tags. Leur performance est meilleure que celle du protocole frame slotted ALOHA [14][23].

Tableau II.2 Exemple de protocole de frame slotted ALOHA

	Trame 0					Trame 1				
		Slot1	Slot2	Slot3	Slot4		Slot1	Slot2	Slot3	Slot4
lecteur	DEMANDE					DEMANDE				
Tag1			10010						10010	
Tag2		01110								
Tag3					00101		00101			
Tag4			11011				11011			
Tag5			10110					10110		
Tag6					01001					01001
ETAT		réussie	collision	vide	collision		collision	réussie	réussie	réussie

II.2.1.4 Le Protocol ISO/IEC 18000-6A

ISO / CEI 18000-6 est une norme qui définit la communication air-interface à 860-960MHz pour le système RFID. Il existe trois types différents (A, B et C) des protocoles de communication définis dans la présente norme. Parmi eux, les types A et C sont des protocoles à base d'ALOHA. Parce que le protocole de type C est une dérivation de type A du protocole, nous allons seulement introduire le protocole de type A.

Dans le protocole ISO / CEI 18000- 6A, le lecteur initie un cycle de la procédure d'identification en envoyant la commande Init_round. Dans cette commande, le nombre de slots temporels dans un cycle (round), nommé la taille du cycle. Il est à noter que le lecteur peut déterminer de façon dynamique la taille du prochain cycle suivant le nombre de collisions survenues dans le cycle actuel. Après avoir reçu la commande, un tag sélectionne au hasard un intervalle de temps pour envoyer son ID (identifient) au lecteur. Le tag garde un compteur de slot et attend pendant la durée du slot actuelle. Lorsque l'intervalle de temps sélectionné arrive, le tag attend un retard aléatoire dans l'intervalle de 0 à 7 périodes et répond avec une signature de tag de quatre bits choisis au hasard. S'il ya un seul tag qui répond dont la signature est reçue par le lecteur correctement, le lecteur va envoyer la commande Next_slot contenant la signature reçue au tag comme une reconnaissance, sinon, la commande Close_slot est envoyée[24]. Le tag présente les comportements suivants:

- Le tag incrémente le compteur d'intervalles de un s'il ne répond pas dans le slot actuel et la commande reçue est Close_slot ou Next_slot.
- Le tag incrémente le compteur d'intervalles de un s'il répond dans le slot actuel et la commande reçue est Close_slot.
- Le tag passe à un état dit Calme(Quiet) si elle répond dans le slot actuel et la commande reçue est Next_slot avec la même signature du tag telle qu'elle est.

Pendant une itération d'un cycle (round), le lecteur peut suspendre le cycle d'interrogation par l'envoi de la commande Standby_round aux tags. La suspension du cycle permet au lecteur de mener un dialogue avec les tags sélectionnés pour les données de lecture / écriture. Lorsque le nombre de slot est égale à la taille du cycle spécifié par la commande Init_round, le cycle est terminé et tous les tags qui ne sont pas dans un état Calme (c'est-à-dire les tags qui ne sont pas encore identifiés) choisiront au hasard un nouveau slot et une nouvelle signature d'une manière aléatoire pour entrer dans un nouveau cycle [14].

II.2.2 Les Protocoles à base de compteur

Ce type de contrôle n'a pas, à l'instar des protocoles à base d'arbre, de problème de famine (oublié) d'étiquettes (tags).

II.2.2.1 Le Protocole ISO/IEC 18000-6B

ISO/IEC 18000-6B est un standard adoptant un protocole d'anticollision d'étiquettes à base de compteur. Dans ce protocole chaque étiquette utilise un compteur variable dynamique et un générateur aléatoire de bits pour l'identification. Chaque compteur est initialisé à 0, et chaque étiquette ayant un compteur égale à 0 peut transmettre son ID pour répondre à la requête du lecteur. Lors d'une collision, le lecteur signale les étiquettes en question. Chaque étiquette ayant comme valeur du compteur supérieur à 0 incrémente son compteur par 1, tandis que celle ayant comme valeur du compteur 0 génère aléatoirement un bit; 0 ou1; et l'additionne à la valeur du compteur [14]. De cette manière, les étiquettes ayant 0 comme valeur du compteur sont divisées en deux sous groupes, l'un contenant les étiquètes avec comme valeur du compteur 0 et l'autre celles ayant la valeur 1. Cette procédure est répété jusqu'à ce qu'il y a une seule étiquette ou il n'y aucune ayant comme valeur du compteur 0. Dans le cas d'une seule étiquette, elle est identifié avec succès est doit rester en mode silencieux jusqu'à la fin de la procédure d'interrogation. Dans le cas d'une seule ou aucune étiquette, le lecteur informe toutes les étiquettes de décrémenter leurs compteurs par 1. Ce processus est répété jusqu'à l'identification de toutes les étiquettes avec succès.

Un exemple démonstratif du protocole ISO/IEC 18000-6B est donné ci-dessous, soit quatre étiquettes avec comme ID **0010, 0110, 1001, 1110,** les étapes de la procédure d'interrogation sont les suivantes [24]:

- Au début, le lecteur envoi une requête aux étiquettes pour commencer un cycle d'interrogation. Les étiquettes initialisent leurs compteurs à 0 et envoient leurs ID simultanément; on a un problème de collision.

- Le lecteur envoi une commande pour signaler la collision, toutes les étiquettes ajoutent aléatoirement 0 ou 1 à leurs compteurs. Les étiquettes 1, 2 et 4 sont avec des 0 dans leurs compteurs, elles répondent simultanément au lecteur et le problème de collision est à nouveau rencontré.

- Le lecteur envoi une commande pour signaler une collision aux étiquettes 1, 2 et 4, ces dernières ajoutent aléatoirement 0 ou 1 à leurs compteurs. L'étiquette 3 décrémente son compteur de 1. l'étiquette 2 ayant comme valeur de compteur 0 répond au lecteur avec son ID et est identifiée avec succès.

- Le lecteur prend en considérations l'ID identifiée avec une commande de notification réussite. L'étiquette 2 entre en mode silencieux et il reste des étiquettes décrémentent leurs compteurs de 1.

II.2.2.2 Le Protocole ABS

Le protocole ABS a été proposé pour améliorer le protocole ISO/IEC 18000-6B. Dans ce protocole, l'étiquette possède deux compteurs : PSC (Progressed Slot Counter) et ASC (Allocated Slot Counter). Le compteur PSC présente le nombre des étiquettes identifiées avec succès. Initialement à 0 il incrémente à chaque fois qu'une étiquette est identifiée avec succès. Avec les compteurs PSC et ASC, l'étiquette peut décider si elle peut transmettre son ID pour répondre à la requête du lecteur. Toutes les étiquettes ayant un ASC égale à PSC peuvent transmettre leur ID. dans le cas d'aucune réponse, les étiquettes avec ASC plus grand que PSC décrémentent leurs PSC de 1. Dans le cas des collisions, le lecteur signal à toutes les étiquettes de ces collisions et, soit elles incrémentent leurs ASC de 1 s'il est plus grand que PSC, soit elles ajoutent aléatoirement 0 ou 1 à leurs ASC qui sont égalent à PSC. Remarquant que les étiquettes avec ASC inférieur à PSC n'incrémentent pas leurs ASC parce qu'elles ont été déjà identifiées. Après l'identification de toutes les étiquettes, ces dernières gardent leurs ASC pour accélérer les prochains cycles (rounds) d'interrogation [14][24].

II.2.3 Les protocoles à base d'arbre :

l'idée de base du Protocole anticollision de tag (étiquette) à base d'arbre est de diviser, d'une manière répétitive, les étiquettes (tags) correspondantes aux collisions en sous groupes suivants leurs IDs jusqu'à ce qu'il y est une seule étiquette dans le sous groupe faisant l'objet d'une identification réussite. Les protocoles peuvent être appliqués aux étiquettes avec ou sans mémoire à écriture. Les étiquettes avec mémoire ont un cout élevé. Cependant les protocoles pour ce genre d'étiquettes ont de meilleure performance. En général, le protocole à base d'arbre a un délai de temps d'activation plus lent que celui à base d'ALOHA (ALOHA-based), mais il n'a pas de problème de famine d'étiquette. Un autre inconvénient du protocole à base d'arbre est qu'il est affecté par la longueur ou la distribution de l'ID de l'étiquette. Ci-dessous, on va introduire quelques protocoles à base d'arbre à savoir : query tree, bit-by-bit binary tree, EPCglobal Class 0, TSA, BSQTA et BSCTTA.

II.2.3.1 Le protocole Query Tree

Dans ce protocole, le lecteur diffuse; en premier lieu; une requête avec un train de bits S aux étiquettes. Celles ayant un préfix de l'ID similaire à S répondent au lecteur avec la totalité de l'ID. Si; en un instant, une seul étiquette répond elle est identifié avec succès. Par contre, si plusieurs étiquettes répondent simultanément, on

a un problème de collision de réponses. Dans ce cas, le lecteur rediffuse un train de bits avec un bit en plus; 0 ou 1; ajouté à la fin de S, soit S0 ou S1. Dans ce cas, les étiquettes avec le préfix S vont être divisées en deux sous groupes S0 et S1. Cette procédure de division en sous groupes sera répéter d'une manière continue jusqu'à ce que chaque étiquette dans la zone d'interrogation sera identifié avec succès. Ce protocole ne nécessite pas des étiquettes équipées de mémoires à lectures intégrées en plus. On peut observer que le retard d'identification de ce genre de protocoles est affecté par la distribution et la longueur de l'ID des étiquettes. Spécialement, si l'ID est continue, le train de bits des requêtes d'identification sera plus long. Dans ce cas le temps de la procédure d'identification augmentera d'une manière significative.

Ci-dessous un exemple de ce type de protocole est expliqué. Soit six étiquettes avec les IDs **0010**, **0011**, **1001**, **1100**, **1101**, et **1110**. La procédure d'interrogation est décrite par les étapes suivantes :

1. Le lecteur envoie une chaîne de bits de requête S=0 et pousse une autre chaîne de bits de requête « 1 » dans la pile (filo). Les tags avec des ID 0010 et 0011 ont le premier bit d'ID correspondant à la chaîne binaire S. Ils répondent de leur ID au lecteur en même temps et la collision se produit.
2. Le lecteur envoie ensuite une chaîne plus grande de bit S = 00 et pousse 01dans la pile. Les tags avec des ID 0010 et 0011 répondent à la requête en même temps et la collision se produit à nouveau.
3. Le lecteur envoie une chaîne de bit de requête encore plus grande S = 000 et pousse 001 dans la pile. Aucun des tags ID n'a un préfixe correspondant à S, donc il n'ya pas de réponse.
4. Pour le cas de non-réponse, le lecteur fait apparaître 001de la pile et l'envoie comme une chaîne de bits de demande. Les tags avec des ID 0010 et 0011 répondent à la demande en même temps et la collision se produit à nouveau.
5. Le lecteur envoie une chaîne de bits S = 0010 et pousse 0011dans la pile. Seul le tag avec l'ID 0010 répond à la demande et sera identifiée avec succès.
6. Dans le cas d'une identification réussie, le lecteur fait apparaître 0011de la pile et l'envoie comme une chaîne de bits de demande. Seul le tag avec l'ID 0011 répond à la demande et sera identifiée avec succès.

La procédure d'identification est exécutée jusqu'à ce que la pile soit vide. Et puis, tous les tags peuvent être identifiés avec succès [25]. Les étapes de la procédure et toute l'arborescence associée sont présentés dans le Tableau II.3.

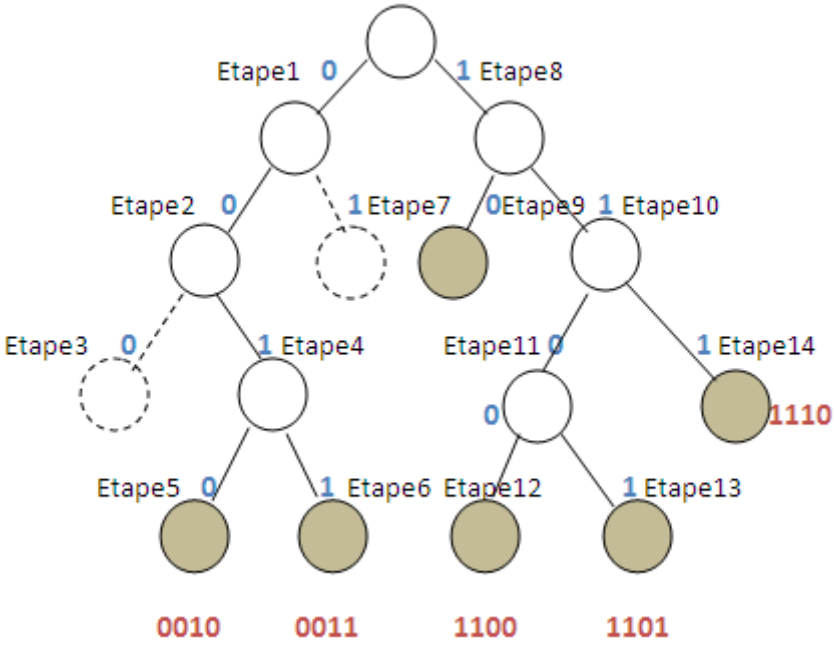


Figure II.8 les étapes de la procédure d'identification du protocole QT

Tableau II.3 étapes de la procédure d'identification du protocole QT

Etape	Les bits demandés	Réponse
1	0	COLLISION
2	00	COLLISION
3	000	NUL
4	001	COLLISION
5	0010	0010
6	0011	0011
7	01	NUL
8	1	COLLISION
9	10	1001
10	11	COLLISION
11	110	COLLISION
12	1100	1100
13	1101	1101
14	111	1110

II.2.3.2 Le Protocole Bit-by-Bit Binary Tree

Avec l'assistance de mémoire à écriture sur étiquette, ce type de protocole réduira efficacement le problème de collision. Le lecteur diffuse, en premier lieu, une commande de requête et les étiquettes répondent avec leur premier bit de l'ID. Si le problème de collision est rencontré, le lecteur ne considérera que les étiquettes avec

comme premier bit 1 (ou 0). Seules ces étiquettes répondront avec leur deuxième bit. Cette procédure est répété bit par bit jusqu'à ce qu'il n'y a qu'une seule étiquette qui répond[26]. Dans ce cas le lecteur demande le reste des bits de l'ID pour l'identification. Avec la mémoire embarquée, les étiquettes peuvent suivre facilement le processus de réponse et d'identification. Ce protocole, contrairement au protocole QT, n'oblige pas le lecteur à transmettre plusieurs bits pour l'identification, par conséquent le temps de la procédure d'identification est réduit [14].

II.2.3.3 Le protcole EPCglobal Class 0

Dans ce protocole l'étiquette répondra avec le premier bit de l'ID à la requête du lecteur. Chaque étiquette répond avec un seul bit à travers l'une des deux sous porteuse, une pour le mot binaire 0 et l'autre pour le 1, dans ce cas le lecteur peut connaitre le 0 et le 1 en même temps. Si le lecteur reçoit un 0 et un 1 à la fois, il va considérer les étiquettes avec le bit 0, sinon il va considérer la valeur du bit reçu. Seules les étiquettes ayant le premier bit similaire au bit considéré peuvent répondre au lecteur avec leurs seconds bits. Les autres étiquettes entrent temporairement en mode silencieux jusqu'à un nouveau processus d'interrogation. Cette procédure se répète bit par bit jusqu'à ce qu'une étiquette réponde avec la totalité des bits de l'ID marquant une identification réussite, dans ce cas cette étiquette entre dans un état désactivé en attendant la prochaine procédure d'interrogation [27].

Soit trois étiquettes avec les IDs **001**, **011** et **110**, la procédure du protocole est décrite par les étapes suivantes :

1. en premier lieu, le lecteur envoi une commande de requête aux étiquettes pour commencer un round d'interrogation, en recevant cette requête les étiquettes répondent avec leurs premiers bits soit **0** pour **001** et **011**, et **1** pour **110**.
2. Le lecteur, en recevant 0 et 1, va considérer les étiquettes commençant par 0, soit la première et la deuxième. La troisième entre en mode muet en attendant la prochaine commande de requête.
3. Le lecteur recevra un 0 et un 1, dans ce cas seul la première étiquète sera considérer. La deuxième entre en mode muet.
4. En recevant le troisième bit, la première étiquète sera considérer comme identifier.
5. Les étapes de la procédure d'interrogation sont répétées jusqu'à ce que tous les tags dans la zone d'interrogation soient identifiés avec succès.

II.2.3.4 Le Protocole TSA

Le protocole Tree Slotted ALOHA(TSA) est un protocole hybride qui intègre les notions de partage d'arbre et le protocole dynamique frame slotted ALOHA. Dans le TSA, le lecteur choisit d'abord la taille initiale de la trame S (le nombre de slots de temps dans la trame) et l'envoie à tous les tags afin de répondre ave/c leurs IDs. Tous les tags choisiront au hasard un slot de temps compris entre 1 et S pour transmettre leurs IDs en réception de la demande. S'il y a un seul tag qui répond dans ce slot de temps, le tag est identifié correctement. Toutefois, s'il existe plusieurs tags qui

répondent dans le même slot temporel, le lecteur se souvient du numéro de slot et il exige que les tags répondent dans la trame suivante. Il est à noter que la taille de la trame est calculée en utilisant une fonction d'estimation particulière. S'il ya encore des tags qui rentrent en collisions dans le slot, la même action est réalisée pour diviser le niveau de collision tags par niveau de manière récursive. L'action est similaire à l'éclatement des collisions tags en sous-groupes selon une arborescence de niveau supérieur et niveau inférieur. C'est pourquoi le protocole est appelé Tree Slotted ALOHA[14].

Dans le protocole TSA, le lecteur comprend à chaque demande la taille du slot, le numéro du slot de partition des tags touchés par la collision et le niveau de l'arbre de décomposition tag. En mémorisant le numéro du slot choisi et le maintien d'un niveau variable de l'arbre de décomposition tag, les tags peuvent suivre l'état de la procédure d'identification. Par conséquent, la procédure d'identification peut être effectuée correctement et tous les tags peuvent ensuite être identifiés avec succès[28].

II.2.3.5 Les Protocoles BSQTA et BSCTTA

Ces protocoles ont été proposés par Choi et al pour améliorer le protocole QT. Quand le lecteur envoi un train de bit S de longueur k, l'étiquette avec un préfixe similaire à S répond avec une partie de son ID de longueur k+1,…,n ou n est la longueur de l'ID. Si le problème de collision est rencontré le lecteur rediffuse une requête avec S0 et S1. Choi et al a observé que S0 et S1 ont les même k premiers bits et ne se diffèrent qu'au dernier bit. A base de cette observation, deux méthodes BSQTA et BSCTTA ont été proposées pour améliorer le temps d'identification en s'aidant de deux slots temporels. Ci-dessous sont définies les étapes de ces méthodes :

1. le lecteur envoi un train de bits de longueur i-1 aux étiquettes;
2. les étiquètes ayant un préfix similaire à i-1 répondent avec leur ID, celles ayant un 0 comme $i^{ième}$ bit de l'ID répondent dans le premier slot de temps, celles ayant un 1 répondent dans le deuxième slot.
3. S'il n'y a pas de collision dans un intervalle(slot) de temps, le tag peut alors être identifié avec succès.
4. Si des collisions se produisent dans l'intervalle de temps de réponse (numérotés 0 ou 1), le lecteur doit envoyer une nouvelle chaîne de bits de requête aux tags.
   - Pour BSQTA, la nouvelle chaîne de bit de requête est S et sera annexé par le numéro d'intervalle de temps (0 ou 1).
   - Pour BSCTTA, la nouvelle chaîne de bit de requête est S et sera annexé par les bits reçus avant que les collisions ne se produisent.

La procédure ci-dessus est répétée jusqu'à ce que tous les tags soient identifiés avec succès. Comme le montre les performances du protocole de l'intervalle QT peut être améliorée de manière significative par BSQTA et BSCTTA [29].

II.2.3.6 Le Protocole AQS

Le protocole AQS est un protocole d'anticollision d'étiquette (tag) adaptatif proposé par Myung et al pour améliorer le protocole QT. Le concept de base est de réduire les collisions en se reportant aux informations sur les IDs obtenus lors du dernier cycle (round) d'identification sous l'hypothèse que la population de l'étiquette ne change pas considérablement lors des différents cycles consécutifs. La procédure d'identification du protocole AQS est similaire à celle du protocole QT à l'exception que le train de bits dans la chaine de bits prêts à être envoyer est copié de le dernier cycle d'identification. La chaine de bits comprend non seulement les trains de bits des étapes d'identification réussites mais aussi les étapes avec aucune réponse. Si la population des étiquettes dans la zone d'interrogation reste la même, toutes les étiquettes seront identifiée avec succès sans modifier aucun train de bits dans la chaine de bits. Mais s'il y a des étiquètes entrantes ou sortantes on doit exécuter les actions suivantes [30] :

- *les étiquettes (tags) entrantes* : si on a un problème de collision avec le train de bits S issue du dernier cycle d'identification, il doit y avoir de nouvelles étiquettes entrantes dans la zone d'interrogation du lecteur. Alors la procédure de division en arbre est exécutée et de nouveaux trains de bits de requêtes plus longs sont rajoutés à la chaine de bits.
- Si on a *des étiquètes (tags) sortantes*, on n'aura pas de réponse pour certains trains de bits S issu des derniers cycles d'identification. Pour améliorer ce cas, le lecteur doit fusionner le train de bit S avec celui de la chaine de bits ayant les mêmes bits à l'exception du dernier.

