UNIVERSITE ASSANE SECK DE ZIGUINCHOR

UFR des Sciences et Technologies
Département d'Informatique

Mémoire de fin d'étude

Pour l'obtention du diplôme de
Master en Informatique mention Génie Logiciel spécialité
Conduite de projet

Sujet : Optimisation d'un protocole d'anticollision centralisé pour les lecteurs RFDI (BACP)

Présenté par :

Sidiya Dieng

Sous la direction de :

Dr Youssou FAYE

Mme MENDY Marius

Mémoire soutenu le 18 Mai 2018 devant le jury composé de :

Prénom et nom	Grade	Qualité	Etablissement
Salomon SAMBOU	Professeur Titulaire	Président de Jury	UASZ
Youssou FAYE	Maître de conférences Titulaire	Encadrant	UASZ
Mme MENDY Marius	Enseignement chercheur	Co- Encadrant	UASZ
Elhadji Malick NDOYE	Maître de conférences assimilé	Examinateur	UASZ
Abel DIATTA	Maître de conférences assimilé	Rapporteur	UASZ

Année Universitaire 2018-2019

Dédicaces

Ce présent mémoire est dédié, avec amour et gratitude, à toutes les personnes qui m'ont soutenu, encouragé dans mes études:

À mes défunts père et mère ***(Ousmane Dieng et Khary Ndoye)*** *:*
Qui ne seront hélas pas présent le jour de ma soutenance pour partager mon stress et ma joie,
Puisse DIEU vous accueillir dans son paradis céleste!

Aux deux femmes les plus importantes de ma vie :

*Ma maman (**Marie Ndiaye**), ton amour et ton affection inestimable, pour ta confiance, et tes sacrifices sans fins, pour toutes les valeurs que tu as su m'inculquer, je te suis redevable d'une éducation dont je suis fier!!!*

*À ma femme (**Nafissatou Ndiaye**)*
Même si aucune dédicace ne saurait exprimer ma profonde gratitude pour ta compréhension et ton soutien, je ne saurai jamais te remercier !

*À mon oncle **Ibrahima Bâ** ancien Directeur de la Direction des Patrimoines de l'UASZ, ma tante madame **Mariama Touré Bâ** et toute la famille sans exception !*
Pour leur soutien inconditionnel et leur amour inestimable qu'ils ont su m'apporter !

Dédicace

À mes sœurs, mes frères, mes neveux et nièces, Ami(e)s, mes cousin(e)s, mes tantes, oncles et parents, pour tous vos encouragements, que ce travail soit le témoignage sincère et affectueux de ma profonde reconnaissance, pour tout ce que vous avez fait pour moi !
Enfin à tous ceux qui sentent participant sur ma réussite,

À vous tous, je vous dédie ce travail et vous dis merci !

Remerciement

"Traitez les gens comme s'ils étaient ce qu'ils doivent être et vous les aiderez à devenir ce qu'ils sont capables d'être"

Tout d'abord, je remercie le Tout-Puissant de m'avoir donné la force et le courage d'arriver à terme de ce travail ;

Je tiens tout d'abord à exprimer mes plus chaleureux remerciements à mes encadrants :

***Docteur YOUSSOU FAYE**, Docteur à l'Université Assane Seck de Ziguinchor et chef du département informatique, d'avoir partagé avec moi ses brillantes intuitions,*

***Madame Mendy (MARUIS DASILVA),** Enseignante chercheur à l'Université Assane Seck de Ziguinchor, une personne de grande ouverture et compréhension.*

Vous n'avez managé aucun effort à mon égard malgré vos calendriers chargés. Je vous témoigne toute ma gratitude et ma reconnaissance pour m'avoir fait l'honneur de m'encadrer. C'est avec vous que j'ai compris finalement le sens des mots rigueur, précision et patience. Vraiment merci pour votre grande disponibilité, pour vos précieux conseils qui m'ont motivé face à certaines difficultés rencontrées. Votre ouverture d'esprit, de connaissances m'ont été d'une très grande utilité. J'espère seulement que ça ne s'arrêtera pas là. Je vous en suis infiniment reconnaissant pour tout.

Je souhaite remercier les membres de mon jury de mémoire :

Monsieur Salomon SAMBOU, professeur à l'Université Assane SECK de Ziguinchor, pour le temps qu'ils a bien voulu consacrer à l'évaluation de ce travail, mais aussi, de m'avoir fait l'honneur de présider le jury de ma soutenance.

***Docteur Elhadji Malick NDOYE**, Docteur à l'Université Assane SECK de Ziguinchor, pour son ouverture et nos discussions riches dans tous les domaines scientifiques. Je vous remercie de m'avoir fait l'honneur d'être rapporteur de mon mémoire.*

***Docteur Abel DIATTA**, Docteur à l'Université Assane SECK de Ziguinchor. Je vous remercie de m'avoir fait l'honneur d'être rapporteur de mon mémoire.*

Mes amicaux remerciements vont à tous les camarades de promotion, pour tous les beaux moments passés ensemble.

*À ma mère **MARIE NDIAYE**, ma femme **Nafissatou NDIAYE**,*
Mes sœurs et mes frères.

Résumé

Les progrès dans les domaines des télécommunications et de technologie ont permis de donner corps à une idée assez ancienne : celle de l'identification à distance par radiofréquence. Les technologies actuelles utilisent des tags passifs ou actifs, couplés de façon magnétique ou radiative à un lecteur. Malgré l'absence d'une véritable standardisation, les tags RFID se développent très rapidement dans des domaines très variés : logistique, identification, contrôle d'accés, protection contre le vol, paiement, etc.

Les progrès dans le domaine de la miniaturisation et des nouveaux matériaux laissent prévoir de nouvelles percées technologiques avec des applications de plus en plus étendues, pouvant aller jusqu'à un «internet des objets ». Cependant, de tels déploiements souffrent d'un problème de collisions. Ces dernières réduisent grandement la qualité des déploiements RFID en délai et en énergie. Il existe trois types de collisions, les collisions de tags qui sont déjà bien définies et normalisées, les collisions de lecteurs et les collisions entre lecteurs et tags.

Par ailleurs, ce mémoire traite des collisions de lecteurs car avec le phénomène de la densification des lecteurs, les collisions lecteurs sont devenues de plus en plus fréquentes et elles affectent les performances du système. Dans ce sens, nous avons proposé un algorithme d'anticollision centralisé BACP+. Ainsi cette solution diminue le délai et permet d'activer plus de lecteurs en un tour.

Keywords: système RFID, collision de lecteur, contrôle d'accès au medium RFID

Abstract

Progress in the fields of telecommunications and technology has helped to give substance to a rather old idea: that of remote identification by radiofrequency. Current technologies use passive or active tags, magnetically or radioactively coupled to a reader. Despite the lack of a real standardization, RFID tags are developing very quickly in a wide variety of areas: logistics, identification, access control, protection against theft, payment, etc.

Advances in the field of miniaturization and new materials point to new technological breakthroughs with more and more extensive applications, including an Internet of Things. However, such deployments suffer from a problem of collisions. These greatly reduce the quality of RFID time and energy deployments. There are three types of collisions: tag collisions that are already well defined and standardized, collisions of readers, and collisions between readers and tags.

In addition, this memory deals with reader collisions because with the phenomenon of densification of readers, reader collisions have become more and more frequent and they affect the performance of the system. In this sense we have proposed a centralized anti-collision algorithm BACP +. So this solution decreases the delay and allows to activate more drive in one turn.

Keywords: system, reader collision, medium access control.

Sommaire

2 Table des matières

Liste des figures

Liste des tableaux

Glossaire

MCMAC	Multi-Channel MAC
LBT	listen Befort Talked
DiMCA	Distributed Multi-Channel Collision Avoidance
EDMC	Enhanced Distributed Multi-Channel
EMRCA	Efficient Multichannel Reader Collision Avoidance
NFRA	Neighbor Friendly Reader Anticollision Protocol
GDRA	Geometric Distribution Reader Anti-collision
DRCA	A Distance Based RFID Reader Collision Avoidance
BACP	Called Beacon Analysis-based Collision Prevention
LPWAN	Low Power Wide Area Network
DiCa	Distributed Tag Access avec prevention des collisions
CSMA	Carrier Sense Multiple Access
MALICO	Maximum Likelihood Colorwave
DCNS	Distributed Color Non-cooperative Selection
PDCS	Probability Distributed Color Selection
DCS	*Distributed Color Selection*
IEJ	Indice d'équité de Jain
ACE	Accès Canal Echoué
ACR	Accès Canal Réussi
IEEE	Institute of Electrical and Electronics Engineers
UPC	Universal Product Code

IoT	Internet of Things
EPC	Electronic Product Code
BAP	Battery Assisted Passive
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
kHz	kilohertz
MHz	Mégahertz
GHz	Gigahertz
MAC	Medium Access Control
TDMA	Time Division Multiple Access
FDMA	Frequency Division Multiple Access
SDMA	Space Division Multiple Access
CDMA	Code Division Multiple Access
RTS	Request to Send
CTS	Clear to Send
ACK	acknowledgement
W	Watt
RCT	Reader communication tag
CRT	Reader tag collision
drt	Reader tag distance

Introduction générale

La RFID (Radio Frequency IDentification) ou Identification par Radio-Fréquence est une technologie qui permet l'identification d'un dispositif appelé "tag" par un "lecteur". Généralement, le système RFID s'appuie sur le RFID passive ou le tag passif qui suite à la réception d'un signal radio émis par le lecteur, est alimenté par ce même signal et répond à la requête. Cette technique est appelée la rétromodulation. L'utilisation de cette technique a permis le déploiement des solutions RFID dans plusieurs domaines d'applications tels que la logistique, la sécurité, les transports, etc.

Ainsi, on peut retrouver aujourd'hui des entrepôts avec des tags rattachés à chaque produit stocké afin de suivre les entrées/sorties, la durée de vie, le statut vis-à-vis de la ligne de distribution. Pour assurer la pérennité d'un tel système, il est nécessaire d'installer un grand nombre de lecteurs : certains lecteurs fixes déployés aux différents accès et sur les tapis roulants, mais également des lecteurs mobiles qui seraient confiés aux ouvriers ou directement montés sur les chariots élévateurs qui circulent au sein de l'entrepôt. Un autre exemple pourrait être une ville intelligente avec des tags rattachés aux infrastructures urbaines afin de surveiller leur état (température, humidité, fissures, etc).cela est rendu possible grâce à des lecteurs qui seraient fixés aux différents coins de rue et montés sur les transports en commun.

Cependant, de tels déploiements souffrent d'un problème inhérent à toutes les technologies radios que sont les collisions. Ces dernières réduisent grandement la qualité des déploiements RFID car elles entraînent des erreurs de lecture qui peuvent être coûteuses en délai et en énergie. Ainsi, il existe trois types de collisions. D'abord, les collisions de tags, qui se produisent lorsque plusieurs tags tentent de répondre simultanément à la requête d'un lecteur. Leurs réponses vont donc entrer en collision et le lecteur ne pourra pas donc en décoder les informations. Ensuite, les collisions de lecteurs qui se passent lorsque deux lecteurs voisins ou plus tentent d'activer simultanément les tags se trouvant à leur portée. Enfin, les collisions entre lecteurs et tags qui surviennent lorsque le signal d'activation d'un lecteur a un tag interfère avec le signal de réponse d'un autre tag se trouvant dans la même porte, à un autre lecteur.

Par ailleurs, ce mémoire traite des collisions de lecteurs car avec le phénomène de la densification des lecteurs, les collisions de lecteurs sont devenues de plus en plus fréquentes et affectent les performances du système. C'est dans ce sillage que **Called Beacon Analysis-based Collision Prevention more** (BACP+) est proposé pour offrir de meilleures performances. C'est un

protocole centralisé qui améliore l'un des plus récents protocoles de cette famille le BACP. La solution proposée utilise pleinement les ressources disponibles, canaux de frequence pour assurer une bonne gestion des collisions et du délai de couverture.

Ainsi, dans la suite, nous allons organiser ce document structuré en trois chapitres.

D'abord, dans le chapitre 1 nous allons présenter l'environnement des systèmes de RFID. Ensuite, le chapitre 2 est consacré à l'étude des protocoles MAC, ce qui a permis d'avoir un aperçu des travaux liés à l'accès au médium. Dans le chapitre 3 nous avons posé la problématique des gestions de collisions et du temps de lecture par les protocoles centralisés. Puis nous présenterons notre solution et analyserons ses performances. Enfin nous terminons ce document par une conclusion générale et des perspectives.

Chapitre 1

Présentation de la technologie RFID

RFID est l'acronyme de Radio Fréquence Identification et désigne le principe de reconnaissance d'objets par transmission radiofréquence. Il s'agit d'une méthode d'identification basée sur l'extraction sans fil des données contenues dans des dispositifs appelés RFID tags ou transpondeurs [1]. Un tag RFID est un petit objet qui peut être attaché ou incorporé à un produit, un animal, ou une personne. Ces dispositifs électroniques sont principalement utilisés pour des applications d'identification, d'antivol, et de suivi de production, d'individus, d'animaux, et de chemins. En effet, la Radio-identification ou la RFID est l'annonce d'une mutation radicale dans l'organisation du commerce, du transport, de la sécurité et de la surveillance. L'objectif de ce chapitre est de présenter la technologie RFID. Dans la première section, une présentation du fonctionnement des systèmes RFID est réalisée. Elle aborde les différents composants existants ainsi que les normes des dispositifs RFID. La seconde section aborde les différents types d'identifiants et les domaines d'applications.

1. La technologie RFID

La **RFID** (Radio Frequency Identification), ou radio-identification, est une technologie qui est composé de lecteurs et de tags.

1.1. Historique de la RFID

La RFID est une méthode pour mémoriser et récupérer des données à distance en utilisant des marqueurs appelés « tag ». Par ailleurs, ce système a trouvé sur place des systèmes d'identification comme les codes à barres. Dans la suite, nous allons voir le code à barres ancêtre de la RFID et la base de la RFID.

1.1.1 Identification par code à barres : ancêtre de la RFID

Le code à barres est aujourd'hui la solution d'identification la plus couramment utilisée, elle présente néanmoins des limites par le nombre restreint d'informations véhiculées qui ne peuvent pas être complétées ou modifiées [2]. La technique d'identification par code à barres utilise divers protocoles de codification, qui diffèrent en fonction des contraintes d'utilisation ou de normalisation. Il existe généralement trois types de codes à barres :

- ✓ les codes à barres unidimensionnels ou linéaires ;
- ✓ les codes à barres linéaires empilés ;
- ✓ les codes à barres à deux dimensions.

Le **code-barres linéaire** est celui qui nous est le plus familier. Toutes les informations du code sont organisées horizontalement sous forme de barres et d'espaces de différentes épaisseurs pour une lecture de droite à gauche. Plusieurs versions des codes 1D ne stockent que des données numériques alors que d'autres peuvent coder des caractères supplémentaires. La hauteur du code varie en fonction de la surface disponible sur le produit et de la capacité du lecteur de code-barres à lire un code-barres de petite ou grande taille

Figure 1:Code à barres linéaire

Le **code-barres linéaire empilé** est composée de plusieurs codes-barres linéaires en couches superposées, ce qui permet de coder une plus grande quantité d'informations. Cependant, pour décoder entièrement les données, un lecteur de code-barres doit pouvoir lire le code à la fois horizontalement et verticalement.

Figure 2:Code à barres linéaire empilé

Les **codes à barres à deux dimensions** se caractérisent par le fait qu'ils contiennent des informations à la fois verticalement et horizontalement. Par conséquent les codes à barres 2D contiennent beaucoup plus d'informations qu'un code barre classique à une dimension.

Figure 3:codes à barres à deux dimensions

1.1.2 Code à barres électroniques : base de la RFID

La caractéristique principale des futurs codes à barres est l'utilisation des codes à barres électroniques EPC (Electronic Product Code) qui sont envisagés par plusieurs industries, comme seconde génération (EPC). Ces codes électroniques (EPC) peuvent emporter plus de données, que les UPC (Universal Product code.), et peuvent être reprogrammés avec de nouveaux renseignements si nécessaires. Ils sont caractérisés par une capacité d'informations assez importantes [2], [3]. La figure 4 montre un exemple d'un code à barres électroniques.

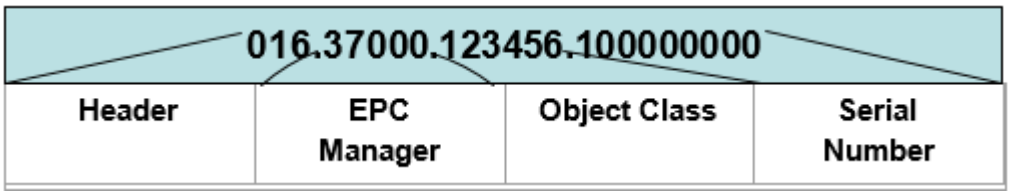


Figure 4 : codes à barres électroniques

- ✓ Header : identifie la version, et la génération d'EPC. Il s'agit d'un en-tête de description de 8 bits.
- ✓ EPC manager : Préfixe identifiant de l'entreprise de 34 bits (code du fabricant).
- ✓ Objet class : Référence produite de 20 bits.
- ✓ Serial number : Numéro de série du produit de 34 bits (unicité du produit).

Ces codes électroniques sont à la base de développement d'autres outils d'identification, à savoir l'identification par radio fréquence. La « radio identification », venant de l'anglais Radio Frequency IDentification (usuellement abrégée RFID), est une méthode pour stocker et récupérer des données à distance en utilisant des marqueurs appelés « radio-étiquettes » (« RFID tag » ou « RFID transpondeur » en anglais). Cette technologie permet un accès non interrompu et facile aux données présentées sur l'étiquette, contrairement au code à barres universels (UPC) où l'identification est limitée par ligne. En se basant sur les ondes radio, la technologie RFID n'exige pas un alignement direct entre les étiquettes et les lecteurs. Ces étiquettes

électroniques sont capables d'emporter un grand nombre de renseignements qui peuvent être effacés, réécrits ou modifiés, et par conséquent elles sont utiles dans la sécurité et l'identification. Ces deux techniques d'identification, du point de vue de leur utilisation pratique, présentent en fait plus de différences que de ressemblances.

1.2. Système RFID

Un système RFID est composé d'un ensemble de dispositifs. Pour son bon fonctionnement ces dispositifs doivent coordonner. Nous allons voir ces dispositifs dans la suite à savoir les composants, l'architecture du système, le principe de fonctionnement, les fréquences et les normes utilisés.

1.2.1.Composition du système RFID

Un système RFID est composé de tags, de lecteurs et d'un système de collecte de données ou ordinateur dans un environnement sans fil. Cependant, il existe plusieurs types de tags avec des caractéristiques différentes.

1.2.1.1. Les tags RFID

Les tags RFID sont des petites puces programmées. Ils comprennent les informations relatives à un produit qui sont entreposées dans une base de données. L'architecture de ses dispositifs RFID est constituée d'un étage de modulation ou de démodulation du signal de la communication. Il est aussi constitué d'un étage de mémorisation des informations transmises par le signal modulant ou des informations stockées localement, et d'une intelligence locale dévolue à un microcontrôleur [4]. En RFID, il existe deux types de tags, les tags passifs et les tags actifs.

1.2.1.1.1. Tags passifs

Ils sont autoalimentés, c'est-à-dire activés par le champ électromagnétique rayonné par le lecteur. Le tag passif utilise généralement l'onde (magnétique ou électromagnétique) issue de l'interrogateur pour alimenter le circuit électronique embarqué. Ainsi nous avons une deuxième forme de tags :

Les *tags passifs assistées par batterie ou* (semi-passifs ou semi-actifs) (BAP: Battery Assisted Passive) : il comporte une alimentation embarquée (piles, batteries...) et fonctionne comme les actifs. L'énergie des tags passifs assistés n'est pas utilisée pour alimenter un émetteur puisque le principe de communication reste la rétromodulation (comme pour le tag passif). Mais, elle est plutôt utilisée pour alimenter le circuit électronique du tag ou tous autres circuits ou capteur connecté au circuit de base. Cette alimentation permet, en théorie, d'améliorer les performances. Ce tag est

largement utilisé pour des applications nécessitant une capture d'information (température, choc, lumière, etc.) indépendante de la présence d'un interrogateur. La figure 5 montre l'architecture de base d'un tag passif.

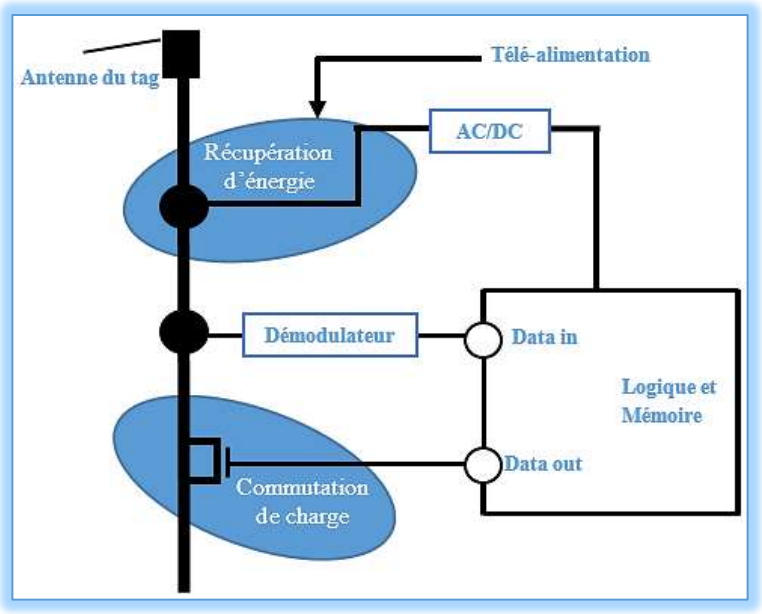


Figure 5: Architecture de base d'un tag passif

Mémoire : elle contient les informations sur le produit stocké dans la base de données.

Antenne : elle est utilisée pour transmettre le signal.

Démodulation : permet de recevoir les messages numériques.

Télé-alimentation : permet de récupérer l'énergie des ondes émises par le lecteur.

a. Domaine d'utilisations des tags passifs

Les tags passifs connaissent des domaines d'application très divers, prenons ces quelques exemples :

- ✓ l'identification d'animaux ;
- ✓ la traçabilité des déchets ;
- ✓ le suivi des colis postaux ;
- ✓ chaîne d'approvisionnement ;
- ✓ la gestion des stocks ; etc.

b. Avantages et inconvénients des tags passifs

L'avantage du tag passif par rapport au tag actif repose sur le coût qui est moins onéreux que les tags actifs. Ce système s'avère très utile pour les marchandises en volume important lorsque les marchandises peuvent être lues à courte distance (passage à la caisse des supermarchés).
Par contre, la distance de lecture est un réel frein à ce système puisque le lecteur doit se situer dans le champ du tag afin d'en récupérer les données.

1.2.1.1.2. Tags actifs

Ils sont activés par une pile interne, et transmettent les données aux lecteurs localisés. Les étiquettes actives sont équipées d'une batterie leur permettant d'émettre un signal. De ce fait, ils peuvent être lus depuis de longues distances (100 m environ), contrairement aux marqueurs passifs. En général, les transpondeurs actifs ont une plus grande capacité mémoire pour stocker diverses types d'information telles que le connaissement (128 Kb et plus). Ils sont principalement utilisés dans des applications de télémétrie, pour communiquer un grand nombre d'informations sur de grandes distances. La figure 6, nous montre l'architecture interne d'un tag actif.

