الجمهورية الجزائرية الديمقراطية الشعبية
REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
وزارة التعليم العالي والبحث العلمي
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE



جامعة الدكتور يحي فارس المدية
UNIVERSITE Dr. YAHIA FARES DE MEDEA
Faculté de Technologie
Département du Génie Electrique

Mémoire de fin d'études de Master

Etude des Performances des Protocoles d'Anticollision des Lecteurs pour les Systèmes RFID

Filière **: Télécommunications**

Spécialité **: Systèmes de Télécommunications**

Présenté par :

TORCHI Sadek

MAHDI Soufyane

Proposé et Dirigé par :

Dr. KALACHE Mohamed Aissa

Année universitaire : **2022-2023**

Dédicace 1

Tout d'abord, je tiens à remercier DIEU,
De m'avoir donné la force et le courage de mener à
Bien ce modeste travail.
Je tiens à dédier cet humble travail à :
A ma tendre mère et mon très cher père
A mes frères et ma sœur
A mon binôme
A mes meilleurs amis
Tous ceux qui m'aiment et que j 'aime
SADEK TORCHI

Dédicace 2

Je dédie ce modeste travail
A ma Chère Mère
A mon Père Dont le mérite
Les sacrifices et les qualités humaines
m'ont
Permis de vivre ce jour
A mes Frères et ma sœur
A tous les gens m'aiment

MAHDI SOUFYANE

Remerciements

Je tiens à remercier toutes les personnes qui ont contribué au succès de mon mémoire et qui m'ont aidée lors de la rédaction de ce mémoire. Je voudrais dans un premier temps remercier, notre promoteur **Dr. Kalache Mohamed Aissa**, pour sa patience, sa disponibilité et surtout ses judicieux conseils, qui ont contribué à alimenter ma réflexion.

Mes parents, pour leur soutien constant et leurs encouragements.

Résumé

L'identification par radiofréquence (RFID) est une technologie émergente qui promet d'être omniprésente dans un futur proche, elle permet l'identification d'objets en échangeant des données à travers des signaux radiofréquence. Le système RFID se compose de trois parties principales : (i) le tag ou transpondeur contenant l'antenne et une puce contenant des informations sur l'objet à définir, (ii) le lecteur ou l'interrogateur pour identifier les informations envoyées depuis le tag, (iii) et enfin un ordinateur avec un logiciel et des bases de données pour stocker et traiter des informations. Dans ce travail, nous avons défini le problème de collision des tags et collision des lecteurs, ce dernier est divisé en deux types de collision : lecteur à tag et lecteur à lecteur. Pour résoudre le problème de collision des lecteurs, il existe plusieurs protocoles d'anticollision de lecteurs. On a présenté dans cette mémoire quelques protocoles. En plus, on a simulé et comparé sur MATLAB les performances des deux protocoles d'anticollision des lecteurs, tels que : DEFAR et DCS, en termes de débit de lecture, nombre de collisions et efficacité.

Mots clés : radio - ondes magnétiques - oscillations - collision - micros

Abstract

Radio Frequency Identification (RFID) is an emerging technology that promises to be ubiquitous in the near future, enabling the identification of objects by exchanging data through radio frequency signals. The RFID system consists of three main parts: (i) the tag or transponder containing the antenna and a chip containing information about the object to be defined, (ii) the reader or interrogator to identify the information sent from the tag, (iii) and finally a computer with software and databases to store and process information. In this work, we have defined the problems of tag collision and reader collision, this latter is divided into two types of collision: tag-reader and reader-reader collision. To solve the reader collision problem, there are several reader anti-collision protocols. A few protocols were presented in this thesis. In addition, we simulated and compared through MATLAB the performance of two reader anti-collision protocols, such as: DEFAR and DCS, in terms of reading rate, collision number, and efficiency.

Keywords: radio - magnetic waves - oscillations - collision - pickups

الملخص

أنظمة تحديد الهوية بموجات الراديو (RFID) هي تقنية ناشئة تعد بأن تكون موجودة في كل مكان في المستقبل القريب، مما يتيح تحديد الأشياء عن طريق تبادل البيانات من خلال إشارات موجات الراديو. يتكون نظام RFID من ثلاثة أجزاء رئيسية: (1) العلامة أو المرسل المستجيب الذي يحتوي على الهوائي وشريحة تحتوي على معلومات حول الشيء المراد تحديده، (2) القارئ لتحديد هوية المعلومات المرسلة من العلامة ، (3) وأخيرًا جهاز كمبيوتر به برامج وقواعد بيانات لتخزين المعلومات ومعالجتها. في هذا العمل، حددنا مشاكل تصادم العلامات وتصادم القراء، وهذا الأخير ينقسم إلى نوعين من التصادم: قراء-العلامات وقراء-قراء. لحل مشكلة تصادم القراء، هناك العديد من بروتوكولات مكافحة تصادم القراء. تم تقديم عدد قليل من البروتوكولات في هذه الأطروحة. بالإضافة إلى ذلك، قمنا بمحاكاة ومقارنة أداء بروتوكولين مضادين لتصادم القراء من خلال MATLAB، مثل DEFAR و DCS، من حيث معدل القراءة وعدد الاصطدامات والفعالية.

الكلمات المفتاحية: الراديو - موجات مغناطيسية - ذبذات – التصادم - اللواقط

Table des Matières

Dédicace 1 ..... **III**

Dédicace 2 ..... **IV**

Remerciements ..... **V**

Résumé ..... **VI**

Table des Matières ..... **IX**

Liste des figures ..... **XII**

Liste des tableaux ..... **XIII**

Liste des Abréviations ..... **XIV**

Introduction Générale **1**

Introduction générale **2**

Chapitre 1 : Les systèmes RFID **3**

Introduction **4**

1. L'historique de la RFID **4**

2. System code barre [20] **6**

3. Définition du RFID : **7**

4. Principe de fonctionnement des systèmes RFID **7**

5. Composants des système RFID **7**

5.1. L'interrogateur 8

5.1.1. Type de lecteurs : **8**

- Le lecteur RFID fixe : 8

- Le lecteur RFID portable : 8

5.2. Le Transpondeur : 9

5.3. Système informatique 9

6. Les types de systèmes RFID **10**

6.1. Systèmes RFID actifs 10

6.2. Systèmes RFID passifs : 11
6.3. Systèmes RFID semi passif : 11
7. Les fréquences utilisées dans les systèmes RFID 12
8. Application 13
9. Les différentes utilisations des tags RFID 14
9.1. Lecture seule 14
9.2. Écriture une fois /lecture plusieurs fois (WORM) 14
9.3. Lecture/ écriture multiples 15
10. Le problème de collision dans les systèmes RFID : 15
10.1. Collision de tag à tag 15
10.2. Collision de lecteurs : 16
10.2.1. Collision de lecteur a tag : **16**
10.2.2. Collision lecteur à lecteur **17**
Conclusion 17
Chapitre 2 : Protocoles d'anticollision 18
Introduction : 19
1. Protocoles d'Anticollision des tags : 19
1.1. Protocole ALOHA 19
1.1.1. Protocole Pure/unslotted ALOHA **19**
1.1.2. Protocole Basic Framed Slotted ALOHA (BFSA) **19**
1.1.3. Protocole "Dynamic Framed Slotted ALOHA" (DFSA) **20**
1.1.4. Protocole "Advanced Framed Slotted ALOHA (AFSA) **20**
1.2. Protocole anticollision basée sur parcoure d'arbre 20
2. Protocole d'anticollision des lecteurs 21
2.1. Catégorisation des protocoles 21
2.1.1. TDMA ou CSMA **22**
2.1.2. Centralisé ou Distribué **23**
2.1.3. Monocanal ou Multicanal **23**

2.2. Protocoles TDMA 24
2.2.1. Approches Distribuées : **24**
2.2.2. Approches Centralisées : **27**
2.3. Protocoles CSMA 28
3.2.1 Approches Distribuées **28**
3.2.2 Approches centralisées : **28**
Conclusion 29
Chapitre 3 : Modèle et résultat de simulation 30
Introduction 31
1. Présentation des critères d'évaluation des protocoles d'anticollision RFID 31
1.1. Débit de lecture 31
1.2. Collisions 32
1.3. Efficacité 32
1.4. Indice d'équité de Jain (IEJ) 33
2. Distributed Efficient & Fair Anti-collision (DEFAR): 33
3. Les résultats de simulation 40
Conclusion 42
Conclusion générale 43
Bibliographie 44

Liste des figures

Figure 1 : Principe de fonctionnement de la RFID **6**

Figure 2 : Principe de fonctionnement de la RFID **8**

Figure 3: un transpondeur RFID **10**

Figure 4 : Exemple des tags **10**

Figure 5 : Type des transpondeurs **13**

Figure 6 : collision de tag a tag **17**

Figure 7 : collision de lecteur a tag **18**

Figure 8 : collision de lecteur a lecteur **19**

Figure 9: structure d'un round-CORA **29**

Figure 10: structure d'un round-DEFAR **36**

Figure 11 : diagramme d'états **37**

Figure 12 : le débit de lecteur en fonction en nombre de lecteur pour 100 rounds **42**

Figure 13 : le débit de lecteur en fonction en nombre de lecteur pour 100 rounds **43**

Figure 14 : L'efficacité en fonction en nombre de lecteur pour 100 rounds **43**

Liste des tableaux

Tableau 1 : Structure d'un code barre EAN **7**

Tableau 2 : défèrent type de fréquence d'utilisation **14**

Tableau 3 : protocoles d'anticollision de tags **23**

Tableau 4 : Récapitulatif des protocoles d'anticollision de lecteur RFID **26**

Liste des Abréviations

IFF	Identification friend or foe
EAN	European Article Number
RFID	Radio Frequency Identification,
AFSA	Advanced Framed Slotted ALOHA
FDMA	Frequency Division Multiple Access)
DCS	Distributed Color Selection
CORA	Coverage Oriented RFID Anti-collision)
NFRA	Neighbor Friendly RFID Anticollision
LBT	Listen Before Talk
IEJ	Indice d'équité de Jain
DEFAR	Distributed Efficient & Fair Anticollision
CDMA	Code Division Multiple Access.
ACR	nombre d'Accès Canal Réussi
ACE	nombre d'Accès Canal Echoué
BFSA	Basic Framed Slotted ALOHA.
DFSA	Dynamic Framed Slotted ALOHA
DS-CDMA	Direct Sequence Code Division Multiple Access.
EDFSA	Enhanced Dynamic Framed Slotted ALOHA.
EPC	Electronic Product Code.
FSA	Framed Slotted ALOHA.
HF	High Frequency.
ID	Identification.
LF	Low Frequency.
MAC	Medium Access Control.
PA	Pure ALOHA. PC Protocol Control.
PIE	Pulse Interval Encoding.
QT	Query Tree.
RF	Radio Frequency.
RFID	Radio Frequency Identification.
SA	Slotted ALOHA.
TDMA	Time-Division Multiple Access.
TS	Tree Splitting.
UHF	Ultra High Frequency.

Introduction Générale

Introduction générale

Depuis la nuit de temps, il a toujours été une préoccupation pour l'homme d'identifier, de localiser et de suivre des objets en utilisant d'abord l'identification visuelle puis remplacée par des équipements électroniques. Plusieurs systèmes pratiques ont été utilisés au cours des années, des motifs uniques ont été placés sur des objets, et des appareils de reconnaissances pouvaient identifier ces codes et par la même voie l'objet sur lequel ils sont collés. De là est né le système de codes à barres qui a permis de réaliser l'identification des objets depuis des années. Cependant, les codes à barres présentent plusieurs lacunes, notamment la taille très limitée de données stockées, la nécessité de scanner à proximité, la durée de vie dépend de la qualité d'impression et du consommable utilisés ...etc. Ces déficits ont continuellement poussé les utilisateurs à chercher une meilleure solution pour pallier à ce manque. L'apparition de technologie RFID qui à priori résolvait les majeurs problèmes d'identification telle que la taille de données plus importante, flexibilité des codes, distance de lecture améliorée, possibilité de localiser les objets, des suivis et analyser ses données.

Le système RFID est composé de plusieurs tags (ou étiquettes ou transpondeurs) et plusieurs lecteurs (ou interrogateurs). Le problème majeur de la RFID est lorsque plusieurs tags et/ou plusieurs lecteurs communiquent entre eux en même temps et même canal. Dans ce cas une collision se produit. On peut classer cette collision en trois types : la collision tag à tag, collision lecteur à tag, et collision lecteur a lecteur. Pour résoudre le problème de collision il existe plusieurs protocoles (ou algorithmes) d'anticollision a été proposé. Les protocoles d'anticollision des tags sont proposé pour résoudre le problème de collision tag à tag, et les protocoles d'anticollision des lecteurs sont proposé pour résoudre les problèmes de collision lecteur à tag et collision lecteur à lecteur. Notre thèse et basé sur les protocoles d'anticollision des lecteurs.

Dans cette thèse, on a expliqué et définit le système RFID. Ainsi qu'expliquer les types de collisions. En plus, on a présenté différent protocoles d'anticollision des tags et des lecteurs. Objectif de cette thèse est de simuler quelques protocoles d'anticollision des lecteurs et comparer leurs performances.

Notre thèse est organisée comme suit : Chapitre 1 explique le système RFID et les type de collision. Dans chapitre 2, les protocoles d'anticollision de tags et des lecteurs sont présentés. Chapitres 3 montre et discute les résultats de simulation obtenus. Finalement, la dernière section conclut la thèse.

Chapitre 1 : Les systèmes RFID

Introduction

Un système RFID est typiquement composé d'un lecteur (également appelé interrogateur), d'un tag (également appelées transpondeurs) et d'un système informatique. Les tags stockent les identifications uniques (ID) et sont attachées aux objets. Dans ce chapitre, on va présenter l'historique de la RFID et les différents types de lecteur et de tags. En plus, on va expliquer le principe de fonctionnement de la RFID.