II.3 Les protocoles d'anticollisions de lecteur :

Plusieurs protocoles d'anticollision lecteur sont proposés pour résoudre les problèmes de collision du lecteur. Ils sont classés en trois catégories: TDMA, FDMA, et les protocoles CSMA. Ci-dessous, nous décrivons certains protocoles d'anticollisions des lecteurs classe par classe.

II.3.1 Les Protocoles *TDMA*

L'idée de base des protocoles d'anticollisions des lecteurs basés sur la technique TDMA consiste à diviser toute la période de communication en intervalles de temps (en anglais « time slot ») et de ne permettre au lecteur de transmettre que dans ses intervalles alloués. De cette façon, la collision peut être évitée. Ci-dessous, nous présentons deux protocoles d'anticollision de lecteur basé sur la technique TDMA: les algorithmes DCS et Colorwave .

II.3.1.1 L'Algorithme DCS

DCS est un protocole d'anticollision de lecteur proposé par Waldrop et al. C'est un algorithme qui permet à chaque lecteur, au hasard et localement, de choisir une couleur (intervalle temporelle) de l'ensemble des couleurs {0, 1, maxColors}, où maxColors est un paramètre fixé et ne changera jamais. Quand un lecteur veut envoyer un message au tag, il sera en file d'attente jusqu'à ce que le slot temporel (intervalle temporelle) de la couleur choisie arrive. Si un lecteur envoi un message dans le slot temporel de sa couleur choisie, mais il constate que des collisions se produisent, il choisira une nouvelle couleur et informe tous ses lecteurs voisins de changer leurs couleurs choisies, en conséquence, algorithme DCS a besoins de synchroniser l'ensemble des intervalles temporelles, mais il n'a pas besoin de synchroniser les valeurs des couleurs pour tous les lecteurs dans le système [16].

Il attribue ensuite à chaque lecteur une couleur qui correspond à une réservation d'un slot temporel spécifique pour transmettre ses signaux. Si tous les lecteurs adjacents ont des couleurs différentes, la collision lecteur est évitée.

II.3.1.2 L'Algorithme Colorwave

L'algorithme **Colorwave**, ou l'algorithme Variable-Maximum Distributed Color Selection (VDCS), est une extension de l'algorithme DCS. En Colorwave, un mécanisme est proposé afin d'optimiser le nombre des couleurs (par exemple, maxColors) est nécessaires pour colorer le diagramme du lecteur. Si les couleurs utilisées sont réduites, l'efficacité de la transmission du signal peut être améliorée.

Quand un lecteur constate par lui-même ou informé par les lecteurs voisins que le débit de transmission est inférieur à un seuil addition_maxColors, ce lecteur augmentera sa valeur locale maxColors et diffuse à nouveau le maxColors à ses lecteurs voisins pour resélectionner leurs couleurs pour réduire les collisions de transmission. En revanche, un lecteur va diminuer sa valeur locale maxColors pour diminuer la duré d'attente lorsque le débit de transmission est au-dessus d'un seuil subtraction_maxColors [16].

II.3.2 Les Protocoles *FDMA*

Les protocoles FDMA divisent toute la bande de fréquence disponible en plusieurs canaux non interférents. Les lecteurs peuvent utiliser des canaux différents et communiquer avec plusieurs tags simultanément. Ci-dessous, nous présentons deux protocoles, HiQ et le EPCglobal Gen 2, qui adoptent la technique FDMA pour résoudre le problème de collision lecteur.

II.3.2.1 Le Protocole HiQ

HiQ est un algorithme hiérarchique et distribué basé sur les techniques TDMA et FDMA pour résoudre le problème de collision lecteur. L'objectif est de maximiser le nombre de canaux de communication simultanée entre les lecteurs et les tags tout en minimisant le nombre de collisions par l'apprentissage des modèles de lecture des

collisions entre les lecteurs, et en attribuant des fréquences à chaque intervalle de temporelle pour les lecteurs d'une manière efficace.

La structure hiérarchique de contrôle du protocole HiQ se compose des lecteurs, R-serveurs et Q-serveurs. Comme la montre la figure II.10 Les lecteurs RFID sont au niveau inferieur de l'hiérarchie, et chaque serveur au niveau du R-serveur gère plusieurs lecteurs. Quand un lecteur a besoin d'envoyer des messages aux tags dans sa zone d'interrogation, il demande des ressources, à savoir le canal fréquentiel et l'intervalle temporel (time slot) de son maître R-serveur. Le lecteur peut envoyer des messages dans un canal de fréquence spécifique et dans un intervalle de temps (time slot) seulement si le R maître-serveur assure ce canal et l'intervalle de temps pour ce lecteur.

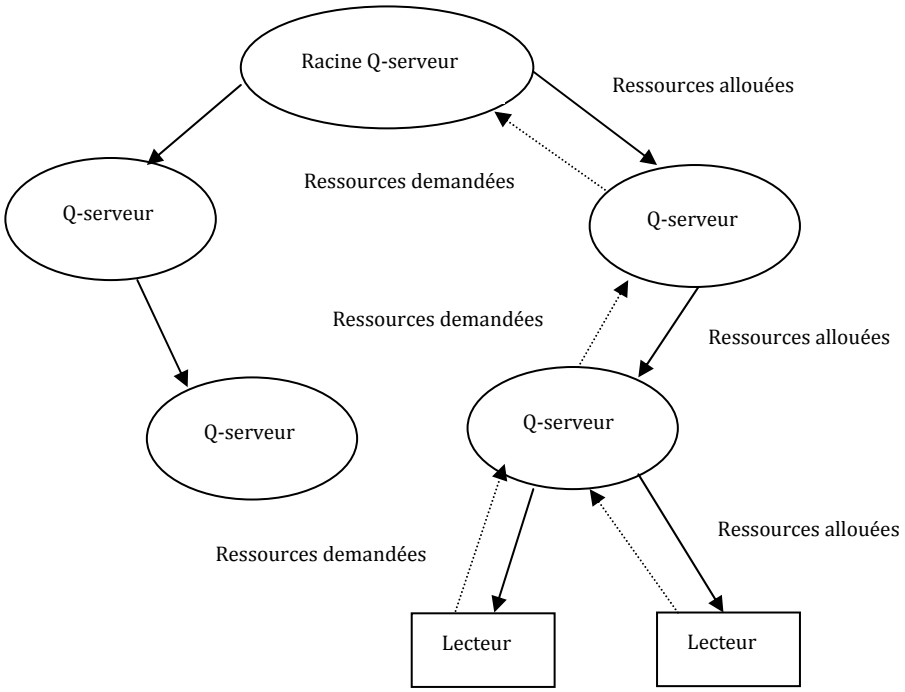


Figure II.9 l'architecture de contrôle dans le protocole HIQ

Avec l'architecture distribuée, les lecteurs voisins peuvent envoyer des messages dans le même intervalle (slot) temporel ou dans le même canal de fréquence ce qu'implique des collisions. C'est la responsabilité des lecteurs de détecter les collisions avec les lecteurs voisins. Chaque lecteur doit indiquer à son maître R-serveur, le nombre de collisions, le type de collisions et le nombre de succès pendant la lecture. Le R-serveur peut alors déterminer quels sont les lecteurs esclaves qui s'interférent mutuellement par les rapports de « feedback » et réaffecte les ressources d'une manière dynamique afin d'éviter les collisions [8].

II.3.2.2 Le Protocole EPCglobal Gen 2

Le standard UHF de classe 1 de deuxième Génération proposé par EPCglobal utilise la technologie FDMA pour réduire les collisions des lecteurs. La bande de fréquences allouée est divisée en canaux. Un lecteur, utilise uniquement certains canaux de communication. Les fréquences porteuses utilisées par les lecteurs et les tags sont distinctes. Dans ce cas les lecteurs (resp les tags) entreront en collision seulement avec les lecteurs (resp les tags). Les lecteurs utilisent la technique d'étalement de spectre et le saut de fréquence pour éviter toute collision. En Europe, une bande passante de 200 kHz est réglementée pour l'attribution des fréquences Il est suggéré que les lecteurs utilisent les canaux paires tandis que les signaux de rétrodiffusion des tags sont dans les canaux impaires. Aux États-Unis, une large bande passante plus de 500 kHz est réglementée pour l'attribution des fréquences. Tous les canaux sont disponibles pour l'interrogation du lecteur, mais le tag peut rétrodiffuser des signaux sur les limites de ces canaux. Le protocole **EPCglobal Gen 2** peut résoudre le problème de collision lecteur, parce que les tags à faible coût n'ont pas la capacité de sélectionner la fréquence et par conséquent le problème de collision des tags existe toujours [18].

II.3.3 Les Protocoles CSMA

CSMA est un mécanisme couramment utilisé dans les systèmes filaires ou sans fil pour éviter les collisions. Dans ce mécanisme, chaque dispositif doit vérifier si le canal de communication est libre avant de transmettre des messages. Si le canal est occupé, le dispositif va attendre jusqu'à ce qu'il soit libéré.

ETSI 302 208 est un règlement européen qui adopte un mécanisme CSMA appelé « LBT » pour résoudre le problème de collision lecteur. Il alloue la bande de fréquences de 865 à 868 MHz pour les applications RFID et divise la bande en 15 canaux de 200 kHz chacun. Avec la puissance de rayonnement effective maximale (ERP) de 2 W, seulement 10 canaux sont disponibles pour la communication et 5 canaux sont définis comme des canaux de garde ou réservés pour les lecteurs de plus faible puissance. Le module de réception d'un lecteur est d'abord activé pour surveiller le canal sélectionné durant une durée déterminée (5 ms) avant la transmission. S'il sent que le canal est inactif au cours de la période de temps spécifiée, le lecteur peut envoyer le message directement après un temps maximum de 4 s, puis le lecteur active le module récepteur pour détecter les interférences de signaux. Si le canal est occupé par d'autres lecteurs, le lecteur cherche un autre canal libre pour transmettre des messages [14].

Conclusion

Nous avons introduit certains protocoles d'anticollision tag qui sont classés comme des protocoles à base d'ALOHA, à base de compteur, et des protocoles à base d'arbre. Nous avons également introduit plusieurs protocoles de collision lecteur qui sont basés sur les concepts de TDMA, FDMA ou CSMA.Technique d'accès multiple CDMA.

La première partie de notre travail est consacrée à l'étude et l'évaluation des performances des différents algorithmes d'anticollision à base d'ALOHA à savoir : l'ALOHA, le Slotted ALOHA et le Farme Slotted Aloha.

La deuxième partie est consacrée à l'élaboration d'un algorithme d'anticollision à base de l'ACI, pour cela nous avons appliquée le détecteur FastICA dans la technique CDMA.

Chapitre 3

Technique d'accès multiple CDMA et Analyse en Composantes Indépendantes

III.1 Techniques d'accès multiple :

Le partage d'un support de communication par plusieurs usagers utilise trois méthodes classiques : la technique FDMA, la technique TDMA et la technique CDMA.

Avec la méthode CDMA (Figure III.1), tous les utilisateurs ont accès simultanément à la totalité de la bande, permettant ainsi d'exploiter au maximum les ressources disponibles. A la réception, les différents utilisateurs sont distingués à l'aide des codes d'étalement, appelés également *signatures* notées $c^{(m)}$, spécifiques à chacun d'entre eux. Au niveau technologique, les performances optimales d'un système mono-utilisateur sont atteintes par des systèmes multiutilisateurs de type CDMA en assignant aux différents utilisateurs des codes orthogonaux entre eux Les codes de Hadamard, qui ont cette propriété d'orthogonalité, sont généralement utilisés pour des transmissions synchrones. Ce type de transmission est représentatif d'une communication sur la voie descendante d'un réseau de télécommunication mobile où la station de base émet vers les différents terminaux mobiles. A l'inverse, lors d'une transmission sur la voie montante, pour laquelle les différents terminaux mobiles émettent indépendamment vers la même station de base, la transmission est dite asynchrone. Dans ce second cas, des codes non orthogonaux ayant des inter-corrélations très faibles, comme les codes de Gold, peuvent être utilisés [33].

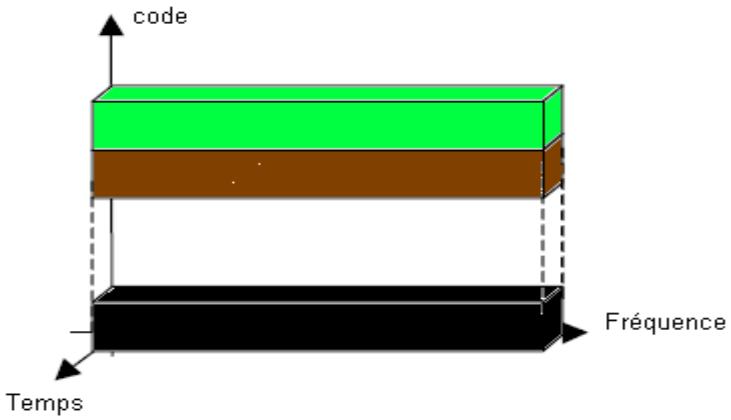


Figure III.1 La technique d'accès multiple CDMA

III.2 Etalement de spectre par séquence directe DS-CDMA:

Les techniques d'étalement de spectre ont des propriétés bien connues actuellement : immunité face aux distorsions apportées par les trajets multiples du canal, faible puissance d'émission robustesse face aux différents types de brouillage et grande sécurité de l'information. Ces avantages sont illustrés par la figure (III.2) On considère à l'émission un rapport signal sur bruit égal à un (SNR=0dB), c'est-à-dire que la puissance du bruit est la même que celle du signal émis. Après l'étalement, la bande passante du signal utile devient plus large et l'amplitude du signal diminue. Le bruit étant un signal indésirable qui s'ajoute à l'information lors de son trajet de l'émetteur vers le récepteur, il reste inaffecté par cette opération. Le niveau du signal devient tellement faible devant le bruit que l'information captée au niveau du canal de transmission sera considéré comme du bruit. A la réception, l'opération de désétalement permet de récupérer l'information utile, tandis que le bruit subit un étalement. Ce qui engendre une diminution du niveau de bruit devant le signal informatif (augmentation du SNR) et la détection devient alors d'une très bonne qualité [33].

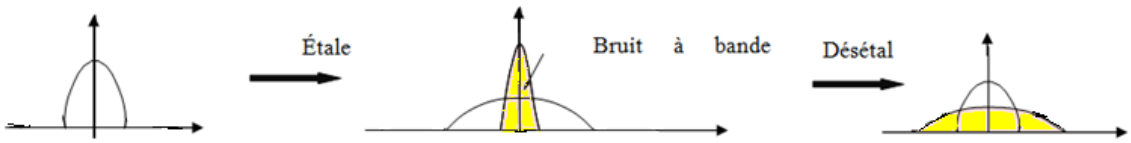


Figure III.2 Robustesse du CDMA face aux différents types de brouillage

L'étalement de spectre peut être réalisé par séquence directe (Direct Sequence Code Division Multiple Access ou DS-CDMA). Cette méthode consiste à multiplier chaque bit à transmettre par un code ou une séquence à un débit nettement supérieur à celui du signal d'origine. Un code d'étalement étant attribué à chaque utilisateur, les performances de ces systèmes dépendent des propriétés d'inter et d'auto-corrélation des codes choisis, du nombre d'utilisateurs et donc du nombre de codes partageant la même bande de fréquence [11].

Les codes d'étalement les plus couramment utilisés dans les systèmes CDMA sont généralement de trois types : les codes de Gold et Hadamard, et les séquences *pseudo-aléatoires* notées PN pour *Pseudo-Noise.* Un code PN noté *c* tel que :

c= $\{c_s$; s=0,…, SF-1$\}$ composé de SF *chips* possède les propriétés suivantes :

- une moyenne approximativement nulle :

$$\sum_{s=0}^{SF-1} c_s \approx 0 \qquad \text{(III.1)}$$

- une propriété d'auto-corrélation donnée par :

$$\rho(t) = \sum_{s=0}^{SF-1} c_s\, c_{s+t} \approx \begin{cases} 1, & \text{si t} = 0 \\ 0, & \text{sinon} \end{cases} \qquad \text{(III.2)}$$

avec $c_s = 0$ si s > SF-1.

Le paramètre SF (Spreading Factor) appelé facteur d'étalement est défini par la formule suivante : $SF = \frac{T_c}{T_s} = \frac{B}{B'}$ (III.3)

Avec T_c correspond à la durée d'un *chip* et T_s à celle du bit,

B= $\frac{1}{T_s}$ est le débit symbole exprimé en bit par seconde (bps) et B'=$\frac{1}{T_c}$ est le débit *chip* ou *chip rate* exprimé en *chips* par seconde (cps)

III.3 Emetteur CDMA :

La structure d'un émetteur CDMA conventionnel pour M utilisateurs émettant d'une manière parfaitement synchrone est illustrée par la figure III.3 :

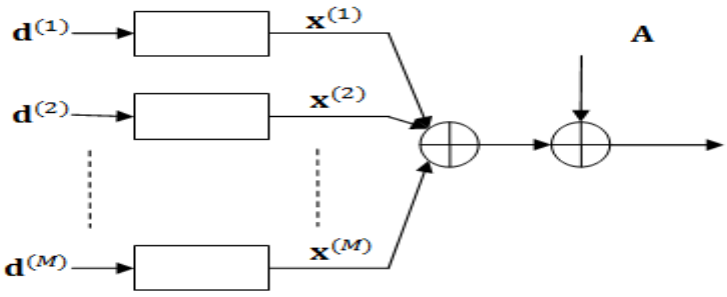


Figure III.3 Structure de l'émetteur CDMA conventionnel pour M utilisateurs

Le principe fondamental de cet émetteur est de transmettre un seul signal contenant les informations provenant des différents utilisateurs multiplexées puis envoyées sur le même canal. On note $\mathbf{d}^{(m)} = \left\{d_k^{(m)}; k = 1, \dots, K\right\}$ l'information provenant de l'utilisateur *m*. Cette information est modulée puis multipliée par un code pseudo-aléatoire $\mathbf{c}^{(m)} = \{c_s^{(m)}\}$ spécifique à cet utilisateur, donnant ainsi naissance à une séquence étalée ou de *chips* $\mathbf{x}^{(m)} = \{x_j^{(m)}; j = 1, \dots, J\}$. Chaque élément du code d'étalement est divisé par la racine carrée du facteur d'étalement, permettant ainsi de répartir l'énergie du *bit* sur des *chips*, et le code d'étalement prend alors sa valeur dans la base $B_s = \{\frac{+1}{\sqrt{SF}}, \frac{-1}{\sqrt{SF}}\}$. Cette opération est connue sous le nom de *normalisation.* Chaque utilisateur possède une signature notée $c^{(m)}(t)$ de durée T_s et qui s'exprime comme suit [33]:

$$c^{(m)}(t) = \sum_{s=0}^{SF-1} c_s^{(m)} p(t - s\,\mathrm{T}_c) \qquad 0 \leq t \leq \mathrm{T}_s \tag{III.4}$$

Où $p(t)$ est une forme d'onde rectangulaire de durée $\mathrm{T}_c = \frac{\mathrm{T}_s}{SF}$ qui est la durée d'un *chip.*

Les propriétés suivantes peuvent être énoncées :

1. Les signatures ont une *énergie* unitaire :

$$\int_0^{\mathrm{T}_s} c^{(m)}(t) \times c^{(m)}(t) = 1 \tag{III.5}$$

2. L'ensemble des signatures a une *fonction d'inter-corrélation* définie par :

$$\rho^{(m)(p)} = \sum_{s=0}^{SF-1} c_s^{(m)} \times c_s^{(p)} \tag{III.6}$$

Le système étant supposé synchrone et les codes orthogonaux entre eux, d'où :

$$\rho^{(m)(p)} \approx \begin{cases} 1, & \text{si } m = p \\ 0, & \text{sinon} \end{cases} \tag{III.7}$$

3. La *matrice d'inter-corrélation* **R** est définie par :

$$\mathbf{R} = \rho^{(m)(p)} \qquad 1 \leq m, p \leq \mathrm{M} \tag{III.8}$$

4. Le *taux de charge* τ_c définit le rapport entre le nombre d'utilisateurs et le facteur d'étalement $\tau_c = \frac{\mathrm{M}}{SF}$ (III.9)

En considérant une modulation BPSK et un canal AWGN, les *chips* émis $x_j^{(m)}$ appartiennent à l'ensemble {+*s*,-*s*} tel que $s = \frac{1}{\sqrt{\mathrm{SF}}}$ et le signal reçu pour les M utilisateurs est formé par des *chips* r_j pouvant s'écrire sous la forme :

$$r_j = \sum_{m=1}^{\mathrm{M}} x_j^{(m)} + w_j \qquad j = 2,\ldots,J \tag{III.10}$$

Où :

- $x_j^{(m)}$ est le $j^{ème}$ *chip* transmis par le $m^{ème}$ utilisateur,
- $\{w_j\}$ sont les échantillons de bruit blanc réel additif gaussien de moyenne nulle et de variance$\sigma_w^2 = \frac{\mathrm{N}_0}{2}$.