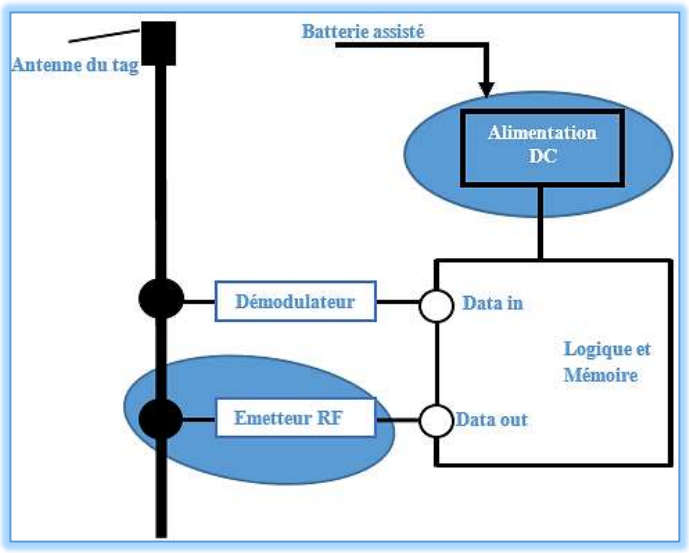


Figure 6: Architecture de base d'un tag actif

La différence des tags actifs avec les tags passifs est l'intégration de l'alimentation et de l'émetteur RF qui lui permettent respectivement de s'alimenter en énergie et d'émettre des ondes au lecteur.

a. Domaine d'utilisation des tags actifs

Les applications avec les Tags actifs offrent un avantage sur la portée de lecture qui est beaucoup plus longue que celle des tags passifs.

Exemples :

- ✓ l'identification et le suivi des personnes : le Tag actif permet de localiser en temps réel et à distance des personnes, des véhicules. C'est le cas pour les contrôles d'accès dans les parkings, la traçabilité des soins pour le suivi des patients dans les hôpitaux ;
- ✓ le suivi de flotte de véhicules, etc. ;
- ✓ la traçabilité des produits à savoir inventaire, suivi et identification d'objets en tout genre, gestion de véhicule sur parc, antivol... ;
- ✓ la traçabilité logistique : contrôle de la chaîne du froid, suivi des véhicules, etc.

b. Avantages et inconvénients des tags actifs

Contrairement au système tags passives, les tags actifs sont équipés d'une énergie propre qui leur permet d'émettre un signal de manière autonome.

De ce fait, le principal avantage repose sur la longue distance à laquelle elles peuvent communiquer les données sans qu'un lecteur RFID se situe à proximité du tag.

L'inconvénient principal du Tag actif repose sur :

- ✓ la confidentialité des informations transmises ;
- ✓ le coût des tags ;
- ✓ l'impact sur la santé très controversée due à l'émission d'ondes magnétiques ;
- ✓ la durée de fonctionnement limité des tags.

Ainsi, un tag actif est généralement plus grand et caractérisé par une portée de transmissions plus importante, mais sa durée de vie est limitée par la durée de vie des batteries. Un tag passif est plus petit, il peut avoir une durée de vie illimitée, et il est caractérisé par une faible portée, due aux propriétés du milieu de transmission et aux limites des sources d'activation [3].

Par contre, une des différences notées entre ces deux types de tags (actifs et passifs) repose sur l'alimentation de la batterie : elle alimente la puce RFID non pas en continu, mais à des intervalles de temps réguliers et programmables et n'envoie aucun signal. Le tableau 1 présente les différentes caractéristiques des tags actifs et passifs.

Caractéristique	Tag passif	Tag actif
Taille petite	Oui	Non
Durée de vie fonctionnelle importante	Oui	Non
Portée important	Non	Oui
L'information peut être effacée, réécrite ou modifiée.	Non	Oui
Coût faible	Oui	Non

Tableau 1 : caractéristique des tags

Le choix d'un tag dépend du type d'application envisagée.

1.2.1.2. Les lecteurs RFID

Un lecteur avec une antenne communique avec le tag pour envoyer et recevoir de l'information. Le lecteur est généralement constitué par une partie analogique regroupant :

- ✓ un *oscillateur local* accordé sur la fréquence du signal ;
- ✓ un *modulateur démodulateur* qui permet de transmettre ou de recevoir les messages numériques ;
- ✓ un *amplificateur* de puissance qui est adapté à l'antenne d'émission/réception ;
- ✓ Aussi le lecteur RFID est formé d'une partie numérique composée :
  - ✓ d'un *microcontrôleur* qui permet la gestion des protocoles de communication, des collisions, du cryptage et du décryptage des informations;
  - ✓ des *interfaces de communication* et une mémoire locale.

Le schéma général d'une chaîne de réception dans le cas d'un système de réception RFID est représenté à la figure 7 : [4]

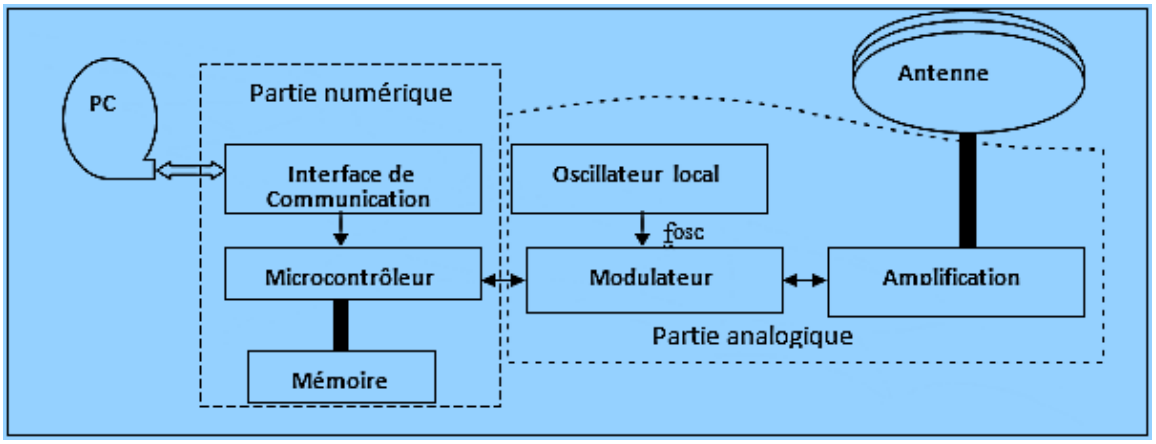


Figure 7: Architecture de base d'un lecteur RFID [8]

Dans le milieu aérien, la communication entre le tag et le lecteur s'effectue par couplage électromagnétique entre les antennes. Un lecteur RFID est un émetteur/récepteur conçu pour communiquer par ondes électromagnétiques avec le tag RFID correspondant. L'énergie contenue dans les ondes radio émises par le lecteur est captée par l'antenne du tag qui entre en communication avec le lecteur en lui transmettant les informations qu'elle contient. La portée de transmission d'un lecteur RFID est déterminée par la puissance et la fréquence émise. Ces lecteurs opèrent généralement avec des bandes de fréquences (voir section 1.2.3.2) [3] [5]. Un lecteur RFID exécute une variété de fonctions. Il permet :

- ✓ d'activer les puces passives en envoyant les signaux nécessaires ;
- ✓ le codage et le décodage de l'information nécessaire.

Historiquement, les lecteurs RFID sont destinés à lire les données d'un seul type du tag, mais aujourd'hui les lecteurs existant sur le marché sont appelés des lecteurs multimodes qui peuvent lire différents types de données.

1.2.1.3. Unité de collection et de gestion d'information

Cette unité représente le troisième composant d'un système RFID, elle est formée par des équipements informatiques et des logiciels de gestion qui convertissent multiples entrées en données d'identification. Cette unité enregistre et traite les renseignements du tag avec des logiciels spécifiques. La technologie RFID a la particularité de fonctionner à distance sur le principe suivant. Un lecteur émet un signal radio et reçoit en retour les réponses des tags qui se trouvent dans son champ d'action.

1.2.2. Architecture et communication des systèmes RFID

Les systèmes RFID offrent la possibilité d'identifier des personnes ou des biens sans contact ni vision directe. Le fonctionnement de ces systèmes dit RFID est basé sur l'émission de champs électromagnétiques réceptionnés par une antenne couplée à une puce électronique. [2]

1.2.2.1. Architecture du système RFID

Cette figure 8 illustre l'échange entre des composants. Un système complet RFID est composé des éléments suivants :

- ✓ un lecteur RFID ou interrogateur, doté d'antennes et capable de lire et écrire des informations par transmission radio ;

- ✓ un tag RFID, ou étiquète, qui contient les données de l'élément à identifier ;
- ✓ une antenne utilisée pour transmettre le signal (ondes radiofréquences) entre le lecteur et le transpondeur ;
- ✓ une application/serveur (qui prend la forme d'un ordinateur) de stockage et de traitement des informations recueillies par le lecteur. La figure 8 montre l'architecture d'un système RFID.

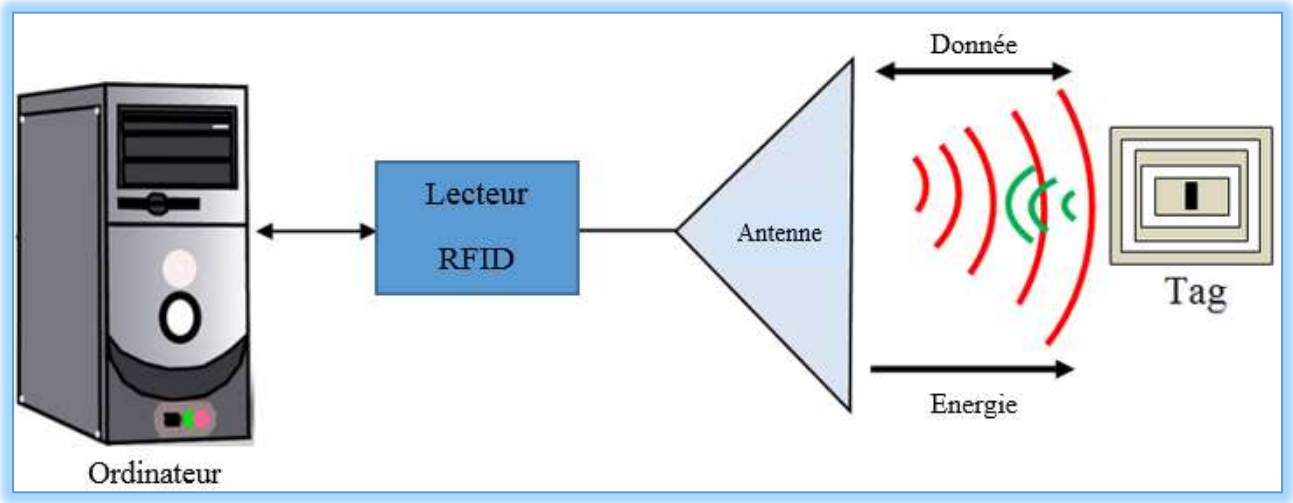


Figure 8 : Architecture du système RFID

1.2.2.2. Architecture en couche du système RFID

Les anciens systèmes n'étaient pas distribués, c'est-à-dire que les données étaient récupérées par une seule application. Mais avec la croissance des besoins des entreprises, il est devenu vital de partager les données de celles-ci avec leurs partenaires et notamment leurs fournisseurs. Afin de répondre à ce nouveau besoin, l'architecture des systèmes RFID a été revue pour y inclure un nouveau composant logiciel ; un middleware ou intergiciel RFID qui exploite l'architecture distribuée de cette technologie et qui permet la coopération entre applications hétérogènes. La figure 9 nous montre la composition en couches de la nouvelle architecture.

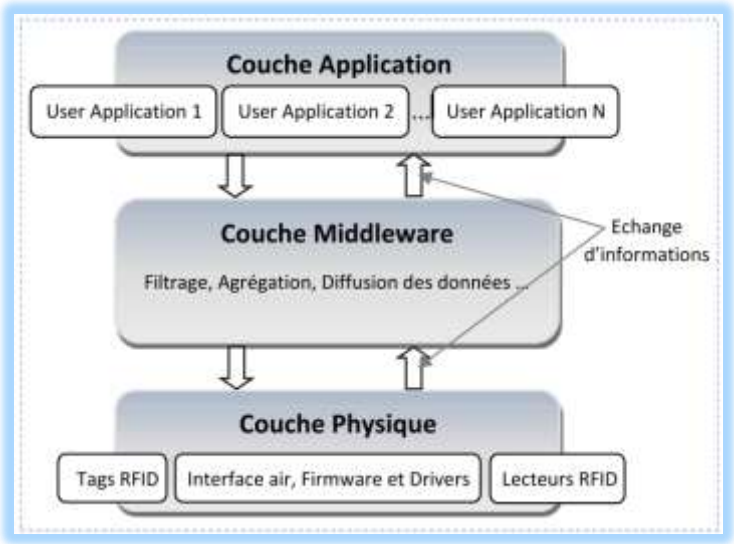


Figure 9:Architecture en couches d'un système RFID

1.2.2.3. Communications dans le système RFID

Dans un système RFID les lecteurs et les tags doivent collaborer pour le bon fonctionnement du système. Alors, cela nécessite une communication entre ces dispositifs. Ainsi nous allons voir les types de communication possibles dans le système RFID, le mode de communication et le model de communication dans le système RFID.

1.2.2.3.1. Type de communication

Lors de l'échange entre lecteur et tag dans le cas de l'utilisation «tags passifs, télé-alimentés», il ne peut y'avoir de communication sans télé-alimentation du tag, donc sans présence initiale de porteuse radiofréquence. Le lecteur doit donc toujours initier la communication en émettant sa porteuse. Dans ce cas, les deux théories peuvent se produire concernant le déclenchement réel de la communication proprement dite.

a. Tag Talks First (TTF) ET Answer To Reset (ATR)

Dès qu'un tag entre dans le champ d'un lecteur et qu'il est réveillé, après avoir effectué son reset interne, il commence immédiatement à communiquer pour signaler sa présence, le lecteur envoi une invitation au dialogue appelé requête, et le tag (TTF) effectue alors une réponse à cette requête. Ce type de déclenchement (TTF) fonctionne très bien si l'on est sûr qu'il n'y aura jamais plus d'un tag à la fois dans la zone d'influence, sinon il y'aura des conflits potentiels de signaux en provenance des nombreux tags.

b. Reader (Interrogators) Talks First (RTF Ou ITF) et Answer To reQuest (ATQ)

Lors de leurs entrées dans la zone d'influence du lecteur, les tags étant (téléalimentés effectuent alors leurs resets internes et passent sans plus attendre dans un état logique particulier (souvent baptisé Ready) dans lequel ils doivent attendre une commande de requête, pour répondre à celle-ci et lui signifier leurs présences, d'où les noms de Reader Talks First (RTF) ou encore Talk After reQuest. Sur le principe, comparativement aux tags TTF, les tags RTF comportent à leurs bords une circuiterie logique supplémentaire leur permettant d'interpréter la commande de requête, son coût légèrement supérieur aux TTF.

c. Coexistence TTF et RTF

Un grand problème consiste à savoir quels peuvent être les problèmes de coexistence susceptibles de survenir lors de la présence simultanée dans le champ électromagnétique de tags de types RTF et TTF, par exemple lorsque le lecteur a déjà commencé de communiquer volontairement avec un tag RTF et qu'un tag de type TTF rentre soudainement dans le champ et commence à signaler sa présence. L'usage des tags TTF devrait alors être limité à des applications dans lesquelles on est sûr qu'ils ne quitteront jamais leur site d'utilisation pour ne pas polluer d'autres sites dans lesquels des RTF pourraient être présents. Afin d'éviter tous ces problèmes, certains pays (en Extrême Orient par exemple) n'admettent pas l'usage de tag de type Tag Talk First (TTF) et pour éviter tous ces soucis, l'ISO n'a normalisé que des cartes à puces sans contact (ISO14443 et 15693) et des tags (famille de normes ISO18000-x) pour la gestion automatique d'articles (Item management) uniquement de types RTF ou ITF.

1.2.2.3.2. Mode de communication

Maintenant que nous savons qui peut déclencher/commencer l'échange, passons à la suite de la structure de celui-ci.

a. Half duplex

Le mode dit half duplex (souvent noté HDX) correspond à un mode « alterné » de communication dans lequel les liaisons de données montantes et descendantes ne sont pas simultanées, et par conséquent dans lequel les messages montants et descendants ne peuvent, par principe, pas se télescoper.

b. Full duplex

Dans ce mode de fonctionnement dit full duplex (souvent noté FDX), les échanges de données lors des liaisons montantes et descendantes s'effectuent simultanément. L'avantage de ce mode d'échange est d'obtenir des temps de transactions plus rapides pour permettre de satisfaire certaines applications au détriment de la complexité électronique du lecteur devant traiter en temps réel simultanément les protocoles de communications montants et descendants ainsi que les erreurs de transmissions toujours possibles.

c. Interlaced half duplex

Ce mode est un dérivé de celui décrit au paragraphe précédent. Dans ce cas, il s'agit de transmissions effectuées en mode full duplex au niveau du lecteur (elle est donc capable d'émettre et de recevoir en même temps) et seulement en mode half duplex au niveau du tag. Ainsi, Dans les dispositifs RFID mise en place à ce jour, le mode d'échange de données le plus couramment employé (pour ne pas dire à 100 %, disons à 95 %) est le mode half duplex. Ce qui signifie que le lecteur et le(s) tag(s) communiquent entre eux alternativement, par tranches de temps, et non simultanément tel que ce serait le cas en mode dit full duplex .Il est à noter que certains types de codages bit et/ou types de modulations de fréquences porteuses et/ou leurs combinaisons permettent ou non d'envisager de communiquer selon le mode full duplex.

1.2.2.3.3. Modèle de communication

La communication du tag vers le lecteur repose sur la technique de rétromodulation. Le signal radio issu du lecteur est alors partiellement réfléchi par le tag RFID. Quels que soient les fréquences ou les modes de couplage, le moyen utilisé pour réaliser cette rétromodulation, consiste à commuter une charge (impédance) placée en parallèle entre l'antenne du lecteur et l'antenne du tag. IL est bien entendu que ce système de commutation de charge fait partie intégrante du tag. Le signal réfléchi par le tag vient alors se superposer au signal provenant du lecteur. Les tags passifs ne possédant pas de source d'énergie embarquée, le rapport entre la puissance du signal émis par lecteur (pour alimenter la puce et transmettre les commandes) et la puissance du signal rétro modulé par le tag peut largement dépasser les 60 dB. Le lecteur doit donc présenter une bonne sensibilité pour détecter et décoder l'information issue du tag. La difficulté de ces systèmes consiste donc à trouver la meilleure charge permettant de créer de fortes variations de signal réfléchi sans pour autant pénaliser l'alimentation du circuit lui-même.

1.2.2.3.4. Modes de transfert d'énergie et de communication

L'échange de l'énergie entre le lecteur et le tag se fait par deux façons.

a. Non simultanée, énergie et communication en deux temps

Dans ce premier cas, l'onde RF se propageant du RFID vers le tag n'a pour but unique que de fournir de l'énergie au tag de façon à charger la « capacité d'alimentation » présente à son bord afin que celle-ci puisse être capable d'alimenter le circuit interne du tag pour assurer son bon fonctionnement. Après cette phase d'alimentation, le tag est apte à recevoir des ordres de commande provenant du lecteur et de retourner des informations vers celle-ci. Puis le cycle recommence et il est à nouveau nécessaire de lui fournir de l'énergie pour continuer la communication et ainsi de suite. Bien évidemment, ceci prend du temps et manque parfois de souplesse.

b. Simultanée, énergie et communication lors de l'échange

Dans ce deuxième cas, au travers des principes et types de modulation utilisés, l'onde provenant du lecteur est capable pendant la phase de l'échange du lecteur vers le tag, d'assurer simultanément la fourniture de l'énergie et l'échange des informations (données).

Figure 10:mode de transfert d'énergie non simultané

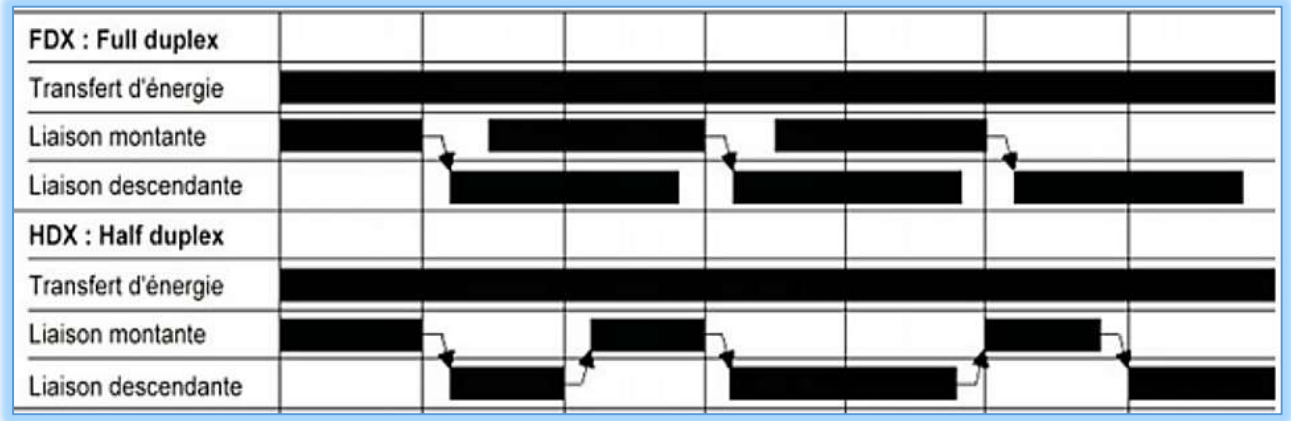


Figure 11:mode de transfert d'égérie simultanée

1.2.3. Principe physique, bande de fréquences et normes RFID

1.2.3.1. Principe physique de fonctionnement

Les systèmes RFID à couplage magnétique mettent en œuvre généralement des tags passifs. L'élément qui assure la communication du tag avec le lecteur est une bobine constituée de plusieurs spires métalliques. Elle permet de produire de l'énergie nécessaire à l'alimentation de l'électronique embarquée dans la puce en exploitant les phénomènes d'induction créés par le champ magnétique émis par le lecteur (figure 12).

Cette technique va introduire un certain nombre de contraintes, essentiellement une distance de communication réduite (typiquement de 0 à 1,5 m). Cela est dû à la nature même de l'émission du champ magnétique en ligne proche du lecteur (moins d'un mètre) et à la génération d'interférences pour d'autres systèmes à proximité du lecteur.

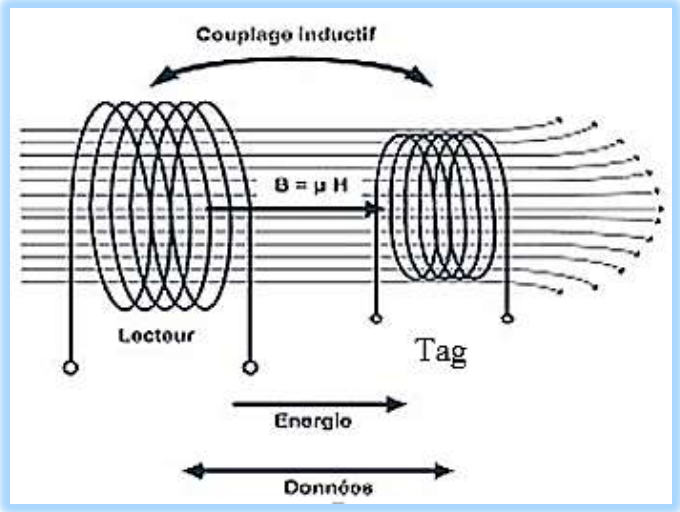


Figure 12:Schéma du principe de couplage magnétique en champ proche [3]

Le mode de fonctionnement en couplage magnétique concerne les systèmes qui fonctionnent en basse fréquence et en moyenne fréquence. Les fréquences UHF et SHF, qui correspondent à des longueurs d'onde allant du mètre au centimètre, ne peuvent pas être utilisés en champ proche. Elles fonctionnent par contre grâce à un couplage radiatif.