1. L'historique de la RFID

La première utilisation du RFID est militaire. Dès 1935, Robert Watson-Watt développe une application destinée à l'armée britannique, pour différencier les avions ennemis des alliés : c'est le système d'identification IFF « *Identification friend or foe* », qui reste le principe de base utilisé de nos jours pour le contrôle du trafic aérien.[1]

En 1945, Léon Theremin invente un dispositif d'espionnage pour l'Union soviétique, appelé *« the thing »*, qui retransmet les ondes radio incidentes augmenté de l'information audio. Ainsi, ce dispositif assure la fonction d'un microphone sans fil transmettant un signal acoustique sur une onde porteuse RF. Les ondes sonores font vibrer un diaphragme qui modifie légèrement la forme du résonateur, lequel module la fréquence radio réfléchie. Même si ce dispositif est plus dispositif d'écoute secrète qu'une étiquette d'identification, il est considéré comme un prédécesseur de la RFID parce qu'il est passif, car alimenté et activé par des ondes provenant d'une source extérieure.[2]

Entre 1948 et 1952, H. Stockman et F. L. Vernon écrivent les premiers articles scientifiques sur la RFID. Ces articles sont considérés comme les fondements de la technologie RFID [3]. Harry Stockman a notamment prédit que « ...un travail de développement et de recherche considérable doit être fait avant que les problèmes fondamentaux de la communication par puissance réfléchie soient résolus et que le domaine des applications utiles soit exploré... ».[4]

Les années 1950 voient le dépôt de plusieurs brevets sur la RFID. En 1952 Donald Harris dépose le premier brevet d'un système de transmission communiquant avec une cible passive [5]. En 1959, J. Vogelman brevète un système communiquant avec une cible qui module le signal radar à travers la variation de la surface équivalente radar d'une antenne (SER) .[6]

Dans les années 1960, les applications ont des buts commerciaux. Le premier tag fait son apparition en 1966. Cette première étiquette RFID (1-bit) est développée et commercialisée sous l'acronyme EAS (*Electronic Article Surveillance*), elle détecte uniquement la présence ou l'absence du tag. Le contrôle d'accès fait l'objet d'autres brevets **[7,8,9,10,11,12,13].** La théorie

fondamentale sur laquelle s'appuie la RFID est décrite dans plusieurs publications, dont celles de R. Harrington et de J. K. Schindler.

Le dispositif de Mario Cardullo et William Parks, breveté le 23 janvier 1973 , est le véritable ancêtre de la RFID moderne[21]. Il s'agit en effet d'un transpondeur radio passif, alimenté par le signal d'interrogation, et disposant d'une mémoire de 16 bits. Il a été présenté en 1971 à la *New York Port Authority* et à d'autres utilisateurs éventuels. Le brevet de Cardullo couvre l'utilisation de la radiofréquence, du son et de la lumière comme supports de transmission. L'argumentaire commercial original présenté aux investisseurs en 1969 montre des utilisations dans les domaines des transports (identification des véhicules automobiles, péage automatique, plaque d'immatriculation électronique, manifeste électronique, routage des véhicules, suivi des performances des véhicules), de la banque (chéquier et carte de crédit électroniques), de la sécurité (identification du personnel, portes automatiques, surveillance), et de la santé (identification, antécédents du patient). [14,15]

Steven Depp, Alfred Koelle et Robert Frayman font une démonstration des étiquettes RFID à puissance réfléchie (rétrodiffusion modulée), à la fois passives et semi-passives, au Laboratoire national de Los Alamos en 1973. Ils établissent l'expression reliant la puissance réfléchie à la charge de l'antenne, ce qui établit d'un point de vue formel le principe de la modulation du signal rétrodiffusé (ou « *modulated backscatter* » en anglais) des tags RFID. Le système portatif opère à 915 MHz et utilise des étiquettes 12 bits. Cette technique est employée par la majorité des étiquettes RFID UHFID et micro-ondes d'aujourd'hui.[16]

Le premier brevet associé à l'abréviation RFID est accordé à Charles Walton en 1983.

Les années 1990 marquent le début de la normalisation pour une interopérabilité des équipements RFID.

En 1999, des industriels créent le centre d'identification automatique (Auto-ID Center) au MIT avec l'objectif de standardiser la technologie RFID. Ce centre est fermé en 2003 lorsque les travaux sur le code produit électronique (EPC) sont achevés, et les résultats sont transférés à la EPC global Inc. fondée par le Uniform Code Council (UCC) et EAN International, dénommés maintenant GS1 US et GS1.

Depuis 2005, les technologies RFID sont majoritaires dans les secteurs industriels (aéronautique, automobile, logistique, transport, santé, vie quotidienne, etc.). L'ISO (International Standard Organisation) a participé à la mise en place de normes tant techniques que pratiques, atteignant un haut degré d'interopérabilité voire d'interchangeabilité.

2. System code barre [20]

Omniprésents dans notre vie quotidienne, les codes barre dominent les systèmes d'identification automatique depuis plus de 20 ans. Le code barre est un code binaire représenté par une s´séquence de barres vides et de barres pleines, larges ou étroites, disposées parallèlement. La séquence peut être interprétée numériquement ou alpha numériquement. Elle est lue par balayage optique au laser, c'est-`a-dire d'après la différence de réflexion du rayon laser par les barres noires et les espaces blancs. On utilise actuellement une dizaine de types de codes barre différents, sans compter les codes barre `a deux dimensions, mais s'agit-il encore de codes barre ?

Le code barre le plus courant est le code EAN (*European Article Number*), crée pour répondre aux besoins de l'industrie alimentaire en 1976. Le code EAN est une évolution de l'UPC (*Universal Product Code*) américain, introduit aux Etats-Unis´ d`es 1973 ; UPC et EAN sont compatibles entre eux.



Figure 1* –Un code barre EAN *(European Article Number)

Identifiant de pays		Identifiant de l'entreprise					Numéro d' article du fabricant					CD
0	4	1	2	3	4	5	0	8	1	5	0	9
FRG		**Nom de la compagnie 1 nom de la route 80001 Munich**					**Lapin**					

Tableau 1 : Structure d'un code barre EAN.

Le code EAN est composé de 13 chiffres : l'identifiant du pays, l'identifiant de la société, le numéro de l'objet chez le fabriquant et un numéro de contrôle. Malgré son grand âge, le code barre conserve des avantages importants comme son coût quasiment nul et sa large diffusion. En revanche, il présente plusieurs inconvénients : il est fragile, doit être lu de manière optique

et peut être remplacé par quelqu'un de malintentionné. De plus, il ne peut pas être modifiée à distance, contient peu d'informations et n'a bien sûr aucune capacité de traitement de données.

3. Définition du RFID :

Le sigle ***RFID signifie Radio*** **Frequency Identification**, comprenez radio-identification. Il désigne une méthode utilisée pour stocker et récupérer des données à distance en utilisant des balises métalliques, les « Tags RFID ». Ces balises, qui peuvent être collées ou incorporées dans des produits, réagissent aux ondes radio et transmettent des informations à distance. Cette technologie pourrait, à terme, remplacer les codes-barres . Mais sa redoutable efficacité pose des problèmes d'éthique et de confidentialité

La technologie RFID est utilisée -- même si c'est au début, de façon confidentielle, pour des applications militaires depuis la seconde guerre mondiale. Mais ce n'est qu'à partir des années 2000 qu'elle se popularise. Dans le secteur de la logistique, elle participe à la traçabilité des produits de l'entrepôt au magasin. Ensuite, elle se transforme en système antivol et en moyen d'identification des produits en caisse. Dans les bibliothèques, la RFID aide à identifier les livres. Et on la trouve aussi sur les passeports, sur les cartes d'accès aux transports en commun et même dans les puces qui servent à identifier nos chiens et nos chats. Plus récemment, elle a permis d'imaginer la commercialisation d'objets communicants.

4. Principe de fonctionnement des systèmes RFID

Le fonctionnement d'un système RFID se déroule généralement de la manière suivante : le lecteur RFID envoie un signal radiofréquence pour interroger les tags RFID à proximité. Les tags détectent ce signal et y répondent en transmettant leurs informations au lecteur. Le lecteur reçoit les réponses des tags et les transmet au système informatique pour traitement. Les données peuvent ensuite être utilisées pour prendre des décisions, générer des rapports, ou effectuer des actions spécifiques en fonction de l'application du système RFID**.**

Le lecteur envoie une requête à l'étiquette qui se trouve dans le champ de lecture et celle-ci répond immédiatement, le tout se fait selon un protocole de communication prédéfini [17].

5. Composants des système RFID

Un système RFID (Radio Frequency Identification) est généralement composé de trois éléments principaux : les tags RFID, les lecteurs RFID (Les interrogateurs) et un système informatique :

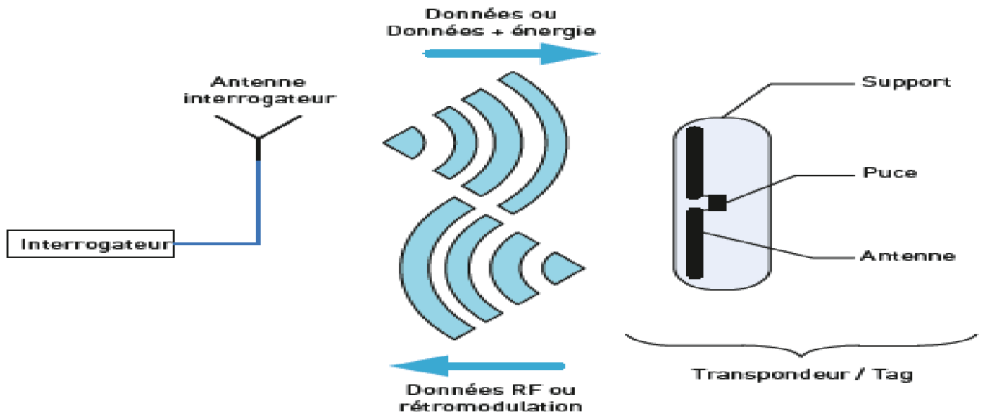


Figure 2 : Principe de fonctionnement de la RFID. [18]

5.1. L'interrogateur

Également appelé lecteur ou station de base, l'interrogateur émet par l'intermédiaire d'une antenne des ondes radio dans un espace pouvant varier de quelques centimètres à plusieurs dizaines de mètres dans le but d'activer tout transpondeur se trouvant dans son champ d'action.

Une fois le tag activé, un dialogue entre l'interrogateur et le transpondeur qui peut être indifféremment fixe ou mobile peut être présenté, dans la majorité des cas, une interface de contrôle, permettant de transmettre les informations recueillies à un système dit « hôte » qui peut être un simple ordinateur ou un serveur rendant ainsi accessible le contenu de la base de données qu'il intègre. On parle alors d'infrastructure RFID étendu.

5.1.1. Type de lecteurs :

Les lecteurs RFID peuvent prendre des formes variées selon l'utilisation à laquelle il sera destiné. Du fait qu'il n'a pas besoin d'être en contact direct avec la puce, le lecteur le plus utilisé est le lecteur fixe, mais il peut également prendre la forme d'un lecteur portable.

- **Le lecteur RFID fixe** :

Comme son nom l'indique il est installé de manière fixe et ne peut donc pas être transporté pour la lecture des puces à distance, il prend la forme de portique ou bornes.

- **Le lecteur RFID portable** :

Le lecteur portable prend la forme d'un flasher portatif qui permet de lire les étiquettes manuellement, les objets n'ont plus besoin d'être transportés à proximité du lecteur, c'est le lecteur qui se déplace.

5.2. Le Transpondeur :

Il doit son nom à ses fonctions d'émission et de réception (TRANSmitter/rePONDER). Il comprend une puce, dotée d'une mémoire, reliée à une antenne, pour transmettre les données stockées dans sa mémoire à l'interrogateur. Le plus souvent, le transpondeur, également appelé TAG ou Etiquette, est collé sur un film en plastique ou moulé dans une carte de crédit, mais en fonction de l'application visé, il pourra être décliné sous différentes formes. Il est donc possible de trouver ainsi des puces autocollantes sur support papier, des gélules en verre, etc. Il peut également, de façon optionnelle, intégrer une batterie et un ou plusieurs capteurs (voir Figure 2).

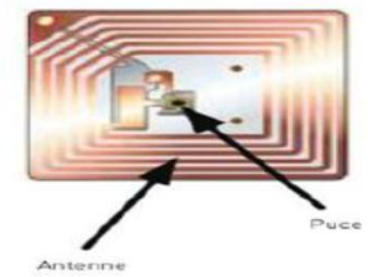
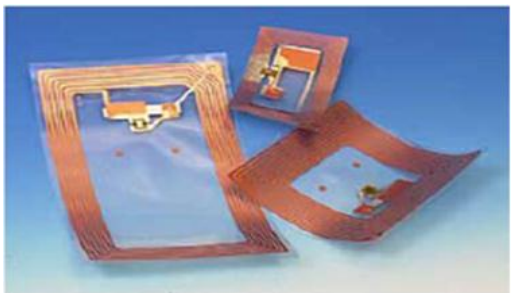


Figure 3 : un transpondeur RFID

On trouve des tags RFID de toutes formes et de toutes tailles comme il est montré dans la Figure 3. Dans la Figure (3.a) le transpondeur (tag) et l'antenne sont fins et souples, collés sur un autocollant. La figure (3.b) distingue bien le transpondeur au centre, entouré d'une antenne de cuivre bobinée. La figure (3.c) le tag est conçu pour être injecté sous la peau des animaux. Il est moulé dans un tube de verre de 1 à 3 cm. La figure (3.d) Les RFID peuvent être miniaturisés à l'extrême. Ces tags, fabriqués par Hitachi mesurent 0.25 mm2; ils sont pratiquement invisibles .[20]

5.3. Système informatique

Le système informatique est responsable du traitement et de l'analyse des données RFID. Il peut être composé de logiciels, de bases de données et d'interfaces utilisateur permettant de gérer les informations collectées par les lecteurs RFID. Le système informatique permet de stocker, organiser et exploiter les données des tags RFID pour des applications spécifiques telles que le suivi des stocks, la gestion des actifs, la gestion des inventaires, la sécurité, etc.