L'équation (II.10) peut être également réécrite comme suit :

$$r_j = \sum_{m=1}^{\mathrm{M}} a^{(m)} \sum_{k=1}^{\mathrm{K}} d_k^{(m)} c_{j-(k-1)SF}^{(m)} + w_j \quad j = 1,\ldots,J \tag{III.11}$$

Où $a^{(m)}$ est l'amplitude du signal reçu provenant de l'utilisateur *m.*

III.4 Détection CDMA :

III.4.1 Détecteur décorrélateur et détecteur MMSE linéaires :

La structure du détecteur linéaire est donnée par la figure II.4 :

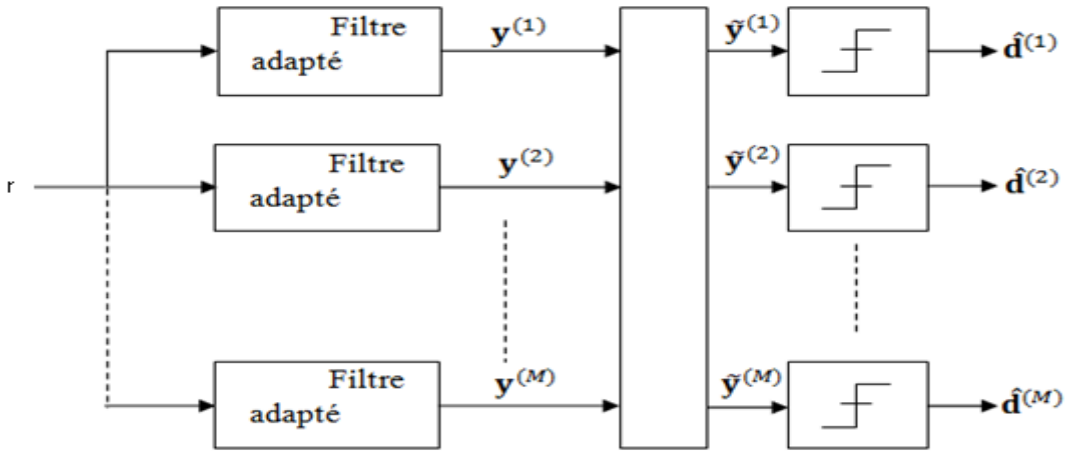


Figure III.4 Structure du récepteur du système CDMA synchrone utilisant le détecteur linéaire

Le principe de fonctionnement de ce type de détecteurs est basé sur le filtrage du vecteur d'observations **y,** en le multipliant par une matrice L, permettant ainsi d'améliorer la qualité de détection du récepteur conventionnel [11].

III.4.1.1 Détecteur décorrélateur

Le détecteur décorrélateur réalise la décorrélation des contributions des utilisateurs aux différentes composantes du vecteur d'observation en appliquant le critère de forçage à zéro appelé ZF.

En l'absence du bruit, l'équation (III.12) devient **y=RAd** et l'élimination totale des interférences peut donc être réalisée en multipliant **y** par l'inverse de la matrice d'inter-corrélation $\mathbf{R}^{-1}$.Cependant, le terme du bruit existe, ce qui engendre une augmentation du bruit en le multipliant par $\mathbf{R}^{-1}$. Ainsi, les performances optimales d'un système mono-utilisateur ne peuvent pas être atteintes par ce détecteur. L'estimation des bits d'information est donnée par la formule suivante :

$$\hat{\mathbf{d}} = \text{sign}(\mathbf{R}^{-1}\mathbf{y})$$

$$= \text{sign}(\mathbf{R}^{-1}(\mathbf{RAd} + \mathbf{w})) \qquad \textbf{(III.12)}$$

L'inconvénient majeur de ce détecteur est la difficulté de calculer l'inverse de la matrice **R** en pratique, à cause de la variation de plusieurs facteurs au cours du temps (nombres des utilisateurs, retard temporel,..) [13].

III.4.1.2 Détecteur MMSE linéaire

Comme son nom l'indique, le principe du détecteur MMSE (Minimum Mean Squared Error) repose sur la minimisation de l'erreur quadratique moyenne de la différence entre les bits estimés et les bits réellement envoyés c'est-à-dire $E(|\hat{\mathbf{d}} - \mathbf{d}|^2)$. Ce détecteur permet un bon compromis entre la suppression d'interférences et la minimisation du bruit, l'estimation de chaque bit d'information s'exprime de la manière suivante :

Dans le cas d'un canal AWGN :

$$\hat{\mathbf{d}} = \text{sign}((\mathbf{R} + \sigma_{\mathbf{w}}^{\mathbf{2}}\mathbf{A}^{\mathbf{-2}})^{-1}(\mathbf{RAd} + \mathbf{w})) \qquad \text{(III.13)}$$

Avec $\mathbf{A}^{-2} = \text{diag}\{\frac{1}{a^{(1)^2}}, \frac{1}{a^{(2)^2}}, \dots, \frac{1}{a^{(m)^2}}\}$.

Il est clair qu'au niveau performance, lorsque la variance du bruit tend vers zéro, le détecteur MMSE converge vers le détecteur décorrélateur. Par contre, à faible SNR, le détecteur MMSE possède de meilleures performances grâce à la prise en compte du bruit par l'intermédiaire de $\sigma_{\mathbf{w}}^{\mathbf{2}}\mathbf{A}^{\mathbf{-2}}$. Contrairement au détecteur décorrélateur, le détecteur MMSE est sensible au phénomène d'´eblouissement car ses performances dépendent du rapport des amplitudes des signaux reçus correspondant à chacun des utilisateurs De plus, le détecteur MMSE nécessite l'estimation de l'amplitude du signal et de la puissance du bruit ou leur rapport. Ce détecteur présente le même inconvénient que celui du récepteur décorrélateur, pour l'opération d'inversion de matrice. Cependant il existe des techniques qui ne nécessitent pas d'inversion matricielle dont les détecteurs à annulation d'interférences [33].

III.5 Technique CDMA Associées au système RFID :

Durant ces dernières années, il ya eu un intérêt croissant dans le développement de systèmes de communication pour l'identification et la localisation des objets Les Techniques d'identification par radiofréquence (RFID) offre ces fonctionnalités. La production des lecteurs et des tags introduit un certain nombre de défis techniques. Bien que les applications traditionnelles de RFID aient généralement un seul tag dans le champ de lecture, de nouvelles applications de la technologie RFID nécessitent souvent l'identification rapide des grandes populations des tags. Si deux ou plusieurs tags RF occupent le canal partagé en même temps, le lecteur RFID ne peut pas décoder les données transmises par les tags et le temps de transmission est gaspillé en raison de la collision. L'efficacité d'identification dans les systèmes RFID diminue généralement si le nombre de collisions tag augmente. [12].

Dans les systèmes RFID avec les grandes populations des tags, les applications probabilistes basées sur le protocole FSA (frame slotted aloha) souffrent de grand nombre de collisions. Le résultat est une augmentation du temps d'identification de tag et une plus faible efficacité du système. La performance du système peut être

améliorée par l'introduction d'un mécanisme permettant de décoder avec succès les réponses des tags dans une collision, par exemple en utilisant l'accès multiple par répartition de code (CDMA) [12].

Dans les systèmes traditionnels à spectre étalé (SS) tels que les systèmes CDMA, chaque utilisateur encode ses données en utilisant un code d'étalement qui est conçu pour être orthogonale ou aussi près que possible d'orthogonale aux autres codes. Ce succès permet le décodage des données transmises par deux ou plusieurs utilisateurs simultanément.

Avec l'utilisation des modulations à étalement de spectre de signaux, nous proposons de lire simultanément plusieurs tags dans un intervalle de temps (slot) et cela réduit ainsi le nombre de collisions où les réponses des tags sont perdues. Cela est bénéfique car elle accélère le processus de lecture en réduisant la communication entre le lecteur et les tags, il réduit les interférences, et il améliore également la sécurité du système [12].

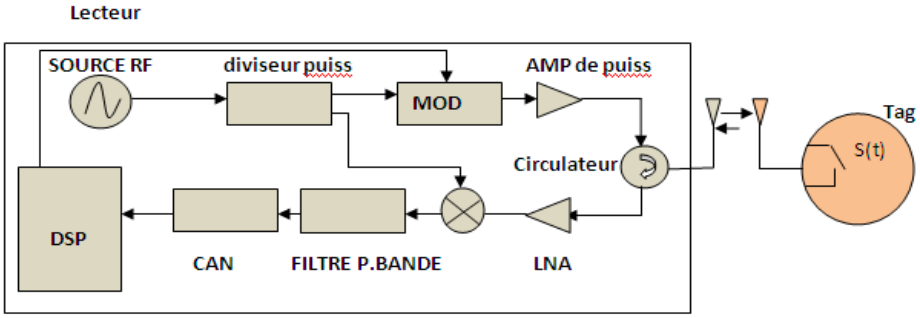


Figure III.5 le système RFID utilisant la modulation de rétrodiffusion

III.5.1 Description des signaux de communication RFID

III.5.1.1 Description du système

Nous ne considérons que la transmission RFID rétrodiffusée dans la figure. III.5. Le lecteur commence à émettre une onde porteuse RF continue [12].

$$x_c(t) = \mathrm{Re}\left[A_c e^{j2\pi f_c t}\right] \qquad \text{(III.14)}$$

Où Re [·] désigne l'opérateur réel, et A_C et f_C désignent respectivement l'amplitude et la fréquence de la porteuse, quand un tag passif entre dans le champ RF du lecteur et après avoir reçu suffisamment d'énergie pour son alimentation, l'onde incidente est modulée par le signal de données :

$$s(t)=\sum_{n=1}^{N_s} S_n\, p(t-nT_S/2) \qquad \text{(III.15)}$$

Où $\{S_n\}$ est la séquence de symboles codés, N_S est le nombre de symboles à transmettre, T_S est la durée d'un symbole, et le signal d'impulsion $p(.)$ est définie par :

$$p(t)=rect(t)=1 \;\text{ Si }\; -T_S/2\le t\le T_S/2$$

Typiquement, le tag envoie les données par commutation de son impédance entre deux états, Le signal modulé peut être s'écrit comme suit :

$$x_{BS}(t)=\mathrm{Re}\left[\tilde{m}(s(t))e^{j(2\pi f_c t+2\phi)}\right] \qquad \text{(III.16)}$$

Tel que $2\phi=2\frac{2\pi}{\lambda}D$ est le retard de phase, λ est la longueur d'onde, D est la distance entre le lecteur et le tag, et $\tilde{m}(s(t))$ désigne l'indice de modulation de la rétrodiffusion. En général, une expression analytique de cet indice de modulation est difficile à obtenir. En remplaçant $\tilde{m}(.)$ avec l'indice m de modulation du signal, le signal modulé de rétrodiffusion peut être approchée par

$$x_{BS}(t)\approx \mathrm{Re}\left[A_{BS}\, ms(t)e^{j(2\pi f_c t+2\phi)}\right] \qquad \text{(III.17)}$$

Avec $m=\frac{\sigma_{\max}-\sigma_{\min}}{\sigma_{\max}+\sigma_{\min}}$, tels que les termes $\sigma_{\max}$ et $\sigma_{\min}$ sont le maximum et le minimum coupes transversales de rétrodiffusion . Après un amplificateur à faible bruit (LNA), une conversion vers le bas avec le facteur de conversion α' est effectuée :

$$x_{BB}(t)=\alpha' ms(t)\cos(2\phi) \qquad \text{(III.18)}$$

La détection homodyne d'une modulation à double bande latérale du signal provoque une différence de phase 2φ non souhaitée, qui peut conduire à l'annulation du signal démodulé. Supposant que le signal dans la bande de base $X_{BB}(t)$ n'est pas annulé par cette différence de phase, et pour un λ et D donnés, le signal converti vers le bas mélangé avec le bruit est donnée par :

$$y(t)=x_{BB}(t)+\omega(t)=\alpha s(t)+\omega(t) \qquad \text{(III.19)}$$

Avec $\alpha=\alpha' m\cos(2\phi)$ Le signal de bruit $\omega(t)$ est modélisé comme un bruit blanc gaussien (AWGN) additif de moyenne nulle, avec $E[\omega(t+\tau)\omega(t)]=\frac{N_0}{2}\delta(\tau)$ où $N_0/2$ désigne la densité spectrale de puissance du bruit. Le signal reçu est passé à travers

un convertisseur analogique-numérique (A / D), dont la sortie est la suite $\{y(\nu)\}$, composé d'échantillons :

$$y(\nu) = \alpha s(\nu) + \omega(\nu), \qquad \nu = 1,\ldots, N_{sc}N_S \tag{III.20}$$

$y(t)$ est le signal reçu échantillonné à des instants de temps $t = \nu \frac{T_S}{N_{sc}}$ où N_{sc} est le nombre d'échantillons / symboles codés ; le bruit blanc gaussien additif (AWGN) discrète est une variable aléatoire supposé être statistiquement indépendantes, gaussiennes distribuée avec moyenne nulle et la variance égale à $N_0/2$. Ainsi, le signal est envoyé au traitement numérique du signal (DSP) qui détecte, décode et traite le signal de données.

Dans la liaison descendante (de lecteur au tag), le signal transmis contient à la fois la porteuse RF continue et des signaux de commandes. Les Conditions et les exigences sont un peu différentes dans la voie montante (du tag au lecteur), où, selon la mise en œuvre, les données sont renvoyées au cours d'une période continue en faisant varier l'amplitude ou la phase. Des types de codage sont utilisés pour assurer une alimentation continue aux tags, par exemple, Manchester, Miller ou biphasé différentiel.

III.5.2 Les systèmes RFID à spectre étalé (SS).

III.5.2.1 Description du système

Un système RFID à étalement de spectre est représenté sur la Figure III.6. Le système se compose d'un groupe de tags n_T et un lecteur avec une antenne. Chaque tag possède un identifiant unique (ID) et un (pseudo bruit) ou code (PN). Le code PN est pseudo aléatoire; parce que bien qu'il semble être un bruit aléatoire, il est prévisible et répétitif. Dans le tag, chaque bit de l'ID est multiplié par le code PN, qui est indépendant de l'ID, pour produire le signal en bande de base [12]:

$$s_i(t) = \sum_{n=1}^{N_s} S_n g_i\left(t - \frac{nT_S'}{2}\right) \tag{III.21}$$

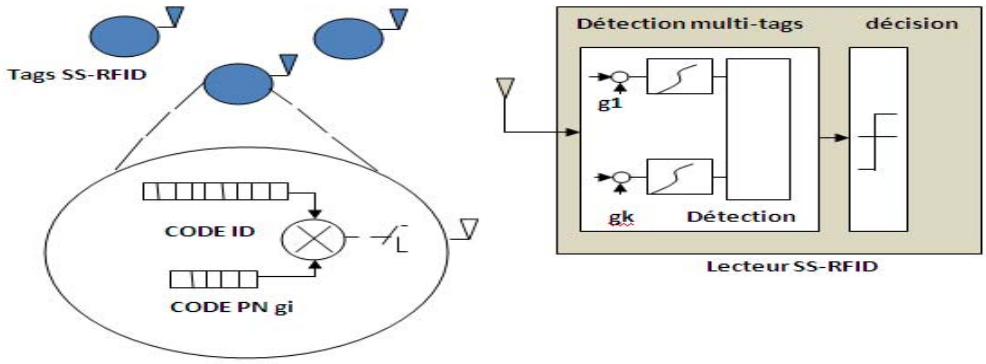


Figure III.6 l'étalement de spectre (SS) dans le système RFID

Où $s_i(t)$ est l'ID (identifient) du tag en utilisant le i^{eme} code PN $g_i(t)$, $T_S^{'} = \beta T_S$ avec la constante $\beta \geq 1$, et $\{S_n\}$ est une séquence de symboles codée par non-retour à zéro (NRZ). Le spectre du signal résultant $s_i(t)$ est réparti sur une large bande de fréquences, et il apparaît comme un bruit blanc gaussien. Puis le tag choisit aléatoirement un slot dans lequel il va transmettre l'ID étalé $s_i(t)$ .En supposant un ensemble de N slots et un nombre n_T des tags dans la zone de lecture du lecteur, le signal reçu à l'antenne du lecteur mélangé avec un bruit AWGN peut être exprimé comme suit:

$$y(t) = \sum_{s=1}^{N} \sum_{i \in \Omega_s} s_i(t) + \omega(t) \qquad \text{(III.22)}$$

Où $i \in \{1,....,n_T\}$ et Ω_s désigne l'ensemble des tags qui choisissent s^{eme} slot de sorte que $[\Omega_1 \cup .... \cup \Omega_N] = n_T$. Le lecteur utilise ensuite un détecteur pour déterminer quels sont les codes présents dans l'ensemble des codes PN, et les identifiants qui ont été envoyés. Le détecteur utilise la connaissance des codes PN pour décoder le signal reçu.

III.5.2.2 Les Détecteurs :

Le choix d'un détecteur approprié est également nécessaire pour les performances du système. Parmi ces détecteurs il y a trois types connus dans les systèmes RFID, à savoir le détecteur optimal, le détecteur classique et le détecteur de décorrélation [12].

Le détecteur optimal, aussi appelé détecteur de maximum de vraisemblance, calcule pour chaque tag dans un slot donné la probabilité de chaque symbole S_n envoyé. Le détecteur optimal choisit alors le symbole avec la probabilité la plus élevée. La complexité de détecteur optimal augmente exponentiellement avec le nombre maximum de codes K, où la valeur K est connue a priori. En transmission

synchrone, le récepteur optimal consiste en un ensemble de K corrélateurs ou filtres adaptés suivis par un détecteur qui calcule les 2^K corrélations correspondantes aux 2^K séquences possibles transmises. Le détecteur sélectionne la séquence correspondante à la plus grande corrélation. Toutefois, le nombre des tags qui répondent dans le même slot n'est pas connu a priori. Le nombre exact est donné par :

$$\binom{K}{K}2^K + \binom{K}{K-1}2^{K-1} + \ldots + \binom{K}{1}2^1,$$

Où $\binom{n}{k}$ définit le nombre de k combinaisons à partir d'un ensemble de n éléments. Par conséquent, dans le cas où le nombre de tags est inferieur à K tags, c'est-à-dire k tags, il y a des $\binom{K}{k}$ combinaisons, et le nombre de calculs nécessaires est énorme.

Dans les transmissions asynchrones, les temporisations de chaque tag doivent aussi être estimées donc il est nécessaire de faire une structure plus complexe de réception. Le détecteur optimal donc n'est pas approprié pour les applications RFID à étalement de spectre.

Le détecteur conventionnel utilise la corrélation du signal reçu avec les K codes possibles, et passe la sortie du corrélateur pour le détecteur, il néglige la présence de réponses des autres tags où il suppose que le bruit total de l'interférence est blanc et gaussien. De toute évidence, si les codes sont orthogonaux, l'interférence avec les autres tags disparaît. D'autre part, si un ou plusieurs codes ne sont pas orthogonaux au code désiré, l'interférence des autres tags augmente mais cette hypothèse n'est plus acceptable. C'est le cas lorsque $n_T/K \rangle\rangle 1$, c'est à dire dans les cas de grand nombre des tags. En transmission asynchrone, ce détecteur est plus vulnérable aux interférences provenant d'autres tags, et le problème des puissances inégales dans les signaux émis par les tags est particulièrement grave. La solution pratique exige une méthode de réglage de puissance qui est contrôlée par le lecteur via un canal de communication distincte que tous les tags sont en permanence sous surveillance.

Le détecteur de décorrélation est conçu pour annuler les effets d'interférence multi-tag, et la complexité dépend linéairement de K. son principe est de corréler le signal reçu avec les K codes possibles, mais il utilise l'inverse de la matrice de corrélation croisée pour décorréler le signal à la sortie du corrélateur. Les symboles détectés sont obtenus en prenant le signe du signal décorrélés. Ce processus élimine les interférences multi-tag, et ne nécessite pas le réglage de la puissance. Le détecteur asynchrone a une plus grande complexité par rapport au détecteur synchrone. Le détecteur de décorrélation est donc bien adapté à des systèmes RFID à étalement de spectre [12].

III.6 L'Analyse en Composantes Indépendantes

L'Analyse en Composantes Indépendantes (ACI) a été proposée, dans la première fois, comme un outil de résolution de BSS. Cependant, bien qu'elle est parfois utilisée comme interchangeable avec BSS, l'ACI a pris une autre dimension différente de BSS après plusieurs méthodes et algorithmes de l'ACI, neuronaux et algébriques, qui ont été développés depuis les années 90 jusqu'à nos jour. En effet, techniquement ACI et BSS sont différents dans leurs tâches. Il s'avère que l'ACI est une méthode statistique d'analyse de données qui peut être considérée comme une extension d'une autre méthode statistique classique d'analyse de données très populaire à savoir l'Analyse en Composantes Principales (ACP) (*en anglais : Principal Component Analysis (PCA)*). En effet, l'ACP cherche à décorréler les variables aléatoires d'entrée en diagonalisant la matrice de covariance de ces variables [11].