Contrairement aux modules de couplage magnétique, les systèmes basés sur un couplage radiatif ne sont pas limités par l'émission localisée autour du lecteur des lignes de champ. En utilisant les propriétés propagatrices du champ électrique rayonné par une antenne, c'est possible de transporter de l'énergie et des données d'un lecteur vers un tag et inversement sur plus d'une dizaine de mètres.

Les dimensions des antennes capables de produire de tels champs électriques sont de l'ordre de la demi-longueur d'onde (pour une fréquence de 100 MHz, l'antenne devra mesurer environ 1,50 m).

Dans le cas des tags passifs, l'énergie d'alimentation est créée par l'exploitation du phénomène du dipôle d'Hertz produit par le champ électrique émis par le lecteur. La densité d'énergie du signal rayonné décroît en fonction de l'inverse du carré de la distance séparant le lecteur du tag. De ce fait, l'utilisation des systèmes passifs se limite à des distances qui ne dépassent pas une dizaine de mètres pour des fréquences aux alentours de 500 MHz. Au-delà de ces fréquences, les transpondeurs nécessitent une alimentation en énergie et deviennent actifs. Un avantage majeur des tags à couplage radiatif réside certainement dans son faible coût.

1.2.3.2. Bande de fréquence

La RFID s'est vue attribuer un certain nombre de fréquences classées en trois groupes [5] :

Basses fréquences (LH) : 100 à 500 kHz avec une distance de lecture de quelques centimètres ; fréquences particulièrement utilisées en milieux industriels ainsi que pour le suivi animalier.
Elles permettent une lecture en tout milieu, mais à courte distance (quelques décimètres au maximum).

Moyennes fréquences (HF) : 10 à 15 MHz avec une distance de lecture de 50 à 80 cm ; ce sont des fréquences particulièrement utilisées en suivi de flux logistiques des bibliothèques et un contrôle d'accès. Ces fréquences permettent une lecture à moyenne distance.

Haute fréquence (UHF): de 850 - 950 MHz à 2,4 - 5,8 GHz pour une distance de lecture de plusieurs mètres (sachant que la distance peut être réduite par la présence du métal). Ces fréquences conviendront particulièrement au suivi des flux logistiques. Ces fréquences récemment disponibles sont porteuses d'espoir pour atteindre des distances étendues de l'ordre de quelques mètres. Mais, elles sont beaucoup plus sensibles en présences des métaux ou des liquides. Pour récapituler, le tableau 2 regroupe les principales fréquences utilisées selon les bandes du spectre radiofréquence.

Classification dans le spectre des fréquences	Fréquences les plus utilisées	Type de couplage	Type Tags
LF	125 et 134,2 kHz	Inductif	Passive
HF	13,56 MHz	Inductif	Passive
UHF	868 MHz (Europe) et 915 MHz (USA)	Inductif	Passive ou active
UHF	2,45 GHz	Radiatif	Active
SHF	5,8 et 5,9 GHz	Radiatif	Active

Tableau 2: principales fréquences utilisées en RFID

1.2.3.3. Norme des systèmes RFID

La normalisation des protocoles de communication entre tag et lecteurs s'inscrit dans le cadre d'un comité technique commun à l'ISO (International Organization for Standardization) et à l'IEC (international Electrotechnical Commission). Les normes relatives aux protocoles de communication (air-interface) ont pour désignation [6] :

- ✓ ***ISO 18000-1 :*** le vocabulaire.
- ✓ ***ISO 18000-2 :*** pour des fréquences de communication inférieures à 135 kHz.
- ✓ ***ISO 18000-3 :*** pour une fréquence de fonctionnement à 13,56 MHz.
- ✓ ***ISO 18000-4 :*** pour une fréquence de 2,45 GHz.
- ✓ ***ISO 18000-6 :*** pour des fréquences comprises entre 860 et 930 MHz.
- ✓ ***ISO 18000-7 :*** pour un fonctionnement en 433 MHz.

Des propriétés physiques sont associées à chaque bande de fréquence utilisée. Elles divisent immédiatement les modes d'interaction entre le lecteur et le tag en deux types [3] [6] : interaction magnétique et interaction radiative.

1.2.4.Pile de protocoles du système RFID

Une pile de protocoles est une mise en œuvre particulière d'un ensemble de protocoles de communication réseau. L'intitulé « pile » implique que chaque couche de protocole s'appuie sur celles qui sont en dessous afin d'y apporter un supplément de fonctionnalité. Dans la communication des lecteurs et des tags des protocoles interviennent de part et d'autres. Le lecteur après lecture des données du tag, remontes ces données à travers une passerelle(Gateway) suivant des protocoles de

lecteur intégrés de part et d'autre du lecteur et du Gateway. Ainsi l'ordinateur peut récupérer ces données à travers le Gateway. La figure 13 montre la démarche.

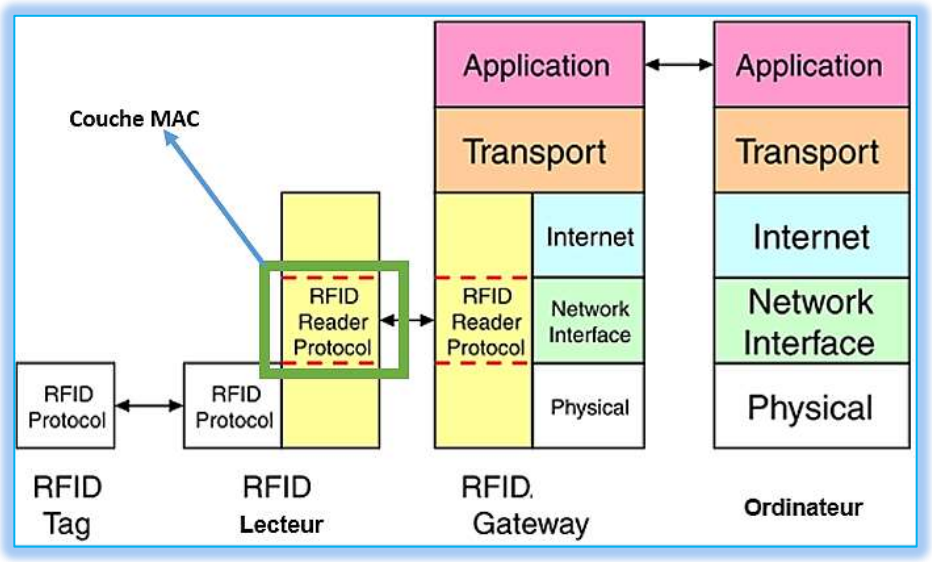


Figure 13: pile protocolaire du système RFID

Figure 14:domaine commercial

Dans le domaine commercial, le système RFID permet aux fabricants et aux fournisseurs de diriger, de distribuer efficacement leurs produits et de contrôler la sécurité, l'identification des délais potentiels et des carences. Ainsi, la technologie RFID permet aux autorités de vérifier la sécurité et la certification d'articles transportés.

Figure 15:domaine militaire

Dans le domaine militaire, la technologie RFID permet d'identifier les appareils. En effet, les militaires ont besoin d'identifier à longue distance les appareils de guerre. La technologie RFID a été fortement utilisée durant la guerre en Irak pour distinguer par radar les avions.

Figure 16:domaine industriel

Dans le domaine industriel, un système RFID sert à relever les données des capteurs et à contrôler les équipements industriels. Il permet également un suivi des produits dans une usine, le stockage et l'achat. En effet, il y a quelque temps, les entreprises testaient le suivi de leurs employés grâce à une puce RFID glissée sous la peau.

1.2.5. Application de la RFID

Les systèmes RFID sont utilisés, depuis plusieurs années, dans des applications relativement classiques comme les systèmes d'antivol dans les magasins. Récemment, les évolutions technologiques ont favorisé leur apparition dans des domaines moins classiques ; ce qui soulève d'importantes questions relatives au respect de la vie privée, de la protection des données et des libertés individuelles.

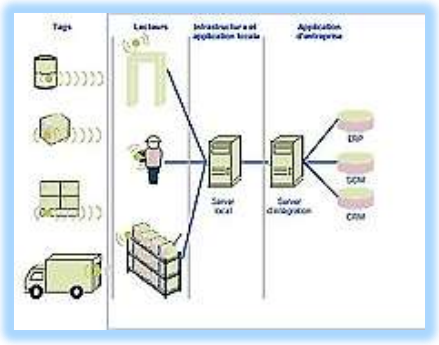


Figure 17:domaine sécurité

Dans le domaine de la traçabilité, la sécurité alimentaire constitue une préoccupation de plus en plus aiguë. Vache folle, grippe aviaire, salmonellose : l'émergence régulière de nouvelles urgences sanitaires.

Traitements chimiques, organismes génétiquement modifiés, produits « bio » : le consommateur se soucie de plus en plus de l'origine du contenu de son assiette, ainsi de ce qu'il a pu subir avant d'y arriver. L'utilisation de la technologie RFID s'étend progressivement à tous les domaines où le souci de traçabilité prend une importance particulière : produits toxiques, industrie pharmaceutique, etc.

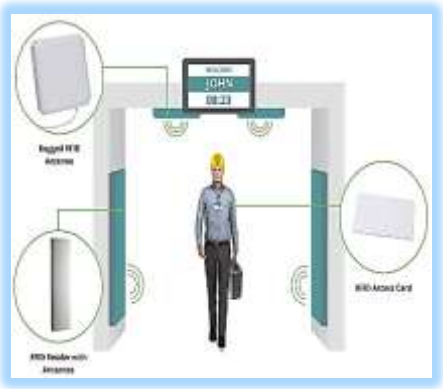


Figure 18:domaine d'accès

Dans le domaine de la sécurité, le contrôle d'accès est l'une des applications les plus connues de la technologie RFID : avec la RFID il n'y a pas besoin d'utiliser des clefs ou des cartes magnétiques. Il suffit de passer une carte d'accès devant un lecteur et la porte s'ouvre ou ne s'ouvre pas en fonction des droits dont dispose le porteur.

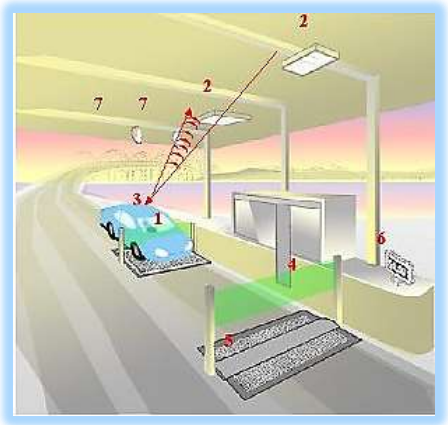


Figure 19:domaine péages

La RFID permet un paiement rapide des péages et une identification rapide des articles. Par exemple, pour le péage au Sénégal, les automobilistes peuvent disposer de la carte **rapido** (tag RFID passive) et à l'approche des barrières, un lecteur RFID est fixé au-dessus de ces barrières pour lire les informations de la carte et la barrière s'ouvre rapidement.

Figure 20:puce sous cutanée

Il est techniquement possible que l'on injecte à chaque nouveau-né une puce, qui pourrait alors fonctionner pour identifier la personne pour le reste de sa vie. De tels plans sont discutés en secret aux États-Unis sans aucune diffusion publique concernant les problèmes liés à la vie privée.

Dans la même lancée, en Suède, le Premier ministre Olof Palme donna la permission en 1973 d'implanter des puces RFID aux prisonniers. L'ex-directeur général Jan Freese révéla que des patients dans les maisons de retrait avaient subi des implantations vers le milieu des années 80.

Figure 21:exemple d'application RFID

Conclusion

La technologie RFID permet de lire des informations sans contact avec l'objet, de mettre à jour l'information contenue, de supporter des températures importantes, d'assurer une lecture de masse et tout ce dont le code-barres est incapable de faire.

Pour l'avenir de cette technologie et selon les spécialistes, la technologie a suscité un engouement important de la part des précurseurs, elle n'a pas encore atteint la maturité.

Ce chapitre a permis d'avoir une idée sur cette technologie, qui présente le système d'identification ; ainsi nous allons voir les protocoles d'anticollision dans le système RFID.

Chapitre 2

Etat de l'art des protocoles d'anticollision de lecteurs RFID

Dans ce chapitre, nous allons parler des spécificités des protocoles MAC pour le système RFID, leur contexte, leur description, leurs scénarios, leurs avantages et leurs inconvénients. Enfin, nous ferons une comparaison des protocoles par famille.

Le développement rapide de la technologie RFID (Radio Frequency ID) a permis sa grande adoption et conduit à des déploiements croissants de solutions RFID dans divers environnements, sous différents scénarios et contraintes. La nature de ces contraintes varie du montant à la mobilité des lecteurs déployés, qui à leur tour affectent fortement la qualité du système RFID, causant des collisions entre les lecteurs ou entre les lecteurs et les tags. Bien que plusieurs solutions soient proposées pour engager la question de ces collisions, peu de ces solutions ont traité la densification et/ou la mobilité des lecteurs.

Par ailleurs, comme tout système de communication sans fil, le système RFID nécessite l'utilisation des protocoles de contrôle d'accès au médium (MAC) pour éviter ses collisions qui gaspillent les ressources (mémoire et énergie) du réseau et ralentissent la procédure de lecture.
Ainsi pour la suite, nous allons d'abord voir la problématique des systèmes RFID. Dans cette partie, nous allons montrer le contexte de création des systèmes RFID et les différents types de collisions. Enfin, nous allons faire l'état de l'art des protocoles Mac utilisés dans systèmes RFID classés par famille.

2. Délimitations des zones et types de collisions

La communication radio, gérée par un protocole MAC rencontre souvent des problèmes de collision. Ainsi, il existe trois types que nous verrons par la suite.

2.1. Délimitation des zones

Pour comprendre les différents types de collisions dans la section suivante, nous allons faire une brève explication de différentes zones : zone de lecture, zone de couverture et zone d'interférence.

- ✓ Une zone de lecture est une zone dans laquelle le signal émis par les tags peut atteindre le lecteur.
- ✓ Une zone de couverture est une zone décrite par la portée du signe d'un lecteur.
- ✓ La zone d'interférence est la zone dans laquelle il y'a chevauchement de deux ou de plusieurs zone de lecture ou de couverture.

Ces différentes zones sont représentées dans la figure 22 ci-dessous. Dans cette figure il y'a deux tags et un lecteur. La zone d'émission du lecteur peut atteindre la portée DC. Ainsi, le tag 1 et le tag 2 peuvent recevoir le signal provenant de ce lecteur car ils se trouvent dans la zone de couverture de ce dernier. Par ailleurs, dans la zone de lecture de distance DL, il y'a que le signal du tag 1 qui peut atteindre le lecteur. Le signal de tag 2 ne peut pas atteindre le lecteur.

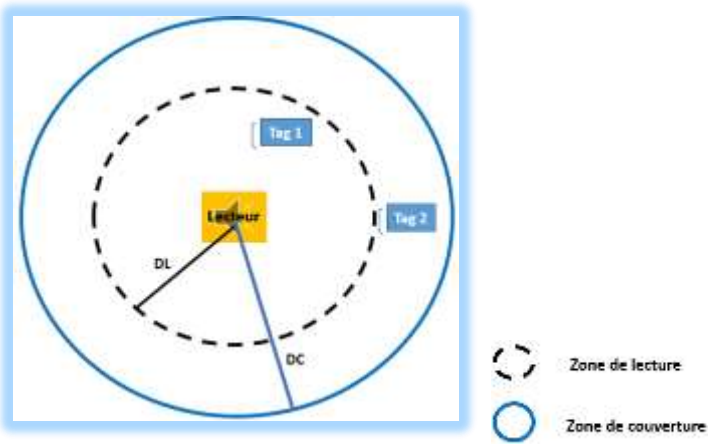


Figure 22:délimitation des zones

2.2. Type de collisions

Le système RFID rencontre des problèmes de collision de lecteurs ou de tags. Ces problèmes sont beaucoup plus fréquents dans un environnement dense (déploiement de plusieurs lecteurs dans une zone restreinte). Ainsi il existe trois types de collision à savoir les collisions entre tags et tag, les collisions entre lecteur et lecteur et les collisions entre lecteur et tag [13] [14] [15].

2.2.1.Collision entre tag et tag

Dans cette partie nous avons deux scénarios possibles. Les tags peuvent être soit actifs, soit passifs. Dans le premier cas nous allons voir comment les tags passifs peuvent engendrer des collisions. Ensuite nous allons montrer comment les tags actifs peuvent eux aussi engendrer de collisions.

✓ Les tags passifs :

Pour initialiser la communication entre le lecteur et le tag :

- ✓ le lecteur transmet par onde radio l'énergie nécessaire à l'activation des tag1, tag2, tag3 et tag4 (voir figure 23 ci-dessous).
- ✓ il lance alors une requête interrogeant les tag1, tag2, tag3 et tag4 à proximité.
- ✓ et simultanément si les tag1, tag2, tag3 et tag4 remontent leurs informations en même temps, alors il y'aura collision au niveau du lecteur, car ce dernier aura du mal à décoder l'information transmise par chaque tag au même moment [13].

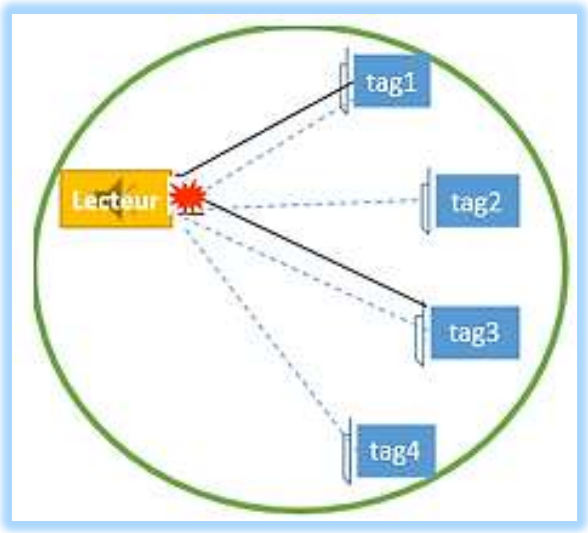


Figure 23:collision entre tags passifs

✓ Les tags actifs:

Les tags actifs n'ont pas besoin d'être activer par un lecteur. Donc, ils peuvent émettre à chaque fois qu'ils ont des données à remonter au lecteur.

À côté des collisions entre tag et tag, nous constatons les collisions entre lecteur et tag dans le processus de communication.

2.2.2.Collision entre lecteur-tag

Pour illustrer le problème de collision de lecteur et tag, il est essentiel de différencier les zones comme indiqué sur la figure 24. Cette figure contient deux lecteurs, le lecteur 1 et le lecteur 2, et des tags. La collision entre lecteurs-tag se produit lorsque le lecteur 1 tente de lire les données de du tag1 en utilisant la fréquence f1 et le lecteur 2 tente de lire les données de tag 2 avec cette même fréquence f1 au même moment. Par exemple sur la figure 24, le signal du lecteur 2 pour lire le tag 2 interférera avec le signal de réponse du tag 1 au lecteur 1 [12,13, 15]. Ainsi, une collision sera enregistrée au niveau lecteur L1 car L1 se trouve dans la zone de couverture du lecteur 2 donc reçoit le signe provenant de L1.

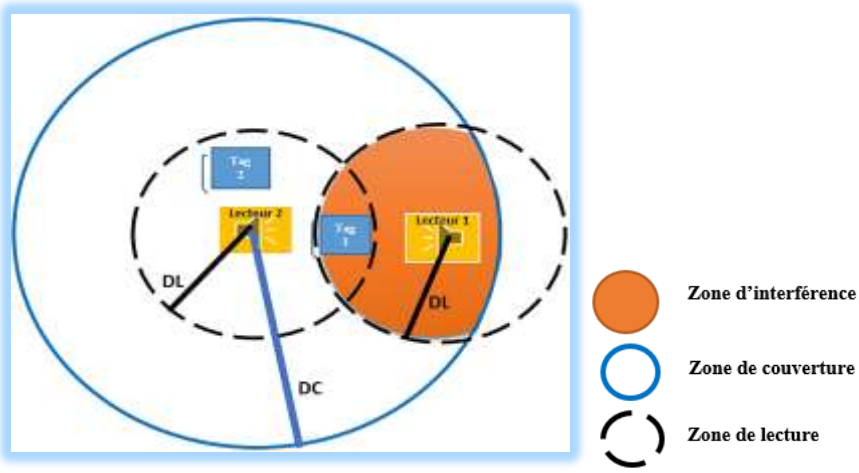


Figure 24:Collision entre lecteur-tag

La figure 25 montre le scénario de collision entre lecteur et tag.

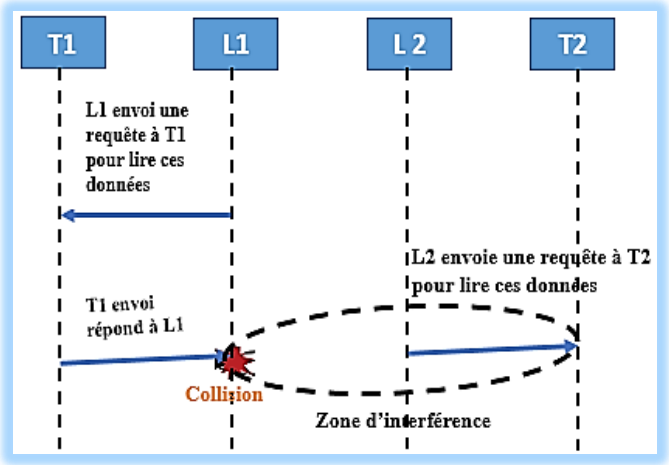


Figure 25:séquence de collision entre lecteur-tag

En plus des collions entre lecteur-tag et celle entre tags-tag, nous notons également les collisions entre lecteur-lecteur.

2.2.3.Collision entre lecteurs-lecteur

Les collisions entre lecteur et lecteur peuvent se présenter en deux types.

- ✓ **Le premier type de collision lecteur-lecteur** est montré sur la figure 26 et se produit lorsque le lecteur 1 et le lecteur 2 tentent de communiquer avec le tag simultanément. Le tag T1 ne peut pas entrer en communication avec ces deux lecteurs au même moment, par conséquent le tag ne sera pas en mesure de répondre [12, 13, 15].
- ✓ **Le deuxième type de collision lecteur-lecteur** est représenté sur la figure 28 et se produit lorsque le lecteur 1 et le lecteur 2 tentent simultanément de communiquer respectivement avec

le tag1 et le tag 2 en utilisant la même fréquence f1. Puisque le tag1 est dans la zone d'interférence du lecteur 2 et la zone de couverture du lecteur 1. les signaux de communication du lecteur 1 et celui de la lecture 2 atteindront T1 entrainant une collision au niveau du tag.