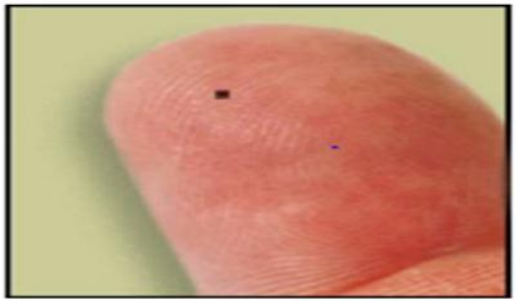
(a)



(b)



(c)



(d)

Figure 4 : Exemple des tags

6. Les types de systèmes RFID

6.1. Systèmes RFID actifs

Dans les systèmes RFID actifs, les étiquettes ont leur propre émetteur et source d'alimentation. Habituellement, la source d'alimentation est une batterie. Les étiquettes actives diffusent leur propre signal pour transmettre les informations stockées sur leurs micropuces. Les systèmes RFID actifs fonctionnent généralement dans la bande ultra-haute fréquence (UHF) et offrent une portée allant jusqu'à 100 m. En général, les étiquettes actives sont utilisées sur de gros objets, tels que les wagons, les grands conteneurs réutilisables et d'autres biens qui doivent être suivis sur de longues distances. Il existe deux principaux types de tags actifs : les transpondeurs et les balises. Les transpondeurs sont "réveillés" lorsqu'ils reçoivent un signal radio d'un lecteur, puis s'allument et répondent en transmettant un signal. Comme les transpondeurs ne rayonnent pas activement les ondes radio jusqu'à ce qu'ils reçoivent un signal de lecture, ils conservent la durée de vie de la batterie. [19]

Les balises sont souvent utilisées dans les systèmes de localisation en temps réel (RTLS), afin de suivre l'emplacement précis d'un bien en continu. Contrairement aux transpondeurs, les balises ne sont pas alimentées par le signal du lecteur. Au lieu de cela, ils émettent des signaux à des intervalles prédéfinis. Selon le niveau de précision de localisation requis, les balises

peuvent être réglées pour émettre des signaux toutes les quelques secondes ou une fois par jour. Le signal de chaque balise est reçu par les antennes de lecture qui sont positionnées autour du périmètre de la zone surveillée, et communique les informations d'identification et la position de l'étiquette.

L'écosystème sans fil pour les clients est très grand et grandit quotidiennement, il y a des cas d'utilisation où RFID active et RFID passive sont déployées simultanément pour une approche additive à la gestion des actifs ou des capteurs.

6.2. Systèmes RFID passifs :

Dans les systèmes RFID passifs, le lecteur envoie un signal radio à l'étiquette via son antenne. L'étiquette RFID utilise ensuite cette onde électromagnétique captée par l'antenne tag pour alimenter la puce et puis renvoyer les informations stockées au lecteur. Les systèmes RFID passives peuvent fonctionner dans les bandes radio basse fréquence (BF), haute fréquence (HF) ou ultrahaute fréquence (UHF). Comme les plages de systèmes passifs sont limitées par la puissance de la rétrodiffusion de l'étiquette (le signal radio renvoyé par l'étiquette au lecteur), elles sont généralement inférieures à 10 m. Comme les étiquettes passives ne nécessitent pas de source d'alimentation ou d'émetteur et ne nécessitent qu'une puce et une antenne, elles sont moins chères, plus petites et plus faciles à fabriquer que les étiquettes actives. [19]

Les étiquettes passives peuvent être emballées de différentes manières, en fonction des exigences spécifiques de l'application RFID. Par exemple, ils peuvent être montés sur un substrat, ou pris en sandwich entre une couche adhésive et une étiquette en papier pour créer des étiquettes RFID intelligentes. Des étiquettes passives peuvent également être incorporées dans une variété de dispositifs ou d'emballages pour rendre l'étiquette résistante aux températures extrêmes ou aux produits chimiques agressifs. RAIN est une solution RFID passive utile pour de nombreuses applications. Elle est généralement utilisée pour suivre les marchandises dans la chaine d'approvisionnement, inventorierez actifs dans le commerce de détail, authentifier des produits tels que les produits pharmaceutiques et intégrer la technologie RFID dans divers appareils.

6.3. Systèmes RFID semi passif :

Les systèmes semi passifs sont des systèmes hybrides des deux autres. Ils ne possèdent pas d'émetteur radiofréquence, mais ils intègrent tout de même une source d'énergie interne(batterie). Comme pour les systèmes passifs, la communication entre l'interrogateur et le transpondeur fait appel aux techniques de retro-modulation et n'utilise pas la batterie interne,

qui sert uniquement à alimenter l'électronique intégrée sur le transpondeur. En effet, certaines applications nécessitent des calculs ou des relevés d'informations, indépendants de la phase de communication. Par exemple, certains conditionnements de vaccins sont équipés de transpondeurs effectuant des relevés de températures réguliers permettant de vérifier les conditions de stockage du produit. Le capteur de température et l'électronique associée sont alimentés par la batterie interne.

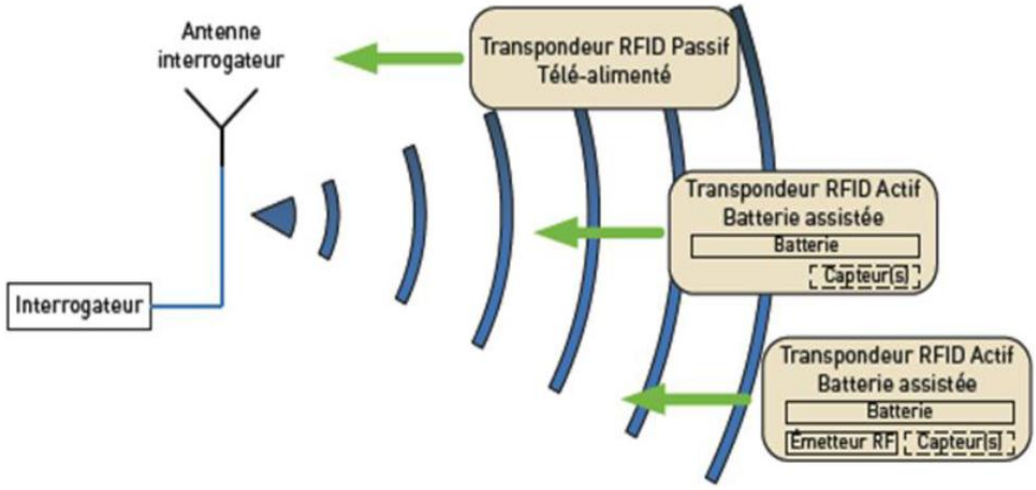


Figure 5 : Type des transpondeurs

7. Les fréquences utilisées dans les systèmes RFID

Un autre facteur important à considérer lors du choix des composantes d'un système RFID est la sélection de la fréquence d'opération. En général, il en existe plusieurs types. Mais les fréquences les plus importantes et les plus utilisées sont les basses fréquences (BF: 125 KHz),les hautes fréquences (HF: 13,56 MHz), les ultra-hautes fréquences (UHF: 860-930 MHz) et les fréquences micro-ondes ou super-haute fréquence (SHF : 2.45 GHz) .L'existence d'une fréquence dépend du pays et du continent, et sa performance est fonction de plusieurs facteurs dont l'environnement d'utilisation, la distance et la viabilité de lecture Par exemple, les BF sont moins sensibles aux contraintes de l'environnement d'utilisation(poussière, métal, liquide ,etc.), mais elles ne permettent qu'une lecture à quelques centimètres. Les UHF, par contre, permettent des lectures à des distances plus importantes, mais elles sont par exemple très sensibles à la poussière, aux liquides et aux métaux. En général, le choix de la fréquence d'opération d'un système RFID va dépendre de nombreux facteurs comme le type

d'application, le type du produit, l'environnement d'opération et le pays d'opération. (Annexes A).[18]

Fréquence	Vitesse	Distance	Informations
Basses fréquences			
125 KHZ	**< 10 Kb/s**	**Jusqu' a 1 m**	**Charge de transpondeur**
134,2 KHZ			
Haute fréquences			
13,56 KHZ	**< 100 kb/s**	Limitation de puissance autorisée	**ISO 144443A-4, ISO 14443B-4, ISSO 14443-3, ISO18000-3, …**
Ultra Haute fréquences			
915 MHZ	**< 100 kb/s**	**Jusqu' a 5-7 m**	**Etats-Unis**
865-868 MHZ			**Union Européenne**
2,45-5,8 GHZ	**< 100 kb/s**	**Jusqu' a 10 m**	**Micro-ondes**

Tableau 2 : défèrent type de fréquence d'utilisation

8. Application

Les applications RFID s'appuient sur différents standards dépendant des fonctionnalités exigées par les processus métier et par certaines contraintes locales. La RFID permet de répondre à un grand nombre de besoins. Elle se développe bien en intra entreprise et dans la logistique. Les principales difficultés auxquelles le standard RFID doit faire face sont en voie d'être surmontées : coût de l'étiquette (plus de 0,10€ pour les moins chères),gestion de l'anticollision en cas de lecture de nombreuses étiquettes en simultané, lecture au travers des fluides, adoption ou convergence trop lente de certains standards, remise en cause de processus anciens, problèmes de sécurité et d'éthique.[20]

Les tags RFID peuvent aussi faire bien plus que simplement renvoyer un numéro, Il existe de nombreuses applications, par exemple les systèmes anti-vol dans les magasins, le contrôle d'accès, la logistique, l'identification du bétail et des animaux de compagnie. La RFID sert

également à identifier les bagages dans les aéroports, les livres dans les bibliothèques, les documents dans les entreprises, à faire payer les conducteurs aux péages, à relever les données de capteurs, à effectuer des micropaiements, à emprunter les transports publics à Londres, Paris ou Venise ou les remontées mécaniques dans les stations de ski, La plupart de ces utilisations sont largement documentées sur Internet.

En générales domaines utilise Les RFID :

- Domaine commercial
- Domaine de la santé
- Domaine du transport
- Domaine de sport, loisirs et biens domestiques
- Domaine de la sécurité.[21]

9. Les différentes utilisations des tags RFID

Il existe 3 types d'utilisation de ces tags :

9.1. Lecture seule

Les données sont inscrites dans l'étiquette par le fabricant, et ne peuvent pas être modifiées ni complétées par la suite. Les utilisateurs ne peuvent que lire les données contenues. ces étiquettes, dont les fonctions peuvent sembler réduites, sont néanmoins sans doute promises à un grand avenir. Leur prix est plus faible que celui de leurs consœurs offrant des fonctions plus complexes. Et, dans de nombreuses applications un simple numéro d'identification, si son unicité est garantie, peut suffire à tracer un objet. Les données complémentaires sur l'objet n'ont pas besoin d'être stockées dans l'étiquette, mais peuvent être mise à disposition, échangée ou retrouvée dans les bases de données des systèmes d'informations.

9.2. Écriture une fois /lecture plusieurs fois (WORM)

L'étiquette est fournie à l'utilisateur, vierge. En fait, dans la majorité des cas le fournisseur l'déjà munie d'une identification. Lors de sa pose sur l'objet à tracer, l'utilisateur va écrire les données qui lui seront utiles par la suite. Lors de la vie ultérieure de l'étiquette, cette information pourra être lue plusieurs fois, mais ne pourra être ni modifiée ni complétée.

9.3. Lecture/ écriture multiples

L'étiquette est fournie, vierge, dans les mêmes conditions que les WORM, mais elle pourra être écrite plusieurs fois, effacée, modifiée, complétée, et lue. Le nombre de répétitions de ces opérations peut dépasser 500 000.[22]

10. Le problème de collision dans les systèmes RFID :

Les systèmes RFID souffrent du problème d'interférence de signal qui peut être divisé en deux types : collision de lecteur et collision de balise. (i) Une collision de lecteurs peut se produire lorsqu'une étiquette se trouve dans les régions d'interrogation de deux lecteurs ou plus qui envoient leurs commandes en même temps, ou lorsqu'un lecteur reçoit des signaux d'interrogation parasites d'autres lecteurs. Par conséquent, un protocole anticollision du lecteur est requis. Une collision d'étiquettes se produit lorsque plusieurs étiquettes se trouvent dans la zone d'interrogation d'un lecteur et répondent simultanément aux commandes du lecteur. La collision du lecteur ou de l'étiquette gêne et ralentit la procédure d'interrogation de l'étiquette.[23]

10.1. Collision de tag à tag

Pour identifier les tags dans la boîte de requête, le lecteur envoie la requête. Les tags sont tenus de renvoyer leurs identifiants (ID). Lorsque la région a plusieurs tags Répondez à la demande en même temps, une collision se produit et le lecteur ne peut pas reconnaître Pas correctement étiqueté, C'est ce qu'on appelle le problème de collision de tags[24]. Comme le montre la figure 6.