L'ACI, en revanche, cherche l'indépendance statistique au-delà des statistiques d'ordre deux en utilisant les statistique d'ordre supérieur des données. En d'autre terme, l'ACI utilise l'hypothèse d'indépendance statistique mutuelle des variables aléatoires recherchées afin de proposer une estimation de ces variables. Ainsi, toute application envisagée de l'ACI doit respecter cette hypothèse d'indépendance statistique. De ce fait, l'ACI est plus flexible et plus générale que BSS. Elle peut être utilisée pour résoudre le problème de BSS, mais BSS ne peut pas être considérée comme ACI seulement et seulement si les hypothèses de l'ACI ont été prise en considération [13].

L'ACI est utilisée dans des domaines aussi divers que le traitement de sources audio, les télécommunications, l'analyse des signaux biomédicaux, la télédétection, le traitement de données géophysiques, la détection et la localisation radar, les séries temporelles en économie, l'extraction de caractéristiques d'images naturelles, la déconvolution aveugle, etc…[11].

III.6.1 Hypothèses

Les hypothèses généralement admises par les méthodes de séparation de mélanges convolutifs appartenant à la classe de l'ACI, sont les suivantes :

- Les sources sont centrées en centrant les observations.
- Les signaux considérés sont stationnaires et ergodiques de sorte que l'on peut estimer les espérances statistiques (mathématiques) par des moyennes temporels.
- La matrice de mélange est inversible à gauche dont la matrice inverse peut être approchée à l'aide de filtres RIF éventuellement non causaux d'ordre suffisamment grands. Ceci implique d'avoir un nombre d'observations supérieur ou égal au nombre de sources.
- Les sources sont supposées statiquement indépendantes
- Les sources à estimer sont non-gaussiennes, sauf une source éventuellement.

III.7 Définition et modèle

La théorie de l'ACI a été développée pour des variables aléatoires. Afin de faciliter les explications de cette théorie, nous nous placerons dans ce cas de figure. Soit un ensemble de variables observées connues x_i avec $i \in \{1,2,\dots,N\}$ où N est le nombre de variables observées. Le terme « connues » traduit la connaissance des réalisations des processus x_i. Leurs densités de probabilité ne sont pas disponibles et seules leurs statistiques sont estimables. Ces variables x_i sont supposées générées par des combinaisons linéaires de variables aléatoires inconnues s_j avec $j \in \{1,2,\dots,P\}$ où P est le nombre de variables cachées, inconnues signifiant qu'aucune information n'est disponible sur ces variables. Par la suite, ce terme perdra son sens original pour signifier plus exactement que très peu d'informations sont supposées connues sur ces variables. Le modèle génératif vectoriel de l'ACI s'écrit alors comme suit :

$$X = AS \qquad \text{(III.23)}$$

où $A = \{a_{ij} | i \in \{1,2,\dots,N\}, j \in \{1,2,\dots,P\}\}$ est matrice de mélange. Cependant, cette définition du modèle de mélange ne suffit pas à estimer de façon unique les variables sous –jacentes de ce modèle. En effet, A étant une matrice non – singulière, le modèle (II.23) est vérifié pour tout couple de matrices $\{A, A^{-1}X\}$. Donc, le modèle de l'ACI doit être compléter par d'autres hypothèses sur les données afin de converger vers une solution unique au problème posé. L'utilisation d'hypothèses supplémentaires sur la structure des mélanges est possible dans certaines applications. Mais à moins de connaître parfaitement la matrice A, ces hypothèses ne feront que réduire l'espace des solutions du problème représenté par (III.23). De ce fait, pour conserver une forme générale au problème et lui designer une méthode de résolution générale, des hypothèses cette fois – ci sur les variables s_j doivent être posées. L'indépendance statistique mutuelle de ces variables se révèle suffisamment

puissante pour proposer une solution unique au modèle (III.23). Elle est plus exigeante puisqu'elle suppose l'annulation de tous les cumulants croisés d'ordre supérieur à deux [13].

Ainsi, nous finissons à cette définition générale de l'ACI: « L'ACI d'un vecteur aléatoire X consiste à estimer le modèle génératif des données (III.23) en déterminant une transformation linéaire $S = WX$ de telle sorte que les composantes de S soient aussi indépendantes que possible par maximisation d'une fonction de mesure de l'indépendance statistique. ». Les méthodes d'ACI reposent donc sur une mesure d'indépendance qui reste à définir. Les différentes approches se différentient par la mesure d'indépendance retenue et par la méthode d'optimisation choisie. Cependant, toute méthode d'ACI repose sur les même hypothèses et restrictions que nous allons répertorier dans le paragraphe suivant [11].

III.7.1 Hypothèses et indéterminations

Les composantes du vecteur S sont supposées statistiquement indépendantes. Cette hypothèse est fondamentale pour garantir l'estimation du modèle de l'ACI. Les composantes indépendantes (CI) ainsi extraites doivent avoir des distributions non – gaussienne. Cependant, il s'avère qu'au plus une CI peut avoir une distribution gaussienne [11].

Une autre hypothèse supposée pour l'ACI est que la matrice de mélange A doit être inversible, c'est – à – dire que ses colonnes doivent être linéairement indépendantes. De ce fait, le nombre de lignes de A reste supérieur ou égal à son nombre de colonnes pour éviter le cas sou déterminé.

Sachant ces deux hypothèses, le modèle de l'ACI est identifiable en utilisant uniquement le vecteur des observations X. Mais quelques indéterminations inhérentes à la modélisation de l'ACI demeurent. En effet, le modèle linéaire et instantané de l'ACI (II.23) peut être se réécrit sou la forme suivante :

$$X = AS = \sum_{j=1}^{p} a_j s_j \qquad \text{(III.24)}$$

Où le vecteur a_j représente la j^{ème} colonne de la matrice de mélange$A$. Cette équation est strictement équivalent à :

$$X = AS = \sum_{j=1}^{p} \left(\frac{1}{\alpha_j} a_j\right)(\alpha_j s_j) \qquad \text{(III.25)}$$

Où les α_j sont des constantes non nulles. La multiplication d'une source s_j par toute constante α_j peut être donc annulée par la division de la colonne correspondante a_j de A par la même constante α_j et ceci sans qu'il ait une influence sur les hypothèses posées sur le modèle de l'ACI. Par conséquent, il est impossible d'estimer les variances des CI extraites. Pour remédier à ce problème, on suppose que les sources possèdent de variance unité.

Aussi, il est impossible de déterminer le signe de chaque CI extraite puisque le choix $\alpha_j = -1$ est possible. Ainsi, le modèle de l'ACI reste valide sous la transformation linéaire suivante :

$$X = AS = AM^{-1}MS \qquad \text{(III.26)}$$

Où la matrice M est une matrice de permutation de même dimension que le vecteur des sources. Dans la somme $\sum_{j=1}^{p} a_j s_j$, les termes $a_j s_j$ peuvent être permutés librement. L'ordre des CI n'est donc pas déterminable.

En conclusion, la prise en compte de ces deux indéterminations signifie que l'extraction des CI n'est possible qu'à une matrice $\hat{A} = DM$ prés, où la matrice D est diagonale d'éléments α_j, de même dimension que le vecteur des sources et de rang plein [11].

III.8 Prétraitements

Des prétraitements sur le vecteur des données, tels que rendre les données centrées et le blanchiment, permettant de s'affranchir de certaines indéterminations précédentes et de simplifier, de ce fait, le problème d'extraction des CI.

III.8.1 Données centrées :

Cette étape de prétraitement est liée aux cumulants croisés et à leurs estimateurs qui sont d'expression beaucoup plus simple dans le cas de variables aléatoires centrées. Le vecteur X est ainsi transformé en :

$$X^c = X - E\{X\} \qquad \text{(III.27)}$$

Par cette opération, les CI sont elle – aussi centrées puisqu'on a :

$$E\{S^c\} = A^{\#}E\{X^c\} = 0 \qquad \text{(III.28)}$$

où le sigle # définit l'inversion matricielle de Moore – Penrose, encore appelée pseudo inverse, qui est utilisée lorsque la matrice A n'est pas carrée. Lorsqu'elle est carrée, l'inversion matricielle est utilisée et l'équation s'écrit :

$$E\{S^c\} = A^{-1}E\{X^c\} = 0 \qquad \text{(III.29)}$$

La matrice de mélange A n'est pas modifiée par cette opération qui peut donc toujours être appliquée aux données sans affecter l'estimation de A [13].

III.8.2 Blanchiment :

Le blanchiment est une transformation linéaire qui consiste à décorréler et à imposer une variance unité aux variables du vecteur centré X^c telle que :

$$Z = VX^c \qquad \text{(III.30)}$$

où les composantes du vecteur Z sont centrées, décorrélées et de variance unité, ce qui signifie que sa matrice de covariance est une matrice identité. L'obtention de matrice de la transformation linéaire V est possible en utilisant l'ACP telle que :

$$V = D^{-\frac{1}{2}}E^T \quad \text{(III.31)}$$

où la matrice D est une matrice diagonale de dimension NxN dont les éléments diagonaux d_i avec $i \in \{1,2,\dots,N\}$ sont les valeurs propres de la matrice de covariance de X et sont rangés par ordre décroissant, c'est – à – dire que $d_1 > d_2 > \cdots > d_N$. La matrice E de dimension NxN est la matrice orthogonale des vecteurs propres de la matrice de covariance de X. L'ACP permet de projeter les données dans un espace de dimension P engendré par les sources. Donc, seules les P premières valeurs propres et les vecteurs propres associés sont conservés. On obtient ainsi :

$$Z = VAS^c = US^c \quad \text{(III.32)}$$

La matrice de covariance de Z peut se mettre sous la forme :

$$Cov_Z = UE\{S^c(S^c)^T\}U^T = UCov_S U^T = UU^T \quad \text{(III.33)}$$

Or les composantes du Z sont centrées, décorrélées et de variance unité, ce qui signifie que : $UU^T = I$, où I est la matrice identité, par conséquent U est une matrice orthogonale. Cependant, le blanchiment de X ne permet pas d'estimer les CI, mais simplifie celle – ci de moitie. En effet, il est nécessaire d'estimer seulement les $P\,(P-1)/2$ inconnues de la matrice U au lieu les NxP éléments de la matrice de mélange A [13].

Il est à noter que le blanchiment des données n'est pas une étape nécessaire pour certains algorithmes de l'ACI développés dans la littérature, comme par exemple, l'algorithme Infomax , mais elle est recommandée parce qu'elle permet d'accélérer la convergence des algorithmes. L'estimation de la matrice U repose sur des critères d'optimisation qui caractérisent l'indépendance statistique recherchée [11].

III.8.3 Algorithme FastICA et la non – gaussianité

Avec l'algorithme FastICA, les CI sont obtenues par la transformation linéaire WZ où Z est le vecteur des données centrées et blanchies et la matrice $W = [w_1, w_2, \dots, w_P]^T$ est l'estimateur de la matrice U^T. Les vecteurs lignes w_j^T de la matrice W sont estimés en maximisant la fonction d'optimisation suivante :

$$J_G(W) = \sum_{j=1}^{P} \left\{ E\{G(w_j^T Z)\} - E\{G(\vartheta)\} \right\}^2 \quad \text{(III.34)}$$

sous la contrainte : $E\{(WZ)(WZ)^T\} = I$. La variable ϑ est une variable gaussienne de même variance que $w_j^T Z$. La fonction G est choisie de telle sorte que l'estimation de W ait une variance minimale et qu'elle soit robuste. Des fonctions ont été déduites de ces considérations et s'avèrent utilisables de manière générale :

$$G_1(s_j) = \frac{1}{\alpha_1} log\left(cosh(\alpha_1 s_j)\right),\ \ G_2(s_j) = -\frac{1}{\alpha_2} exp\left(-\frac{\alpha_2 s_j^2}{2}\right),\ \ G_1(s_j) = \frac{1}{4} s_j^4$$

où $1 \leq \alpha_1 \leq 2$ et $\alpha_2 \approx 1$ sont des constantes. La minimisation de (III.34) par la matrice W s'appuie sur un algorithme du point fixe. La mise à jour de chaque ligne de la matrice W est selon la procédure itérative suivante :

$$w_j = E\{Zg(w_j^T Z)\} - E\{g'(w_j^T Z)\}w_j \quad \text{(III.35)}$$

$$w_j = w_j - \sum_{k=1}^{j-1}(w_j^T w_k)w_k \quad \text{(III.36)}$$

$$w_j = \frac{w_j}{\sqrt{w_j^T w_j}} \quad \text{(III.37)}$$

où g et g' sont respectivement les dérivées de G et g. L'équation (III.35) sert à rendre le vecteur w_j orthogonal aux lignes de W déjà extraites aux étapes précédentes de l'algorithme. Afin d'assurer que les CI extraites soient de variance unité, on normalise les w_j selon l'équation(III.37) [11].

III.9 Application de l'ACI dans le système RFID

De nombreux algorithmes de traitement du signal appliqués dans le système RFID. Dans ce mémoire, un algorithme FASTICA est introduit dans le système RFID.

Pour appliquer l'ACI, nous devons adapter cet algorithme. L'initialisation est une phase très importante de l'algorithme de séparation. Dans notre cas, nous initialisons le vecteur de séparation de chaque utilisateur par sa séquence d'étalement. La matrice de séparation ainsi obtenue joue le rôle des séquences d'étalement mais avec des coefficients d'intercorrélation plus fiables. L'opération de séparation est donc effectuée conjointement avec le désétalement. Le traitement du signal dans le lecteur est illustré comme suit [12] :

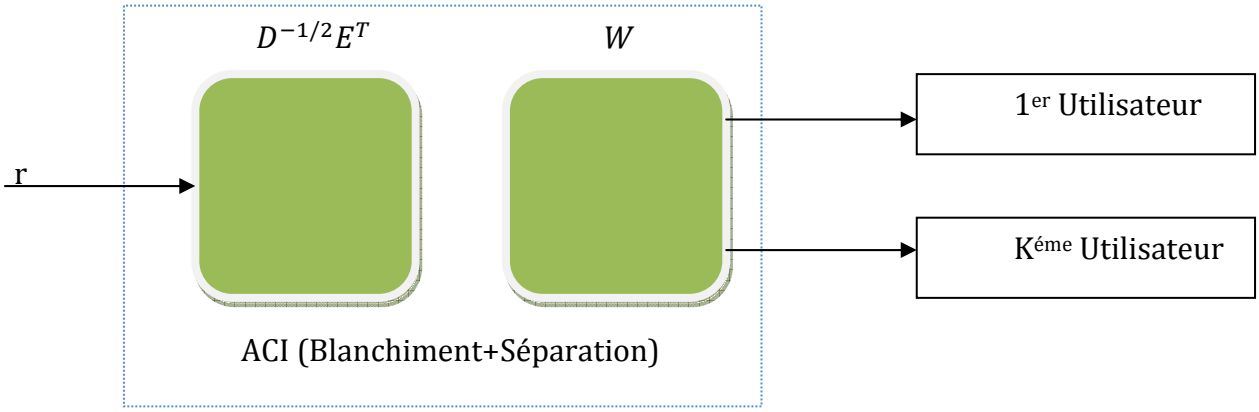


Figure III.7 la communication dans le système RFID en utilisant l'ACI

Conclusion

Dans ce chapitre, nous avons abordé le domaine de la technique d'accès multiple CDMA et la séparation de sources, en mettant en évidence la manière de partager le canal de communication par l'accès multiple les différentes stratégies pour résoudre le problème de séparation des sources. Ainsi, les applications de CDMA et les algorithmes à base de l'ACI dans le système RFID.

Chapitre 4

Résultats de Simulation : Tests et Evaluation

Introduction

Notre objectif est de proposer une étude comparative d'algorithmes d'anticollisions de signaux RFID passifs et de montrer l'intérêt apporté par l'application des techniques d'étalement du spectre associé aux méthodes conventionnelles comme la technique ALOHA et ses différentes variantes.

La première partie de notre travail est consacrée à l'étude et l'évaluation des performances des différents algorithmes d'anticollision à base d'ALOHA à savoir : l'ALOHA, le Slotted ALOHA et le Farme Slotted Aloha. Les performances des techniques ALOHA et Slotted ALOHA sont évaluées par la probabilité de succès et le temps de réponse moyen.

La deuxième partie est consacrée à l'élaboration d'un algorithme d'anticollision à base de l'ACI, pour cela nous avons appliquée le détecteur FastICA dans la technique CDMA. En utilisant la technique d'étalement de spectre du signal, nous proposons la lecture des plusieurs Tags simultanément dans une durée d' un slot de temps dans l'algorithme FSA ce qu'implique la réduction du nombre de collisions, ce qui est bénéfique pour accélérer le processus de lecture par la réduction de la communication entre le lecteur et les Tags, réduire l'interférence, et assurer la sécurité du système.

Dans notre travail, nous ne considérons pas le cas de la technique CDMA simple à cause de complexité du récepteur, mais nous utilisons la combinaison de TDMA et CDMA.

Les performances de la technique CDMA appliquée dans le système RFID sont évaluées par l'aptitude à résister aux perturbations, c'est-à-dire à assurer un BER aussi faible que possible.

Ces simulations ont été réalisées sous l'environnement MatLab version 7.1.il est à noter que les simulations sont faites suivant les conditions suivantes :

- La communication est entre un lecteur et plusieurs tags.
- Tous les tags sont à la même distance par rapport au lecteur.
- Les codes utilisés sont les codes de gold de différents facteurs d'étalements.

Les résultats se présentent comme suit:

1. Les performances des protocoles d'anticollisions ALOHA et Slotted ALOHA en terme de probabilité de succès et le temps de réponse moyen.
2. Les performances de protocole FSA sont évaluées par l'efficacité du système.
3. Les récepteurs utilisés dans la technique CDMA sont le décorrelateur et MMSE et les comparer avec un récepteur à base de l'algorithme FASTICA. A la fin nous avons évalué les performances de la technique CDMA appliqué dans le système RFID en termes d'efficacité.
4. Comparaison entre les résultats.

V.1 Simulation de la chaine de réception d'un système RFID :

Les conditions de simulation de la chaine de réception dans une communication entre un lecteur et un tag dans un système RFID sont :

Tableau IV.1 les conditions de simulation de la chaine d'E/R

Le paramètre	**La valeur**
La taille de symbole	20 bits
Le nombre des Tags	1
La période du signal	$2.5*10^{-6}$
La fréquence porteuse	F_P =14MHZ

V.1.1 Le Signal en bande de base et le codage du signal en bande de base :

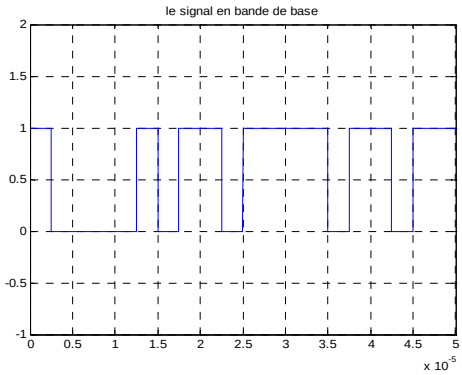


Figure IV.1 Le signal en bande de base

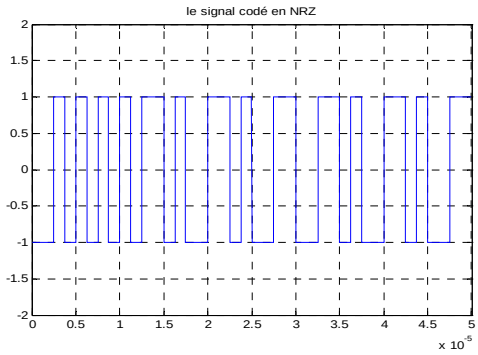


Figure IV.2 signal codé en NRZ

V.1.2 Le signal dans canal AWGN reçu par le lecteur et le spectre du signal démodulé :

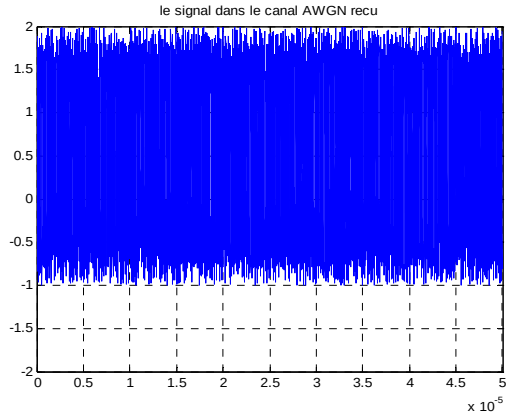


Figure IV.3 Le signal dans canal AWGN reçu par le lecteur

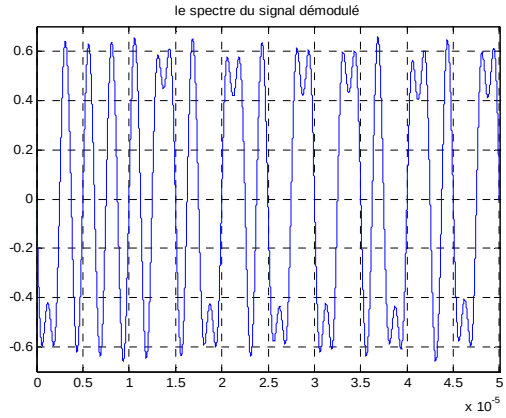


Figure IV.4 Le spectre du signal démodul

V.1.3 Le signal reçu démodulé et le signal original:

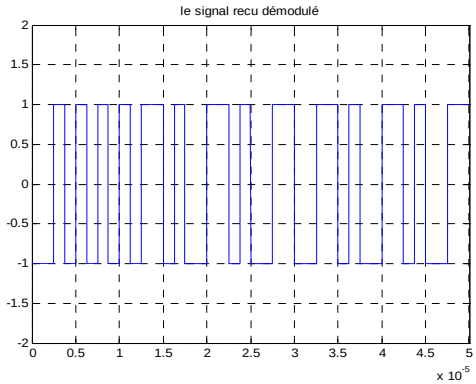


Figure IV.5 le signal reçu démodulé

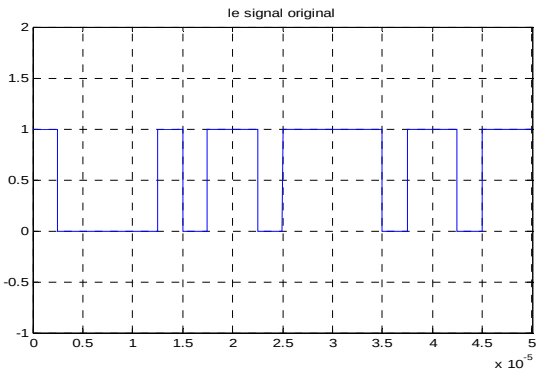


Figure IV.6 le signal original après la réception

V.2 Simulation de la distance entre le lecteur et le Tag dans un système RFID :

Cette simulation est faite pour trouver la distance séparant le tag au lecteur suivant les conditions suivantes :

Pour chaque puissance d'émission du lecteur nous avons calculé la puissance reçue par le Tag à chaque distance qui les sépare. La fréquence porteuse est de 900MHZ.

$$P_{recu} = G_t G_r P_x C^2 / (4\pi F D)^2 \qquad \text{(IV.1)}$$

P_{recu} : La puissance reçue par le tag.