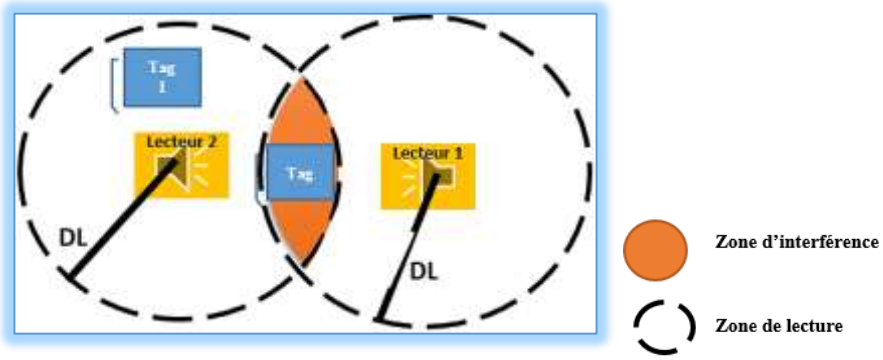


Figure 26:Collision entre lecteurs-lecteurs (a)

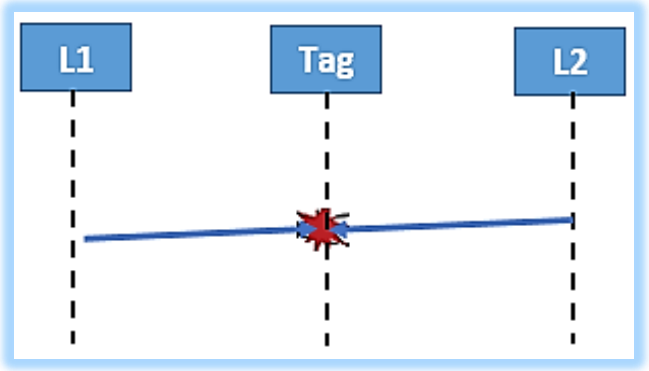


Figure 27:diagramme de séquence entre lecteurs-lecteur (a)

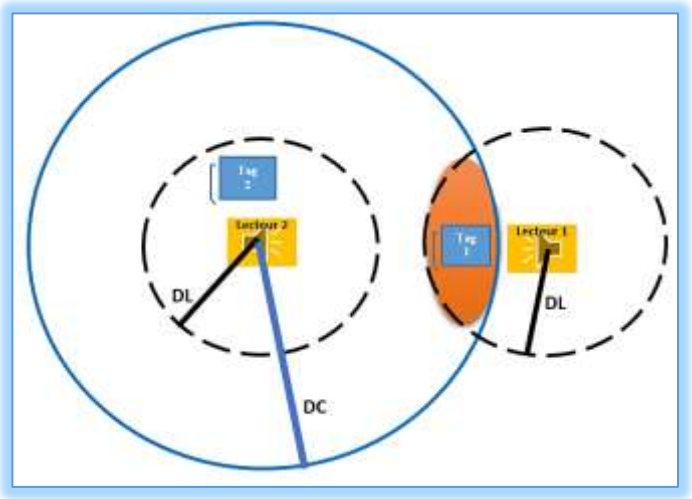


Figure 28:collision lecteur-lecteur (b)

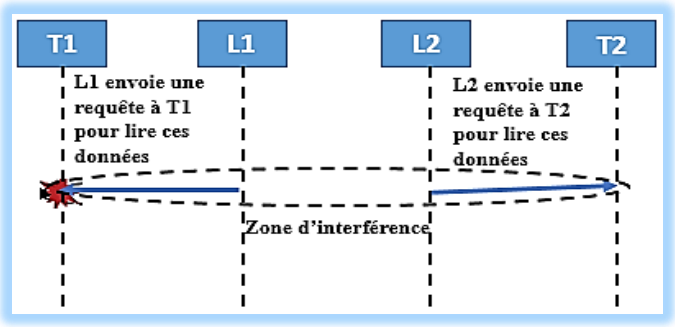


Figure 29:diagramme de séquence entre lecteurs-lecteurs (b)

Ces différents types de collisions présentent un défi majeur pour les systèmes RFID. Nous présentons dans la section suivante les protocoles de la couche MAC dans les systèmes RFID.

3. Les méthodes d'accès pour les réseaux sans fil classiques

Le médium radio est un médium partagé. Toutes les stations à portée radio les unes des autres s'entendent. D'où l'importance de la couche MAC (Medium Access Control). Il existe plusieurs façons de partager ou d'accéder au médium (TDMA, FDMA, SDMA, CSMA) [9].

Pour éviter les collisions qui se définissent par un transfert de données simultané entre plusieurs nœuds sur le même support ; des protocoles de contrôle d'accès au support (MAC) ont été proposés pour aider les nœuds à accéder au support sans se heurter dans le canal de communication. Parmi ces méthodes d'accès au médium, nous présentons ceux basés sur le temps, la fréquence et les codes.

3.1. Space Division Multiple Access (SDMA)

SDMA, est protocole d'accès par répartition dans l'espace qui permet l'accès à la ressource telle que la capacité du canal dans une zone séparée dans l'espace afin de réduire la plage de lecture des lecteurs dans l'espace. Il utilise une antenne directionnelle qui s'oriente dans l'espace et qui peut lire les tags présents dans cette zone.

Une option est de réduire significativement la portée d'un seul lecteur, mais pour compenser, il faut alors utiliser un grand nombre de lecteurs pour former un réseau, fournissant ainsi la couverture d'une zone. La seconde option est d'utiliser une antenne directionnelle sur le lecteur. De manière à ne scanner, à un instant t, qu'une partie des tags. Un des inconvénients de la technique SDMA est le coût relativement élevé de la mise en œuvre du système de lecteur et d'antenne.

La figure 30 permet d'illustrer la représentation de cette méthode.

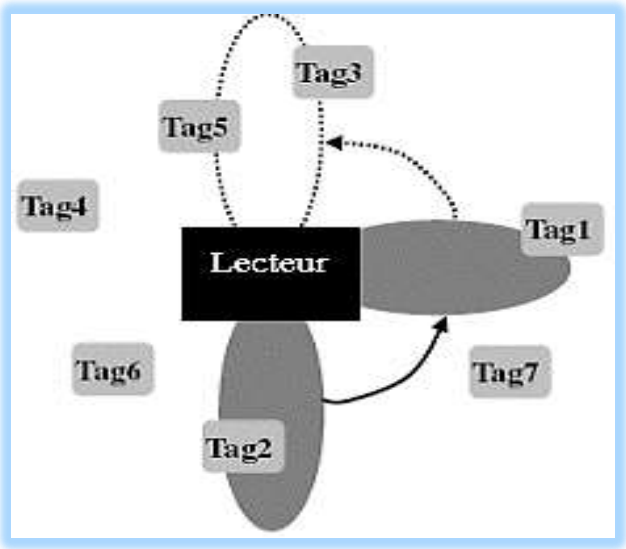


Figure 30:Illustration SDMA

3.2. Time Division Multiple Access (TDMA)

TDMA est une technique d'accès multiple par répartition dans le temps. Le lecteur se charge d'allouer un temps aux tags ainsi ils pourront envoyer leurs données dans les créneaux horaires au lecteur. Dans la méthode TDMA le lecteur parle, les tags écoutent. La plupart des protocoles d'anticollision dans le système RFID (DCS, PDCS, BACP) utilise la technique du TDMA [42] qui consiste à répartir le temps de parole entre les tags en leur fournissant des fenêtres temporelles dans lesquelles chacun communique [42].

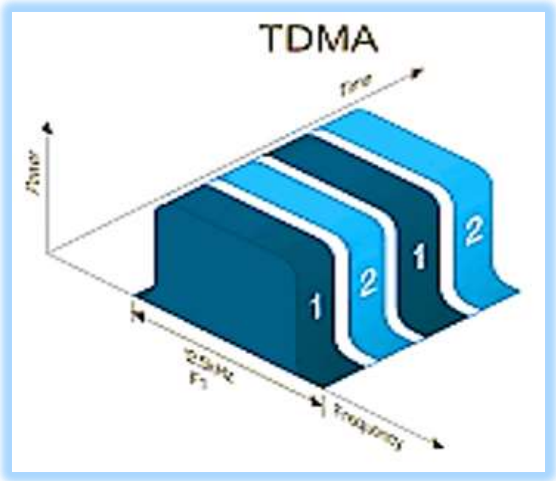


Figure 31:illustration TDMA

3.3. Frequency Division Multiple Access (FDMA)

Dans cette méthode, la ressource existante (fréquence) est divisée en plusieurs canaux de transmission avec des fréquences différentes disponibles simultanément. Les tags répondent au

lecteur avec des fréquences différentes. FDMA consiste à doter le lecteur de plusieurs canaux de transmission permettant ainsi aux tags de communiquer simultanément.

Un des inconvénients de la procédure FDMA est le coût élevé des lecteurs qui peuvent couter jusqu'à 10000 euros, de plus un récepteur dédié doit être fourni pour chaque canal de réception [42].

La figure 32 donne l'illustration du schéma FDMA.

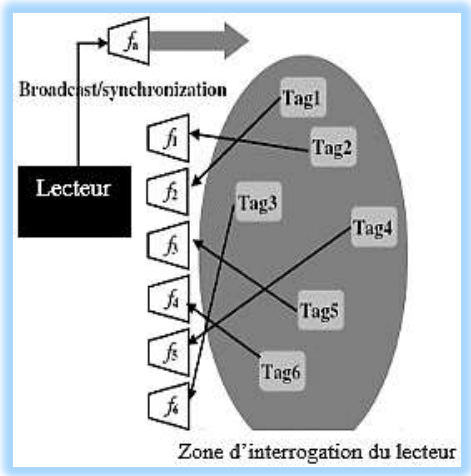


Figure 32:illustration FDMA

3.4. Code Division Multiple Access (CDMA) Technique

Cette méthode est utilisée essentiellement dans la communication des cellulaires. Son application se passe ainsi : les lecteurs sont identifiés par leurs codes et ils se synchronisent entre eux. La mise en place de cette méthode dans les systèmes RFID est très compliquée, car il demande un temps de calcul tant pour les tags ainsi qu'aux lecteurs. La figure 33 illustre le protocole CDMA.

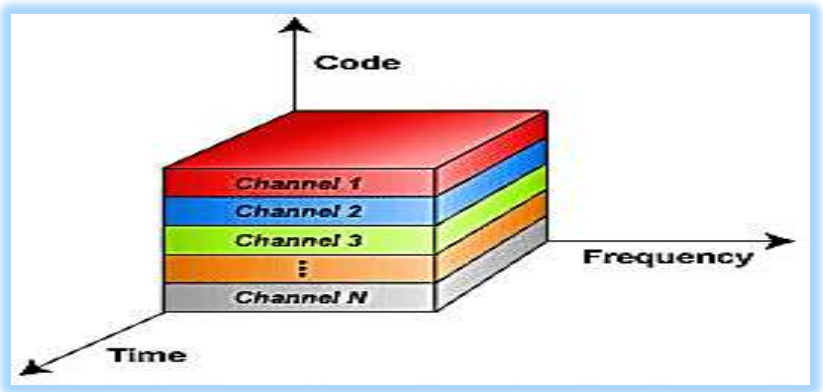


Figure 33:illustration CDMA

Dans le chapitre qui suit, nous allons voir de manière générale les types de collisions ainsi que leurs gestions par les protocoles de la couche Mac.

4. Présentation générale des protocoles de la couche MAC pour les systèmes RFID

La sous-couche de contrôle d'accès au support (**Media Access Control** en anglais ou MAC) est dans la couche de liaison de données du modèle OSI, selon les standards de réseaux informatiques IEEE 802.*x*. Elle sert d'interface entre la partie logicielle contrôlant la liaison d'un nœud (Contrôle de la liaison logique) et la couche physique (matérielle). Par conséquent, elle est différente selon le type de média physique utilisé. Ainsi, nous notons une spécification des différents protocoles utilisés dans cette couche. Certains de ces protocoles MAC sont utilisés uniquement pour les systèmes RFID. Ces protocoles sont catégorisés en deux familles : décentralisée et centralisée.

Nous notons des protocoles d'anticollision tag-tag, des protocoles d'anticollision lecteur-lecteur et lecteur-tag. Dans la suite, nous allons nous pencher sur les collisions entre lecteurs.

4.1. Présentations des exigences et des métriques des protocoles MAC pour la RFID

Dans cette section, nous allons présenter les exigences et les métriques d'évaluation des protocoles RFID.

4.1.1. Présentation des exigences des protocoles RFID

Les critères à remplir par les protocoles MAC RFID dépendent largement des fonctionnalités et des performances attendues [16]. Avant de concevoir un nouveau protocole MAC d'identification RFID, il est important de prendre en compte un certain nombre d'exigences qui doivent être satisfaites. Ces exigences sont liées à des questions de confidentialités, de sécurités et de performances [17].

4.1.1.1. Confidentialité

Une des principales préoccupations des systèmes RFID est la confidentialité. Les communications non protégées entre les tags et les lecteurs sur un canal sans fil peuvent divulguer des informations sur les tags et leurs positions. Deux questions de confidentialité majeures sont identifiées [18].

Confidentialité des informations du tag : quand un lecteur lit l'information venant d'un tag, il reçoit son identification. Si cette identification est par exemple un numéro de sécurité sociale alors l'identification elle-même devient une donnée sensible. Pour éviter les fuites d'informations, il faut contrôler les lectures [17,18].

Confidentialité de la localisation : Si les réponses d'un tag sont différentiables des autres. Alors, avec plusieurs lecteurs, il est possible, par trilatération, de géolocaliser les déplacements d'un porteur du tag par exemple. Il faut que les messages provenant des tags soient anonymes [17,18].

4.1.1.2. Performance

Les performances de stockage et de puissance de calcul des tags étant extrêmement limitées, elles ne peuvent pas utiliser de systèmes cryptographiques lourds. Les ressources doivent aussi être utilisées avec parcimonie dans le cas des tags actifs ou semi-actifs [16].

Minimisation du stockage : le volume de données stockées dans un tag doit être minimisé en raison de la taille limitée de sa mémoire [16, 17].

Minimisation de la puissance de calcul : les calculs du côté des tags doivent être minimisés à cause de sa puissance de calcul et de son énergie très limitée [16, 17].

Limitation des communications : le volume de données que chaque tag peut transmettre par seconde est limité par la largeur de bande disponible pour tous les tags [16, 17].

Évolutivité : le lecteur doit être capable de gérer des quantités croissantes de donnée, de travail dans une concentration de tag élevée. Il doit être en mesure d'identifier plusieurs tags en utilisant le même canal radio [21]. Effectuer une recherche exhaustive pour identifier les tags individuels peut être difficile dans une forte concentration de tags [16].

Ainsi, pour faciliter la vue d'ensemble sur ces différents protocoles, nous établirons un catalogage suivant différents paramètres permettant de guider le choix d'un algorithme ou d'un autre en fonction des contraintes de l'application à servir.

4.1.2.Les métriques d'évaluations des protocoles anticollision RFID

Afin d'appréhender les performances des différentes solutions proposées pour remédier aux collisions, il est nécessaire d'établir les métriques de mesures 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. Dans [31], les auteurs proposent 10 métriques d'évaluations différentes. Dans la suite nous retiendrons 7 métriques. Ce choix a été guidé par le fait que ces sept métriques sont non seulement les plus utilisées dans la littérature, mais aussi parce qu'elles sont suffisamment représentatives.

4.1.2.1. 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 possible. 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 réussi se traduit par une lecture des tags à porter. Ainsi en fonction du protocole d'anticollision choisi, un Accès Canal Réussi (ACR) sera décompté à chaque fois qu'un lecteur remporte la contention pour avoir l'accès au canal et lire les tags à portée. La contention est définie comme la phase de compétition engagée par un lecteur RFID pour avoir accès au canal. La résolution de cette contention se déroule 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 qu'un seul sous-ensemble des lecteurs accède 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.

4.1.2.2. Collisions

Les collisions, comme exprimer en Section 2.2.3, 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.), voir 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 Echoués (ACE). On comptabilisera donc un ACE à chaque fois qu'un lecteur échouera en contention pour l'accès au canal. 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 accéder au canal échoue, il perd de l'énergie. En fonction de l'algorithme utilisé, il peut même 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.

4.1.2.3. Efficacité

Cette métrique combine les deux précédentes afin de déterminer les dispositions des algorithmes à éviter les collisions et autoriser l'accès au canal et aux lecteurs. L'efficacité se calcule comme suit : *Efficacité =ACR* / (*ACR* + *ACE*)
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 [53]. 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 [53].

4.1.2.4. Indice d'équité de Jain (IEJ)

Cette métrique, très partagée dans plusieurs domaines [44], permet d'apprécier l'équité dans l'accès au canal entre les différents lecteurs. L'IEJ se calcule comme suit :

L'IEJ permet d'avoir une idée de la distribution spatiale des lecteurs ce qui est impossible avec le débit de lecture. En effet, si les lecteurs ont tous les mêmes valeurs en termes d'ACR, l'IEJ est égale à 1. 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 sous 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.

4.1.2.5. Délai de couverture

Cette métrique permet e connaître le temps nécessaire pour interroger l'ensemble des tags à portée de lecture. Quand bien même l'Indice d'Équité de Jain permet d'avoir une idée sur les performances de l'ensemble des lecteurs, il ne garantit pas une lecture rapide des tags déployés. Dans l'exemple de l'application logistique dans un entrepôt avec des produits alimentaires, si un produit périmé est recherché dans l'ensemble, il est nécessaire de pouvoir le retrouver au plus vite.

Ainsi utiliser un algorithme offrant un délai de couverture rapide est préférable. En fonction de l'application concernée, un temps de couverture élevé peut être considéré comme un inconvénient.

4.1.2.6. Consommation d'énergie

L'un des paramètres les plus importants d'un réseau RFID est la consommation d'énergie des lecteurs. Dans un réseau RFID, la consommation électrique maximale survient lorsque le lecteur balaie les tags dans la plage d'interrogation, et non lorsqu'il tente d'accéder au canal [34].

4.1.2.7. Mobilité

La mobilité est nécessaire dans certaines applications RFID. Les lecteurs peuvent être mobiles. Bien que la mobilité puisse aider dans le traitement de certains problèmes d'identification. Il introduit une certaines contraintes dans le système. La nature de ces contraintes va de la quantité à la mobilité des lecteurs déployés ce qui affecte la qualité du système RFID en provoquant des collisions de lecture parfois.

5. Les méthodes d'accès d'anticollision spécifique aux lecteurs RFID

Les collisions dégradent les performances du système RFID. Au cours des dernières années, beaucoup de recherches ont été faites pour concevoir des mécanismes d'anticollisions afin d'atténuer ces effets nocifs [22, 23, 24].

De nombreux algorithmes d'anticollision de lecteurs ont été développés et publiés dans la littérature pour réduire les interférences dans les réseaux de lecteurs RFID.

Ainsi, pour assurer la coordination nécessaire entre les lecteurs afin d'éviter les collisions, une forme de communication doit être établie entre les lecteurs 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. Les protocoles d'anticollision de lecteur proposés dans la littérature possèdent leurs propres propriétés et fonctionnalités. La figure 34 montre la classification des approches existantes [53] ; à savoir l'approche décentralisée qui consiste à laisser les lecteurs fonctionner sans un coordonnateur et l'approche centralisée où les lecteurs nécessitent un coordinateur du réseau RFID.

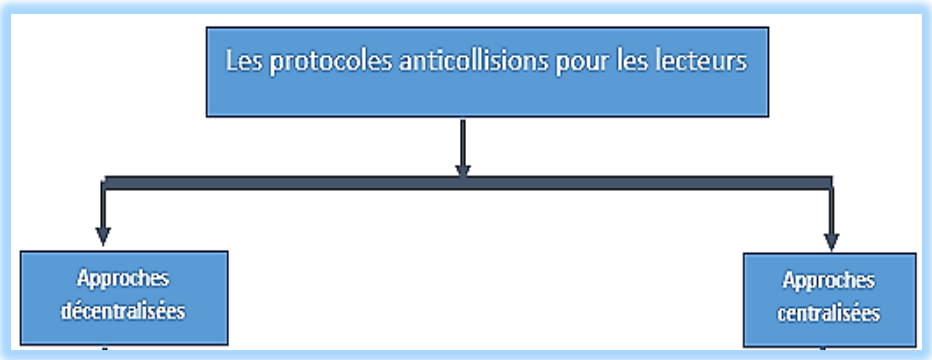


Figure 34:Classification des protocoles anticollision pour les lecteurs RFID

5.1. Approche décentralisée

Les ressources système disponibles telles que les fréquences et le temps sont réparties entre les lecteurs pour les empêcher de transmettre simultanément. Ce genre d'approche peut réduire efficacement les risques de collisions avec les lecteurs. Les protocoles suivants sont dans cette catégorie [15].

5.1.1.Approche décentralisées basées sur le mécanisme TDMA

La plupart des approches d'anti-collision RFID TDMA distribuées dérivent d'un algorithme antérieur appelé Distributed Color Selection et utilisent un canal de communication dédié entre lecteurs pour organiser leur activité [15].

L'objectif de ces protocoles est de colorer un réseau de lecteurs de sorte que chaque lecteur rencontre un plus petit nombre possible de lecteurs adjacents avec la même couleur. Une couleur est une période de réservation pour la transmission de données sans collision.

5.1.1.1. Distributed Color Selection (DCS)

DCS est un protocole qui consiste à colorer un réseau de lecteurs à l'aide d'un algorithme distribué pour que chaque lecteur possède le plus petit nombre possible de lecteurs adjacents de même couleur. Cette approche permet de réserver facilement des créneaux horaires. Une couleur est une réservation de temps périodique pour la transmission de données sans collision (c'est-à-dire une communication lecteur-tag) [24,25].

a. Description de DCS

Dans DCS [24,25], les lecteurs réservent périodiquement des intervalles de temps (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 différentes 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. [24,25].

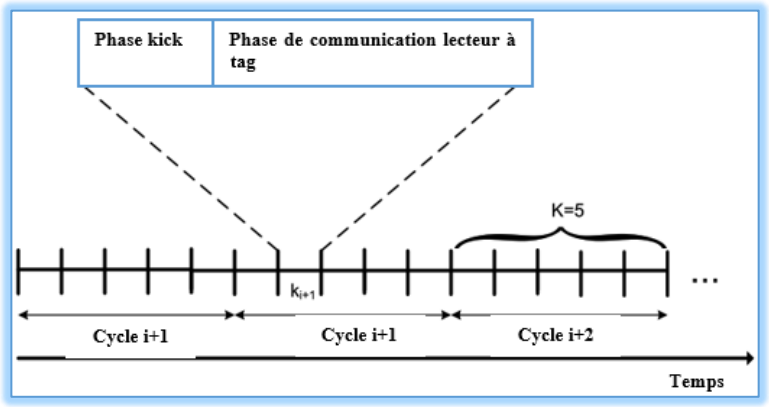


Figure 35:Gestion du temps d'identification dans le protocole DCS

Scenario

Considérons 10 intervalles de temps (time slot) L7 et L6 sélectionnent au hasard, le même intervalle de temps (1).

Constatons le fonctionnement du protocole dans la figure 36 :

- ✓ L7 et L6 démarrent simultanément leur communication ;
- ✓ une collision aura lieu entre L7 et L6 ;
- ✓ L7 et L6 vont choisir chacun un nouvel intervalle de temps (*timeslot*) ;
- ✓ Ils vont envoyer des messages aux lecteurs voisins
  - ✓ L6 envoie un message à son voisin L4 ;
  - ✓ L7 envoie un message à son voisin L5 ;
- ✓ Quand les voisins reçoivent le message de kick, ils vérifient si l'intervalle de temps qu'ils ont reçu est égal aux siens. Si oui, ils doivent laisser leur intervalle de temps puis sélectionner un autre qui sera différent.

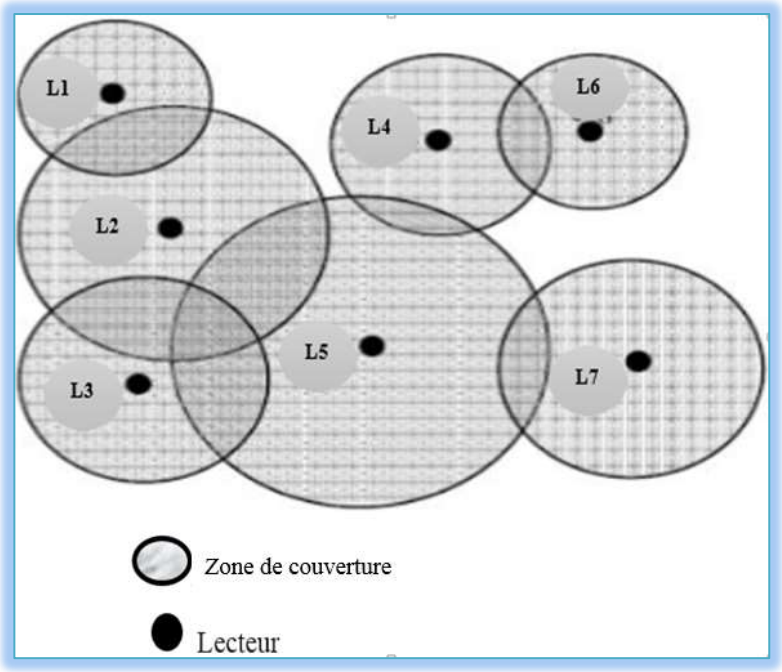


Figure 36:Scénario appliqué au DCS

Avantage:

- ✓ La probabilité d'un lecteur d'entrer en collision immédiatement après avoir subi une collision est réduite au minimum au détriment de ses voisins.