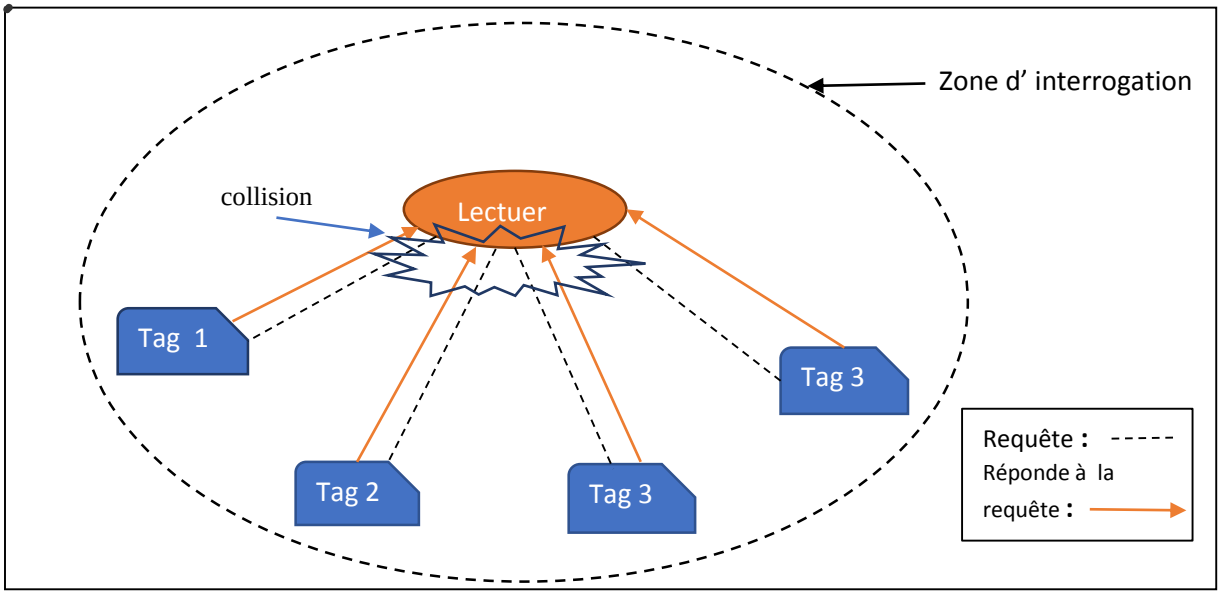


Figure 6 : collision de tag a tag

10.2. Collision de lecteurs :

Les transmissions simultanées dans les systèmes RFID peuvent entraîner des collisions parce que le lecteur et le tag fonctionnent sur le même canal. Pour comprendre cela ,Nous utiliserons le concept de zone d'interrogation sur un lecteur RFID. La zone d'interrogation est la zone autour du lecteur où un seul tag peut être lu avec succès sans interférence d'autres tags ou du lecteur.

Sans aucune coordination entre le lecteur et le tag, la réponse du tag de lecteur peut entrer en collision et empêcher le lecteur du tag. Ce problème de collision dans la RFID a été résumé comme le problème de collision de tag et de lecteurs.[24]

10.2.1. Collision de lecteur a tag :

L'interférence de Lecteur à étiquette se produit quand une étiquette est simultanément située dans les zones d'interrogation de deux lecteurs ou plus et que plus d'un lecteur essaie de communiquer avec cette étiquette en même temps. Dans ce type d'interférence, chaque lecteur peut croire qu'il est le seul à communicant avec l'étiquette lorsque l'étiquette communique avec les lecteurs multiples en même temps.

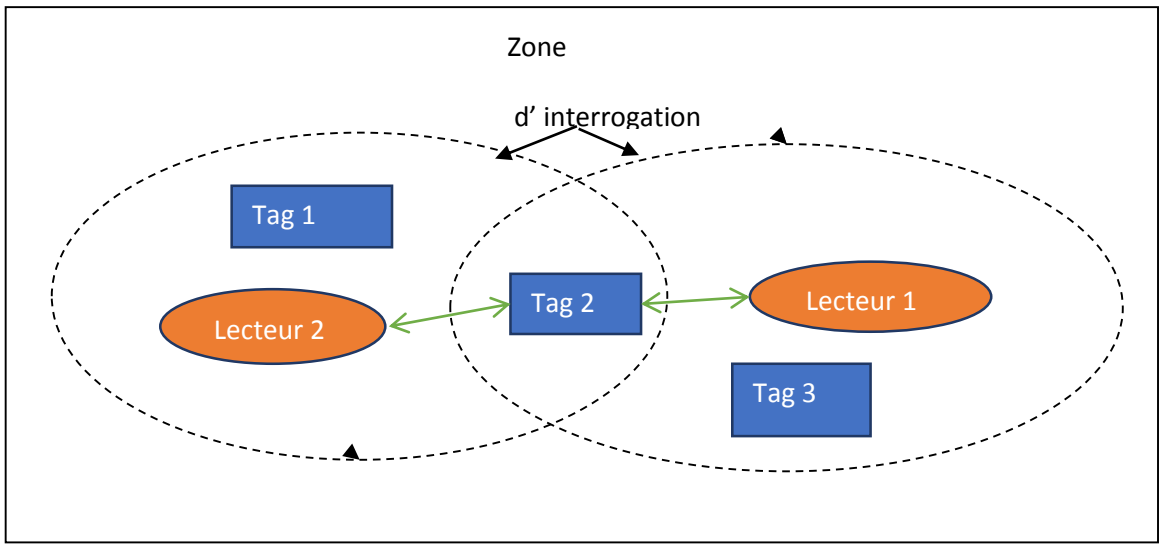


Figure 7 : collision de lecteur a tag

10.2.2. Collision lecteur à lecteur

Une interférence de lecteur à lecteur se produit lorsqu'un lecteur transmet un signal perturbateur l'action d'un autre lecteur. Cela empêche un deuxième lecteur d'interagir avec tag dans sa boîte de requête. Ce type d'interférence se produit lorsque le signal envoyé par un lecteur a une puissance suffisante et il est reçu par le second lecteur. Ce signal bloque ou empêche le tag de communiquer avec le second lecteur.

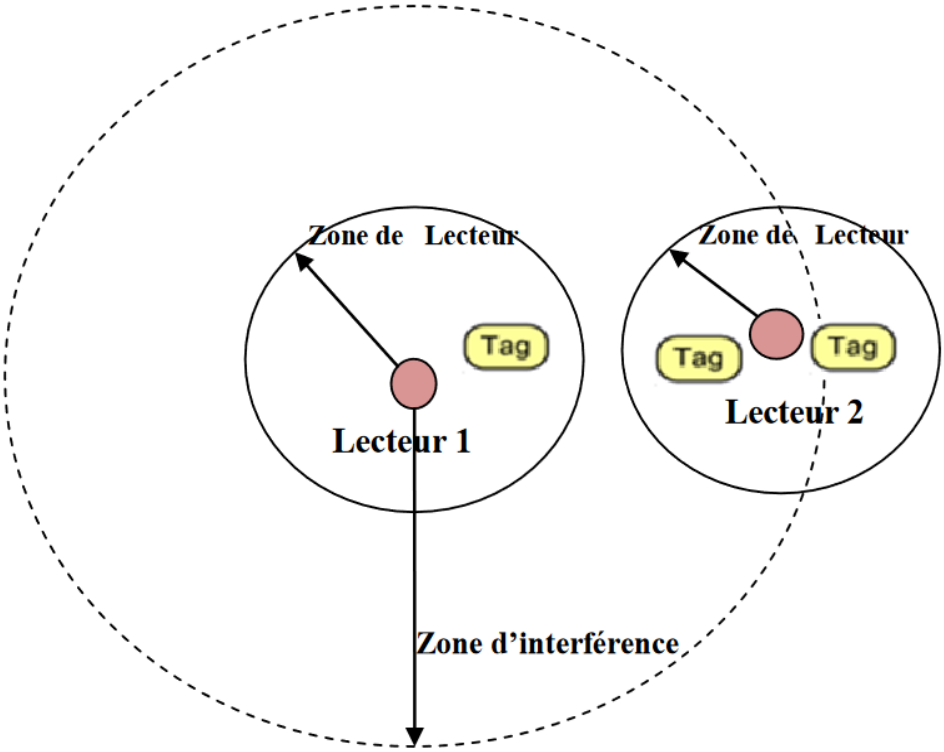


Figure 8 : collision de lecteur a lecteur

Conclusion

Le système RFID (Radio Frequency Identification) est une technologie puissante qui permet l'identification et le suivi des objets de manière efficace et automatisée. Il offre des avantages par rapport le code bar tels que : (1) dans la RFID la distance entre le lecteur et le tag est plus long. (2) La RFID peut identifier plusieurs tags à la fois. (3) En plus, le lecteur peut lire les tags même s'il n'y a pas une visibilité directe. Mais il peut également être confronté au problème de collision. Dans ce chapitre, nous avons discuté généralement les systèmes RFID et des différents types de collisions dans un système RFID.

Chapitre 2 : Protocoles d’anticollision

Introduction :

Dans les systèmes RFID, il existe plusieurs algorithmes d'anticollision utilisés pour gérer les collisions et permettre une communication efficace entre les lecteurs RFID et les tags. Qui se divise en deux protocoles : protocole d'anticollision des tags et protocole d'anticollision des lecteurs.

1. Protocoles d'Anticollision des tags :

En raison des collisions, la faible efficacité d'identification des étiquettes reste un inconvénient majeur pour les systèmes RFID. L'accès multiple se produit lorsque de nombreux tags transfert des données au lecteur en une seule fois. Par conséquent, le temps doit être partagé entre les tags. Voici quelques-uns des algorithmes d'anticollision des tags couramment utilisés :

1.1. Protocole ALOHA

Le genre type de protocoles d'anticollision populaires sont les protocoles de type ALOHA. Ils sont de type TDMA. Ils sont simples et offrent de bonnes performances lorsque le nombre de radio-étiquettes à lire est réduit. Cependant, ils nécessitent généralement une augmentation exponentielle du nombre de fenêtres de temps lorsque le nombre de radio-étiquettes augmente. Ces protocoles ont des approches stochastiques, on ne peut déterminer quelle radio-étiquette répond à quel moment.[25]

1.1.1. Protocole *Pure*/*unslotted* ALOHA

Dès qu'un paquet de données est disponible, il est envoyé par la radio-étiquette au lecteur. Le temps de transmission étant relativement faible. Le temps de transmission de données ne représente qu'une fraction du temps de répétition, il y a donc des pauses relativement longues entre les transmissions. En outre, les temps de répétitions pour les transpondeurs individuels diffèrent légèrement. Il y a donc une certaine probabilité que deux radio-étiquettes peuvent transmettre leurs paquets de données à des instants différents et que les paquets de données n'entrent pas en collision. L'efficacité de transmission est approximativement de 18 %.[25]

1.1.2. Protocole *Basic Framed Slotted ALOHA* (BFSA)

Dans cette procédure, les radio-étiquettes ne peuvent commencer leur transmission que dans des fenêtres de transmission prédéfinies. La synchronisation de toutes les radio-étiquettes doit être contrôlée par le lecteur. La taille de la fenêtre étant fixe, sa mise en œuvre est simple.

Cependant, il a un point faible qui plombe l'efficacité de l'identification des radio-étiquettes dans le cas d'une taille de fenêtre importante en présence d'un nombre réduit de radio-étiquettes. L'efficacité de transmission est approximativement de 36 %. [25]

1.1.3. Protocole "*Dynamic Framed Slotted ALOHA"* (DFSA)

Le protocole DFSA peut identifier les radio-étiquettes plus efficacement puisque le lecteur régule la taille de la fenêtre en fonction du nombre de radio-étiquettes. Mais le changement de taille seul ne peut pas réduire indéfiniment les collisions en présence d'un nombre trop important de radio-étiquettes car il ne peut pas augmenter la taille de la fenêtre indéfiniment.

1.1.4. Protocole "*Advanced Framed Slotted ALOHA* (AFSA)

Le protocole AFSA calcule combien de fenêtres sont nécessaires pour lire 99 % des radio-étiquettes. Puis, il sélectionne la taille de la fenêtre qui donne le plus petit nombre d'emplacements. Puisque le protocole AFSA estime le nombre de radio-étiquettes et détermine la taille de la fenêtre afin de minimiser la probabilité de collision, il est ainsi plus efficace. Néanmoins, la taille de la fenêtre ne peut toujours pas être augmentée indéfiniment.

D'autres protocoles basés sur ALOHA ont été proposés, souvent nommés *Enhanced Framed Slotted ALOHA (EFSA)*, ces protocoles proposent chacun des points d'améliorations de performance dans certaines conditions.[25]

1.2. Protocole anticollision basée sur parcoure d'arbre

Ils sont également apparus comme une solution au problème de l'accès multiple. L'idée n'est plus de partager le temps de parole pour éviter les collisions mais d'essayer de les résoudre. Grâce à la désactivation temporaire de radio-étiquette, ces protocoles ont des approches déterministes.

Quelques exemples d'implémentations basés sur parcourent d'arbre :

- *Protocole Binary Search (BS)*
- *Protocole Dynamic Binary Search (DBS)*
- *Protocole Query-Tree*
- *Binary Tree Traversal Algorithm*
- *ID-BinaryTree Stack Algorithm*

Encore une fois, d'autres variantes basées sur les arbres de recherche ont été développées, chacune ayant des points forts dans certains cas.

Aloha	Parcours d'arbre	Hybrides
Aloha pur [26] **Aloha slotté [26]** **Aloha fenêtré- slotté**	**Division d'arbres [27]** **Arbre de requête [28]** **Rechercher binaire** **Arbitrage bit à bit**	**Arbre- slotté Aloha [29]** **Arbre de requête Hybride** **Variantes HQT [30]** **Arbre de has [31]**

Tableau 3 : protocoles d'anticollision de tags

Le tableau **3** détaille les différentes catégories de protocoles proposés dans la littérature pour réduire les collisions de tags RFID, les auteurs font une revue des principaux protocoles avec une évaluation permettant un choix guidé d'un protocole d'anticollision de tags RFID. On retiendra principalement 3 familles de protocoles à savoir :

- Les protocoles ALOHA fonctionnent sur la base d'un accès stochastique des tags au canal afin de transmettre leurs données au lecteur à portée. Ils fonctionnent bien avec un nombre réduit de tags en collisions mais sont plus laborieux dans des environnements denses ;
- les protocoles de parcours d'arbres sont basés sur une interrogation à tour de rôle des différents tags. Les tags sont classifiés selon un arbre binaire à l'aide de leur identifiant, cet arbre sera par la suite parcouru parle lecteur afin d'éviter les collisions entre tags ;
- Les protocoles hybrides, comme le nom l'indique, font une combinaison des techniques ALOHA et de parcours d'arbre.