G_t : Le gain de l'antenne du lecteur.

G_r : Le gain de l'antenne du Tag.

P_x : La puissance émise par le lecteur.

F : La fréquence porteuse.

D : La distance entre le lecteur et le Tag.

$G_r = G_t = 1$

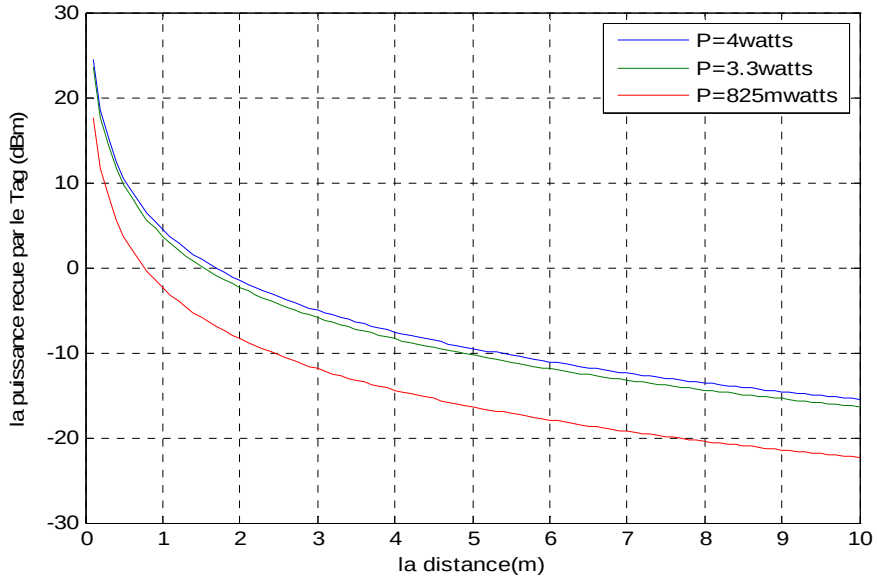


Figure IV.7 la distance entre le lecteur et le Tag dans un système RFID

V.3 Performances des protocoles d'anticollision ALOHA et Slotted ALOHA et Frame Slotted ALOHA:

V.3.1 Les performances du protocole ALOHA :

Les résultats de simulation que nous allons présenter ici nous permettront d'analyser les performances du protocole ALOHA qui est une technique d'anticollision probabiliste utilisée dans le système RFID. Notre objectif est d'évaluer la probabilité de succès ,et le temps de réponse moyen en fonction de la densité des paquets.

La simulation du protocole ALOHA est faite par le calcul de la probabilité de succès, pour chaque valeur de la densité des paquets ($G \in [0,2]$).

Les résultats obtenus sont comparés par rapport aux résultats trouvés par la formule théorique.

$$S = Ge^{-2G}$$

Où $G = \frac{K}{N}$ est la densité des paquets entrant dans le système.

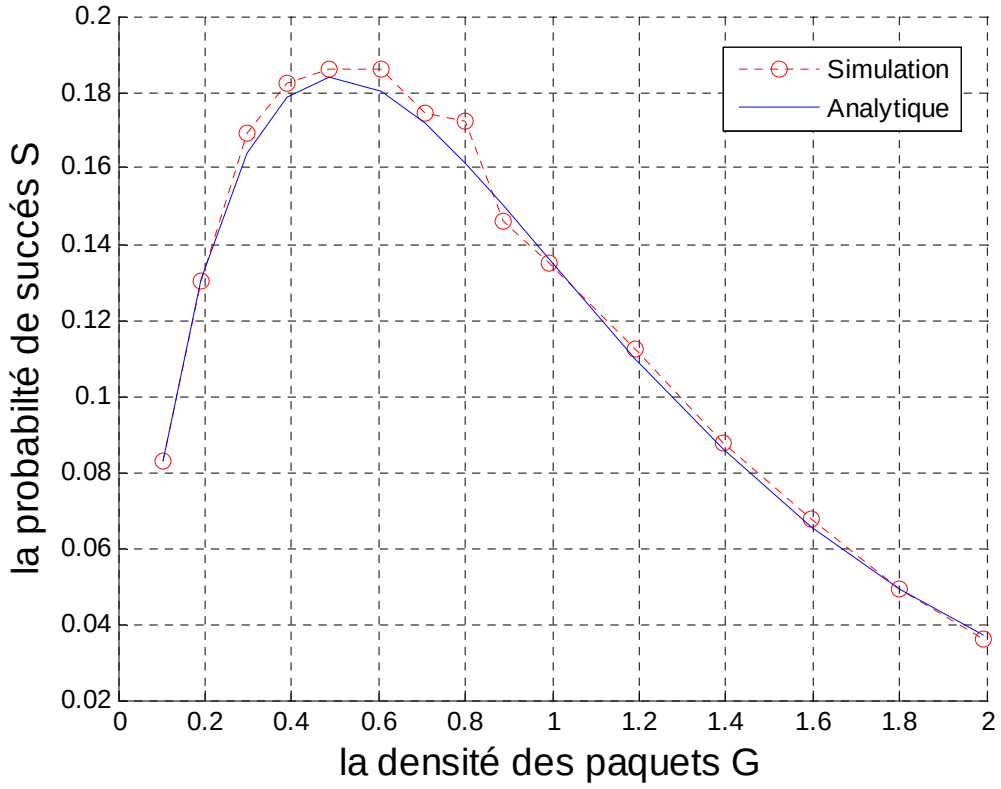


Figure IV.8 la probabilité de succès S du protocole ALOHA en fonction de la densité des paquets G

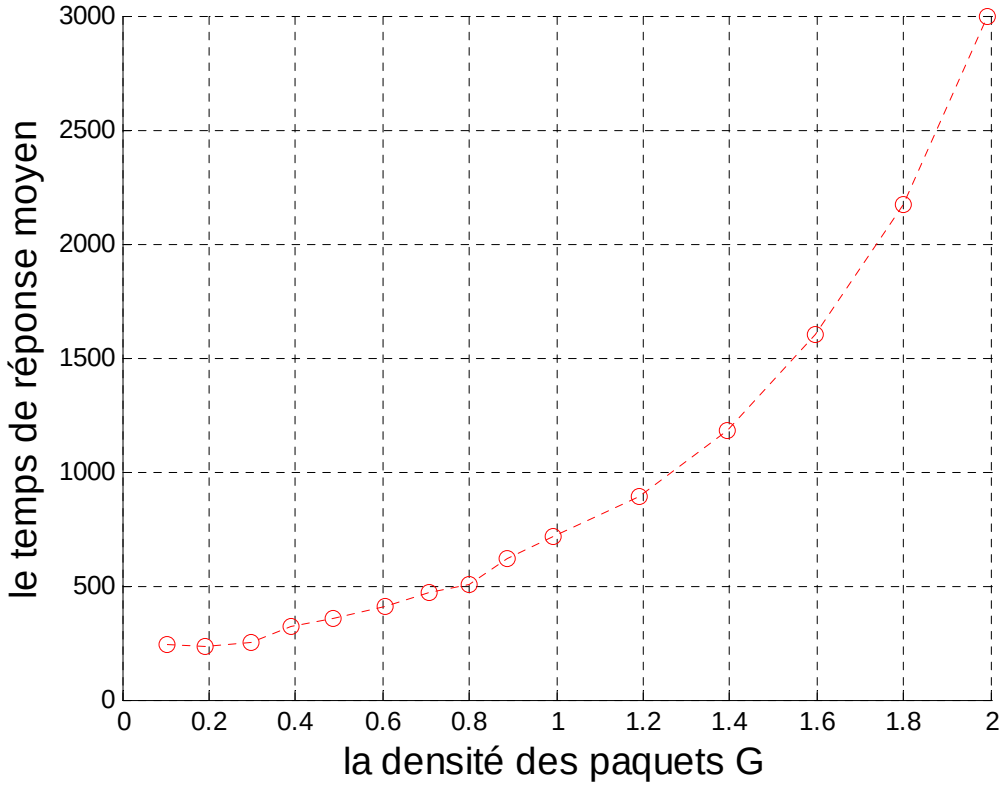


Figure IV.9 Le temps de réponse moyen en fonction de la densité (G) du protocole ALOHA

- **Interprétation des résultats :**

La Figure IV.8 nous montre que la probabilité de succès attient sa valeur maximum lorsque la densité des paquets de données égale à 0.5 :

$G = \frac{1}{2} \Rightarrow K = \frac{N}{2}$ Dans ce cas le débit maximum est égale à : $Débit_{max} = \frac{1}{2T_p} e^{-1}$ paquets/s.

Si le nombre des tags (K) est supérieur à N/2 c'est-à-dire G est supérieur à 0.5, le nombre des collisions augmente et le débit de transmission est considérablement diminué.

L'inconvénient de ce protocole est la diminution du débit de transmission en le comparant par rapport aux techniques TDMA et FDMA :

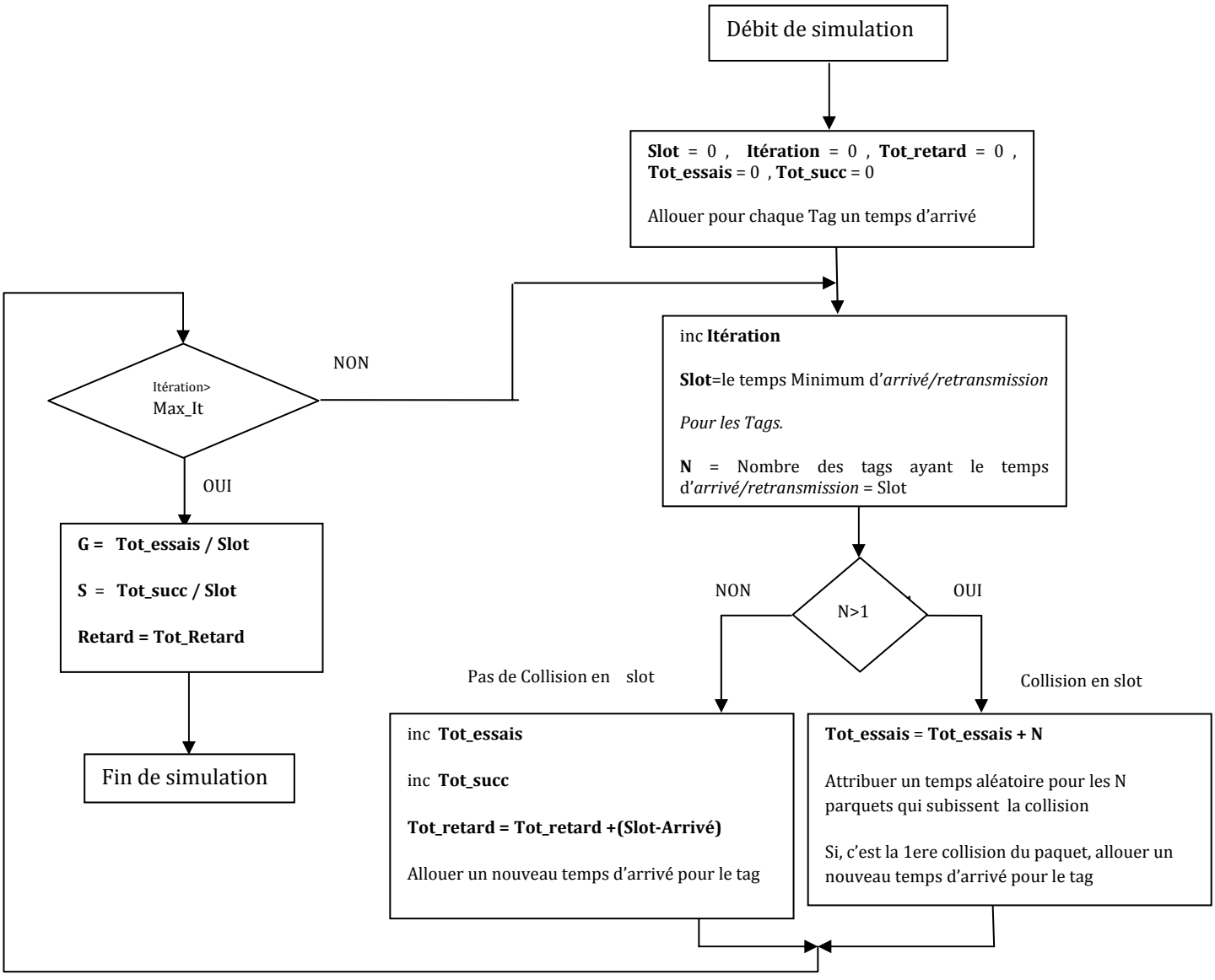
Dans le cas de TDMA et FDMA le débit maximum est attient lorsque touts les utilisateurs ont transmis avec la vitesse maximale égale à $R_{\max} = \frac{1}{T_P}$ donc :

$Débit_{\max,TDMA} = Débit_{\max,FDMA} = \frac{1}{T_P}$ Ce qui implique que : $\frac{(Débit_{\max} T_p)ALOHA}{(Débit_{\max} T_p)TDMA} = \frac{1}{2e} = 0.1839$

Dans la Figure IV.9 le temps de réponse moyen augmente en fonction de la densité des paquets de données, en effet si on augmente la densité **G** c'est-à-dire l'augmentation du nombre des Tags ce qui conduit à l'appariation des plusieurs collisions des données, cette explication se voit au niveau de l'équation du temps de réponse moyen : $D_{Aloha} = T_d + \Delta(e^{2G} - 1)$

G augmente $\Rightarrow$ e^{2G} augmente $\Rightarrow$ e^{-2G} diminue $\Rightarrow$ la probabilité de transmission des paquets diminue $\Rightarrow$ la probabilité de collision augmente.

V.3.2 Performances du protocole Slotted ALOHA



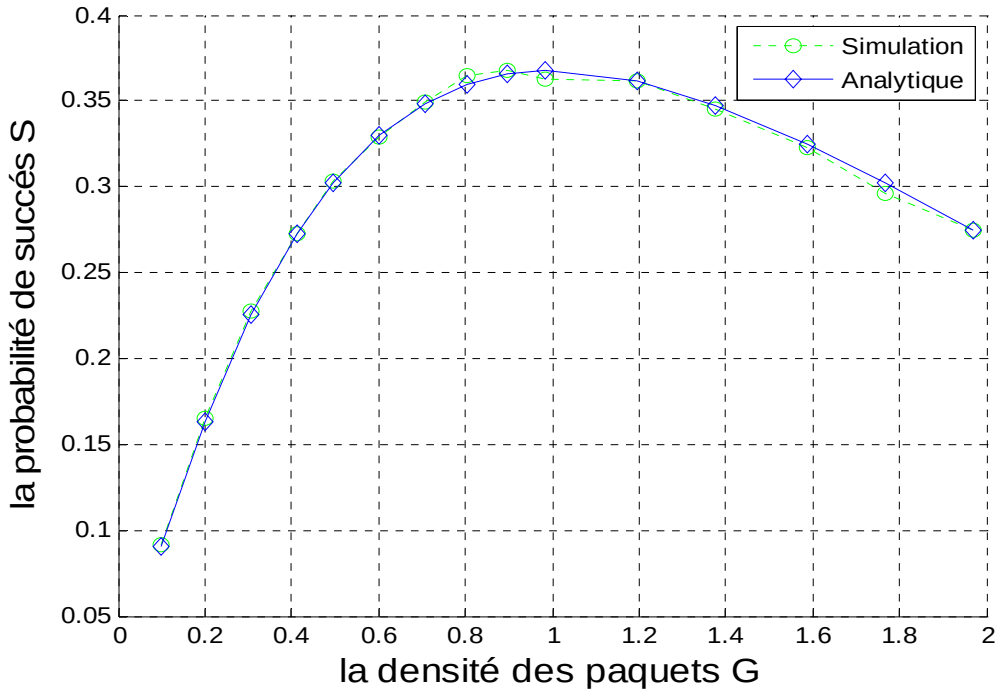


Figure IV.10 la probabilité de succès de Slotted Aloha en fonction de la densité des paquets

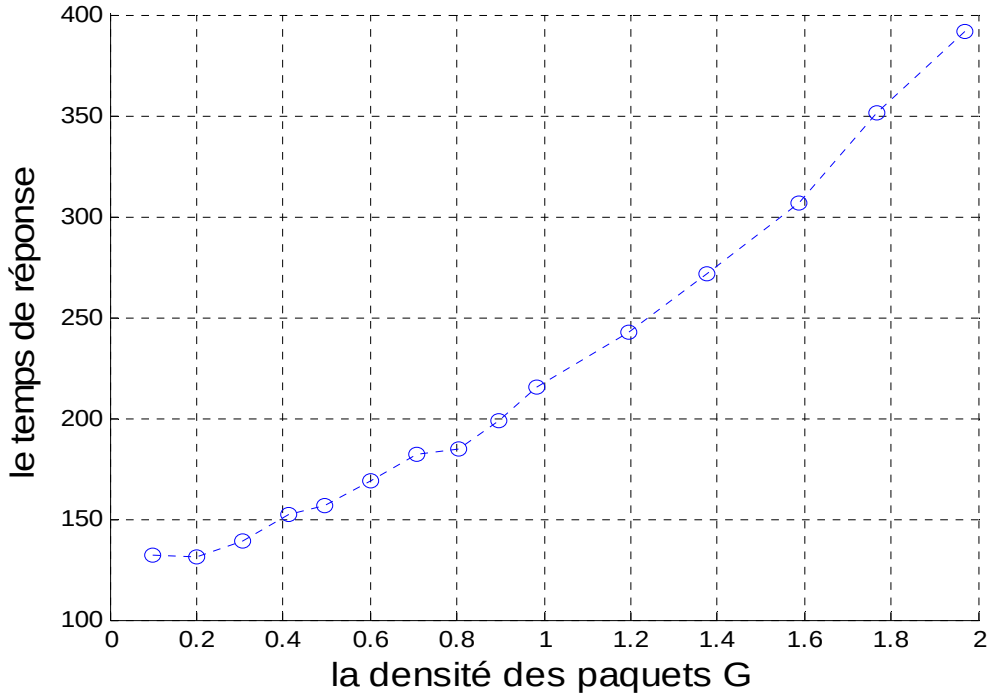


Figure IV.11 le temps de réponse de Slotted Aloha en fonction de la densité des paquets

- **Interprétation des résultats :**

La Figure IV.10 nous montre que la probabilité de succès attient sa maximum lorsque la densité des paquets de données égale à 1 :

$G = 1 \Rightarrow K = N$ Dans ce cas le débit maximum est égal à $Débit_{\max} = \frac{1}{T_P} e^{-1}$ paquets/s.

Si le nombre de Tags (K) est supérieur à N, le nombre des collisions augmente ce qu'implique une diminution exponentielle de débit de transmission.