Inconvénients:

- ✓ Dans un environnement dense de lecteur, il est facile de voir à quel point le protocole DCS serait instable [26].
- ✓ Longue attente des lecteurs en collision avant de participer à nouveau à un tour.
- ✓ Lorsque la majorité des couleurs est épuisée alors les lecteurs pourraient subir des collisions [27].
- ✓ L'inconvénient principal de cet algorithme est qu'en fonction du nombre maximum de couleurs disponibles, le système RFID est fortement affecté.
- ✓ Si la valeur des couleurs max est trop faible alors un grand nombre de lecteurs finissent par choisir les mêmes couleurs et entrent en collision.
- ✓ Si la valeur des couleurs max est trop élevée alors certains intervalles de temps peuvent ne pas être occupés car il y'aura beaucoup de collisions et par conséquent des pertes d'intervalle.
- ✓ Le débit et le délai de couverture sont aussi impactés [27].

5.1.1.2. Probability Distributed Color Selection (*PDCS*)

Le protocole PDCS est une version améliorée du DCS. PDCS utilise la probabilité pour la résolution de collision tout en conservant les fonctionnalités de DCS. Différemment des protocoles de division de temps précédents, PDCS autorise les transmissions multicanaux, conformément aux réglementations RFID internationales.

a. Description de PDCS

PDCS [29] est une autre version améliorée et probabiliste de DCS et la première dérivée à proposer une solution multicanal. Un paramètre p est introduit comme la probabilité pour un lecteur de changer sa couleur après une collision. Trois cas sont donc possibles :

- ✓ cas 1 : les lecteurs impliqués dans la collision ne changent pas de couleur, ils envoient des messages kick qui inciteront les lecteurs voisins à changer de couleur;
- ✓ cas 2 : un des lecteurs change de couleur et envoie un message kick pour réserver la nouvelle couleur, l'autre lecteur interroge les tags avec la couleur précédente sans changer;
- ✓ cas 3: les lecteurs changent de couleur, dans ce cas ils envoient des messages kick et réservent leurs nouvelles couleurs, c'est l'algorithme basique de DCS.

Scenario

Considérons le scénario dans DCS ci-dessus :
Après collision de L6 et L7, puis que le protocole est multicanal contrairement au DCS, les lecteurs L6 et L7 peuvent sélectionner des canaux séparés.

Avantages :

- ✓ Le PDCS est multicanal.
- ✓ La performance temporelle fournie par le PDCS est meilleure que le DCS.
- ✓ La raison en est que, dans le PDCS, les lecteurs n'ont pas besoin de coopérer donc pas besoin de serveur pour atteindre les ressources et travailler de manière indépendante[30].
- ✓ Selon [30], PDCS consomme moins d'énergie et montre une meilleure efficacité énergétique par rapport au protocole DCS.

Inconvénients:

- ✓ Comme pour DCS, le nombre maximum de couleurs est fixe, induisant les mêmes problèmes.

- ✓ La présence des lecteurs mobiles affecte les performances de PDCS, car les lecteurs mobiles ne peuvent pas atteindre une couleur constante [27].
- ✓ PDCS ne s'adpte pas à la mobilité des lecteurs [26, 27].
- ✓ Compte tenu des facteurs statiques et en faisant varier le nombre de voisins, l'équité de PDCS est fortement affectée par le nombre de couleurs utilisées [27].

5.1.1.3. Colorwave

Le protocole Colorwave est une version améliorée de DCS et de PDCS. Dans DCS, la couleur maximum (max couleurs) est fixée. Ainsi, Colorwave implémente un mécanisme de gestion dynamique pour changer le nombre maximum de couleurs.

a. Description de Colorwave

Colorwave aussi connu sous Variable-maximum DCS [52], 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 maximal en fonction de l'état du réseau, deux variables seuils sont introduites 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.

Scenario

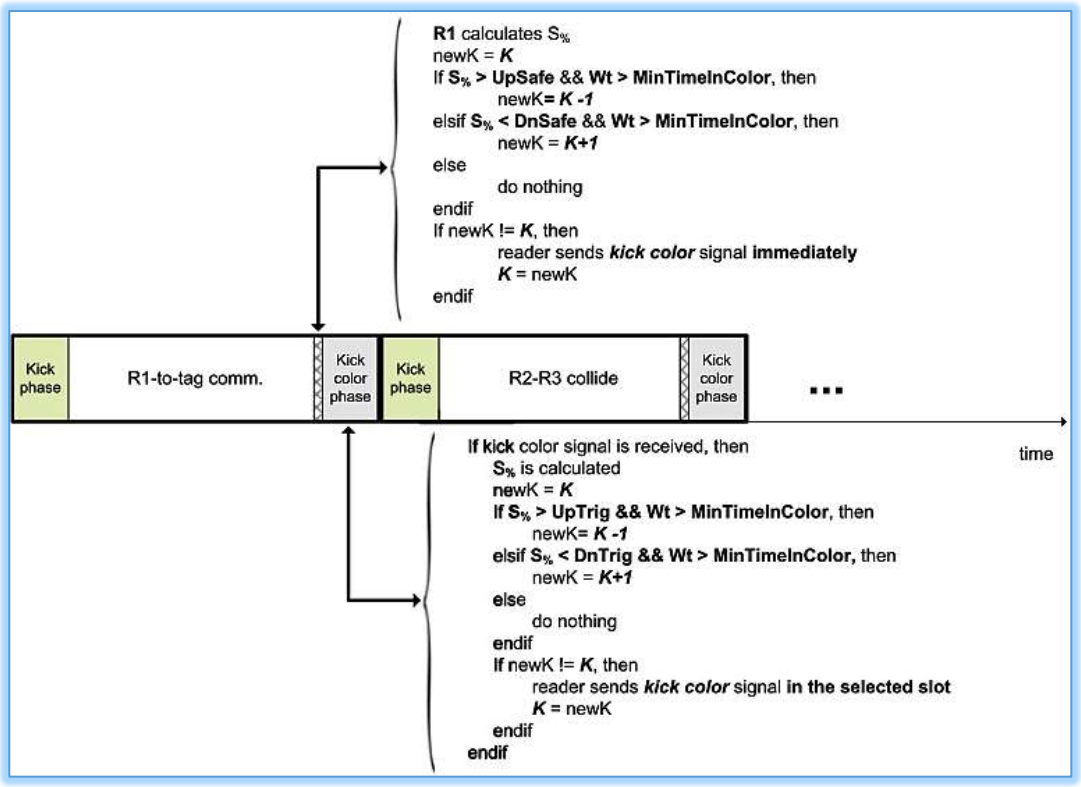


Figure 37:Gestion du temps d'identification dans le protocole Colorwave

Avantages:

- ✓ Colorwave intègre le mécanisme de dynamisation des intervalles de temps [24,31].
- ✓ Il a plus de débit que le protocole PDCS et DCS.
- ✓ Colorwave permet au Système RFID de s'adapter facilement aux perturbations locales, telles que l'installation d'un nouveau lecteur RFID ou présence d'un lecteur RFID mobile.
- ✓ La simplicité de Colorwave est indéniable sa performance supérieure, en particulier sous haute communication.
- ✓ Les capacités de réservation, d'adaptabilité de Colorwave sont essentielles à ses performances sous une charge de communication élevée [31].

Inconvénients:

- ✓ Le principal inconvénient de ce protocole est la synchronisation temporelle requise entre les lecteurs [32].
- ✓ L'efficacité du protocole Colorwave diminue en présence de plusieurs lecteurs, puisque les effets négatifs dus à l'impossibilité d'atteindre une configuration de couleur stable sont réduits.

- ✓ Le débit de Colorwave est supérieur que celui de DCS car il utilise un paramètre pour augmenter et diminuer les intervalles de temps.
- ✓ Colorwave consomme plus d'énergie que le DCS, PDCS [30] à cause de son débit élevé.
- ✓ 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.

5.1.1.4. Distributed Color Non-cooperative Selection (DCNS)

DCNS est un protocole qui vient améliorer les performances de Colorwave pour diminuer le taux de collision.

a. Description de DCNS

DCNS [51] est encore un autre algorithme dérivé de Colorwave. La première différence avec Colorwave est que les lecteurs n'envoient pas de messages kick mettant à jour leur valeur du nombre de couleurs maximales, ici nommée μ. Un autre paramètre introduit est η qui détermine la probabilité pour un lecteur d'interroger les tags une fois sur son créneau temporel. Les lecteurs sont classés en trois différents types :

- ✓ killer pour μ == 2, avec une gamme de couleurs si faible, ces lecteurs interrogent fréquemment les tags, donc ils n'envoient pas de kick ni ne changent de canal pour éviter les collisions avec les autres killers voisins ;
- ✓ normal pour 2 < μ < threshold, ces lecteurs agissent comme des lecteurs standards suivant Colorwave ;
- ✓ killed pour μ > threshold, ces lecteurs envoient constamment des kick et interrogent rarement les tags, ils augmentent leur valeur de η afin d'augmenter leurs chances d'interrogation.

Avantages:

- ✓ DCNS a un débit plus élevé que DCS, PDCS, NFRA et Colorwave.
- ✓ DCNS fournit toujours le meilleur débit en moyenne 16 % supérieure à NFRA [51].
- ✓ DCNS innove par une réduction de contrôle des canaux, un nouveau mécanisme de mise à jour des couleurs, la gestion dynamique des priorités.
- ✓ DCNS fait partie des meilleurs protocoles d'anticollision de lecteur à lecteur pour les réseaux statiques, mais aussi prouve plus d'efficacité que les protocoles à exigences élevées [51].

Inconvénients:

- ✓ Avec cette configuration le système RFID n'atteint jamais vraiment l'état de convergence stable [51].
- ✓ Dans le cas d'utilisation de lecteurs mobiles, le délai de couverture peut être affecté si les tags éloignés sont couverts par des lecteurs en position killed.

5.1.1.5. MAximum LIkelihood COlorwave (MALICO)

MALICO est un protocole distribué basé sur un mécanisme qui exploite un estimateur de maximum de couleur pour améliorer les performances du protocole Colorwave.

a. Principe de fonctionnement

MALICO [50], apporte encore une autre amélioration à Colorwave par rapport à sa convergence. Au lieu de s'appuyer sur un ensemble de seuils et de déclencheurs entrés manuellement, les lecteurs mettent automatiquement à jour leur nombre de couleurs disponibles pour réduire les collisions. La mise à jour est effectuée par chaque lecteur suite à l'observation des contentions réussies, en collision et au repos dans la ronde précédente pour estimer le nombre de voisins. Sur la base de cette estimation, un certain nombre de couleurs disponibles est défini pour optimiser le débit de lecture.

Avantages:

- ✓ Il est plus adaptable à l'évolution des scénarios tels que la mobilité ou la densification des réseaux de lecteurs.
- ✓ Au lieu de limiter les lecteurs à une seule fréquence, il permet aux lecteurs d'opérer jusqu'à quatre fréquences.
- ✓ Il a l'avantage de rejeter les phases de *kick* présentes dans Colorwave pour augmenter les interrogations et le débit. [50]

Inconvénients:

- ✓ Les lecteurs utilisant MALICO doivent disposer d'antennes bi-statiques afin d'écouter et d'enregistrer les collisions possibles pendant qu'ils accèdent au canal.
- ✓ Dans les déploiements mobiles si la vitesse de déplacement de lecteurs mobile est rapide alors la mobilité est affectée en raison de l'écoute et du calcul de chaque lecteur.
- ✓ Si le calcul peut être fait pour un état donné de voisins lors d'un tour d'interrogation donné, cela change malheureusement en raison de la mobilité lors du tour suivante.
- ✓ La planification des transmissions est un problème différent de celui de la gestion de l'énergie.

Dans la suite, nous allons voir les protocoles décentralisés qui utilise le mécanisme CSMA.

5.1.2.Approches décentralisée basées sur les mécanismes CSMA

Cette approche est basée sur le protocole CSMA pour diminuer le problème des collisions entre lecteurs en transmettant des notifications de paquets de contrôle tels que les signaux de balise (beacon). Après avoir reçu un signal de balise, les lecteurs qui s'interférent, vont interrompre leur communication en cours et attendent le cycle suivant. Cette approche résout efficacement le problème des collisions lecteur à lecteur. Cependant, la communication réelle a lieu entre le lecteur et tag. Ce type de protocole n'est pas conçu pour résoudre les problèmes de collision entre lecteur et tag, ce qui réduit les performances RFID. Les protocoles suivants entrent dans cette catégorie.

5.1.2.1. Pulse

Pulse est un protocole distribué, conçu pour réduire les collisions de lecteurs causer par les lecteurs fixes ou mobiles.

a. Description de Pulse

Ce protocole [33, 34], permet aux lecteurs d'écouter le média avant d'interroger les tags. Cependant, dans ce cas, pour éviter les problèmes d'écoute, les lecteurs envoient constamment un signal pour alerter leurs voisins pendant le fonctionnement. Lorsqu'un lecteur reçoit la "pulsation" d'un voisin, il se désactive et attend que le support soit disponible. Cela a l'avantage d'assurer qu'un seul lecteur interroge les tags dans un voisinage donné.

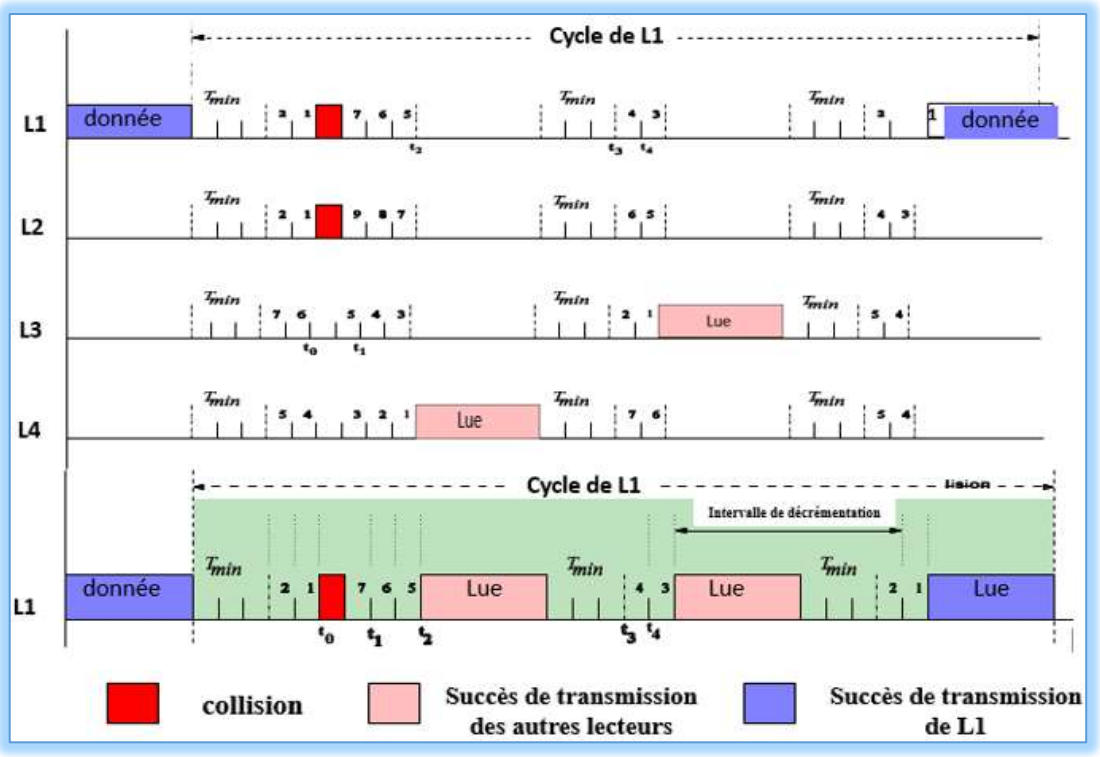


Figure 38: illustration protocole Pulse

Scénario

Les réseaux RFID résistent également au problème des terminaux cachés. Comme on le voit dans la figure 39, L1 et L2 ne se trouvent pas dans la zone de détection de l'autre, mais des signaux provenant de L2 pourraient interférer avec les signaux de L1 au tag T. Pour un tel scénario, un mécanisme de notification est nécessaire entre L1 et L2 de sorte que L2 soit informé des transmissions de L1 avant de communiquer avec le tag T. Pulse propose d'avoir cette notification par un message diffusé appelé « beacon » sur un canal de contrôle. La communication dans ce canal est telle que deux lecteurs quelconques pouvant interférer sur le canal de données (canal utilisé pour lire les tags), sont capables de communiquer sur le canal de contrôle. Ainsi à la figure 39, puisque L1 et L2 interfèrent l'un avec l'autre sur le canal de données, ils pourront communiquer sur le canal de contrôle.

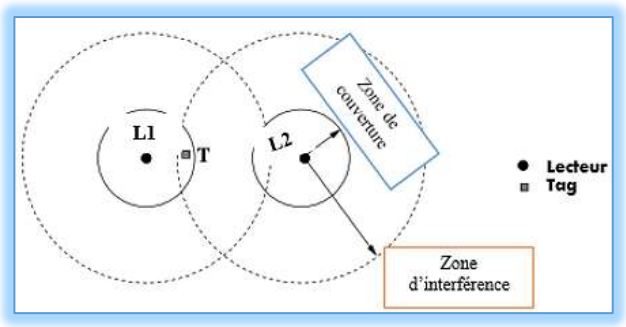


Figure 39:scénario du protocole Pulse

Avantages :

- ✓ Pulse, diminue les collisions et durant toute la communication le lecteur envoie périodiquement des beacons aux lecteurs voisins.
- ✓ Pulse montre une amélioration du débit et de l'efficacité du système.
- ✓ Pulse est efficace même dans les réseaux mobiles denses. [15]

Inconvénients:

- ✓ Pulse, ne résout pas le phénomène de terminal caché.
- ✓ Dans un environnement mobile dense, les lecteurs qui envoient une «impulsion» pourraient finir par désactiver un grand nombre de leurs voisins inutilement, ce qui aurait un impact considérable sur le débit et l'efficacité du système. [15]
- ✓ chaque fois que deux canaux sont utilisés, un émetteur-récepteur peut être requis pour chaque canal. Une grande quantité d'énergie est consommée lors de la détection de la porteuse, réception de balises et la lecture des balises. [15]
- ✓ Protocole Pulse peut entraîner un délai élevé lorsque le nombre de lecteurs est important [28].

5.1.2.2. Dica [14]

Le protocole Dica (Distributed Tag Access avec prévention des collisions) convient considérablement aux environnements des réseaux mobiles sans fil éco énergétiques coopérant avec RFID. DiCa est capable non seulement d'éviter les collisions, mais aussi de changer les états de puissance de manière autonome par simple interaction avec les lecteurs adjacents.

a. Description de Dica

DiCa [15] presque similaire au protocole pulse, il possède également un canal de données et un canal de contrôle. L'utilisation du canal de données est obtenue par les lecteurs via le canal de

contrôle. Le gagnant de la contention lit les tags via le canal de données pendant que les autres lecteurs attendent que le canal soit inactif. Les paquets suivants sont échangés entre les lecteurs pour éviter les collisions :

- ✓ **BRD_WHO :** utilisé pour identifier si le canal est occupé ou non.
- ✓ **BUSY :** indique que le lecteur est en train de lire les tags.
- ✓ **BRD_END :** paquet utilisé pour indiquer que le canal est inactif après la lecture des balises.

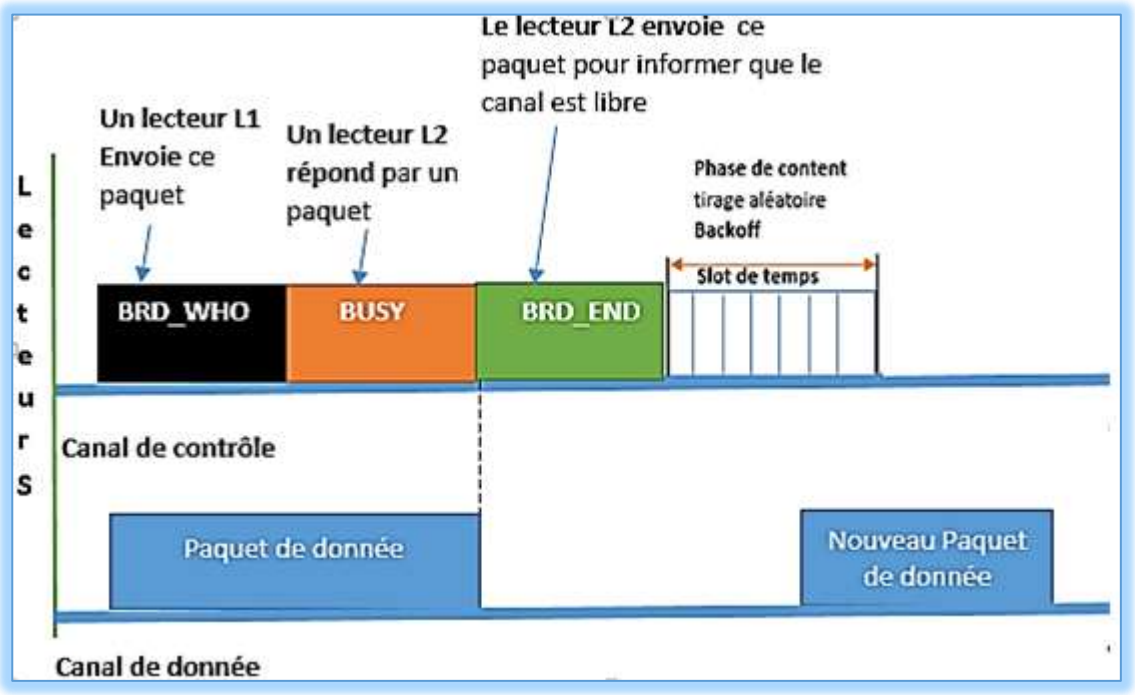


Figure 40:illustration protocole Dica

Scenario

Un lecteur qui veut lire les tags (par exemple, L1) diffuse le message BRD_WHO aux lecteurs dans la même zone d'interrogation pour prendre connaissance des lecteurs qui sont entrains de lire des tags. Ensuite, le lecteur situé dans la même zone d'interrogation (par exemple, L2) envoie le message BUSY s'il lit des tags. Maintenant, L1 doit attendre jusqu'à ce qu'il reçoive BRD_END du lecteur L2.

Par contre, si L1 ne reçoit pas de message BUSY après avoir envoyé un BRD_WHO pendant un certain temps, il suppose que le canal de données est libre et il peut commencer à lire les tags.

Avantages:

- ✓ Contrairement au protocole Pulse, Dica prend en compte les problèmes de terminaux cachés et exposés en ajustant la plage du canal de contrôle à deux fois le rayon depuis le premier lecteur.
- ✓ DiCa n'exige aucune solution centralisée ni de synchronisation globale.
- ✓ Ce réglage du canal dans DiCa réduit la consommation d'énergie, il est donc plus approprié pour systèmes RFID mobiles à contraintes énergétiques.
- ✓ DiCa consomme moins d'énergie que Pulse, CSMA, et ALOHA [15].