2. Protocole d'anticollision des lecteurs

2.1. Catégorisation des protocoles

En fonction de leur procédure de contention, les protocoles d'anticollision de lecteurs peuvent être classés en deux catégories : les accès multiples à répartition dans le temps **(*Time Division Multiple Access*, TDMA)** et accès multiple par détection de porteuse **(*Carrier Sense Multiple Access*, CSMA)**. Ces deux catégories, peuvent elles-mêmes être sous découpées en fonction de l'organisation des lecteurs et le fait que les protocoles soient **centralisés** ou **distribués**. En plus de cette catégorisation, d'autres paramètres moins déterminants peuvent également être considérés comme l'utilisation d'un canal unique ou de plusieurs canaux.[39]

2.1.1. TDMA ou CSMA

Afin d'accéder au canal et interroger les tags, les lecteurs peuvent soit suivre une méthode de réservation suite à un découpage temporel ou "écouter" le canal pour s'assurer de son inactivité au préalable

Dans le premier cas, on parlera de protocoles **TDMA.** Dans cette configuration, le temps d'activité des lecteurs est divisé en unités de temps appelées timeslots. Ces intervalles de temps sont attribués ou choisis par les lecteurs, en fonction du protocole d'anticollision en cours, pour accéder au canal et interroger les tags. Ce schéma garantit qu'un seul lecteur fonctionne dans son voisinage pendant son timeslot. Aucune collision n'est possible puisque les lecteurs voisins sont soit choisi des intervalles de temps différents, soit été désactivés pendant la procédure de contention. De tels systèmes permettent une meilleure gestion de l'énergie puisque les lecteurs peuvent dormir et rester inactifs jusqu'à ce que leur timeslot arrive, s'activer puis retourner au repos garantissant un bornage temporel de l'activité du système.

Dans le deuxième cas où les lecteurs vont écouter l'activité sur le canal pour s'assurer de son inactivité, on parlera d'algorithmes **CSMA.** Puisque le médium est partagé entre les lecteurs, ils peuvent sentir l'activité de leurs voisins. Si le canal est inactif, ils pourront interroger les tags sans collision. Dans le cas où le médium est occupé, les lecteurs attendent une période aléatoire ou prédéfinie avant de vérifier à nouveau l'activité du canal. Cela garantit une meilleure flexibilité vu qu'aucune répartition préalable n'est à effectuer. La mise à l'échelle est plus simple. Cependant, le principal défi de cette solution est que dans le cas d'un déploiement dense de lecteurs, le temps d'attente pour un lecteur peut être long avant qu'il n'ait la chance d'accéder au canal afin d'interroger les tags, ce qui en retour affecte les performances du système. Cela rend ces protocoles inadaptés aux applications impliquant l'utilisation de tags mobiles.

Bien que nous ayons réparti les propositions selon ces deux schémas, il est important de noter que certaines approches reposent également sur des techniques de Frequency Division Multiple Access (**FDMA**) pour éviter les collisions. Les lecteurs peuvent fonctionner sur différents canaux pour éviter les collisions de lecture. Néanmoins, ne dépendre que de ces différents canaux pour éviter les collisions ne suffit pas compte tenu de l'éventuel déploiement dense des lecteurs RFID et de leur proximité. Certaines propositions ont pris en compte l'aspect multicanal, mais toujours sur un schéma TDMA ou CSMA pour planifier les opérations.

2.1.2. Centralisé ou Distribué

Afin d'assurer la coordination nécessaire entre les lecteurs pour éviter les collisions, une forme de communication doit être établie entre les lecteurs eux-mêmes ou avec une entité supérieure chargée de leur synchronisation. Le choix de cette forme de communication définit non seulement la nature de l'algorithme mais affecte également ses performances.

Dans le cas centralisé, les lecteurs communiquent avec une entité supérieure (serveur central) responsable de la planification des opérations. Le serveur central est capable, après avoir recueilli toutes les informations concernant la topologie des lecteurs, de calculer un schéma de lecture optimal réduisant les collisions. Cependant, en général, l'utilisation d'un serveur central limite la mobilité des lecteurs au détriment d'un niveau de calcul et de latence plus élevé que dans le cas d'un algorithme distribué. Un lien de communication doit également être établi entre les lecteurs et cette entité supérieure. Ajouté à cela, avoir des lecteurs dépendant d'une entité supérieure pour toute opération rend les solutions moins réactives. Les solutions dépendant de l'utilisation d'un serveur central se trouvent généralement dans les schémas basés sur du TDMA.

Dans une configuration distribuée, les lecteurs communiquent directement les uns avec les autres et localement (dans le temps et l'espace) pour s'accorder de pair à pair sur leurs activités et réduire les collisions. Dans le cas sans-fil, les lecteurs sont capables d'échanger avec leurs pairs dans l'étendue de leur portée de communication définissant leur voisinage. Cela permet aux solutions basées sur ce paradigme d'être évolutives et de supporter des changements dynamiques en topologie comme ce serait le cas avec les lecteurs mobiles. Chaque décision prise par un lecteur donné est dictée par sa connaissance de l'état son voisinage à un moment donné. Des solutions distribuées sont trouvées dans les algorithmes TDMA et CSMA.

2.1.3. Monocanal ou Multicanal

Aux débuts de la RFID, tous les lecteurs devaient identifier les tags en utilisant un seul canal commun. Ce média monofréquence est devenu une ressource rare avec des déploiements denses où plusieurs lecteurs sont à proximité et entraînent des collisions croissantes. Pour pallier cette déficience, le multicanal a été introduit dans la mise à jour de la norme apportée par le standard. Les lecteurs sont maintenant en mesure d'interroger les tags sur quatre canaux différents, ce qui rend les lectures de tags moins compétitives et moins sujettes à des collisions. En effet, en affectant efficacement ces canaux aux lecteurs situés dans le même voisinage, la capacité peut être multipliée par quatre fois, améliorant ainsi l'efficacité des systèmes RFID.

Cependant, avoir plus de fréquences n'empêche pas les signaux issus des lecteurs RFID d'entrer en collision. En effet, les tags sous lecteurs concurrents, même sur des canaux différents, ne peuvent toujours pas être lus et sont soumis aux interférences sur canaux adjacents.

	Centralisé	Distribué
TDMA	ACoRAS [33] FRCA [34] GD-MRSOA [35] GDRA [36] NFRA NFRA++ [37] NFRA-AIC CASE	DCS [32] Colorwave [32] DCNS MALICO PDCS **DEFAR** [39] **CORA** [39]
CDMA	**HiQ [38]**	APR DiMCA [40] EDMC HAMAC Pulse [41] EMRCA

Tableau 4 ; Récapitulatif des protocoles d'anticollision de lecteur RFID

2.2. Protocoles TDMA

Comme décrit plus-haut, les approches TDMA sont retrouvées aussi bien dans le cadre d'algorithmes centralisés que distribués. Dans cette section, nous passerons en revue les principaux protocoles TDMA de l'état de l'art.

2.2.1. Approches Distribuées :

La plupart des approches d'anticollision RFID TDMA distribuées dérivent d'un algorithme antérieur appelé Distributed *ColoSélection* et utilisent un canal de communication dédié entre lecteurs pour organiser leur activité

2.2.1.1. Distributed Color Selection (DCS) : les lecteurs réservent périodiquement des intervalles de temps (ici appelés couleurs) en choisissant au hasard parmi la gamme de couleurs disponibles. Ces intervalles de temps sont ensuite utilisés pour communiquer avec les tags. Si deux ou plusieurs lecteurs voisins choisissent les mêmes couleurs, leurs signaux entrent en collision et les tags couverts sont manqués. En cas de collision, les lecteurs concernés sélectionnent de nouvelles couleurs parmi celles disponibles et envoient un message.

Kick aux voisins pour réserver l'intervalle de temps pour la ronde d'interrogation suivante. Tous les lecteurs de la couleur correspondante au kick doivent passer à un intervalle de temps différent pour le tour suivant. Le nombre de couleurs disponibles est fixe et est donné au début. Les lecteurs disposent donc de deux interfaces de communication : la première pour interroger les tags et la deuxième pour la coordination locale entre voisins. L'inconvénient principal de cet algorithme est qu'en fonction du nombre maximum de couleurs disponibles,

le système RFID est fortement affecté. En effet, si la valeur des couleurs max est trop faible, un grand nombre de lecteurs finissent par choisir les mêmes couleurs et entrent en collision, alors que si la valeur est trop élevée, certains intervalles de temps ne sont pas occupés et le débit et le délai de couverture sont impactés.[32]

2.2.1.2. Colorwave : Aussi connu sous Variable-maximum DCS, cet algorithme résout le problème principal de DCS. Comme son nom l'indique, il permet de modifier le nombre de couleurs maximum disponibles tout au long de la vie du système RFID. Afin de définir la valeur du nombre de couleurs maximale fonction de l'état du réseau, deux variables seuils sont introduits **UpSafe& DnSafe**. Chaque lecteur surveille son nombre d'interrogations réussies. Selon qu'il atteigne la valeur de **UpSafe ou DnSafe**, les lecteurs augmentent ou diminuent respectivement leur valeur locale du maximum de couleurs disponibles et envoient un message kick contenant la nouvelle couleur choisie. Cependant dans un voisinage proche où plusieurs lecteurs entrent en collision, une fois qu'ils atteignent une valeur seuil, ils envoient tous des messages kick pour réserver leurs couleurs, générant une vague de mise à jour de couleurs d'où le nom **Colorwave.[32]**

2.2.1.3. Distributed Efficient & Fair Anti-collision for RFID (DEFAR)

DEFAR est un algorithme multicanal, distribué et TDMA d'anticollision de lecteurs RFID. Il se base sur l'utilisation de deux interfaces de communications par les lecteurs. Une première interface d'interrogation des tags et une seconde pour la communication entre voisins. Un critère récurrent des solutions d'anticollision de lecteurs RFID est l'inactivité

systématique de l'ensemble des lecteurs en collision, si lors de la phase de contention, une collision potentielle est détectée. L'ensemble des lecteurs concernés sont inactifs et manquent donc l'opportunité de lire les tags à portée. Un autre défaut remarqué parmi les solutions de l'état de l'art était le manque d'équité. En effet, les tags étant déployés à plusieurs endroits, donner l'accès régulièrement au même sous-ensemble de lecteurs constitue un risque important d'information ratée pour des applications de surveillance urbaines. Il est donc nécessaire d'avoir un accès équitable au canal pour les différents lecteurs

Afin de remédier à cela, DEFAR propose la récupération d'au moins un des lecteurs en contention pour permettre la lecture des tags à sa portée. Ce mécanisme permet parallèlement d'augmenter le débit de lecture et de diminuer le délai de couverture du système RFID. Par ailleurs, pour corriger l'équité, DEFAR met en place un système de priorisation des lecteurs lors de la contention. Cette hiérarchisation est accordée en fonction des succès/échecs de contentions sur les tentatives d'accès au canal précédentes. [39]

2.2.1.4. Coverage Oriented RFID Anti-collision (CORA)

CORA est un protocole distribué, TDMA et monocanal d'anticollision de lecteurs RFID. Tout comme DEFAR, il nécessite l'utilisation de deux interfaces de communication par lecteur afin d'interroger les tags à portée et de coordonner les activités. Dans la conception de CORA, nous sommes partis d'un constat supplémentaire concernant les différentes propositions d'anticollision en RFID. La plupart des solution proposées envisagent la désactivation de l'ensemble des lecteurs en collisions sans égard au nombre de tags couverts par chacun d'entre eux. Avec CORA, nous proposons de prendre la densité de déploiement et la mobilité des lecteurs à notre avantage afin d'augmenter le débit de lecture et réduire le délai de couverture totale quitte à augmenter, dans des proportions raisonnables, le nombre de collisions. On repose sur le fait que les collisions ne sont pas totales vu que certains tags peuvent quand même être lus car hors zone de collision. CORA tire donc profit des contraintes environnementales de déploiement pour améliorer ses performances.

L'organisation de l'activité des lecteurs a, en fonction de notre schéma TDMA, été organisée en "rounds". Tout comme pour DEFAR, un round désigne une durée durant laquelle l'ensemble des lecteurs entre en contention pour l'accès au canal d'interrogation une et une seule fois. Ces mêmes rounds sont ensuite organisés en deux phases de tailles max_slots :

1. une phase d'échange de messages entre lecteurs voisins sur l'interface de communication de portée D_{com}. Cette phase est subdivisée en max_slots timeslots d'échange de message de

durée $\boldsymbol{T_{Beacon}}$.Ainsi chaque lecteur en fonction d'un choix aléatoire définira son timeslot de diffusion.

2. une phase d'interrogation des tags sur l'interface de communication de portée T_{CRT} . Cette phase est également subdivisée en max_slots timeslots de lecture de durée T_{CRT} . A chaque timeslot de diffusion de message correspondra un timeslot d'interrogation de tags.[39]

La durée d'un round dans CORA sera donc définie comme suit :

$$Tround = max_slots \times T_{Beacon} + max_slots \times T_{CRT}$$
$$= max_slots \times (T_{Beacon} + T_{CRT})$$

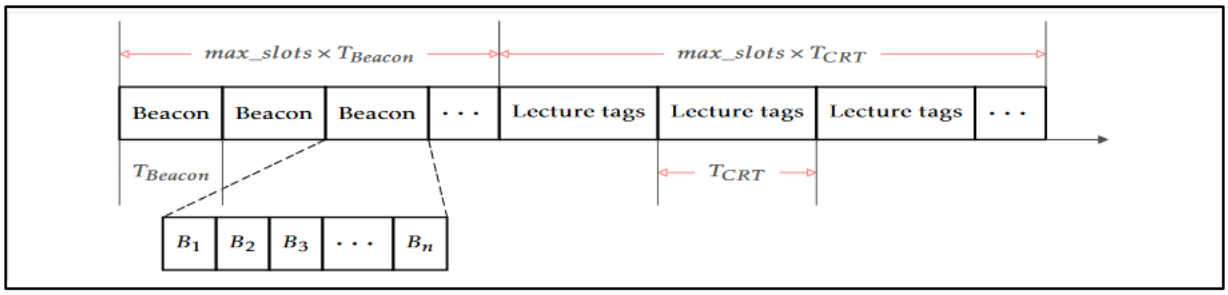


Figure 9: structure d'un round-CORA

2.2.2. Approches Centralisées :

Ces approches dépendent de l'utilisation d'un serveur central chargé d'allouer les timeslots aux différents lecteurs soit aléatoirement en suivant une distribution donnée, soit sur la base d'informations recueillies sur le système telles que la position des lecteurs, leur voisinage ou leur activité sur les tours précédents.