En comparant le débit de transmission de Slotted Aloha avec la technique TDMA on trouve que :

$$\frac{\left(Débit_{\max} T_p\right) S - ALOHA}{\left(Débit_{\max} T_p\right) TDMA} = 0.3688$$

La Figure IV.11 montre que le temps de réponse augmente en fonction de la densité des paquets de données, cette explication se voit au niveau de l'équation du temps de réponse: $D_{S-Aloha} = T_d + \Delta\left(e^G - 1\right)$

G augmente $\Rightarrow$ e^{2G} augmente $\Rightarrow$ e^{-2G} diminue $\Rightarrow$ la probabilité de transmission des paquets diminue $\Rightarrow$ la probabilité de collision augmente.

V.3.3 Technique d'accès au canal basée sur FSA.

Dans le protocole FSA (framed slotted ALOHA), le lecteur commence l'interrogation par l'envoie de la longueur de trame «*frame* » (plusieurs slots) aux Tags, chaque Tag sélectionne d'une manière aléatoire un slot parmi les slots disponibles ; et transmet son ID (identifient ou numéros de série de longueur maximale égale à 32bits). L'efficacité η avec n_T Tags et N slots dans une trame « *frame* » est donnée par :

$$\eta\left(n_T, N\right) = \frac{n_T}{N}\left(1 - \frac{1}{N}\right)^{n_T - 1} \qquad \text{(IV .2)}$$

Il est évident, d'après l'équation ci-dessus que l'efficacité du protocole FSA dépend du choix de la longueur de trame (*frame*) N, en donnant le nombre des Tags existants dans la gamme de lecture.

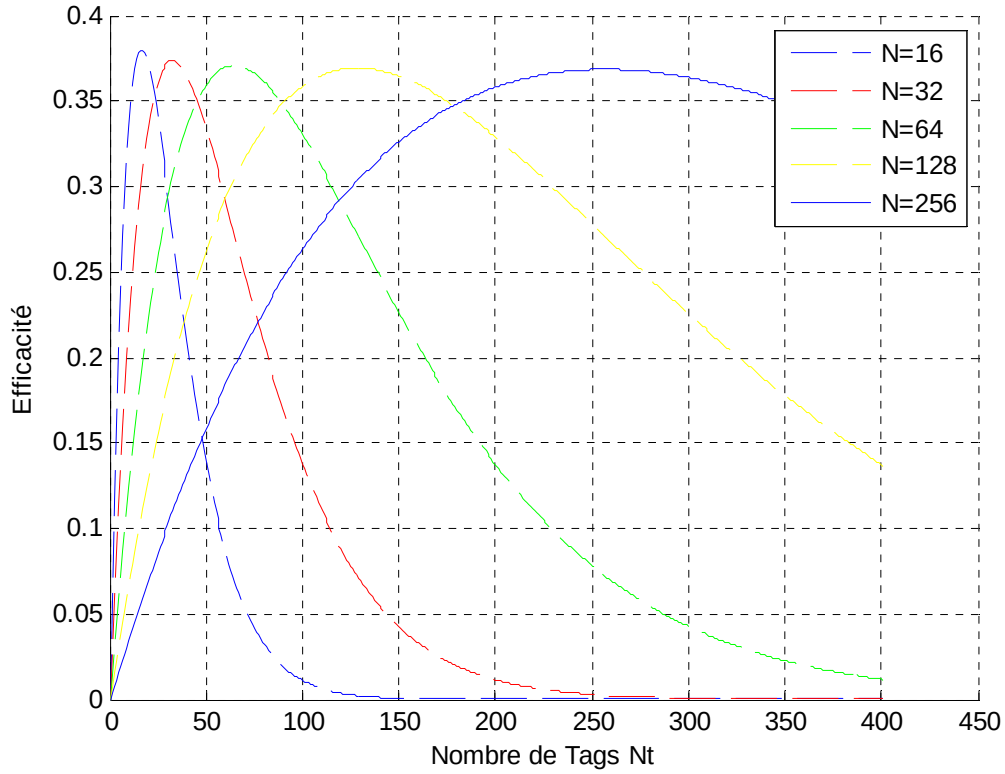


Figure IV.12 l'efficacité du protocole FSA en fonction du nombre des Tags pour un nombre de slots N donné.

D'après la Figure IV.12 nous remarquons que l'efficacité du système en utilisant le protocole FSA dépend du nombre des Tags et le nombre des slots, on voit que les courbes de l'efficacité sont maximales dans le cas où le nombre des slots égale au nombre des Tags c'est-à-dire $N = n_T$.

V.4 Performances de la technique CDMA appliquée dans système RFID.

V.4.1 Les performances des récepteurs décorrélateur et MMSE dans la technique CDMA appliqués dans le protocole FSA.

Les résultats de simulation que nous allons présenter ici, nous permettront d'analyser les performances des détecteurs décorrélateur et MMSE dans le système RFID basé sur la technique CDMA associée au protocole FSA avec un nombre des slots NS=1. L'objectif est d'évaluer le taux d'erreurs binaire BER suivant les conditions ci-dessous :

- Pour une longueur des séquences d'étalement SF et le nombre de bits à transmettre par chaque tag N=32 codé par NRZ (non retour à zéro), nous faisons varier le nombre de tag K et traçons sur le même graphe les différentes courbes de la variation de BER en fonction de SNR.

- Pour un nombre de tags K et le nombre de bits à transmettre par chaque tag N fixés, nous faisons varier la longueur des séquences d'étalement SF et les résultats sont présentés sous forme de graphiques du taux d'erreur binaire BER.

Il est à noter que les données utilisées dans la simulation sont choisies de telle manière que la séquence des bits de chaque identifiant (ID de tag) est unique et de longueur de 32 bits, ce qui assure un nombre maximum des séquences des IDs égale à 2^{32}, en suite ces séquences de bits seront codées par NRZ. Les quatre premiers IDs des Tags sont représentés ci-dessous dans le tableau IV.2. La simulation est faite en utilisant 64 séquences de longueur de 32 bits.

Tableau IV.2 les numéros de séries (IDs) utilisés dans la simulation

TAG	SEQUENCE DES BITS DES IDENTIFIANTS (IDs) UTILISEE DANS LA SIMULATION
TAG1	1 1 1 1 0 1 0 1 0 0 1 0 0 1 0 0 1 0 1 0 0 1 1 1 0 0 0 0 0 0 0 1
TAG2	0 1 1 1 0 1 0 1 0 0 1 0 0 1 0 0 1 0 1 0 0 1 0 1 0 0 0 0 0 0 1 0
TAG3	1 0 1 1 0 1 0 1 0 0 1 0 0 1 0 0 1 0 1 0 0 1 1 1 0 0 0 0 0 0 1 1
TAG4	0 0 0 1 0 1 0 1 0 0 1 0 0 1 0 0 1 0 1 0 0 1 0 1 0 0 0 0 1 0 0 0

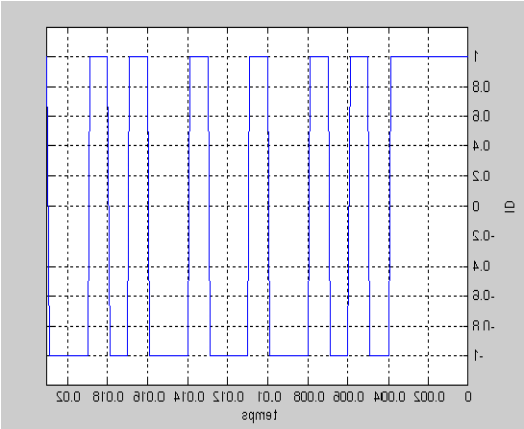


Figure IV.14 l'identifiant ID de longueur 32 bits du numéro 1 codé par NRZ

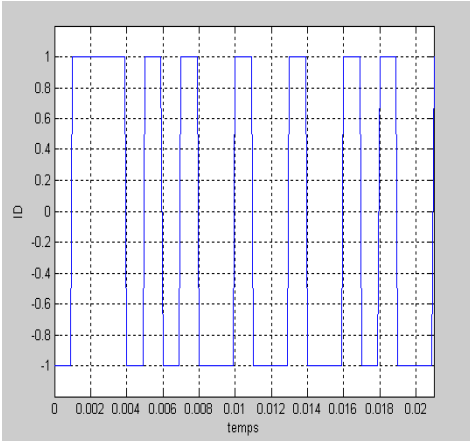


Figure IV.13 l'identifiant ID de longueur32 .
bits du tag numéro 2 codé par NRZ

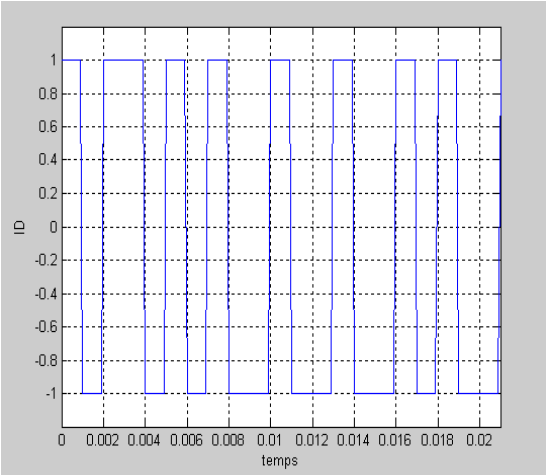


Figure IV.16 l'identifiant ID de longueur 32 bits du numéro 3 codé par NRZ

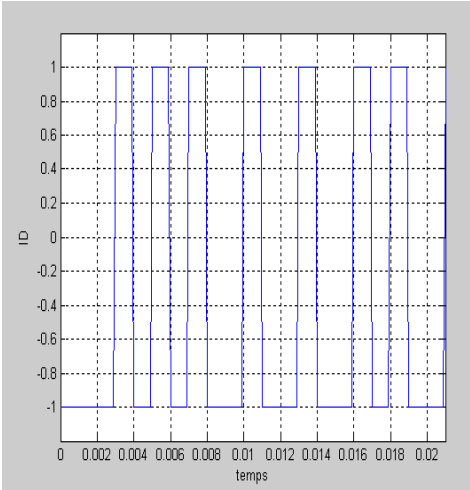


Figure IV.15 l'identifiant ID de longueur 32 bits du numéro 4 codé par NRZ

V.4.1.1 Performances du récepteur Décorrélateur

V.4.1.1.1 Etudes de l'influence du nombre de tags :

Ici nous avons fixé le nombre des données transmises N=32bits codés par NRZ et la longueur des séquences d'étalement (SF) et ensuite nous avons évalué pour chacun des détecteurs les performances de point de vue BER en fonction de SNR en variant le nombre de tags K. il convient de préciser que les codes gold qui sont utilisés.

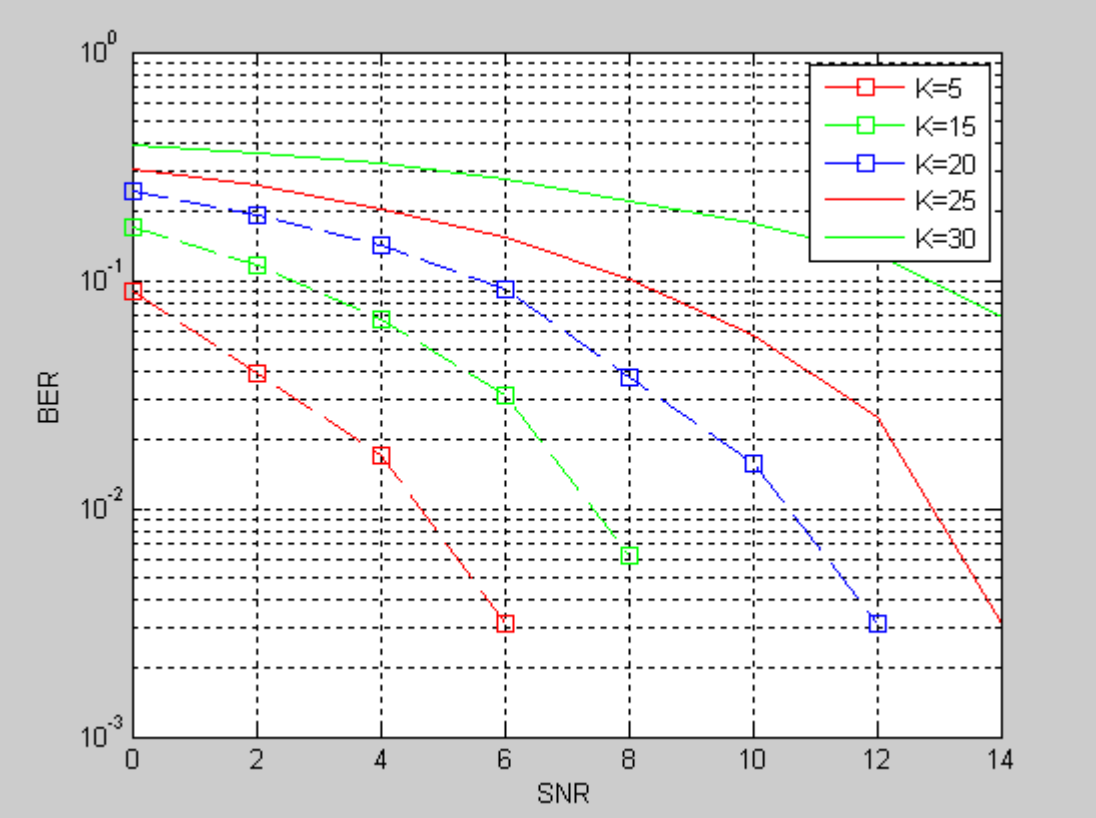


Figure IV.17 Performances du détecteur décorrélateur pour K (nombre des tags) variable. Le canal considéré est de type AWGN, gain d'étalement SF=31, la taille des données transmises N= 32bits codées NRZ,

V.4.1.1.2 Etudes de l'influence du gain d'étalement :

Dans cette étude, nous allons maintenir constant le nombre de Tags K et la taille des données transmises N=32bits codées par NRZ. Ensuite, nous faisons varier le gain d'étalement (SF). Ainsi nous évaluons les performances de chacun des détecteurs à l'aide des courbes représentant les variations du BER en fonction de celles du SNR.

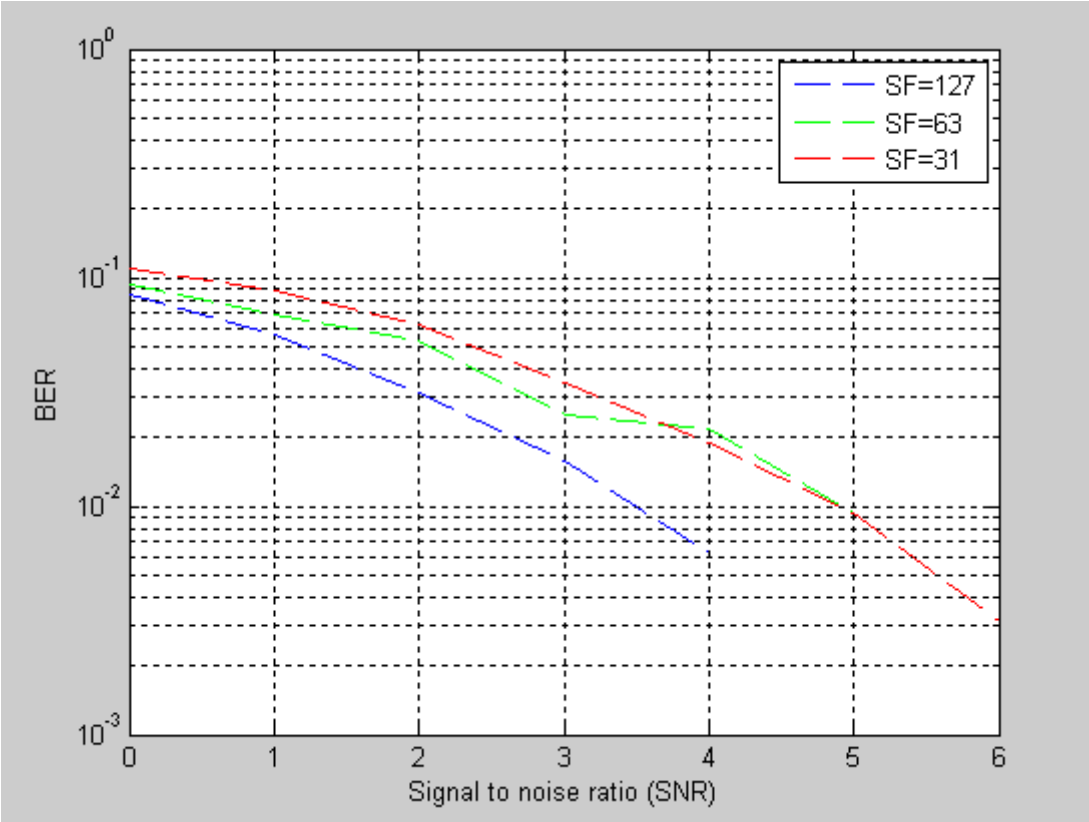


Figure IV.18 Performances du détecteur décorrélateur pour SF (gain d'étalement) variable. Le canal considéré est de type AWGN, nombre de tags K=5, la taille des données transmises N=32bits codées par NRZ,

V.4.1.2 Performances du récepteur MMSE

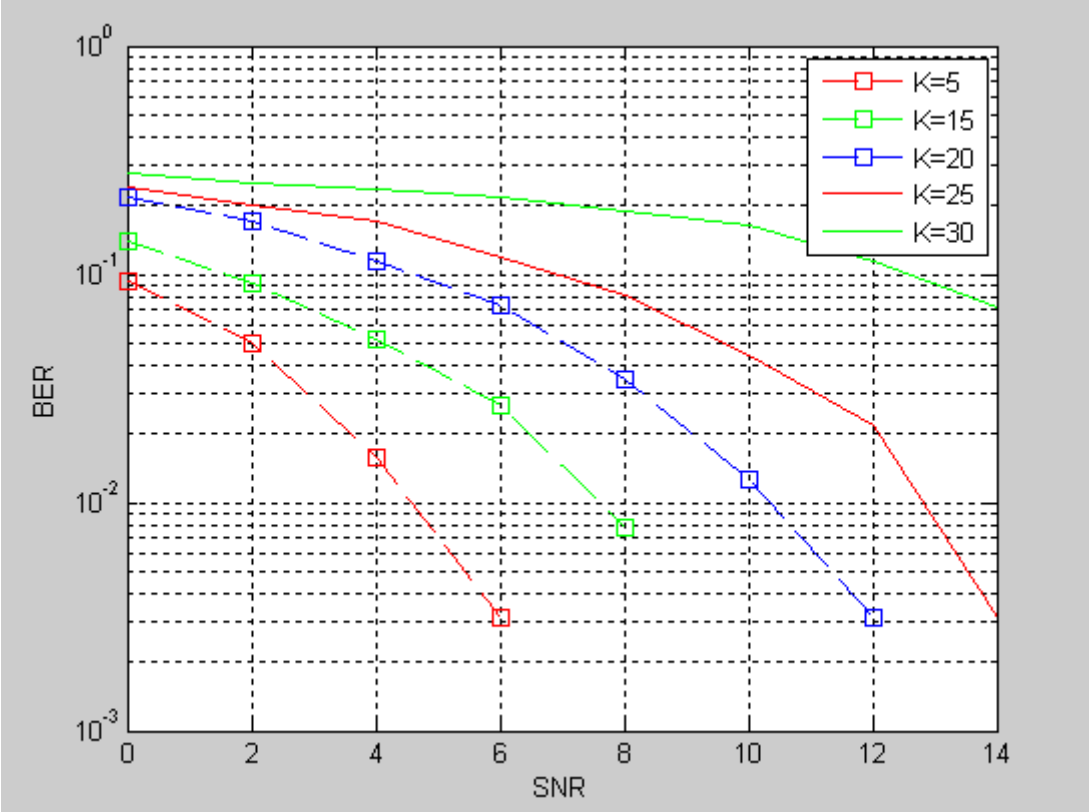


Figure IV.19 Performances du détecteur MMSE pour K (nombre des tags) variable. Le canal considéré est de type AWGN, gain d'étalement SF=31, la taille des données transmises N=32bits codées par NRZ.