Inconvénients:

DiCa a besoin de suffisamment de temps pour échanger le message de contention ce qui augmente la probabilité de collision [15].

5.1.2.3. MCMAC

Le protocole multicanal MCMAC est mis en place pour amélioration le débit du réseau et de diminuer les collisions de lecteurs.

a. Description de MCMAC

Le protocole MAC multicanal (MCMAC) [35] est basé sur la contention, il est similaire au Pulse et au LBT (listen Befort Talked) qui permet d'écouter le canal avant d'émettre. Avec MCMAC un lecteur diffuse un message de contrôle une fois qu'il a remporté la contention dans un canal de contrôle et accède ainsi au canal de données et l'occupe. Puis il envoie un message de contrôle aux lecteurs voisins pour les informer de son occupation du canal de donnée pour un certain temps. Après avoir reçu un message de contrôle d'un lecteur voisin, les autres lecteurs n'utilisent pas ce canal pendant un certain temps et tentent d'accéder à un autre canal. [36]

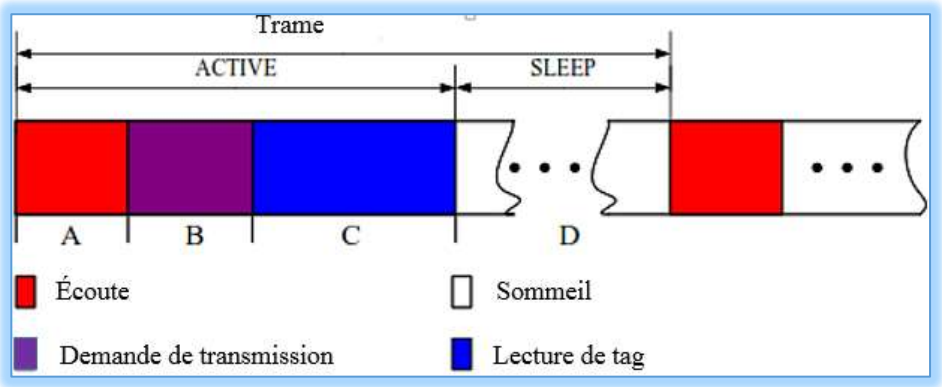


Figure 41:Structure de communication d'une trame

Comme le montre la figure 41, dans chaque cycle de communication il y'a une période active et une période de sommeil, la période active est divisée en trois étapes (A, B, C). Ces trois étapes sont les suivantes :

- ✓ A : écoute du canal de donnée ;
- ✓ B : demande de transmission ;
- ✓ C : lecture de tag.

Avantages:

- ✓ Dans [36], nous pouvons voir que le protocole MAC multicanal (MCMAC) proposé consomme moins d'énergie que les autres protocoles Colorwave.
- ✓ MCMAC diminue considérable les collisions des lecteurs, ainsi que la redondance des données dans la communication avec les tags RFID et une réalisation d'environ 100 % d'économie d'énergie. [36]
- ✓ MCMAC peut améliorer l'utilisation multicanal du lecteur RFID, réduit le nombre de collisions de paquets et augmente le débit de données grâce à l'affectation dynamique de canaux.
- ✓ Les performances de MCMAC par le biais de la simulation et les résultats montrent que le protocole a permis aux lecteurs d'obtenir une diminution du nombre de collisions et d'améliorer le débit [36].

Inconvénients:

- ✓ Les collisions entre lecteur et tag persistent avec cette approche. Les tags passifs étant incapables de distinguer deux canaux de données, plusieurs canaux de données ne peuvent pas être utilisés directement dans un environnement de tag passif.
- ✓ Deux lecteurs peuvent utiliser des canaux de données différents, mais causent toujours des collisions si elles lisent le même tag simultanément.
- ✓ MCMAC souffre de des collisions de lecteur et tag et de la collision entre les paquets de contrôle.

5.1.2.4. Distributed Multi-Channel Collision Avoidance (DiMCA)

DiMCA est un algorithme multicanal, il permet de résoudre les problèmes de collision de lecteurs dans un environnement RFID dense. Il ne nécessite pas de synchronisation globale dans le réseau RFID.

a. Description de DiMCA

Légèrement différent des algorithmes CSMA précédents, le protocole DiMCA [49] propose aux lecteurs d'échanger des messages sur deux canaux de contrôle différents fonctionnant sur des portées différentes. Le premier canal couvre la portée d'interrogation du lecteur où les messages contenant l'ID du lecteur sont envoyés et le deuxième canal couvre la plage d'interférence où les messages contenant à la fois l'ID du lecteur et le canal d'interrogation choisi sont envoyés. Avant d'interroger des tags, un lecteur attend une période aléatoire au cours de laquelle il peut recevoir des messages sur les canaux de contrôle. Ainsi, selon le type de message reçu, un lecteur conserve deux listes de voisins en collision : ceux avec lesquels il peut fonctionner en même temps, mais sur une fréquence différente et ceux pour lesquels il doit impérativement fonctionner à des instants différents. Avant de lancer son opération d'interrogation, un lecteur vérifie sa file d'attente selon l'état choisit un canal déférent pour opérer et le diffuse à ses voisins ou attend un signal END de ses voisins pour fonctionner à un autre moment.

Avantages:

- ✓ DiMCA améliore à la fois le débit et l'efficacité du système RFID. [49]
- ✓ DiMCA a réduit le total temps nécessaire à l'identification des tags et a augmenté le taux d'interrogations réussit dans le réseau. [49]
- ✓ DiMCA vise à résoudre tous les types de collisions de lecteurs.
- ✓ Minimisait le délai total d'interrogation par rapport au délai des approches centralisé, même lorsque les retards augmentent dans des environnements denses.
- ✓ Le nombre total de paquets échangés reste limité, contrairement à MCMAC où les lecteurs continuent à diffuser paquets de contrôle pendant leur temps d'interrogation pour garder leurs voisins notifie de leur utilisation du canal de données.

Inconvénients :

- ✓ Elle repose sur un surcoût créé par les messages échangés entre les lecteurs, ce qui peut avoir un impact sur le retard.
- ✓ Lorsque le nombre de lecteurs augmente, les collisions entre lecteurs augmentent. Ces messages peuvent ne pas être les plus récents pour certaines raisons.

5.1.2.5. Enhanced Distributed Multi-Channel (EDMC)

EDMC est un protocole d'anticollision de lecteurs multicanaux, basé sur le protocole DiMCA. EDMC propose une méthode de contrôle pour décider si le lecteur reçoit les dernières informations de contrôle après avoir sélectionné les canaux donnés.

a. Description de EDMC

EDMC [48] propose une version améliorée de DiMCA en demandant aux lecteurs de vérifier s'ils ont reçu d'autres messages des voisins après avoir choisi leur canal et avant d'envoyer leur propre message. Cela réduit le risque de collisions de messages ou de messages mal reçus de la part des voisins juste avant l'interrogation des tags.

Avantages :

- ✓ Les auteurs prétendent améliorer légèrement le délai ainsi que réduire les collisions en utilisant cette technique par rapport à DiMCA.
- ✓ Ce protocole réduit le risque de collisions de messages ou de messages mal reçus de la part des voisins juste avant l'interrogation des tags.
- ✓ EDMC réduira le délai d'interrogation par rapport à DiMCA.

Inconvénients:

- ✓ Le lecteur doit garder le canal de contrôle actif tout le temps : gaspillage d'énergie.

5.1.2.6. Efficient Multichannel Reader Collision Avoidance (EMRCA)

EMRCA est un protocole multicanal de prévention efficace pour les collisions de lecteurs. Il est basé sur le protocole pulse, qui a un canal de contrôle et plusieurs canaux de données, et il convie pour le système RFID à multiples lecteurs.

a. Description de EMRCA

EMRCA [47] propose une version améliorée de DiMCA en demandant aux lecteurs de vérifier s'ils ont reçu d'autres messages des voisins après avoir choisi leur canal et avant d'envoyer leur propre message. Cela réduit le risque de collisions de messages ou de messages mal reçus de la part des voisins juste avant l'interrogation des tags.

Scenario

La Figure 43 est un exemple de distribution de lecteur, qui est utilisé pour expliquer le processus permettant d'éviter les collisions dans ce protocole. Nous supposons que tous les lecteurs ont la même plage de lecture et la même zone d'interférences. Il y a cinq lecteurs dans la sous-région de l'ensemble du domaine d'application. Basant sur leur position, le processus d'évitement des collisions est le suivant.

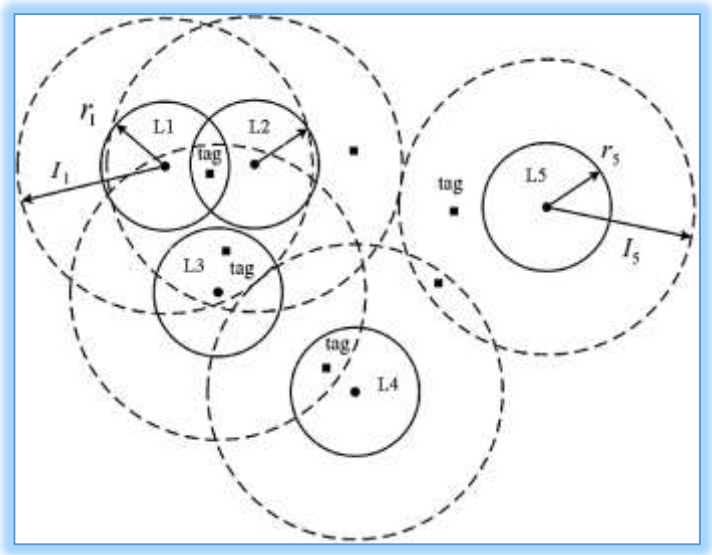


Figure 42:Un exemple de distribution de lecteur

Dans la figure 42 et 43, nous pouvons voir que :

- ✓ le temps d'attente de L2 est plus petit que celui de L1 qui est respectivement 4 et 6. Le délai de L2 réduit à zéro est antérieur à celle de L1, donc L2 lira les balises en premier. Quand L2 est en communication avec les tags, L1 devrait attendre dans son canal, car les deux lecteurs voisins doivent utiliser des tranches de temps différent. Le même cas s'applique également à L2.
- ✓ Le canal de données de L3 est différent de L1 ou L2 pour éviter les collisions de lecteurs. comme vous pouvez le voir sur la figure 43, L3 n'est pas limité par la plage horaire de L1 ou L2.
- ✓ L4 n'a aucun lien avec et L1, et L2 est un lecteur qui interfère avec L3. Ainsi L3 et L4 devraient être disposés dans des canaux différents pour empêcher les collisions entre lecteur et tag. De même, L4 n'est pas limité par les intervalles de temps de L1 et L3.
- ✓ L5 n'a aucun lien avec L1 et L4, il peut choisir au hasard un créneau horaire. La Figure 44 montre le résultat quand le temps d'attente de L3, L4 et L5 sont différents. Quand les valeurs du temps d'attente sont réduites à zéro, les trois lecteurs peuvent communiquer avec des tags

immédiatement et ne tiennent pas compte des intervalles de lecture des autres lecteurs, à moins que leurs voisins lisent au même moment.

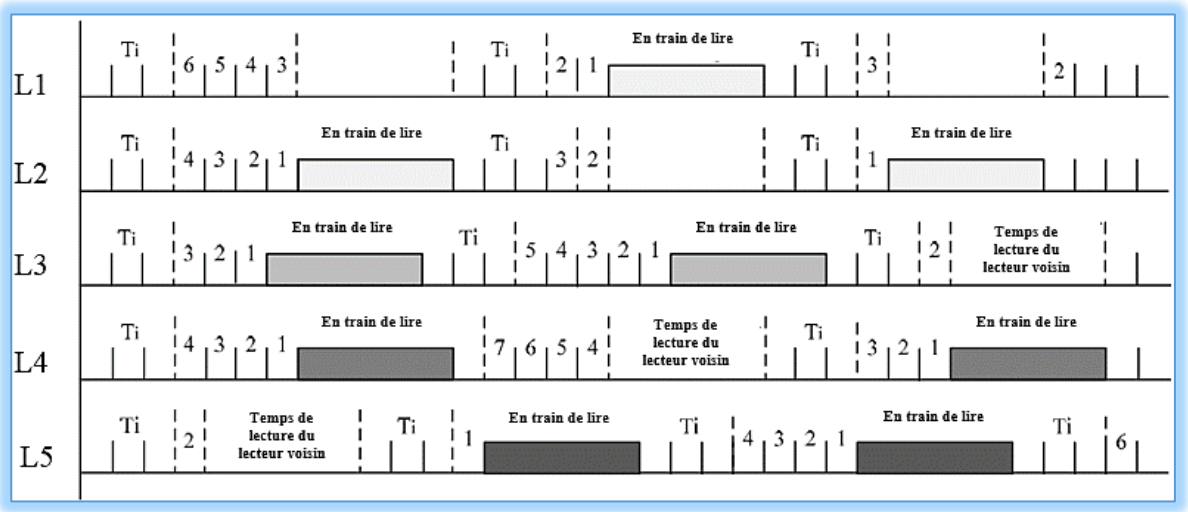


Figure 43:la chronologie de cinq lecteurs

Avantages:

- ✓ EMRCA améliore l'équité et l'efficacité globales de Pulse.
- ✓ EMRCA montre une meilleure performance que les protocoles précédents en termes de nombre d'interrogatoires ayant échouée, le temps de traitement d'interrogation, et la surcharge du réseau. [47]
- ✓ Les lecteurs peuvent prévenir toutes les collisions potentielles, EMRCA peut réduire les zones d'influence de lecteurs pertinents en utilisant les différents canaux, ce qui peut améliorer considérablement le débit du système.

Inconvénients :

- ✓ Ce protocole soufre encore de la mobilité et de la forte densité de déploiement des lecteurs.

Dans la suite, nous allons faire une étude comparative des protocoles d'anticollision de l'approche décentralisée.

5.1.3. Étude comparative des protocoles de l'approche décentralisée

La comparaison des caractéristiques des approches distribuées est faite à l'aide du tableau 3. Ces caractéristiques sont importantes pour le traitement de collision lecteur-lecteur. La revue de la littérature prouve que les algorithmes décentralisés basés sur la méthode CSMA sont tous multicanal et utilisent un canal de contrôle. De plus, la plus part de ces algorithmes règlent dans certains cas

les types de collisions lecteur-tag en plus de celle entre lecteur-lecteur. Par contre les algorithmes basés sur la méthode TDMA sont tous monocanal et ne gèrent que le type de collisions lecteur-lecteur. Le tableau 3 ci-dessous appuie bien cette analyse.

	DCS	PDCS	Colorwave	DCNS	MALICO	Pulse	DiCa	MCMAC	DiMCA	EDMC	EMRCA
Collision lecteur-lecteur	oui	oui	oui	oui	oui	oui	oui	oui	oui	oui	oui
Collision lecteur-tag						oui	oui		oui	oui	oui
Distribué	oui	oui	oui	oui	oui	oui	oui	oui	oui	oui	oui
Multi canal		oui				oui	oui	oui	oui	oui	oui
Utilisation canal de contrôle						oui	oui	oui	oui	oui	oui
Gérant la mobilité			oui	oui	oui	oui	oui	oui	oui	oui	oui
Basé sur FDMA									oui		oui
Basé sur TDMA	oui	oui	oui	oui	oui				oui		oui
Basé sur CSMA						oui	oui	oui	oui	oui	

Tableau 3: Récapitulation de caractéristiques des protocoles d'anticollision décentralisés lecteur-lecteur

Par ailleurs, nous proposons de faire une évaluation des performances des protocoles d'anticollisions décentralisées représentés dans la figure 44 selon les métriques vues dans la section 4.1.2. Cela va nous permettre d'avoir une vue global des performances de chacun de ces protocoles. La figure est réalisée à l'aide du diagramme de Radar et les données sont abstraites. C'est-à-dire qu'elles ont été obtenues à partir d'une étude comparative des résultats de simulations de l'ensemble des protocoles étudiés. Dans cette figure, plus la courbe concernant un protocole se rapproche des bordures extérieures plus ces performances sont bonnes.

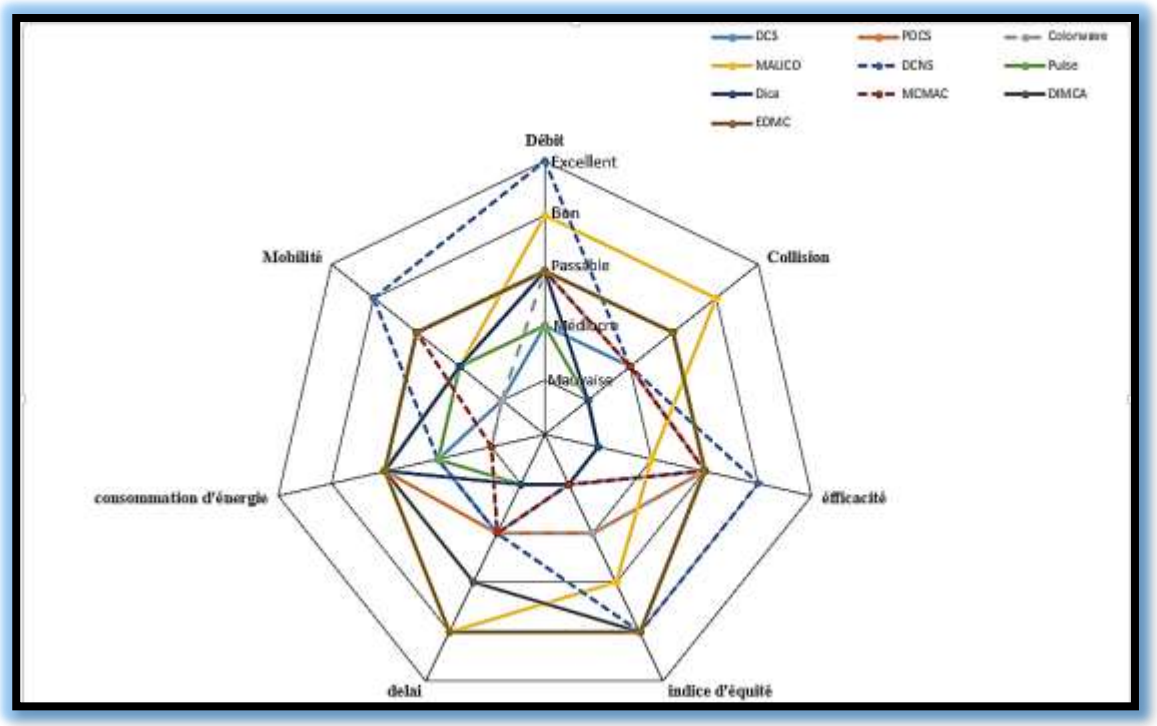


Figure 44:évaluation des performances des protocoles d'anticollisions décentralisés

Nous constatons que les résultats des protocoles décentralisés illustrés sur la Figure 44 en termes de délai de couverture et d'équité sont généralement bons. Par contre, ils enregistrent un nombre de collisions considérables et une consommation d'énergie importante. On remarquer que plus le débit de lecture et l'index d'équité sont importants, moins le protocole sera adapté à éviter les collisions. Un protocole tel que DCNS permet d'obtenir de bonnes performances en termes de débit de lecture, collisions et d'index d'équité. Il soufre cependant du délai de convergence nécessaire pour atteindre de bonnes performances, ce qui peut se voir sur son délai de couverture. De plus, dans MCMAC les auteurs ne nous disent pas comment des collisions de paquet de contrôle pourraient être gérées. Pareillement pour DiMCA, les auteurs n'abordent pas non plus la façon dont ils évitent les collisions concernant les messages échangés.

Dans la suite nous allons voir les protocoles d'anticollision de lectures. Les collisions de lecteur à lecteur persistent, le débit et le calcul sont généralement très faibles. Le faible calcul noté dans les protocoles décentralisés à pousser le chercheur à mettre en place une nouvelle famille de protocole appelée centralisée. Ce dernier remédie à ce problème et d'augmenter dans le même sens le débit des protocoles basés sur cette famille.

5.2. Approche centralisée

Dans les protocoles centralisés, un serveur central gère et alloue des ressources aux lecteurs. Les lecteurs peuvent communiquer au serveur avec ou sans fil. Dans le cas du sans-fil, la fréquence de communication entre les lecteurs et le serveur central est diffèrent de la fréquence que les lecteurs utilisent pour communiquer avec les tags [38]. Généralement les protocoles de cette famille sont basés sur le mécanisme TDMA.

5.2.1. Neighbor Friendly Reader Anticollision Protocol (NFRA)

Dans un environnement dense, la collision entre lecteurs devient un problème. Les informations d'échange entre les lecteurs sont envoyées à un serveur. Ces échanges peuvent ne pas convenir aux réseaux RFID denses et dynamiques avec des lecteurs mobiles. NFRA fonctionne avec un serveur dans des réseaux RFID denses et dynamiques avec des lecteurs mobiles. Grâce à l'assistance du serveur, les lecteurs peuvent travailler sans interférer avec les voisins et peuvent être synchronisés.

a. Description de NFRA

Dans NFRA [37], 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 d'intervalle de temps 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 time-slot 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.

Scénario

Compte tenu du réseau illustré à la figure 45 :

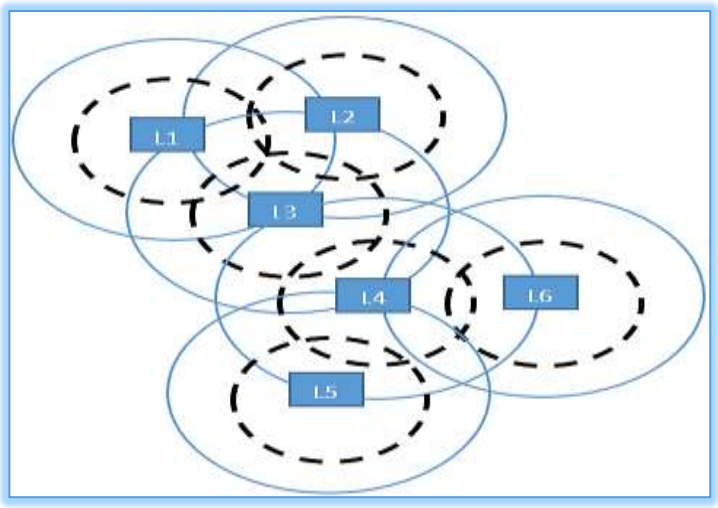


Figure 45:environnement d'un scénario NFRA

Les lecteurs suivants ont des collisions entre eux : {L1, L2, L3}, {L3, L4} {L4, L5} et {L4, L6}. Nous appliquons le protocole NFRA sur ce réseau et comme nous pouvons le constater à la figure 46 :

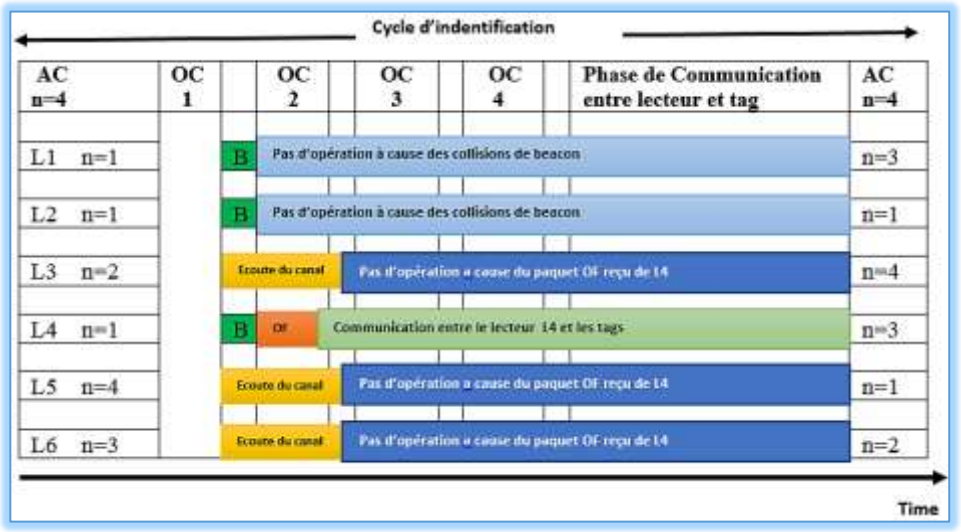


Figure 46:illustration du protocole NFRA

- ✓ les lecteurs {L1, L2} sont confrontés à une collision de balises ;
- ✓ de plus, les lecteurs {L3, L5, L6} sont bloqués par l'OF envoyé par L4 ;
- ✓ ainsi L3, L5 et L6 doivent attendre le tour suivant ;
- ✓ d'autre part, seul le lecteur L4 peut utiliser le canal et communiquer avec le tag ;
- ✓ en d'autres termes, un seul lecteur peut communiquer avec le tag lors de ce cycle.