2.2.2.1. Neighbor Friendly RFID Anticollision (NFRA) : les interrogations des lecteurs sont organisées en rondes coordonnées par un serveur. Ce dernier arrange les différentes rondes grâce à la diffusion d'une Commande d'arrangement (Arrangement Command) annonçant le nombre maximum de timeslots disponibles. À sa réception, chaque lecteur sélectionne aléatoirement un intervalle de temps et attend la Commande d'Ordonnancement (Ordering Command OC) du serveur correspondant au timeslot choisi. A la réception de l'OC correspondant, le lecteur diffuse un message à ses voisins. Si aucune collision n'est observée pendant cette diffusion, le lecteur envoie un Message de Priorité (Overriding Frame OF) pour désactiver tous les voisins de la ronde en cours.

Quand un lecteur reçoit un OF, il attend le prochain AC du serveur pour être de nouveau en contention. Dans les déploiements très denses, cet algorithme a un nombre élevé de lecteurs

désactivés dû aux OF. Par ailleurs, les lecteurs ayant choisi une valeur de timeslot faible sont privilégiés par rapport aux autres.

2.3. Protocoles CSMA

Ces protocoles sont basés sur une écoute du canal pour s'assurer de sa disponibilité avant activité et interrogation des tags à portée, certains algorithmes nécessitent d'implémenter**2** interfaces de communications sur les lecteurs afin d'interroger les tags et converser avec les autres lecteurs.

2.3.1 Approches Distribuées

Étant donné que la disponibilité du canal est une variable locale à chaque lecteur dans son voisinage direct, la plupart des approches CSMA sont distribuées.

Ainsi les lecteurs interagissent en fonction de l'activité dans leur voisinage.

2.3.1.1 Listen Before Talk (LBT) C'est le protocole standard pour les collisions de lecteurs. Dans cette proposition, les lecteurs "écoutent" le canal pendant une période définie avant d'essayer de "parler" (interroger les tags). Si jamais le média est occupé, le lecteur bascule sur un canal différent et effectue une nouvelle session d'"écoute". Cependant, dans le cas de déploiements très denses des lecteurs, ces derniers peuvent être bloqués dans une boucle d'écoute en essayant de trouver un canal de communication disponible. De plus, ce protocole peut prés enter des performances très médiocres dans un scénario mobile, car un lecteur ayant écouté le canal dans une disposition donnée ne pourrait pas assurer un canal disponible tout au long de son trajet d'interrogation. Inversement, ce n'est pas parce-que le lecteur se trouve dans une zone radio occupée lors de son écoute que le canal ne sera pas disponible sur le reste de son trajet.[42]

2.3.2 Approches centralisées :

Les protocoles CSMA reposent sur les lecteurs qui écoutent le canal d'interrogation comme mentionné. Ainsi, avoir un serveur central est superflu puisque les lecteurs peuvent être autonomes dans de telles configurations. Cependant, quelques solutions CSMA sont encore centralisées en utilisant un serveur pour allouer des ressources aux lecteurs sur la base d'une vue globale et de l'historique du système RFID. C'est le cas de l'algorithme **HiQ.**, entités sont définies : lecteurs, serveurs **R** et serveur **Q**. Le nombre et le type de collision enregistrées sont communiqués par les lecteurs au serveur **Q**. Sur la base de ces informations et en utilisant un algorithme Q-learning, le serveur **Q** définit ensuite les slots et la distribution de fréquences

optimale pour les lecteurs. Un ensemble de slots qui optimise le fonctionnement des lecteurs est ensuite donné aux serveurs **R**. Les lecteurs reçoivent ensuite des emplacements par leur serveur **R** répondant dans la plage disponible. Cet algorithme décrit simplement la construction de cette topologie à trois niveaux. La complexité de l'algorithme d'apprentissage pour trouver une solution optimale est corrélée à la densité de déploiement des lecteurs. Dans le cas d'un réseau dense, la complexité peut induire un surcoût important. De plus, cet algorithme ne conviendrait pas dans un scénario mobile avec des paramètres changeant de façon permanente.[38]

Conclusion

En combinant ces techniques et protocoles, l'anticollision des tags et l'anticollision des lecteurs RFID permet de résoudre le problème de collision qui conduit à maximiser les performances du système et d'améliorer la fiabilité des d'identification des tags dans des environnements où plusieurs lecteurs et tags sont déployés. Dans ce chapitre, on a présenté quelques protocoles d'anticollision existent.

Chapitre 3 : Modèle et résultat de simulation

Introduction

Dans ce chapitre, Nous effectuerons des simulations de deux protocoles d'anticollision des lecteurs, tel que : Distributed Efficient & Fair Anticollision (DEFAR) et Coverage Oriented RFID Anticollision (CORA) en utilisant le logiciel MATLAB, afin de comparer leurs résultats en termes de débit de lecteur, collisions, l'efficacité, et le délai de couverture.

1. Présentation des critères d'évaluation des protocoles d'anticollision RFID

Afin d'appréhender les performances des différentes solutions proposées pour remédier aux collisions, il est nécessaire d'établir des métriques de mesure de performances. L'utilisation de ces métriques permet d'avoir une vision plus claire des protocoles proposés et de fournir une comparaison équitable de leurs performances, les auteurs proposent 10 métriques d'évaluations différentes, nous en retiendrons 5 dans la suite de nos travaux. Ce choix a été guidé par le fait que ces 5 métriques choisies sont non seulement les plus réutilisées dans la littérature, mais aussi parce qu'elles sont suffisamment représentatives.[39]

Elles sont d'ailleurs pertinentes pour évaluer d'autres technologies.

1.1. Débit de lecture

La plupart des solutions RFID sont mises en place pour effectuer des inventaires et donc arriver à lire un maximum de tags avec le moins de tentatives possibles. Le débit de lecture permet de comptabiliser le nombre d'accès fructueux au canal pour l'ensemble des lecteurs, sachant qu'un accès au canal réussisse traduit par une lecture des tags à portée. Ainsi en fonction du protocole d'anticollision choisi, un **Accès Canal Réussi (ACR)** sera décompté à chaque fois qu'un lecteur remportera la contention pour avoir l'accès au canal et lire les tags à portée. La contention est ici définie comme la phase de compétition engagée par un lecteur RFID pour avoir l'accès au canal. La résolution de cette contention se déroulera en fonction de l'algorithme d'anticollision défini. On pourrait supposer que plus le débit de lecture est important, plus les lecteurs ont accès au canal pour lire les tags. Cependant, cette métrique ne permet pas, à elle seule, d'inférer sur la distribution spatiale et temporelle des lectures au cours de l'activité des lecteurs. En effet, un débit de lecture élevé peut signifier que seul un sou ensemble des lecteurs accèdent régulièrement au canal tandis que les autres sont constamment en échec. Un autre exemple pourrait être qu'en fonction du déplacement des lecteurs, ils aient tous accès au canal à un instant donné et plus du tout à d'autres moments à cause d'une forte congestion. Il est donc

nécessaire de combiner le débit de lecture à d'autres métriques pour estimer la qualité de service d'un système RFID.

1.2. Collisions

Les collisions, se traduisent sur le plan applicatif par des erreurs de lecture et donc des tags non lus. Ces erreurs de lecture peuvent se révéler coûteuses dans le cadre d'applications commerciales (gestion de stock, point de vente, etc.) voire même critiques pour d'autres types d'applications (surveillance d'animaux, contrôle d'accès, etc.). Cette métrique permet donc d'identifier le nombre **d'Accès Canal Échoués (ACE).** On comptabilisera donc un ACE à chaque fois qu'un lecteur échouera en contention pour l'accès au canal. Grâce à nos outils de simulation, nous pourrons comptabiliser les accès de prime abord réussis mais ayant conduit à des collisions dans les **ACE.** Un nombre important de collisions peut être interprété comme une perte d'énergie importante, ce qui va à l'encontre du principe d'utilisation de la RFID.

En effet, lorsqu'un lecteur entre en contention pour l'accès au canal pour finalement échouer, il a perdu inutilement de l'énergie. En fonction de l'algorithme utilisé, il a même pu faire échouer d'autres lecteurs. Par ailleurs, cette contention se solvant par un échec impacte le délai de lecture des tags que nous verrons ultérieurement.

1.3. Efficacité

Cette métrique combine les deux précédentes afin de déterminer les dispositions des algorithmes à éviter les collisions et autoriser l'accès au canal aux lecteurs. L'efficacité se calcule comme suit :

$$Eff = \frac{ACR}{(ACR + ACE)}$$

La distribution temporelle desACR pointée plus haut comme indéterminée avecle débit de lecture, peut ici être inférée. En effet, en combinant les ACR et ACE,on arrive à définir la distribution des accès au canal en fonction des contentions. Ainsi, avec un débit de lecture faible, exprimant un accès au canal difficile car congestionné, les collisions sont nombreuses et donc l'efficacité reste faible. Par contre, si l'efficacité et le débit de lecture sont tous deux élevés, on peut en déduire que les collisions sont faibles et donc que l'accès au canal est plus libre.

1.4. Indice d'équité de Jain (IEJ)

Cette métrique, très partagée dans plusieurs domaines, permet d'apprécier l'équité dans l'accès au canal entre les différents lecteurs. L'IEJ se calcule comme suit :

$$IEJ = \frac{[\sum_{i=1}^{n} ACR_i]^2}{n \times \sum_{i=1}^{n} ACR_i^2}$$

L'IEJ permet d'avoir une idée de la distribution spatiale des lectures ce qui est impossible avec le débit de lecture. En effet, si les lecteurs ont tous les mêmes valeurs en terme d'ACR, l'IEJ est égale à 1. A l'inverse, dans le pire cas, un seul lecteur concentre tous les ACR et l'IEJ vaut 1/n. Ainsi, plus les ACR seront équitablement répartis, plus la valeur de l'IEJ se rapprochera de 1. Sinon elle tendra vers 0. Dans le cadre d'applications de logistique, de bonnes performances en IEJ permettent d'affirmer que l'ensemble des produits sou surveillance sont vérifiés régulièrement et qu'aucun groupe de produits n'est délaissé. Dans l'ensemble, un indice d'équité performant renseigne sur une répartition équitable de la consommation énergétique des lecteurs. Dans le cas où ils seraient alimentés par une batterie, l'ensemble des batteries se déchargeraient de manière plus ou moins synchronisée en fonction de la durée de l'activité des lecteurs.[39]

2. Distributed Efficient & Fair Anti-collision (DEFAR):

DEFAR a été conçu en vue d'améliorer les performances des solutions RFID dans les déploiements denses et mobiles et s'appuie sur l'observation des aspects négatifs des algorithmes de l'état de l'art. Ainsi avons-nous choisi de base DEFAR sur une approche TDMA. L'utilisation d'une telle solution permet de s'affranchir des phases d'écoute de canal plus ou moins longues et donc de définir un "agenda" d'activité pour les lecteurs. Nous avons également choisi d'opter pour une solution distribuée avec les lecteurs qui déroulent localement le même algorithme. Se passer d'un serveur central, peut certes augmenter le nombre de collisions mais permet d'avoir des décisions locales des lecteurs en fonction de leur environnement direct et non pas d'un calcul global. Les décisions locales ne subissent pas la latence induite par la collecte d'informations globales d'un serveur, leur calcul et redistribution aux lecteurs. L'ensemble de ces choix a donc été effectué dans l'optique de maximiser les performances en termes de débit de lecture, efficacité, équité et réduction de latence afin d'obtenir un protocole adapté aux contraintes des environnements et déploiements étudiés.

L'utilisation d'un mécanisme TDMA permet d'organiser les activités de lecteurs sur le temps. A cet effet, l'accès au canal a été organisé en "rounds". Un ***round*** définit une durée

durant laquelle l'ensemble des lecteurs déployés entrent en contention pour l'accès au canal une et une seule fois. Ces rounds sont ensuite eux-mêmes subdivisés en max_slots timeslots de durée $\mathbf{T_{Slot}}$. A chaque timeslot, un sous-ensemble du nombre total de lecteurs entre en contention pour l'accès au canal.

- Premièrement, une phase d'échange de messages entre lecteurs voisins sur leur interface de portée $\mathbf{d_{Com}}$. Chaque lecteur découvre son voisinage et s'assure de pouvoir accéder au canal. Le voisinage désigne l'ensemble des lecteurs à portée de communication sur le canal dédié et donc susceptible d'être en collision de lecture sur le canal d'interrogation. Avant de diffuser un message durant cette phase, chaque lecteur observe d'abord un temps d'attente tiré aléatoirement afin de réduire les collisions de diffusion. La conception de ces temps d'attente a été faite de sorte à ce que chaque lecteur puisse diffuser son message à ses voisins avec un nombre négligeable de collisions. Cette phase de diffusion de messages est subdivisée en différents slots d'attente notés B1, B2, ……, Bn (voir Figure 3.1). Cette phase sera notée $\mathbf{T_{Beacon}}$;
- Deuxièmement, une phase d'interrogation des tags pendant une durée elle aussi déterminée notée $\mathbf{T_{CRT}}$. Au vu de la phase d'échange de messages précédente, les lecteurs en collision sont désactivés et ne participent pas à la phase de lecture des tags. Aucune collision n'est donc possible durant la lecture des tags. En effet, seul au plus un lecteur par slot et par fréquence pourra être actif dans un voisinage donné.