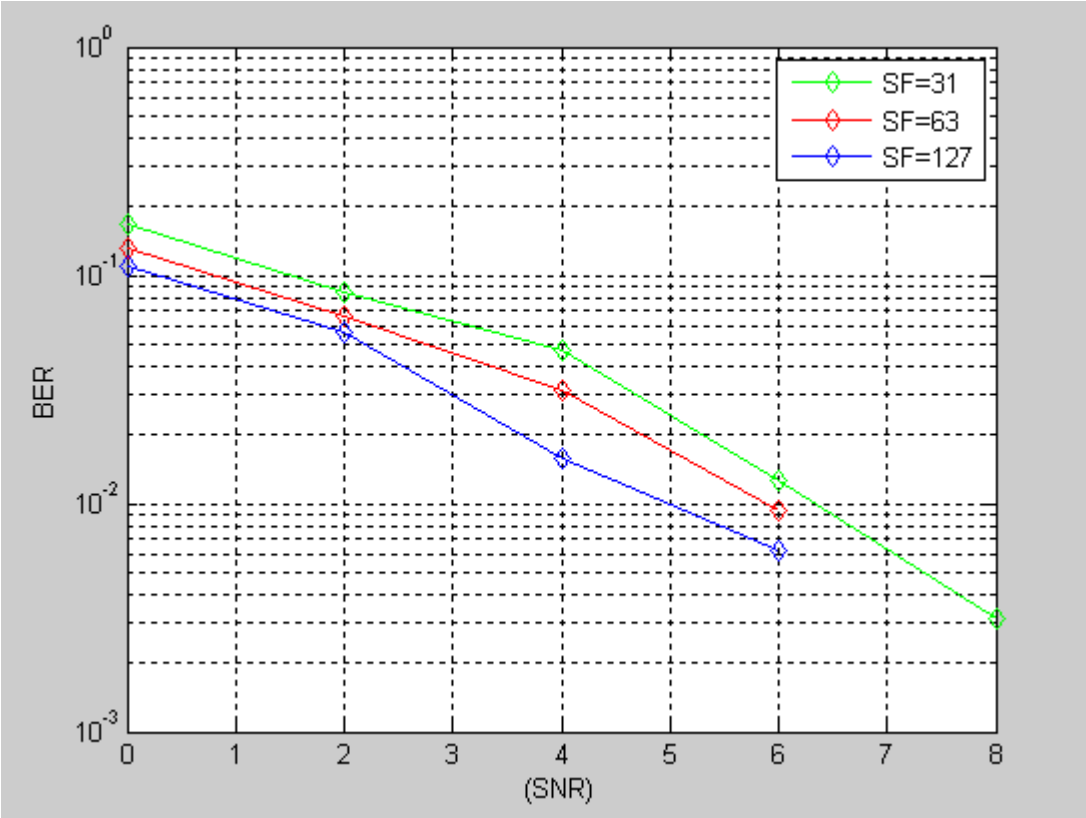


Figure IV.20 Performances du détecteur MMSE pour SF (gain d'étalement) variable. Le canal considéré est de type AWGN, nombre de tags K=25, taille des données transmises N=32bits codées par NRZ,

- Interprétation des résultats :

- L'influence du nombre des Tags :

Les performances du détecteur décorrélateur sont illustrées dans la Figure IV.17 :

Il est clair, d'après ces figures montrent que l'augmentation du nombre des Tags dans la zone de lecture. c'est-à-dire, dans le même slot du temps augmente le BER, par exemple pour le SNR égale à $6dB$, le BER égale à 0.5×10^{-3} pour 10 Tags et 10^{-2} pour 20 Tags ,ce qui implique une dégradation de la qualité du signal reçu dans le lecteur, mais ca reste toujours acceptable, en effet cette caractéristique due à la suppression du bruit inter-Tags, pour cette raison ,ce détecteur est utilisé dans le système RFID à étalement de spectre.

Les performances du détecteur MMSE sont illustrées dans la Figure IV.19

D'après cette figure, l'augmentation du nombre des Tags implique l'augmentation du BER pour une même valeur du SNR. par exemple pour SNR égale à $4dB$, le BER est proche de 10^{-2} pour 10 Tags et il est proche de 10^{-1} pour 20 Tags, nous remarquons que la variation du BER est faible en augmentant le nombre des Tags à cause de l'annulation du bruit inter-tags d'une part, et d'autre part la variation du BER est due à l'utilisation

des codes d'étalements avec l'intercorrélation qui n'est pas nulle par conséquence ils sont quasi-orthogonaux.

- L'influence du gain d'étalement :

Les Figures IV.18 et V.20 nous montrent que l'augmentation du gain d'étalement a une influence positive sur la variation du BER cela est expliquée par le fait que la puissance de chaque symbole b^i est multipliée par le carré du facteur d'étalement et par conséquent, l'augmentation du facteur d'étalement améliore bien la puissance du Tag seul par rapport à la puissance d'interférence inter-Tags.

V.4.2 Les performances du récepteur à base de l'analyse en composantes indépendantes .

Nous avons utilisé l'algorithme FastICA pour l'élaboration du récepteur ACI des signaux CDMA, FastICA est un algorithme très puissant pour la séparation des sources non- gaussiennes. Il est basé sur le principe de l'algorithme de point fixe, l'algorithme est résumé dans le chapitre 2.

V.4.2.1 Etudes de l'influence du nombre de tags :

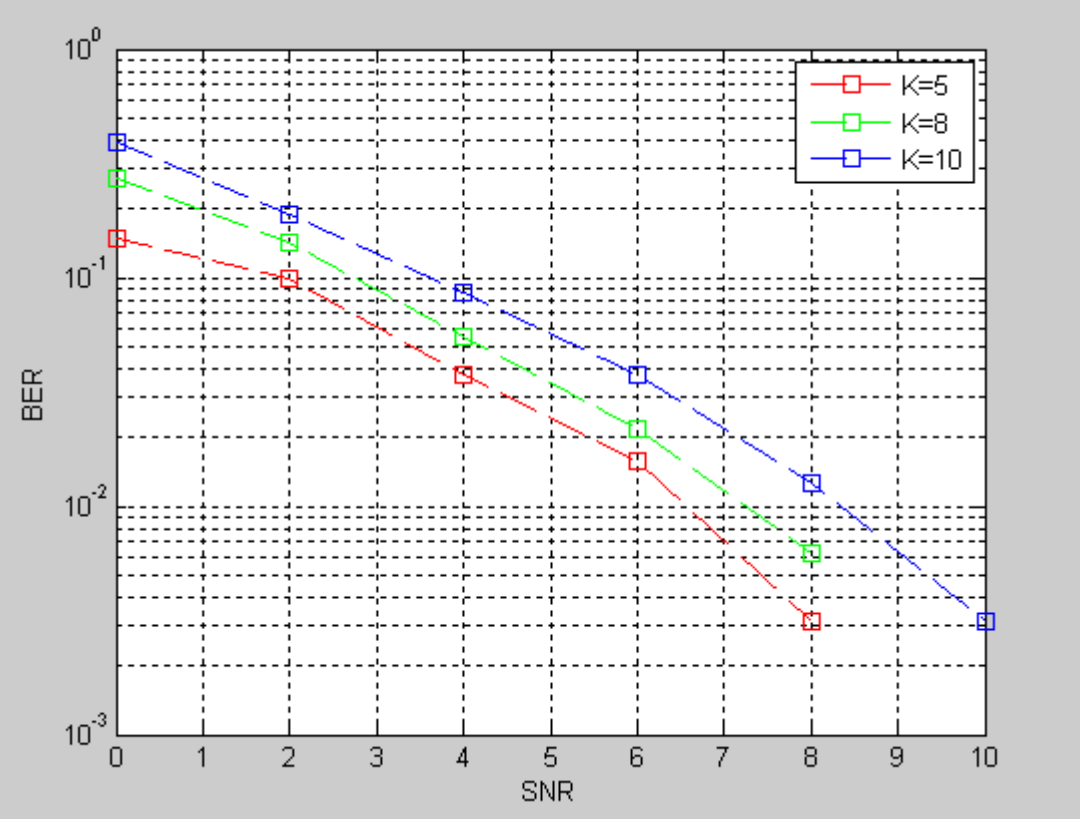


Figure IV.21 Performances du détecteur ACI pour K variable, le canal considéré est de type AWGN, gain d'étalement SF=31, taille des données transmises égale à 32 bits.

La figure IV.21 nous donne les courbes des performances du système CDMA associés au protocole FSA avec un seul intervalle de temps (time slot) sur un canal AWGN, en utilisant l'ACI à la réception, pour différents nombres de tags. A partir de cette figure, nous pouvons remarquer que le détecteur ACI donne des bonnes performances pour des valeurs de SNR élevées. Même en augmentant le rapport($\tau_c = \frac{K}{SF}$) le récepteur FastICA donne des bonnes performances. Donc on peut dire que l'ACI possède un bon comportement vis-à-vis les interférences à taux de charge élevé (τ_c).

V.4.2.2 Etudes de l'influence du gain d'étalement :

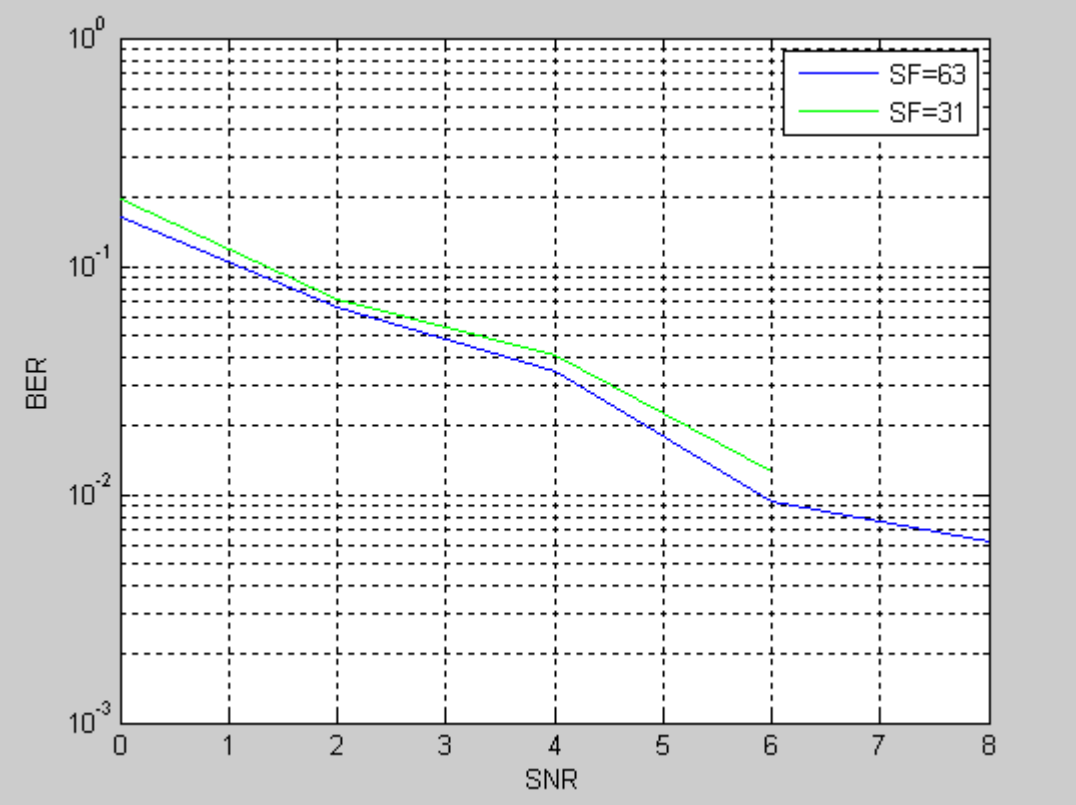


Figure IV.22 Performances du détecteur ACI pour SF variable, le canal considéré est de type AWGN, nombre d'utilisateur K=5, taille des données transmises égale à 32 bits.

Dans cette partie, nous avons fait une simulation de 5 Tags chacun envoyant 32 bits codés par NRZ. Les données sont une fois étalées par un facteur d'étalement égale à 31 et une deuxième fois avec un facteur d'étalement égale à 63.

La figure IV.22 nous montre les performances du système qui sont meilleurs au fur et à mesure que nous étalons avec facteur d'étalement plus grand. En effet, en augmentant le facteur d'étalement, les interférences inter-symboles diminuent et donc le détecteur arrive mieux à séparer les données.

Nous observons que : pour un SNR de 6 dB, nous avons un BER de $\mathbf{9,37.10^{-3}}$ pour SF=63 et un BER de $1,25.\mathbf{10^{-3}}$ pour SF=31(facteur d'étalement).

V.4.3 Comparaison entre le protocole Aloha et Slotted Aloha

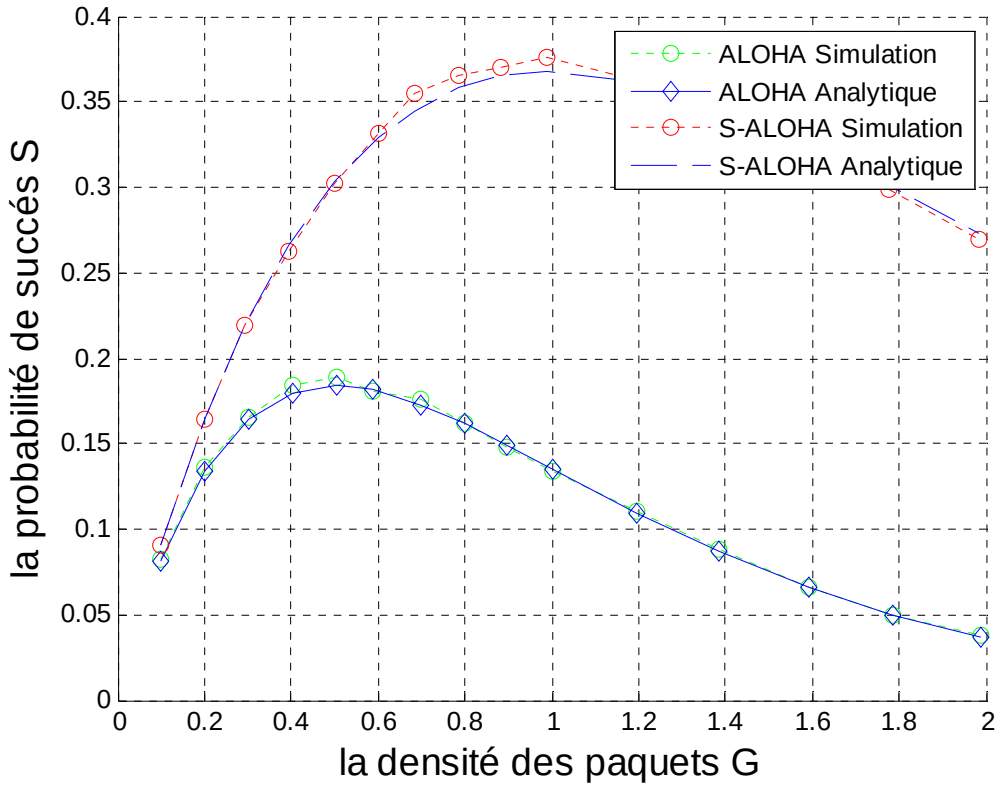


Figure IV.23 comparaison entre les probabilités de succès du protocole Aloha et Slotted Aloha

La simulation des protocoles d'anticollision est faite par le calcul du débit de transmission des protocoles ALOHA et Slotted ALOHA pour chaque valeur de la densité des paquets G en calculant le temps qu'il faut pour transmettre le paquet des données.

Les résultats obtenus sont comparés par rapport à ceux trouvés avec les formules théoriques $S_{slottedaloha} = G.e^{-G}$ et $S_{aloha} = G.e^{-2G}$.

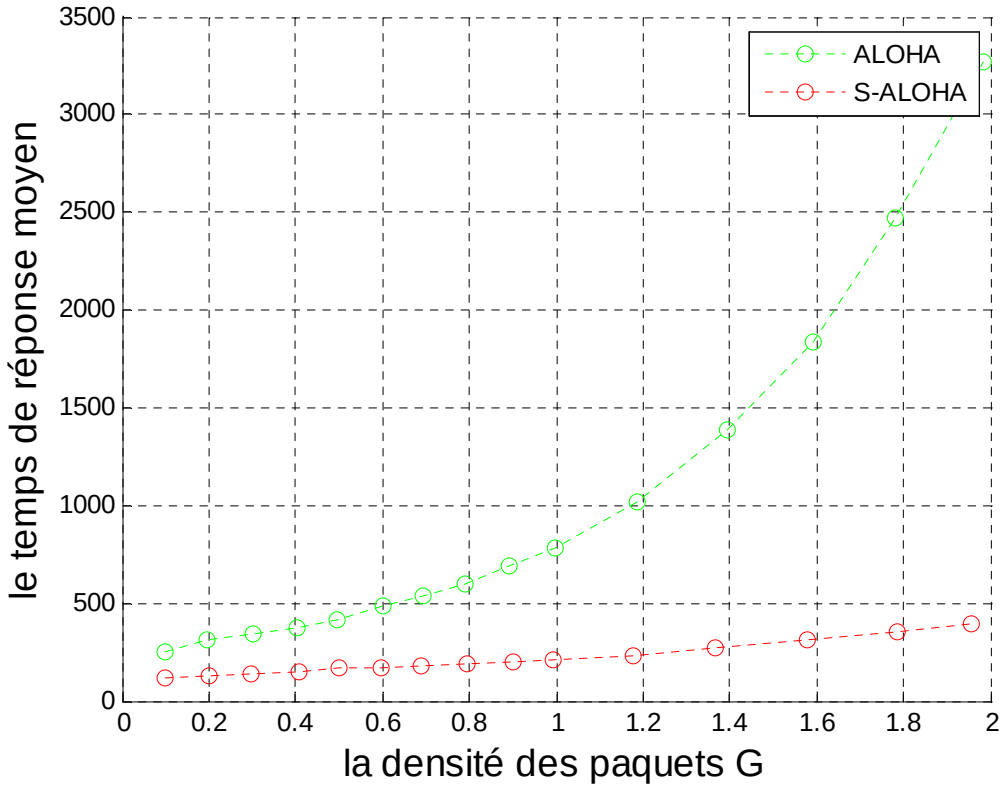


Figure IV.24 comparaison entre le temps de réponse de protocole Aloha et Slotted Aloha

- **Interprétation des résultats :**

D'après la figure IV.23, en comparant les débits des protocoles Aloha avec Slotted Aloha on trouve que :

$$\frac{\left(Débit_{\max} T_p\right) S-ALOHA}{\left(Débit_{\max} T_p\right) ALOHA} = \frac{0.3688}{0.1839} = 2$$

D'après la figure IV.24, le temps de réponse moyen du protocole Slotted Aloha est inferieur à celui de protocole Aloha, en effet dans les équations ci-dessous nous avons :

$D_{S-Aloha} = T_d + \Delta\left(e^{G} - 1\right)$ Est inferieur à $D_{Aloha} = T_d + \Delta\left(e^{2G} - 1\right)$

V.4.4 Comparaison entre les différents récepteurs de la Technique CDMA.

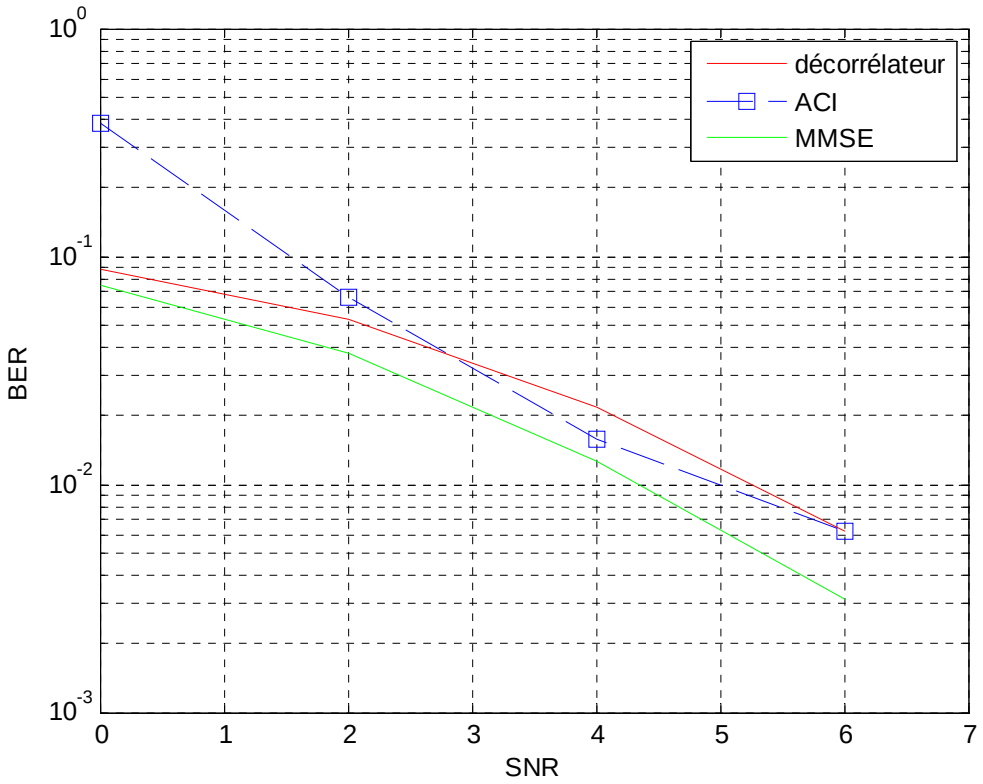


Figure IV.25 comparaison entre les récepteurs décorrélateur, MMSE et ACI

Nous allons comparer le système CDMA à base de l'ACI appliqué dans le système RFID, en utilisant l'algorithme FastICA, avec deux types de détecteurs à savoir : le décorrélateur et MMSE.

Les conditions de simulation sont les suivantes :

- des séquences de Gold de taille SF=31.
- un canal AWGN.
- une taille de données égale à 32 bits codés avec NRZ.
- un nombre d'itérations égale à 250 pour l'ACI.