Avantages:

- ✓ Dans NFRA le serveur et le mécanisme d'échange entre les lecteurs voisin permettent de diminuer les collisions.

- ✓ Résolutions du problème de synchronisation par le serveur diminue la charge de calcul contrairement aux protocoles décentralisés basés sur TDMA.
- ✓ Évaluation approfondit de la performance et les résultats de la simulation montrent que NFRA est indépendant du changement du nombre de lecteurs voisins et surpasse les autres protocoles.
- ✓ Le NFRA surpasse les autres protocoles en débit et en nombre moyen de transmissions par seconde.
- ✓ Il résout à la fois les collisions lecteur-lecteur et les collisions tag-lecteur à travers un algorithme centralisé pour les lecteurs fixes et mobiles.

Inconvénients:

- ✓ Dans les déploiements très denses, NFRA a un nombre élevé de lecteurs désactivés dû aux OF. Par ailleurs, les lecteurs ayant choisi une valeur de time-slot faible sont privilégiés par rapport aux autres.
- ✓ Le débit de NFRA est affecté par la sélection aléatoire de MN et il pourrait être encore amélioré en modifiant la procédure de contention [39].

5.2.2. Neighbor Friendly Reader Anti-collision Protocol (NFRA_C)

NFRA_C est basé sur le mécanisme NFRA en révisant sa position procédure pour fournir un débit plus élevé dans le réseau de lecteurs. Il est un protocole d'anticollision de lecteur RFID performante.

a. Description de NFRA_C

NFRA-C [39] vient améliorer NFRA en rajoutant sur les démarches de ce dernier :

- ✓ Un compteur de communication entre lecteur et tag (CRT). L'état qui montre que le lecteur communique avec les tags présents dans sa zone couverture.
- ✓ Comparaison du compteur (CC) qui est un nombre dont chaque lecteur possède, qui montre le nombre de CRT réussie effectuée par ces derniers. La valeur initiale du compteur est un nombre aléatoire compris entre 0,1 ou 0,3.

Scénario

Considérons le scénario dans la figure 45 ou les lecteurs suivants ont des collisions entre eux : {L1, L2} {L2, L3} {L3, L5} et {L4, L5, L6}. Nous appliquons en premier lieu le protocole NFRA

sur ce réseau et, comme vous pouvez le constater à la figure 47, les lecteurs {L1, L2} sont confrontés à une collision de balises. LI et L2 ne communiquent pas ils vont attendre le prochain tour.

En appliquant le protocole NFRA_C dans la figure 48, après la détection d'une collision entre les lecteurs L1 et L2, leurs compteurs sont comparés et le lecteur avec la petite valeur CC aura accès au canal. Comme on le voit à la Figure 48, le lecteur L2 à une très petite valeur de compteur, par conséquent, il a participé à la ronde en cours.

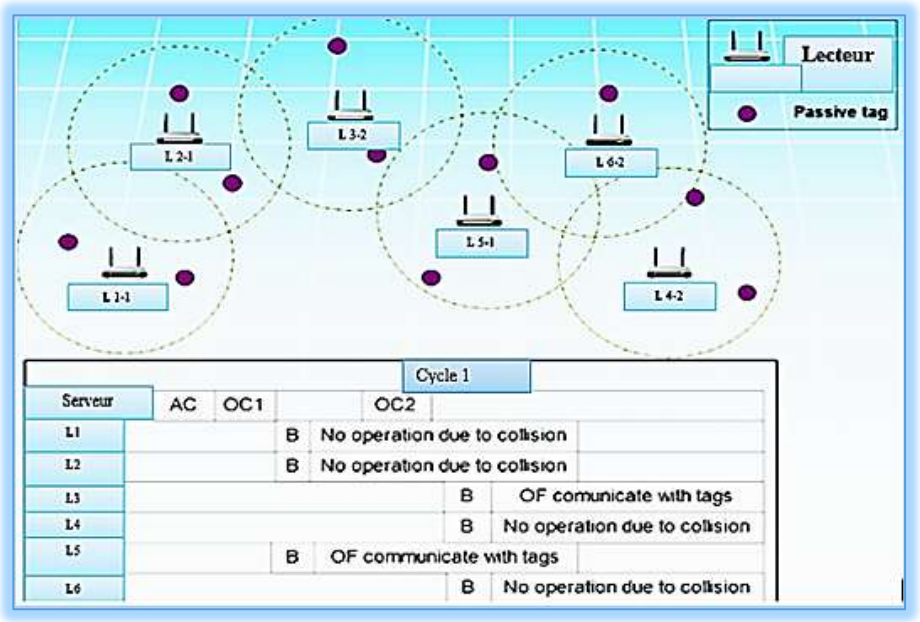


Figure 47:illustration d'un scénario du protocole NFRA

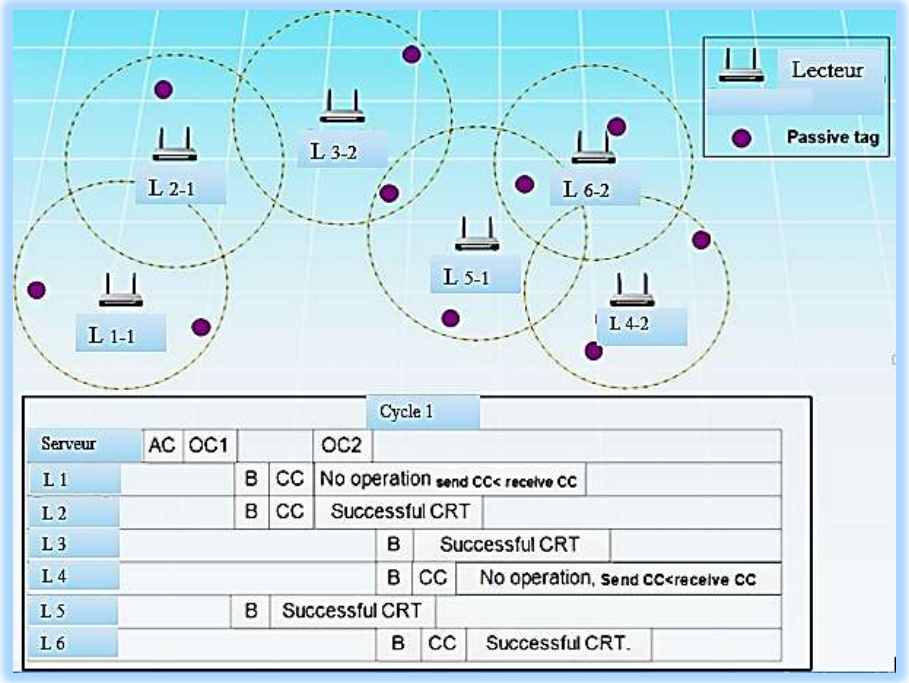


Figure 48:illustration appliquée au scénario des protocoles NFRA_C

Avantages :

- ✓ NFRA-C assure une bonne équité au moyen du mécanisme de priorité. La priorité la plus élevée est attribuée aux lecteurs qui ont fait moins d'identification de tag. Les études comparatives prouvent que la gestion des priorités augmente significativement l'équité du réseau. [39]
- ✓ Pour 100 lecteurs, l'efficacité de NFRA_C augmente dans la gestion des collisions et du débit de 15 % par rapport à la NFRA, de 21 % par rapport à Pulse et une augmentation de 43 % en efficacité par rapport à COlorwave. [39]
- ✓ NFRA-C peut être utilisé pour les réseaux de lecteurs denses et avec une faible probabilité de collision [39].

Inconvénients:

- ✓ NFRA-C ne prend pas de décision si les compteurs des lecteurs qui entrent en collision sont les mêmes.

5.2.3.Geometric Distribution Reader Anti-collision (GDRA)

Le protocole NFRA est un protocole monocanal, s'il devient multicanal, il aura une plus grande efficacité. En outre, dans le système NFRA, l'équité entre les lecteurs n'est pas observée parce que les lecteurs qui ont une plus petite valeur de compteur ont une grande chance d'avoir accès au canal. Dans [40], est présenté un système centralisé basé sur NFRA, appelé le lecteur d'anticollision à distribution géométrique (GDRA), dont le but est de multi canaliser et de réduire les problèmes de NFRA. Elle est entièrement décrite dans les sections suivantes.

a. Description de GDRA

Les cycles d'identificaion sont composés d'une phase de contention et d'une phase de communication du lecteur avec les tags. Un cycle d'identification commence lorsqu'un serveur centralisé envoie un paquet AC à tous les lecteurs. Il existe un nombre K dans l'AC qui indique le nombre d'intervalles de temps. Lorsque les lecteurs reçoivent l'AC, ils utilisent une fonction de distribution appelée Sift [53] pour choisir un nombre aléatoire k. Ce nombre correspond à leur intervalle de temps dans lequel ils doivent transmettre leurs balises. Cette fonction minimise la probabilité de collision entre les lecteurs et augmente la probabilité qu'un seul lecteur prenne l'intervalle de temps k. Après avoir sélectionné k, les lecteurs attendent l'intervalle de temps k-1 sans écoute du canal, et cela pour économiser leur énergie. Les lecteurs qui ont choisi k = 1 envoient directement une balise et écoutent le canal pour voir si la collision entre balises aura lieu ou non. Si

un lecteur envoie une balise à ses voisins, mais n'en reçoit aucune, il gagne le conflit et obtient le canal. Ainsi il peut commencer à communiquer avec les tags tout en continuant de les identifier jusqu'à la fin du tour. Si deux lecteurs entrent en collision, ils quittent la contention, choisissent un nouveau canal et attendent un nouveau paquet AC. Les lecteurs qui ont terminé de communiquer avec le tag restent sur le canal, attendent un nouveau AC et démarrent un nouveau tour [41, 42].

Scenario

Considérons le scénario d'écrit dans la figure 49 :

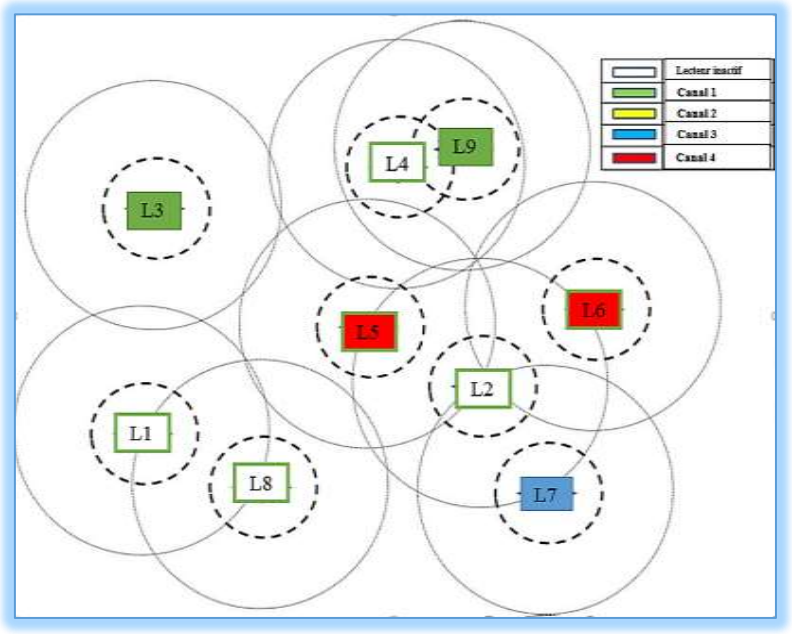


Figure 49:environnement d'un scénario

- ✓ Après avoir sélectionné les intervalles de temps, les lecteurs qui ont sélectionné le premier intervalle de temps envoient un message de balise. Si le message de balise n'entraîne pas de collision, le lecteur entre dans la phase de communication lecteur à tags et commence à lire le message balises (comme les lecteurs L3 et L7) comme le montre la figure 50.
- ✓ Comme le montre la figure 50, les lecteurs L1 et L8, qui ont sélectionné le troisième intervalle de temps (k=3), commencent à écouter le canal à partir du deuxième intervalle de temps (k=2). Ainsi L1 et L8 sont en collision sur le même canal.
  De plus, les lecteurs L1 et L8, malgré la possibilité de lire avec deux canaux de fréquence différents, restent inactifs jusqu'au prochain tour à cause de la collision.
- ✓ le lecteur L2, qui a sélectionné un intervalle de temps numéro 3, écoute le canal de l'intervalle de temps k=2. Considérant que le lecteur L2 est dans la plage d'interférence du

lecteur L7 alors que L7 lit avec succès les tags dans le même canal de fréquence (canal 3), le lecteur L2 abandonne le canal et attend le tour suivant.

<table>
<tr><th>Envoi de balise (be)</th><th colspan="3">Collision à l'écoute (L)</th><th colspan="2">Balise de collision</th><th>Entente AC</th><th>Collision lecteur tag</th></tr>
<tr><td>Canaux</td><td>K=1</td><td>K=2</td><td>K=3</td><td>K=4</td><td>K=5</td><td>K=6</td><td colspan="2">Communication lecteur à tags</td></tr>
<tr><td rowspan="3">1</td><td>L3</td><td colspan="6">Lecteur L3 communique avec les tags</td></tr>
<tr><td></td><td></td><td>L9</td><td>L9</td><td colspan="3">Lecteur L9 communique avec les tags</td></tr>
<tr><td></td><td></td><td></td><td></td><td>L4</td><td colspan="2">Pas d'opération car le canal est occupé</td></tr>
<tr><td rowspan="2">2</td><td></td><td>L1</td><td>L1</td><td colspan="4">Pas d'opération car le canal est occupé</td></tr>
<tr><td></td><td>L8</td><td>L8</td><td colspan="4">Pas d'opération due à la collision</td></tr>
<tr><td rowspan="2">3</td><td></td><td>L2</td><td colspan="5">Pas d'opération car le canal est occupé</td></tr>
<tr><td>L7</td><td colspan="6">Lecteur L7 communique avec les tags</td></tr>
<tr><td rowspan="2">4</td><td></td><td></td><td>L5</td><td>L5</td><td colspan="3">Lecteur L5 communique avec les tags</td></tr>
<tr><td></td><td></td><td>L6</td><td>L6</td><td colspan="3">Lecteur L6 communique avec les tags</td></tr>
</table>

Figure 50:scénario du protocole GDRA

Avantages :

- ✓ Dans NFRA [43], un serveur central synchronise le système via des commandes de diffusion.
- ✓ GDRA est multicanal.
- ✓ L'utilisation d'une distribution géométrique [32] a permis d'atténuer les collisions.
- ✓ La possibilité de réserver un canal parmi les quatre et un intervalle de temps permettent de réduire les collisions. [45]

Inconvénients:

- ✓ Deux lecteurs qui entrent en collisions abandonnent le canal puis sélectionnent un autre canal aléatoire et attendent le tour suivant. En conséquence, le canal abandonné, est inutilisé et les ressources sont gaspillées.
- ✓ GDRA malgré le fait qu'il s'agisse d'un protocole multicanal, il n'utilise pas cette fonctionnalité correctement, car il est possible qu'un lecteur lise les tags avec un autre lecteur dans le canal sans l'apparition de toute ingérence. Cependant, cette question n'est pas prise en compte dans ce protocole et les lecteurs abandonnent le canal dès qu'il est occupé.
- ✓ Malgré le fait que GDRA ait fourni un débit plus élevé, il consomme plus d'énergie.

- ✓ Cependant de grandes exigences, nécessitant des lecteurs capables de communiquer simultanément avec un serveur central, entre eux et avec les tags, tout en tenant compte de l'utilisation d'antennes bi-statiques pour pouvoir écouter sur leur canal pendant la transmission [45].

5.2.4.A Distance Based RFID Reader Collision Avoidance (DRCA)

Ce protocole est mis en place pour améliorer les performances de GDRA. Il utilise toutes les ressources disponibles pour donner une seconde chance aux lecteurs en collision d'être actifs dans le cycle en cours.

a. Description de DRCA

La DRCA [45] est un protocole d'anticollision de collision basée sur la résolution de distance. Ce protocole résout dans une certaine mesure le second problème de la GDRA. Dans l'algorithme DRCA, lorsqu'un lecteur sélectionne l'intervalle de temps k, il écoute les canaux à partir de l'intervalle de temps (k-1). Cependant, contrairement au l'algorithme GDRA, si le canal est occupé à l'intervalle de temps (k-1), le lecteur calcule la distance qui la sépare avec le lecteur qui occupe le canal sur la base de la force du signal reçu. Si la distance calculée est supérieure à une valeur 2 * Drt (où Drt est la plage de lecture) de sorte que :

- ✓ le nouveau canal sélectionné n'entraîne pas de RTC (collision de lecteur et de tag), le lecteur a alors une seconde possibilité d'accéder au canal. Dans ce cas, le lecteur augmente son intervalle de temps à k + 1 et sélectionne au hasard un nouveau canal.
- ✓ au début de l'intervalle de temps (k + 1), si le canal n'est pas occupé à l'intervalle de temps k, le lecteur commence à envoyer des messages balises. S'il n'y a pas de collision entre les messages balises envoyées, le lecteur a alors la possibilité de lire les balises dans un nouveau canal. Toutefois, si la distance calculée est inférieure à 2 * drt, un RTC se produit, même si le lecteur utilise une fréquence différente pour lire les tags. Ainsi, le lecteur n'est pas autorisé à réessayer et attendez le tour suivant.

Scénario

Considérons le même scénario précédent à la figure 49. En appliquant l'algorithme DRCA,

la figure 51 est un exemple, dans lequel :

- ✓ le lecteur L2, qui a sélectionné l'intervalle de temps k=3, écoute le canal de l'intervalle de temps k=2. Le canal 3 est déjà occupé par le lecteur 7 ;

- ✓ le lecteur 2 calcule sa distance par rapport au lecteur 7 en fonction de la force du signal reçu. La distance entre les deux lecteurs est supérieure à 2 * drt ;
- ✓ alors le lecteur L2 augmente son intervalle de temps de k=3 à k=4 puis écoute le canal à l'intervalle de temps k=3 en sélectionnant un nouveau canal (canal 4);
- ✓ Cependant, le scénario est différent pour le lecteur L4 qui sélectionne l'intervalle de temps k=6 puis écoute le canal situé dans l'intervalle de temps k=5. Étant donné que le canal est utilisé par le lecteur L9 alors le lecteur L4 va calculer sa distance au lecteur 9 ;
- ✓ Puis que la distance est inférieure à 2 * drt alors même s'il change de canal, la RTC(collision entre lecteur et tag) se produit. Donc le lecteur L4 n'a pas une seconde chance d'accéder au canal et doit attendre jusqu'au prochain tour.

Envoi de balise (be)	**Collision à l'écoute (L)**			**Balise de collision**			**Réécoute (L)**	**Entente AC**	**Collision lecteur tag**
Canaux	K=1	K=2	K=3	K=4	K=5	K=6	Communication lecteur à tags		
1	L3	Lecteur L3 communique avec les tags							
			L9	L9	Lecteur L9 communique avec les tags				
					L4	Pas d'opération car le canal est occupé			
2		L1	L1	Pas d'opération due à la collision					
		L8	L8	Pas d'opération due à la collision					
3		L2							
	L7	Lecteur L7 communique avec les tags							
4			L2	L2	Pas d'opération due à la collision				
			L5	L5	Pas d'opération due à la collision				
			L6	L6	Pas d'opération due à la collision				

Figure 51:scénario du protocole DRCA

Avantages:

- ✓ En DRCA, lorsque le lecteur détecte que le canal est occupé, s'il est suffisamment éloigné du lecteur actif, incrément son intervalle de temps à 1et choisis un autre canal.
- ✓ Les ressources du réseau sont utilisées à bon escient.
- ✓ Le protocole suggéré à un débit plus élevé et un temps d'attente moyen inférieur à celui des autres protocoles. [45]

Inconvénients:

- ✓ Dans certains cas le protocole DRCA ne résout pas le deuxième problème du système GDRA, ce qui fait que la DRCA fonctionne encore plus mal que la GDRA comme le cas entre L1 et L8 dans la figure[51].
- ✓ Si deux lecteurs entrent en collision dans un même canal et un même intervalle de temps alors ce canal est inutilisé, car ils vont choisir un autre canal.
- ✓ Un autre problème avec le DRCA est que, les lecteurs qui ont la possibilité d'accéder à nouveau au canal sont autorisés à sélectionner au hasard l'un des quatre canaux existants. Par conséquent, avec une probabilité de 25 %, un lecteur peut choisir son canal précédent. Cependant, cela gaspille de l'énergie, car amenant le lecteur à tenter vainement d'accéder au canal. [46]
- ✓ DRCA la probabilité d'interférence dans les intervalles de temps les plus élevés augmente et éventuellement, le canal est abandonné, reste inutilisé ou plus de lecteurs sont inactifs.

5.2.5.Called Beacon Analysis-based Collision Prevention (BACP)

Ce protocole a pour objectif de proposer un système qui, en plus de résoudre les problèmes des systèmes GDRA et DRCA, alloue des ressources aux lecteurs de manière à garantir une utilisation maximale des ressources disponibles. Ce protocole tente également d'activer le plus grand nombre de lecteurs par tour afin qu'ils puissent lire les tags avec un minimum d'interférences.

a. Description de BACP

Dans [46], les lecteurs communiquent avec un serveur central avec ou sans fil. Le serveur annonce le début de chaque tour en envoyant un message AC aux lecteurs. La durée de chaque AC est considérée comme étant de 2,83 ms et chaque tour est divisé en deux phases principales. La phase de contention, au cours de laquelle les lecteurs sont en contention pour accéder au canal en envoyant un message de balise. Dans la phase CRT (communication entre lecteur et tag), le lecteur se connecte aux tags s'il accède au canal avec succès. La phase de contention est divisée en K slots, la durée de chaque intervalle de temps est Tslot = 5 ms. Les lecteurs sont équipés d'une antenne bistatique et peuvent donc envoyer un message de balise dans chaque intervalle de temps, en plus de l'écoute du canal. La durée d'envoi d'un message de balise est TBeacon = 0,3 ms.

Dans le protocole BACP, chaque intervalle de temps est divisé en 16 sous-slots, et chaque lecteur en sélectionne dans son intervalle de temps pour envoyer un message de balise de manière aléatoire. Considérant la durée de chaque intervalle de temps comme étant le temps qu'il faut pour envoyer un message de balise. Chaque lecteur envoie un message de balise pendant le sous-slots sélectionné

à partir de son intervalle de temps et écoute les canaux pour recevoir des messages de balises des lecteurs voisins. Dans un même intervalle de temps si un nombre élevé de lecteurs voisins s'y trouvent alors une collision entre les messages de balises envoyés dans les sous-slots sera noté, mais avec une probabilité très faible.