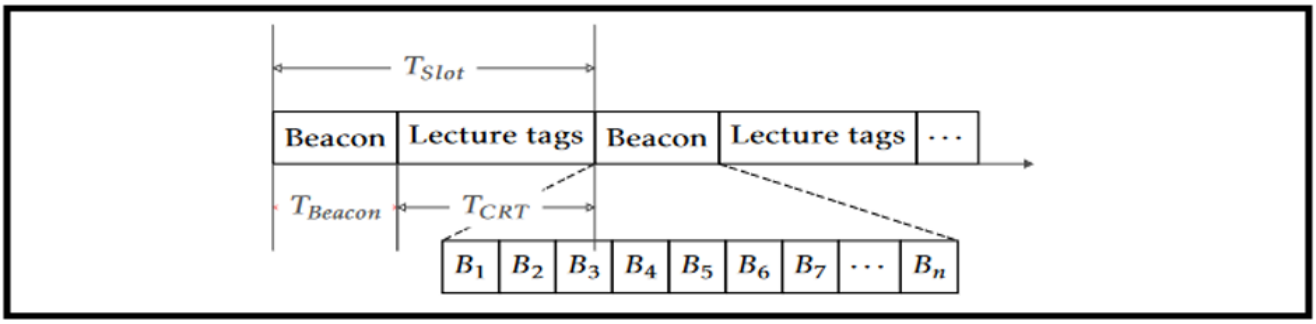


Figure 10 : structure d'un round-DEFAR

Les lecteurs sont en mesure de suivre l'évolution des rounds et timeslots grâce à une approche TDMA basée sur l'utilisation d'horloges internes aux lecteurs. La durée d'un round sera donc définie comme :

$$\boldsymbol{Tround = max_slots \times TSlot = max_slots \times (TBeacon + TCRT)}$$

Afin d'éviter la désactivation de l'ensemble des lecteurs lors d'une contention, nous avons introduit un système de comparaison d'ID permettant de conserver au moins un lecteur qui sera alors capable de lire les tags à portée. Par ailleurs, pour éviter que les mêmes lecteurs aient constamment accès au canal, nous définissons différents niveaux de priorité pour augmenter les chances des lecteurs en échec face aux lecteurs ayant réussi sur les rounds précédents.

— **NEUTRAL** est le niveau de priorité de l'ensemble des lecteurs au départ ;

— **LAZY** est le niveau de priorité inférieur affecté aux lecteurs ayant réussi leur contention sur le round précédent ;

— **PUMPED UP** est le niveau de priorité supérieur accordé aux lecteurs en échec sur le round précédent et leur permettant d'augmenter leurs chances d'accès au canal sur le round en cours.

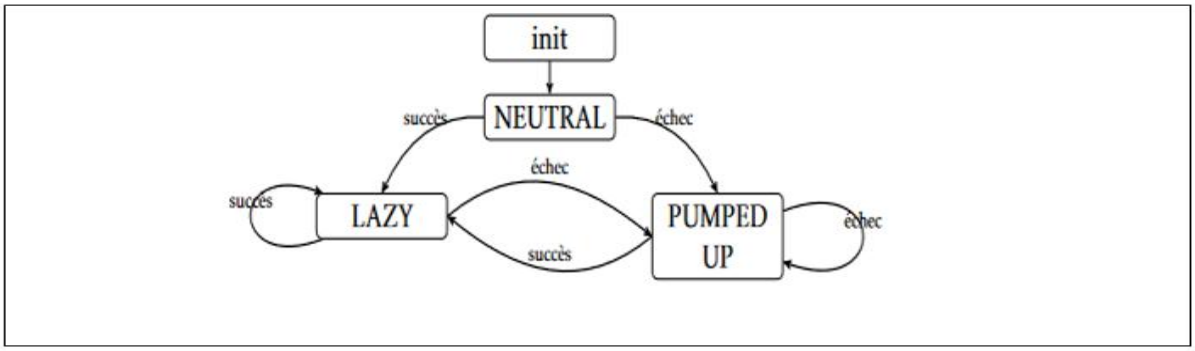


Figure 11 :diagramme d'états

A l'initialisation, les lecteurs sont dans le premier round, avec le niveau de priorité NEUTRAL, et choisissent aléatoirement un slot sur la plage $[0; max_slots[$ et un canal parmi ceux accordés par ETSI. Chaque lecteur Ri, connaissant la durée d'un slot, attend donc son slot choisi $slot_i$ pendant une durée $t = sloti \times TSlot$. Une fois au slot correspondant, Ri observe un temps aléatoire avant de diffuser un message à ses voisins contenant son ID et le canal d'interrogation fi choisi.

Ce message est diffusé sur l'interface de communication dédiée et sur la portée $\mathbf{d_{Com}}$. Deux scénarios peuvent alors se produire (voir Algorithme 1) :

Scénario 1 : Ri ne reçoit aucun message durant $\mathbf{T_{Beacon}}$. $\mathbf{R_i}$ considère alors qu'il est le seul lecteur sur ce slot dans son voisinage. Il peut alors accéder au canal fi choisi et interroger les tags pendant TCRT avant de passer en priorité LAZY (Algo 1 lignes 6-7) .

Scénario 2 : Ri reçoit au moins un message d'au moins un de ses voisins ayant choisi le même canal d'interrogation sur la durée $\mathbf{T_{Beacon}}$. $\mathbf{R_i}$ compare alors les IDs contenus dans les messages reçus avec le sien (Algo 1 lignes 9-10) :

— Ri a l'ID le plus petit parmi ceux en contention. $\mathbf{R_i}$ remporte alors la contention et lit les tags à portée pendant TCRT avant de passer en état LAZY pour le round suivant ;

— Ri n'a pas le plus petit ID, un ou plusieurs ID parmi ceux reçus est plus faible que celui de $\mathbf{R_i}$. Ce dernier perd alors la contention et passe en priorité PUMPED UP pour le tour suivant. $\mathbf{R_i}$ enregistre alors une collision (Algo 1 ligne 11).

Ce processus de contention est maintenu pendant le premier round où l'ensemble des lecteurs démarrent en priorité NEUTRAL.

Algorithm 1 DEFAR - Premier *round* pour un lecteur R_i

```
1:  slot_i ← (int)random[0; max_slots]
2:  f_i ← (int)random[1; f_max]
3:  prio_i ← NEUTRAL
4:  if slot en cours == slot_i then
5:      Diffusion message
6:      if Pas de message reçu then                    ▷ Pas de collision
7:          Lecture tags; prio_i ← LAZY
8:      else                          ▷ Au moins un lecteur sur le même canal f_i
9:          if R_i a l'ID le plus petit then           ▷ R_i remporte la contention
10:             Lecture tags; prio_i ← LAZY
11:         else prio_i ← PUMPEDUP
12:         end if
13:     end if
14: end if
```

Sur les rounds de contention suivants, on conserve la même technique de résolution de contention avec quelques modifications pour prendre en compte les nouvelles priorités introduites. En effet, suite au premier round, tous les lecteurs sont soit en LAZY, s'ils ont réussi leur contention, soit en PUMPED UP s'ils ont échoué. Pour le nouveau tour de contention, les lecteurs choisissent à nouveau aléatoirement un $\mathbf{slot_i}$ et un canal fi. Ils attendent le slot

correspondant à leur choix pendant le temps t = sloti × TSlot, observent le temps d'attente déterminé avant de diffuser leurs messages aux voisins sur le canal de communication dédié. Cependant, cette fois-ci le message diffusé contient en plus de l'ID et du canal choisi, l'état priori du lecteur. Ainsi en fonction du niveau de priorité d'un lecteur Ri , on peut avoir les cas suivants :

1. Scénario 1 : Ri est priorité LAZY et a donc réussi sa contention sur le round précédent (Algo. 2 lignes 8) :

— pas de collisions enregistrées lors de l'échange de messages : il n'y donc aucun lecteur concurrent dans le voisinage de Ri qui peut de nouveau accéder au canal et lire les tags à sa portée pendant TCRT (Algo 2 lignes 5-6) ;

— au moins un voisin diffuse un message avec le même canal fi : dans ce cas, la résolution de la contention se fera en fonction du niveau de priorité des lecteurs :

— les autres lecteurs en contention sont également en priorité LAZY : l'ensemble des lecteurs engagés ont déjà eu accès au canal sur le round précédent. Dans ce cas, la résolution se fera par rapport à l'ID comme lors du premier round. Si Ri a l'ID le plus faible, il accède au canal et interroge les tags, sinon, il passe en PUMPED UP pour le round suivant (Algo 2 lignes 11-16) ;

— au moins un des lecteurs en contention est en priorité PUMPED UP : Ri perd la contention et passe en PUMPED UP pour le tour suivant (Algo 2 lignes 9-10).

2**. Scénario 2** : Ri est en priorité PUMPED UP et a échoué lors de la contention sur le round précédent (Algo 2 ligne 17).

— pas de collisions enregistrées lors de l'échange de messages : il n'y donc aucun lecteur concurrent dans le voisinage de Ri qui peut enfin.

Accéder au canal et lire les tags à sa portée pendant $\mathbf{T_{CRT}}$. Ri passera en priorité LAZY sur le round suivant (Algo 2 lignes 5-6).

— au moins un voisin diffuse un message avec le même canal fi : dans ce cas, la résolution de la contention se fera en fonction du niveau de priorité des lecteurs :

— au moins un des lecteurs en contention est en priorité PUMPED UP : les lecteurs sont dans le niveau de priorité supérieur car ayant échoué sur le round précédent. Dans ce cas, la résolution se fera par rapport à l'ID comme lors du premier round. Si Ri a l'ID le plus faible, il

accède au canal et interroge les tags avant de passer en LAZY, sinon, il reste en PUMPED UP pour le round suivant (Algo 2 lignes 20-25).

— les autres lecteurs en contention sont en priorité LAZY : Ri gagne la contention et lit les tags à sa portée pendant $\mathbf{T_{CRT}}$ avant de passer en priorité LAZY pour le tour suivant (Algo 2 lignes 18-19).

Dans le cas de l'arrivée d'un nouveau lecteur dans le système, il prend la priorité LAZY et grâce à son interface de communication dédiée écoute le canal en attente du prochain round. Il choisit alors un timeslot et un canal aléatoirement comme les autres lecteurs et attend le slot correspondant avant de diffuser son message. L'ordre de priorité définit est : PUMPED UP puis NEUTRAL et enfin LAZY. Le nouveau lecteur prendra donc la main face à des lecteurs LAZY en cas de collision avant de passer lui-même en LAZY pour le tour suivant (Algo 2 lignes 27-28). En cas de contention face à un lecteur PUMPED UP, il perdra la contention et passera lui-même en PUMPED UP (Algo 2 lignes 29-

30). Sinon, face à un autre nouveau lecteur, en priorité NEUTRAL également, la contention sera résolue comme lors de l'initialisation (Algo 2 lignes 31-34).[39]

Algorithm 2 DEFAR - *rounds* suivants pour un lecteur R_i

```
1:  slot_i ← (int)random[0; max_slots]
2:  f_i ← (int)random[1; f_max]
3:  if slot en cours == slot_i then
4:      Diffusion message
5:      if Pas de message reçu then                          ▷ Pas de collision
6:          Lecture tags; prio_i ← LAZY
7:      else                          ▷ Au moins un lecteur R_j avec le même canal
8:          if prio_i == LAZY then
9:              if prio_j == PUMPEDUP or prio_j == NEUTRAL then
10:                 prio_i ← PUMPEDUP                        ▷ R_i perd la contention
11:             else
12:                 if R_i a l'ID le plus petit then         ▷ R_i gagne la contention
13:                     Lecture tags; prio_i ← LAZY
14:                 else prio_i ← PUMPEDUP
15:                 end if
16:             end if
17:         else if prio_i == PUMPEDUP then
18:             if prio_j == LAZY or prio_j == NEUTRAL then
19:                 Lecture tags; prio_i ← LAZY
20:             else
21:                 if R_i a l'ID le plus petit then         ▷ R_i gagne la contention
22:                     Lecture tags; prio_i ← LAZY
23:                 else prio_i ← PUMPEDUP
24:                 end if
25:             end if
26:         elseprio_i == NEUTRAL
27:             if prio_j == LAZY then
28:                 Lecture tags; prio_i ← LAZY
29:             else if prio_j == PUMPEDUP then
30:                 prio_i ← PUMPEDUP
31:             else                                         ▷ prio_j == NEUTRAL
32:                 if R_i a l'ID le plus petit then         ▷ R_i gagne la contention
33:                     Lecture tags; prio_i ← LAZY
34:                 else prio_i ← PUMPEDUP
35:                 end if
36:             end if
37:         end if
38:     end if
39: end if
```

3. Les résultats de simulation

Dans cette thèse, on a simulé les protocoles d'anticollision des lecteurs : DEFAR et DCS en termes de débit de lecteur, collisions et efficacité. Dans la simulation, Nous fixons le nombre de slots de temps dans un round est 4 slots (*max_slot* = 4) et le nombre de canaux de fréquence est 1 canal (*max_canal* = 1), c à d on utilise une seule fréquence pour tous les protocoles.

On considère un nombre croissant de lecteurs allant de 1 à 20 lecteurs. On suppose que tous les lecteurs concourent pour identifier les tags. C'est-à-dire la distance entre les deux plus loin lecteurs est inférieure à la portée de communication notée d_{com}. La portée de communication est la distance maximale à laquelle les lecteurs sont en mesure d'échanger des messages pour leur coordination.

On fixe le nombre de rounds pour tous les protocoles est constant et égal à 100 rounds. Pour mieux comparer le débit de lecteurs, collision, et efficacité des protocoles.

La figure 9 montre le débit de lecteur en fonction du nombre de lecteurs des protocoles d'anticollision DEFAR et DCS. On peut remarquer que le débit de lecteur de DEFAR est meilleur que DCS pour un nombre de lecteurs supérieur à 4 lecteurs. Aussi les performances de DCS est décroît avec l'augmentation de nombre de lecteur. Contrairement, la performance de DEFAR est stable.