Les résultats obtenus sont donnés par la figure IV.25. Nous constatons que le détecteur ACI améliore les performances du système CDMA pour SNR élevées, dans cette graphique au delà de SNR=4 dB les valeurs de BER ne sont pas considérées à cause des erreurs de calcul dues aux calculs dans Matlab. Les performances du détecteur MMSE sont atteintes par le détecteur ACI, ce qui permet de réduire la complexité du système en éliminant les calculs complexes par le MMSE.

V.4.5 L'efficacité du système RFID à étalement de spectre.

L'efficacité du système RFID à étalement du spectre est donnée par :

η_{SS} = Nombre des tags identifiés/nombre maximum des tags qu'on peut identifier.

L'efficacité est définie dans une trame (*frame*) de N intervalles de temps (time slot) du protocole FSA. Dans ce cas le nombre maximum qu'on peut décoder est NK, et la probabilité pour que un tag choisisse un intervalle de temps (slot) et un code est donnée par $1/NK$. On considère que le nombre des tags dans la zone de lecture est n_T, l'efficacité du système est donnée par :

$$\eta(n_T, N) = \frac{n_T}{NK}\left(1 - \frac{1}{NK}\right)^{n_T - 1} \qquad \text{(IV.3)}$$

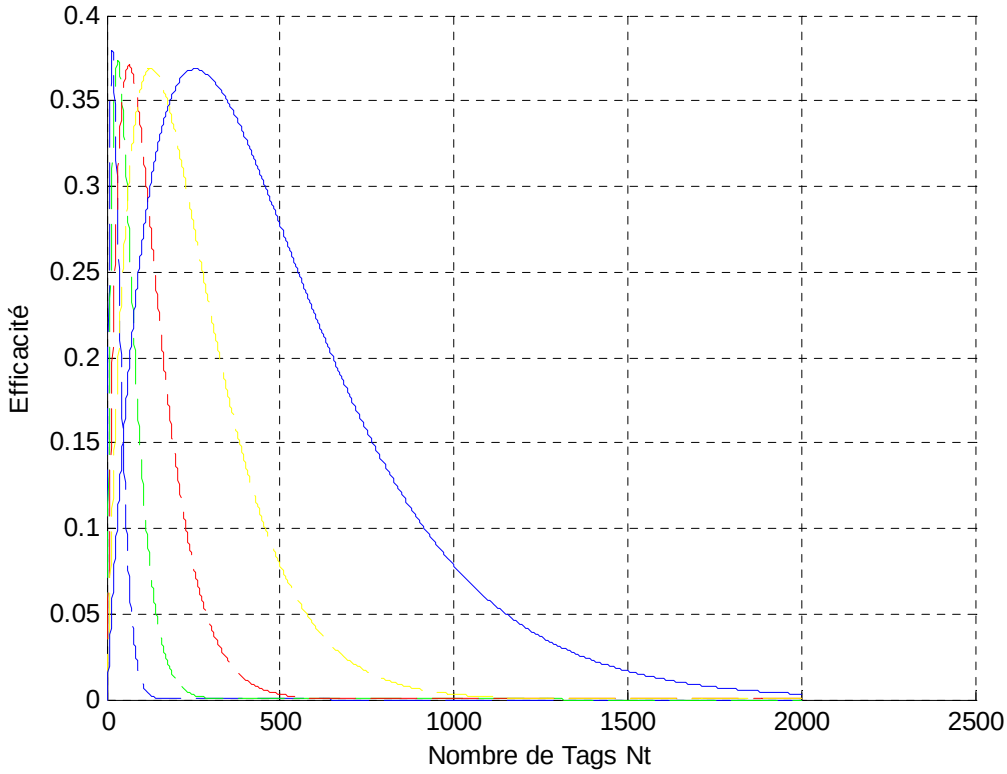


Figure IV.26 L'efficacité du système RFID en fonction du nombre des tags pour Un nombre des codes d'étalement K=1

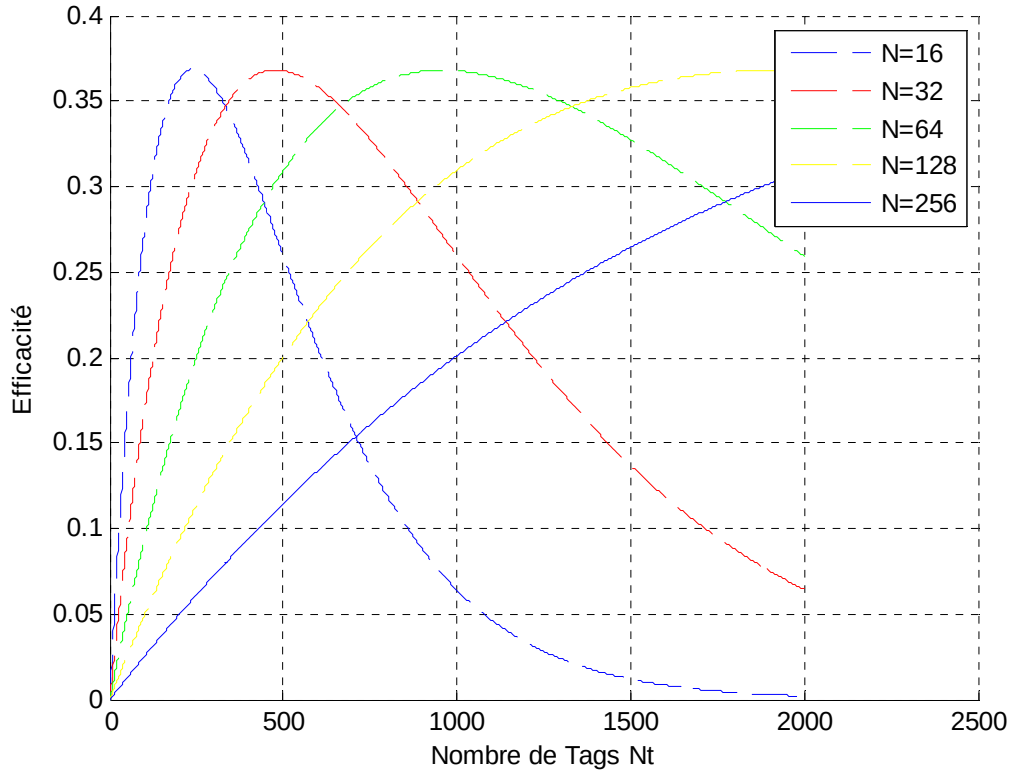


Figure IV.27 L'efficacité du système RFID en fonction du nombre des tags pour un nombre des codes d'étalement K=15

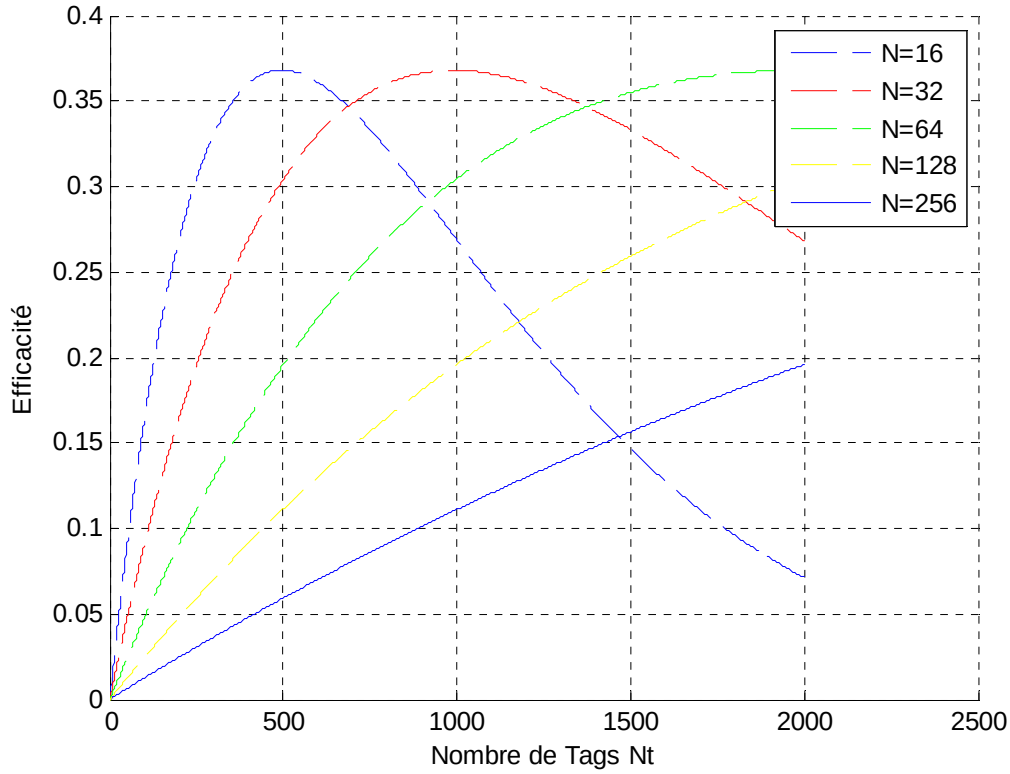


Figure IV.28 L'efficacité du système RFID en fonction du nombre des tags pour un nombre des codes d'étalement K= 31

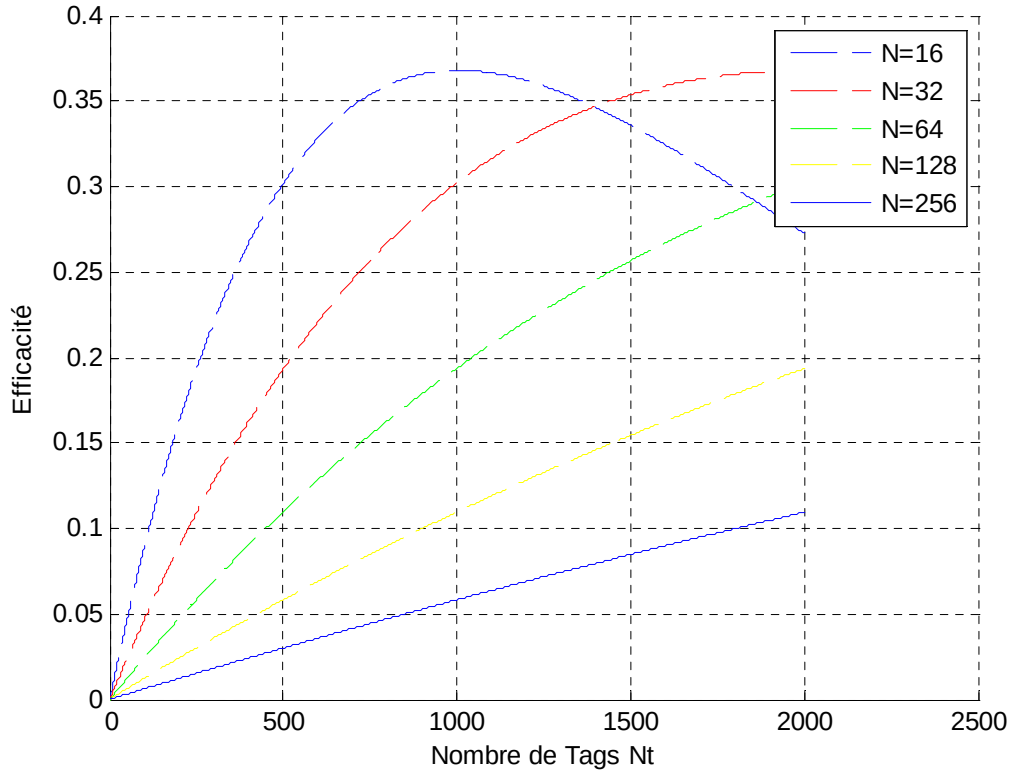


Figure IV.29 L'efficacité du système RFID en fonction du nombre des tags pour un nombre des codes d'étalement K= 63

D'après les figures IV.26, IV.27, IV.28 et IV.29 l'efficacité maximale est égale à ($0.37=1/e$) pour une valeur élevée de NK, ce maximum est atteint si $n_T = NK$, en effet si le nombre des tags est connu, le lecteur peut fixer le nombre d'intervalles de temps et les codes d'étalements.

Ces figures montrent quelques exemples des résultats d'efficacités analytiques, il est évident que pour K=1 (équivalent au système dans le cas du protocole FSA simple), le système est limité à un nombre petit des tags, pour un grand nombre des tags le système est inefficace. Par conséquent le nombre des codes est utilisé comme un moyen en plus pour gérer l'efficacité du système.

Conclusion

Les résultats présentés dans ce chapitre nous ont permis d'évaluer les performances de système RFID. Dans un premier temps, nous avons évalué les performances des protocoles ALOHA et Slotted ALOHA en termes de probabilité et débit de transmission et le protocole Frame Slotted ALOHA (FSA) en termes d'efficacité.

Dans un second temps, nous nous sommes intéressés aux techniques d'accès multiples CDMA appliqués aux signaux RFID Où nous avons évalué les performances de système en termes d'efficacité ainsi les performances de différents détecteurs.

L'avantage principal de l'utilisation de la technique CDMA combinée avec la technique TDMA en utilisant le protocole FSA est l'amélioration de ce dernier pour éviter le problème de perte de quelques Tags non identifiés à cause de leurs collisions successives entre eux. Et ceci est garanti de faite que la technique CDMA ayant le pouvoir d'éviter ces collisions dans chaque intervalle de temps (slot). La simulation des différents détecteurs (récepteurs) de la technique CDMA appliquée dans le système RFID montre que le choix du détecteur dépend de l'application envisagée, si on connaît apriori le nombre des tags dans un slot de temps (ce qui est en générale difficile), on utilisera le décorrélateur et l'application du détecteur FastICA résout ce problème parce qu'il sépare les différents IDs d'une manière aveugle. D'autre part le détecteur MMSE n'est pas utilisé à cause de la complexité des calculs. Pour rendre le décorrélateur applicable en pratique il faut faire une estimation du nombre des tags dans un slot temporel.

Conclusion et perspectives

Ce mémoire de Magister a été consacré essentiellement à évaluer les performances des protocoles d'anticollision à base ALOHA à savoir le protocole ALOHA, Slotted ALOHA et Framed Slotted ALOHA (FSA) comparés aux techniques d'accès multiples.

Le système RFID à étalement du spectre est utilisé dans notre travail en appliquant la combinaison d'accès multiples par répartition de codes (CDMA) avec le protocole FSA.

Les résultats de simulation montre que l'application de CDMA améliore l'efficacité des procédures d'anticollision pour du grand nombre des Tags, ainsi nous avons évalué les performances des différents détecteurs à savoir le décorrélateur et le MMSE en les comparent avec un détecteur à base de l'ACI, les résultats obtenus montrent que ce détecteur est meilleur par rapport au décorrélateur et attient les performances de MMSE pour des SNR élevées. D'autres part, le détecteur à base de l'ACI est meilleur par rapport aux autre détecteurs parce que le détecteur décorrélateur nécessite une phase d'estimation du nombre des tags dans un slot temporelle et le MMSE présente des complexités des calculs, deux contraintes dont le détecteur ACI s'affaranchit.

Comme perspectives, nous pensons que ce travail peut être amélioré en tenant compte de :

- L'amélioration du protocole FSA par l'estimation du temps d'une trame et son adaptation avec le nombre des tags. dans ce dernier c'est-à-dire rendre le slot dynamique, et l'application de la technique CDMA dans ce protocole.
- Des performances des protocoles d'anticollisions à base d'arbre et à base de compteur.
- L'application de la technique d'accès multiples par répartition des codes CDMA dans un protocole à base d'arbre.
- L'application de l'algorithme noisy FastICA comme récepteur de la technique CDMA associée au protocole Frame Slotted ALOHA.

Bibliographie

1 Dominique Paret, « Applications en identification radiofréquence et cartes à puce sans contact », collection EEA, Dunod, 2003.

2 G. Avoine, "RFID et Sécurité Font-Elles Bon Ménage?", SSTIC06, 2006.

3 P. Hauet, "L'Identification par Radiofréquence (RFID) Techniques et Perspectives".

4 M. Schubler, C. Damm, M. Maasch, R. Jakoby, "Performance Evaluation of Left- Handed Delay Lines for RFID Backscatter Applications", IEEE MTT-S International Microwave Symposium (IMS2008), Atlanta, 2008.

5 S. Hu, C. L. Law, W. Dou, "Measurements of UWB Antennas Backscattering Characteristics for RFID Systems", ICUWB 2007. IEEE International Conference on Ultra-Wideband, Singapore, 2007.

6 S. Hu, C. L. Law, W. Dou, "A Balloon-Shaped Monopole Antenna for Passive UWB-RFID Tag Applications", Antennas and Wireless Propagation Letters, IEEE,

7 K. Finkenzelle, "RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification", John Wiley & Sons, Second Edition, 2003.

8 D. Paret, "Identification Radiofréquence et Cartes à Puce Sans Contact", Dunod, 2001.

9 B. Jamali, D. C. Ranasinghe, P. H. Cole, "Analysis of a UHF RFID CMOS Rectifier Structure and Input Impedance Characteristics", Proceedings of SPIE, Brisbane, Australia, December 2005.

10 P. V. Nikitin and K. V. S. Rao, "Performance of RFID Tags with Multiple RF Ports", IEEE Antennas and Propagation Symposium, Honolulu, HI, June 2007.

11 Hamza Abdelkrim, ''Détection et Séparation des signaux des systèmes CDMA par la méthode d'analyse en composantes indépendantes'' Thèse de doctorat, usthb, 2010.

12 Carlo Mutti et Christian Floerkemeier,'' CDMA-based RFID Systems in Dense Scenarios: Concepts and Challenges'', 2008 IEEE International Conference on RFID The Venetian, Las Vegas, Nevada, USA April 16-17, 2008

13 El hadi Meftah, « Détection des signaux dans les systèmes OFDM-CDMA »,USTHB ,bab ezzouar,ALGER , 2009.

14 Yan Zhang, Laurance T.Yang, and I. Jiming Chen, "RFID AND SENSOR NETWORKS,"

15 Zhijun Tang , Yigang He '' Research of Multi-access and Anti-collision Protocols in RFID Systems'' College of Electrical and Information Engineering , Hunan University , Changsha , Hunan , China

16 T. Umeda et al., A 950-MHz rectifier circuit for sensor network tag with 10-m distance, IEEE J. Solid State Circ, Janvier 2006.

17 A.GHIOTO, '' conception d'antennes de Tags RFID UHF'', labo LCIS, Institut polytechnique de Grenoble, Novembre 2008.

18 A. Facen and A. Boni, A CMOS analog frontend for a passive UHF RFID tag, in Proc. Int. Symp. on Low Power Electronic and Design, pp. 280–285, Tagernsee, Germany, October 2006.

19 V. Pillai et al., An ultra-low-power long range battery/passive RFID tag for UHF and microwave bands with a current consumption of 700 nA at 1.5 V, IEEE Trans. Circuits Syst., 2007.

20 A. Ricci and I. De Munari, Enabling pervasive sensing with RFID: An ultra low power digital core for UHF transponders, in Proc. IEEE Int. Symph. on Circuit and Systems (ISCAS), New Orleans, 2007.

21 H. Yan, H. Jianyun, L. Qiang, and M. Hao Design of low-power baseband-processor for RFID tag, in Proc. Int. Symp. on Applications and the Internet Workshops, Phoenix 2006.

22 R. Barnett, G. Balachandran, S. Lazar, B. Kramer, G. Konnail, S. Rajasekhar, and V. Drobny, A passive UHF RFID transponder for EPC Gen 2 with −14 dBm ensitivity in 0.13 μm CMOS , San Francisco, 2007.

23 W.G. Yeoh, Y.B. Choi, K.Y. Tham, S.X. Diao, and Y.S. Li, A CMOS 2.45-GHz radio frequency identification tag IC with read/write memory, in Dig. Radio Freq. 2005.

24 K.V.S. Rao and P.V. Nikitin, Theory and measurement of backscattering from RFID tags, 2006.

25 EPC Global, 860 MHz–930MHz class 0 radio frequency identification tag protocol specification candidate recommendation, Version 1.0.0. MIT Auto-ID Center, 2003.

26 J.-P. Curty, N. Joehl, C. Dehollain, and M.J. Declercq, Remotely powered addressable UHF RFID integrated system, 2005.

27 H.T. Friis, A note on simple transmission formula, Proc. Inst. Radio Eng.,1946.

28 International Standards Organization, Type B UHF RFID, ISO/IEC WD 18000 2004.

29 R.J. Marhefka and J.D. Kraus, Antennas, McGraw-Hill, New York, 2002.

30 A. Navarro and J.L. Del Valle, Voltage generator for UHF RFID passive tags using Schottky diodes based on a 0.5 μm CMOS technology, in 3rd International Conference on Electrical and Electronics Engineering, 2006.

31 www.vole.com,'' Protocoles d'accès aux réseaux locaux de PC ''.

33 MAHAFENO Irène. « Etude de la technique d'accès multiple IDMA (Interleave Division Multiple Access) » ; Thèse. doctorat : Sciences pour l'ingénieur : UBS, Institut Télécom-Télécom Bretagne.2007.

34 Michel Terré. « Protocoles d'Accès ». Cours du Conservatoire National des Arts et Métiers.ELE208.2007.