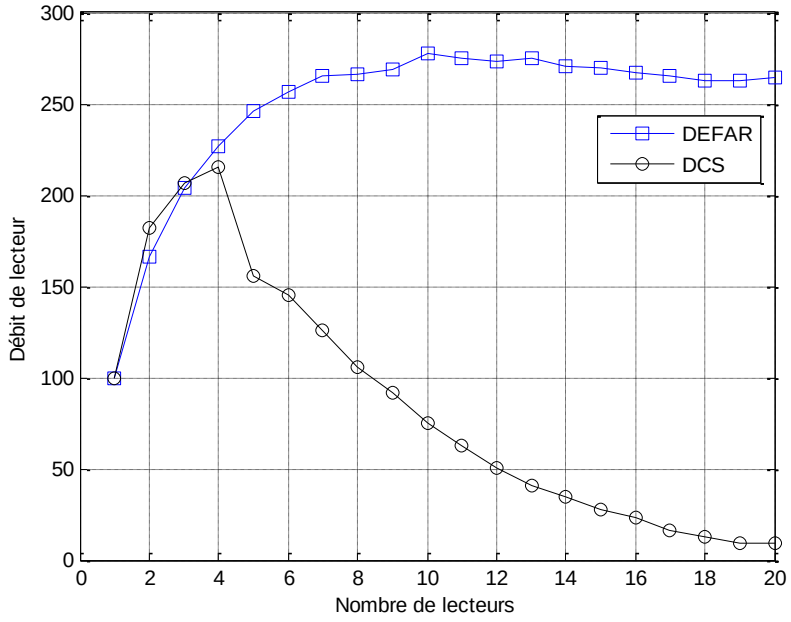


Figure 12 : le débit de lecteur en fonction en nombre de lecteur pour 100 rounds

La figure 10 montre la collision ou le nombre d'accès canal échoués (ACE) en fonction du nombre de lecteurs des protocoles d'anticollision DEFAR et DCS. On peut observer que ACE de DEFAR est inférieur de DCS c-à-d le résultat de DEFAR est mieux que DCS.

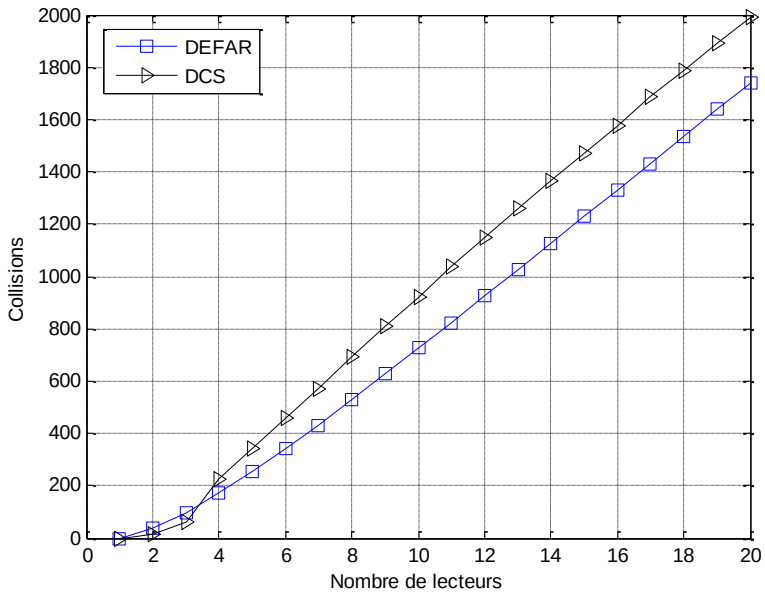


Figure 13 : le débit de lecteur en fonction en nombre de lecteur pour 100 rounds

La figure 11 montre l'efficacité en fonction du nombre de lecteurs des protocoles d'anticollision DEFAR et DCS. On peut remarquer L'efficacité DSC est meilleure que DERAF pour un nombre de lecteurs inférieur à 4 lecteurs. Après que la valeur de 4 devient L'efficacité DERAF est meilleure que DSC. Aussi les performances de DCS est décroît avec l'augmentation de nombre de lecteur.

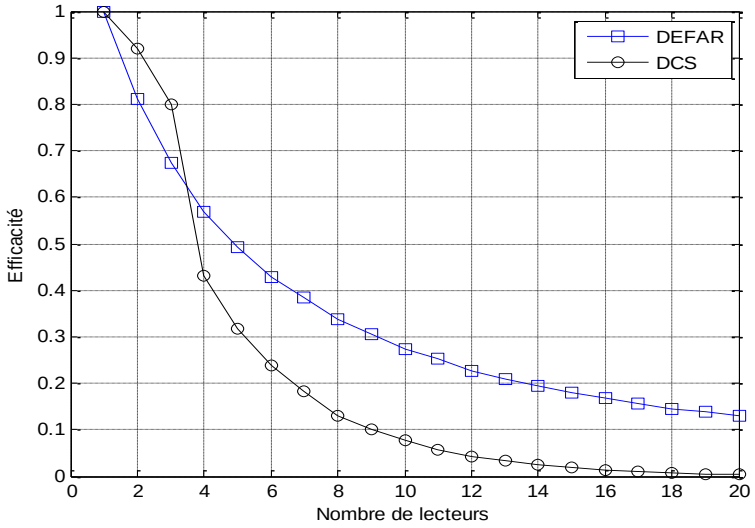


Figure 11 : L'efficacité en fonction en nombre de lecteur pour 100 rounds

Conclusion

Dans ce dernier chapitre on a simulé sur MATLAB et on a comparé les performances des deux protocoles d'anticollision des lecteurs DEFAR et DCS en termes de débit de lecture, collisions et efficacité. Les résultats de simulation obtenus dans ce chapitre montrent que le protocole d'anticollision DEFAR est meilleur que DCS.

Conclusion générale

Dans ce mémoire, nous avons donné en premier temps des généralités sur les systèmes RFID et nous avons défini le problème de collision des tags et des lecteurs. Ce travail s'intéresse au problème des collisions de lecteurs. Pour résoudre ce problème de collision, il existe plusieurs protocoles d'anticollision de lecteurs. On a présenté dans cette mémoire quelques protocoles d'anticollision de lecteurs qui on peut le diviser en deux catégories : distribué et centralisé.

Dans ce travail, on a simulé deux protocoles d'anti collision de lecteur tels que : DEFAR et DCS, et on a comparé leur performance en termes de débit de lecture (ou nombre d'Accès Canal Réussi, ACR), nombre d'Accès Canal échoué (ACE) et efficacité. Les résultats ont montré que le protocole DEFAR est mieux que le protocole DCS.

Les travaux de recherches qui ont été réalisés dans les systèmes RFID ouvrent le domaine de recherche pour la proposition et l'élaboration de nouveaux protocoles d'anti collision de lecteurs, plus performants qui réduisent au maximum les collisions.

Bibliographie

[1] Anthoy Ghiotto, Conception d'antennes de tags RFID UHF, application à la réalisation par jet de matière (Thèse d'exercice), Institut polytechnique de Grenoble, 26 novembre 2008.

[2] ISECOM, Hacking Exposed Linux: Linux Security Secrets & Solutions, McGraw-Hill Osborne Media, 2008.

[3] Hunt et D. V., RFID - A guide to radio frequency identification, John Wiley & Sons, 2007.

[4] Rajit Gadh, George Roussos, Katina Michael, George Q. Huang, B. Shiv Prabhu et Peter Chu, « RFID - A Unique Radio Innovation for the 21st Century », Proceedings of the IEEE, vol. 98, n^{o} 9, September 2010, p. 1546-1549.

[5] Brevet US 2927321[archive] enregistré le 16 aout 1952, publié le 1er mars 1960.

[6] Donald B. Harris, Radio transmission systems with modulatable passive responder, Google Patents, 1960.

[7] Brevet US 3391404 [archive] enregistré le 18 mai 1959, publié le 2 juillet 1968.

[8] Brevet US 3299424 [archive] enregistré le 07 mai 1965, publié le 17 janvier 196.

[9] Joseph H Vogelman, Passive data transmission technique utilizing radar echoes, Google Patents, 1968.

[10] Brevet US 3299424 [archive] enregistré le 07 mai 1965, publié le 17 janvier 1967.

[11] (en) Jorgen P Vinding, Interrogator-responder identification system Google Patents, Google Patents, 1967.

[12] Brevet US 3460139 [archive] enregistré le 06 septembre 1967, publié le 5 août 1969

[13] Otto E Rittenbach, Communication by radar beams, Google Patents, 1969.

[14] Daniel Dobkin, RF in RFID: Passive RFID UHF in Practice, Amsterdam, Newnes, 2008, 2^{e} éd., 529 p.

[15] Himanshu Bhatt et Bill Glover, RFID Essentials, O'Reilly, 2006, 260 p.

[16] « Real Time Location Systems » [archive], clarinox, Novembre 2009 .

[17] David TIHAY. –APPLICAION DE LA RFID A LA PREVENTION DES RISQUES PROFFIONELLES EN ENTREPRISE.INRS- Hygiène et sécurité du travail, ND 2232, pp12-13-14, 1er trimestre2012.

[18] Frédéric LETIENT. - Etat de l'art et applications des RFID. UE ELE114 – Epreuve TEST Travail d'Etude et de Synthèse Technique en ELECTRONIQUE. - Grenoble, CUEFA GRENBOLE UNIVERSITES, pp15-16-17, le 9 Juin 2008.

[19] BACHOTI Youssef ; BELHAJ SENDAGUE ; Bassim et RODRIGUES OLIVEIRA Joao Gabriel, Projet de fin d'étude

[20] Nicolas Seriot, Les systèmes d'identification radio (RFID) -fonctionnement, applications et dangers - , pp14-15,13 janvier 2005.

[21] Network World, 3 mai 2004, Volume 21, édition 18.

[22] SADAOUI KENZA, SENHADJI RAZIKA, projet fin d'étude

[23] M. A. Kalache and L. Fergani, "Performance's comparison of RFID anti-collision algorithms," in International Conference on Multimedia Computing and Systems (ICMCS), 2014, pp. 808–813.

[24] Yan Zhang, Laurance T. Yang, and I. Jiming Chen, "RFID AND SENSOR

[25] TaoCheng, LiJin, Analysis and Simulation of RFID Anti-collision Algorithm, school of Electronics and Information Engineering, BeijingJiaotong University, Beijing100044, P.R. China, Feb. 12-14, 2007 ICA CT 2007.

[26] Dheeraj K Klair, Kwan-Wu Chin et Raad. « An investigation into the energy efficiency of pure and slotted aloha based Reid anti-collision protocols ». In: Proceedings of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM. IEEE. 2007, p. 1–4.

[27] Yuan-Cheng Lai, Ling-Yen Hsiao et Bor-Shen Lin. « Optimal slot assignment for binary tracking tree protocol in RFID tag identification ». In: IEEE/ACM Transactions on Networking 23.1 (2015), p. 255–268.

[28] Yuxiao Hou et al. « PHY-Tree: Physical Layer Tree-Based RFID Identification ». In: IEEE/ACM Transactions on Networking (TON) 26.2 (2018), p. 711–723.

[29] Haifeng Wu et al. « Binary tree slotted ALOHA for passive RFID tag anticollision ». In: IEEE Transactions on Parallel and Distributed Systems 24.1 (2013), p. 19–31.

[30] Yu-Min Hu, Iang-Chong Chang et Jung-Shian Li. « Hybrid blocking algorithm for identification of overlapping staying tags between multiple neighboring readers in RFID systems ». In: IEEE Sensors Journal 15.7 (2015), p. 4076–4085.

[31] Hong Zhang, Lei Han et Yu-Lu Li. « Design of hash-tree anti-collision algorithm ». In: Proceedings of 3rd International Conference on Natural Computation ICNC. T. 5. IEEE. 2007, p. 176–179.

[32] James Waldrop, Daniel W Engels et Sanjay E Sarma. « Colorwave: an anticollision algorithm for the reader collision problem ». In: Proceedings of ICC. 2003.

[33] Essia Hamouda, Nathalie Mitton et David Simplot-Ryl. « Reader Anti-Collision in Dense RFID Networks with Mobile Tags ». In: Proceedings of Int. Conf. on RFID-Technologies and App. RFID-TA. 2011.

[34] Hadiseh Rezaie et Mehdi Golsorkhtabaramiri. « A fair reader collision avoidance protocol for RFID dense reader environments ». In: Wireless Networks (2017)

[35] Litian Duan, Zizhong John Wang et Fu Duan. « Geometric Distribution-Based Readers Scheduling Optimization Algorithm Using Artificial Immune System ». In: Sensors 16.11 (2016)

[36] Victoria Bueno-Delgado et al. « A geometric distribution reader anti-collision protocol for RFID dense reader environments ». In: IEEE T-ASE(2013).

[37] Renato Ferrero et al. « A fair and high throughput reader-to-reader anti-collision protocol in dense RFID networks ». In: IEEE Transactions on Industrial Informatics 8.3 (2012).

[38] S.E. Sarma J. Ho D.W. Engels. « HiQ: a hierarchical Q-learning algorithm to solve the reader collision problem ». In: Proceedings of Int. Symposium on Applications and the Internet Workshops, SAINT. USA, 2006

[39] Abdoul Aziz MBACKE « Collecte et remontée multi-sauts de données issues de lecteurs RFID pour la surveillance d'infrastructures urbaines », Thèse de Doctorat, université de Inria Lille-Nord Europe, 2018.

[40] Haidar Safa, Wassim El-Hajj et Christine Meguerditchian. « A distributed multichannel reader anticollision algorithm for RFID environments ».In: Journal of Computer Communications 64 (2015).

[41] S. Birari et S. Iyer. « PULSE: A MAC Protocol for RFID Networks ». In:Proceedings of Int. workshop on RFID and Ubiquitous Sensor Networks (USN).2005.

[42] EPC TM radio-frequency identity protocols class-1 generation-2 UHF RFID protocol for communications at 860 MHz - 960 MHz version 1.2.0. EPC global Standard specification, 2007.