Comme le montre la figure 52, dans le protocole BACP, chaque lecteur envoie une balise appelée Preference_Code. Chaque Preference_Code contient Reader_ID et un bit appelé Prev_state. Chaque lecteur du réseau à une unité spécifique appelée Reader_ID. Prev_state est un bit (le dernier bit en partant de la gauche) qui fait référence à l'état du lecteur dans le tour précédent. Si le lecteur a réussi à lire les balises du tour précédent, alors la valeur de Prev_state est zéro ; sinon, c'est un.

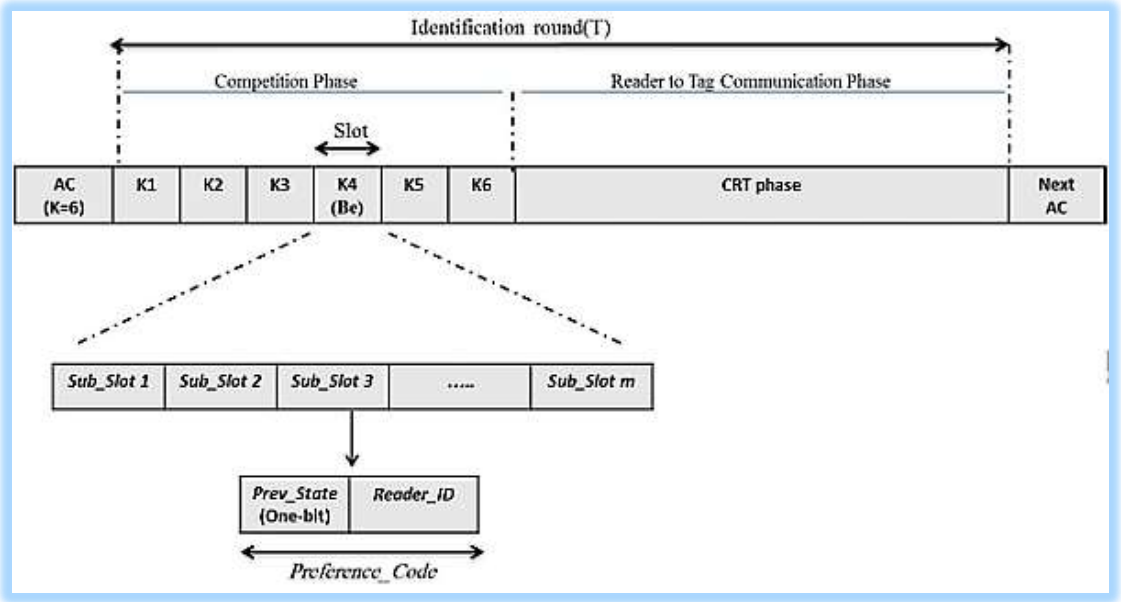


Figure 52:Illustration découpage d'un intervalle de temps en sous-slots

Scénario

Reconsidérons la figure 49 qui montre un exemple du protocole BACP pour un tour. Les lecteurs choisissent au hasard des intervalles de temps et des canaux de fréquence après l'envoi du message AC par le serveur central. Après la sélection, les lecteurs sont répartis dans les quatre catégories suivantes : canal 1 = {L3, L9, L4}, Canal 2 = {L1, L8}, Canal 3 = {L2, L7} et Canal 4 = {L5, L6}.

<table>
<tr><th>Envoi de balise (be)</th><th colspan="3">écoute de Collision (L)</th><th colspan="2">Code de préférence faible</th><th>Réécoute (L)</th><th>Attend prochain AC</th><th>Communication lecteur tag</th></tr>
<tr><td>Canaux</td><td>K=1</td><td>K=2</td><td>K=3</td><td>K=4</td><td>K=5</td><td>K=6</td><td colspan="3">Communication lecteur à tags</td></tr>
<tr><td rowspan="4">1</td><td>L3</td><td colspan="8">Lecteur L3 communique avec les tags</td></tr>
<tr><td></td><td></td><td>L9</td><td>L9</td><td colspan="5">Lecteur L9 communique avec les tags</td></tr>
<tr><td></td><td></td><td></td><td></td><td>L4</td><td colspan="4">Pas d'opération car le canal est occupé</td></tr>
<tr><td></td><td></td><td></td><td></td><td>L2</td><td>L2</td><td colspan="3">Lecteur L2 communique avec les tags</td></tr>
<tr><td rowspan="2">2</td><td></td><td>L1</td><td>L1</td><td></td><td></td><td></td><td colspan="3"></td></tr>
<tr><td></td><td>L8</td><td>L8</td><td colspan="6">Lecteur L8 communique avec les tags</td></tr>
<tr><td rowspan="3">3</td><td></td><td>L2</td><td></td><td></td><td colspan="6"></td></tr>
<tr><td></td><td></td><td></td><td>L1</td><td>L1</td><td colspan="4">Lecteur L1 communique avec les tags</td></tr>
<tr><td>L7</td><td colspan="8">Lecteur L7 communique avec les tags</td></tr>
<tr><td rowspan="3">4</td><td></td><td></td><td>L2</td><td>L2</td><td></td><td></td><td colspan="3"></td></tr>
<tr><td></td><td></td><td>L5</td><td>L5</td><td colspan="5">Lecteur L8 communique avec les tags</td></tr>
<tr><td></td><td></td><td>L6</td><td>L6</td><td colspan="5">Lecteur L8 communique avec les tags</td></tr>
</table>

Figure 53:Illustration d'un tour du protocole BACP

- ✓ Au début du premier intervalle de temps k=1, les lecteurs L3 et L7 envoient respectivement leur Preference_Code aux canaux de fréquence 1 et 3. Ensuite, ils écoutent le canal jusqu'à la fin du premier intervalle de temps, puisqu'ils ne reçoivent aucun Preference_Code des lecteurs voisins alors ils occupent le canal et commencer à lire les tags.
- ✓ Lorsque le deuxième intervalle de temps commence, les lecteurs L1, L8 et L2 écoutent le canal. Étant donné que le lecteur L7 lit les tags, le lecteur L2 comprend que le canal est occupé et calcule par conséquent sa distance au lecteur L7. Puis que le lecteur L2 se trouve dans la plage d'interférence du lecteur L7 et de plus la distance entre les deux lecteurs est supérieur à 2*drt alors L2 augmente son intervalle de temps d'une unité et sélectionne au hasard un autre canal (canal 4, k = 4).
- ✓ Après la fin du deuxième intervalle de temps k=2, les lecteurs L1 et L8 comparent les Préference_codes qu'ils ont reçus l'un de l'autre. Puis que le Preference_Code du lecteur L8 est plus grand, il occupe le canal (il est supposé que Prev_state de tous les lecteurs est zéro dans ce tour) et L2 va changer de canal. Il choisit au hasard le canal 3 et incrémente son intervalle de temps à k = 5.
- ✓ Au début du quatrième intervalle de temps, puis que dans le troisième intervalle de temps, les lecteurs L2, L5 et L6 ont identifié que le canal est libre. Ils commencent à envoyer leur Preference_Code dans les sous-slots sélectionnés. À la fin du quatrième intervalle de

temps, L2 compare les codes reçus de L5 et L6 avec son Preference_Code, comme son Preference_Code est plus petit. Le lecteur L5 compare également son Preference_Code avec les codes reçus. Comme L5 n'a reçu que le Preference_Code du lecteur L2 et que son code de préférence est plus grand que ce dernier, il parvient à accéder au canal, il va de même pour le lecteur L6.

Avantages:

- ✓ Le protocole BACP active plus de lecteurs en un tour, il utilise pleinement les ressources disponibles et les canaux de fréquence disponibles sont utilisés par les lecteurs.
- ✓ Dans le protocole BACP, aucun lecteur n'a besoin d'écouter continuellement le canal. Si le lecteur a sélectionné l'intervalle de temps k, il écoute uniquement le canal pendant l'intervalle de temps (k-1), cela permet de réduire la consommation d'énergie.
- ✓ L'évaluation de BACP avec les autres protocoles indiquent qu'il présente un bon débit. En raison du débit accru et de l'équité de BACP, le délai est réduit par rapport aux autres protocoles centralisés.

Inconvénients:

- ✓ Le choix aléatoire des intervalles de temps.
- ✓ Les intervalles de temps inutilisés.
- ✓ La priorité peut bloquer l'activation d'un nombre maximum de lecteurs.

Dans la suite nous allons faire une étude comparative des protocoles centralisés.

5.2.6.Étude comparative des protocoles de l'approches centralisés

La revue de la littérature prouve que les algorithmes centralisés sont plus efficace en termes de débit et d'équité par rapport aux algorithmes décentralisés. Les protocoles centralisés sont principalement basées sur TDMA ou FDMA. Le tableau 4 suivant permet de résumer les caractéristiques de ces protocoles.

	NFRA	NFRA_C	GDRA	DRCA	BACP
Collision lecteur-	oui	oui	oui	oui	oui
Collision lecteur-tag	oui		oui	oui	oui
Centralisée	oui	oui	oui	oui	oui
Multi canal			oui	oui	oui
Utilisation canal de contrôle					
Gérant la mobilité	oui	oui	oui	oui	oui
Basé sur FDMA			oui	oui	oui
Basé sur TDMA	oui	oui	oui	oui	oui
Basé sur CSMA	oui				

Tableau 4:Récapitulation des caractéristiques des protocoles d'anticollision centralisés lecteur-lecteur

Dans la Figure 54 où les protocoles centralisés sont illustrés, nous remarquons que les performances en matière de délai de couverture sont faibles pour l'ensemble de cette famille. Cela est dû au fait que ces derniers nécessitent généralement une phase de collecte d'informations avant l'attribution des intervalles de temps de fonctionnement, ce qui a tendance à rajouter un surcoût en matière de latence. Pour l'ensemble des protocoles, la consommation d'énergie est importante à cause de la latence et du haut débit utilisé en générale par cette famille de protocole.

Les protocoles de type NFRA, GDRA ou DRCA sont également impactés par le fait qu'un grand nombre de collisions enregistrées désactive un grand nombre de lecteurs ce qui par conséquent augmente le délai de couverture des tags à porter et réduit considérablement l'index d'équité de Jain. Le protocole NFRA utilise un seul canal de données comme Dica, et il ne mentionne pas comment les collisions entre les tags sont détectées par les lecteurs.

Les collisions de lecteur à lecteur, les phénomènes de canal inutilisés, de délai de coordination longue et la consommation accrue d'énergie entravent encore les propositions de performance des protocoles de cette famille. De plus, la dépendance des lecteurs au serveur central rend ces solutions moins réactives.

Par contre cette famille de protocole a réglé le problème de débit, d'équité et même de collision dont souffre la famille décentralisée. De plus, la famille centralisée permet de régler parfois les deux types de collisions : lecteur-lecteur et lecteur-tag, chose que la famille décentralisée n'a pas pu gérer. Ces différents facteurs nous amène à travailler avec cette famille de protocole dans le but d'améliorer l'un des plus récents protocoles de cette famille qui montre plus de performance que les autres protocoles de la famille.

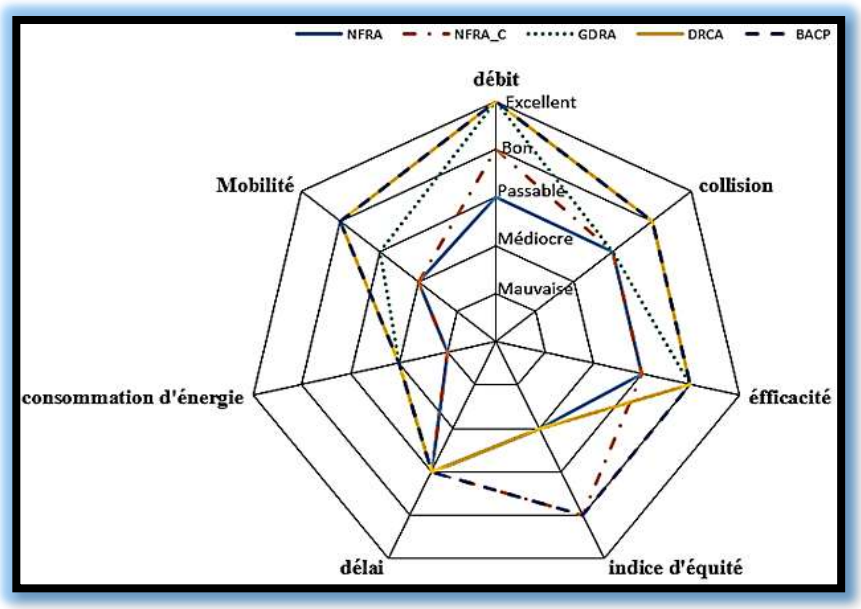


Figure 54:évaluation des performances des protocoles centraliser

Dans la suite, nous allons faire une étude comparative des deux approches. Nous remarquons généralement que :

- ✓ plus le débit est moins élevé plus nous notons des collisions qui entraîne une longue latence ;
- ✓ le débit d'un réseau mobile est inférieur à celui d'un réseau statique, car les lecteurs doivent s'adapter à l'évolution des voisinages ;
- ✓ un protocole qui fonctionne bien en matière de délai de couverture et d'équité, interroge les tags plus rapidement, car plus les lecteurs sont activés avec succès plus ils lisent les tags à portée. Ainsi le délai de couverture et l'équité donnent un avantage dans le cas des scénarios dynamiques avec lecteurs et/ou tags mobiles. Relativement, les performances en matière de débit de lecture, de collisions et d'efficacité donnent une idée des performances du protocole dans les environnements de déploiement de lecteurs denses ;
- ✓ l'introduction de la priorité dans les algorithmes augmente l'équité des protocoles.

Ainsi, le choix d'un protocole ou d'un autre se fait en fonction des contraintes en matière de débit de lecture, de collision ou de délai de couverture de l'application. Une solution maximisant l'ensemble des métriques n'est malheureusement pas disponible au vu de l'état actuel des propositions faites dans la littérature. Nous recommandons des protocoles qui peuvent s'adapter suivant les types d'applications.

6.1. Choix d'un protocole dans le système RFID

Pour guider le choix d'un protocole ou d'un autre en fonction des contraintes de déploiement et de performances. Nous allons cibler certaines applications les plus utilisées dans les RFID pour indiquer des protocoles qui pourront être adéquat pour ces dernières.

- ✓ Pour les **applications de surveillance** de plusieurs cartons dans un entrepôt avec des lecteurs RFID fixés aux murs. Les produits doivent être rapidement identifiés et traités pour éviter les pertes. Nous pouvons utiliser les protocoles DiMCA, EDMC, DRCA et BACP pour cette application car ils fonctionnent dans des conditions de déploiement denses de lecteurs avec sensibilité du délai.
- ✓ Les **applications mobiles** (montés sur des chariots élévateurs ou portatifs par des travailleurs ou un port avec des lecteurs fixés au sol et des tags rattachés aux conteneurs) peuvent utiliser le protocole MALICO et BACP car ils montrent les meilleures performances dans les déploiements mobiles, par contre nécessite une amélioration du délai de couverture.
- ✓ Les applications de **surveillance RFID pour l'agriculture**, les lecteurs ne nécessitant pas une surveillance constante d'humidité et de la température avec des données non sensibles et un déploiement dense de lecteurs. Colorwave est plus adapté comme solution. Par contre si les lecteurs sont rattachés aux agriculteurs ou à leurs moissonneuses-batteuses mobiles. Dans ce cas Pulse pourrait être mise en œuvre.

Le tableau 7 nous permet de récapituler les protocoles qui vont avec les types d'applications qui y sont énumérées:

Type d'applications	applications de surveillance de plusieurs cartons	applications avec mobilité	surveillance RFID pour l'agriculture
Protocole adopté	DiMCA, EDMC, DRCA et BACP	MALICO et BACP	Colorwave et Pulse

Tableau 5:récapitulatifs des protocoles recommandés

Conclusion

Le problème des collisions en RFID demeure un souci important dans la mise en place de solutions basées sur la technologie. En effet, les erreurs de lecture peuvent se prouver critiques en fonction de l'application entraînant des dégâts matériels, financiers, voire humains. Il est donc nécessaire d'y remédier. Les nombreuses solutions proposées dans l'état de l'art parviennent toutes

à réduire les collisions tant bien que mal en utilisant des mécanismes différents. Toutefois, en fonction des contraintes de déploiements des dispositifs (lecteurs et/ou tags) et des exigences des applications, les performances des algorithmes varient grandement, pouvant guider vers le choix d'un algorithme ou d'un autre. Une solution utilisable, quelles que soient les conditions aurait certes été une aubaine, mais malheureusement, compte tenu de l'état de l'art actuel, cela est difficilement concevable.

En sommes dans ce chapitre, nous avons fait une analyse profonde des protocoles. En effet, pour se faire nous avons donné une comparaison des différents protocoles suivant les métriques : débit, équité, collision, efficacité, mobilité, consommation d'énergie. Enfin nous avons terminé le chapitre en montrant le choix des protocoles dans différents types d'applications RFID.

Dans la suite, nous allons nous focaliser sur le protocole BACP+ qui est à la base de notre contribution.

Chapitre 3

Contribution: Called Beacon Analysis-based Collision Prevention more (BACP+)

Dans le chapitre précédent, nous avons étudié les protocoles d'anticollision qui sont classés en deux grandes catégories: décentralisés et centralisés. Pour chaque classe nous avons fait une comparaison entre protocoles suivant les paramètres et métriques d'évaluation. Dans cette même lancée nous avons vu que la famille centralisée a été mise en place pour régler le problème d'insuffisance de calcul et de débit dont soufrent les protocoles décentralisé. Le protocole BACP est l'un des protocoles les plus performants de la famille centralisée. Par contre il montre des insuffisances liées au délai et aux pertes d'intervalles de temps.

Nous allons montrer comment le protocole BACP a résolu la perte de canal dans DRCA par la priorité. Par la suite nous verrons les problèmes de BACP, liés à la gestion des collisions qui se traduit très tard et à la surcharge des canaux à la fin de l'AC. Ainsi, nous allons présenter une solution qui va améliorer BACP, nommée BACP+ et va permettre d'améliorer la gestion des collisions, d'éviter les pertes de canaux notées aussi dans BACP, de diminuer également le temps d'un cycle de lecture et qui permet d'activer plus de lecteur dans un cycle de lectures.

1. Description du protocole BACP

Le protocole BACP que nous avons étudié dans le chapitre 2 section 5.2.5 est récent. En effet, il permet d'activer beaucoup de lecteurs en un tour. Il utilise les ressources disponibles comme les canaux et intervalle de temps disponibles. De ce fait, les lecteurs choisissent aléatoirement un canal parmi les quatre disponibles et un time-slot entre 1 et 128. La durée des intervalles de temps est 5 ms. Ainsi en étudiant de près ce protocole, nous décelons des points d'amélioration qui peuvent rendre ce protocole plus performant.

1.1. Les limites du protocole BACP

Le choix aléatoire des intervalles de temps constitue un véritable problème pour BACP. En effet, à chaque fois que les lecteurs ont la possibilité d'avoir un nouveau canal, cela signifie que la probabilité d'interférence dans les intervalles de temps les plus élevés augmente et éventuellement, plus de lecteurs sont inactifs. Cela est dû à l'utilisation de la fonction sift [40] définie par $\boldsymbol{pk = \delta * \frac{1}{\alpha^k}}$ par ce protocole. Cette fonction permet de sélectionner avec une forte probabilité des intervalles de temps supérieurs: $\boldsymbol{\delta = \frac{(1-\alpha)+\alpha^k}{1-\alpha^k}}$ où α est une constante comprise entre 0 et 1 et δ une constante calculable où K est le nombre de intervalle de temps et k prend ces valeurs entre 1 et K.

Par ailleurs, ce protocole rencontre plusieurs problèmes qui sont :

- ✓ si la zone de lecture de deux lecteurs sont en interférence alors ces lecteurs devront attendre le prochain AC s'ils ont choisi le même slot;
- ✓ si la zone de couverture de deux lecteurs se chevauche alors le lecteur le plus prioritaire va garder le canal et l'autre va changer de canal dans le time-slot suivant. Par contre, si la collision se passe dans les intervalles de temps élevés alors les lecteurs risquent d'attendre le prochain tour ;
- ✓ l'application de l'équité pour des lecteurs qui se trouvent dans le même canal et le même *time-slot,* peut réduire la chance de lire plusieurs lecteurs dans ce time-slot. Par exemple dans le canal 4 de la figure 55, si L2 étais plus prioritaire que L5 et L6 alors ces derniers devront lui laisser le canal. Dans ce cas nous perdons deux lectures à faveur d'une seule lecture.
- ✓ Le délai est long car les lecteurs n'ont pas commencé leurs interrogations très tôt.

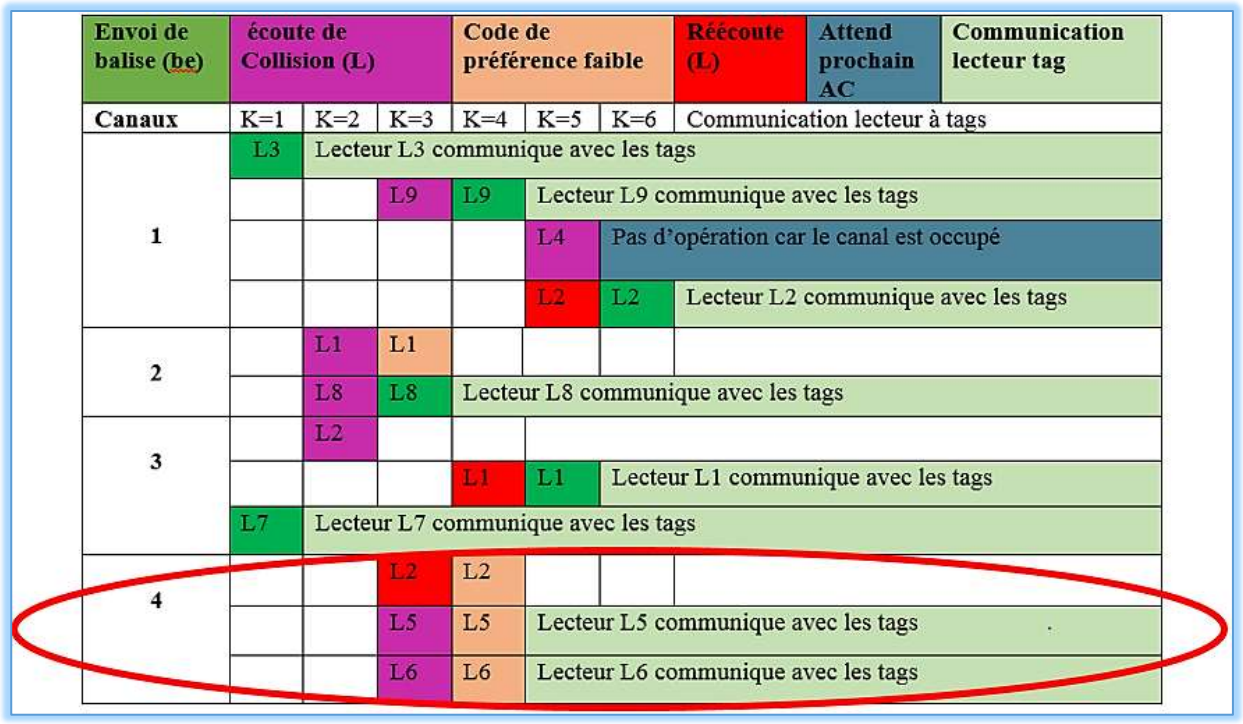


Figure 55:problèmes de collisions dans BACP

Ainsi nous avons fait une petite description du protocole BACP, qui est un protocole centralisé avec quatre canaux de fréquence et k intervalle de temps, k compris entre 16 à 128. Enfin, nous avons montré les limites du protocole BACP. Les limites notées dans cette section permettent d'améliorer les performances du protocole BACP. Ainsi, dans la section suivante, nous allons montrer des possibilités d'améliorations du BACP.

2. Description du BACP+

Ce protocole a pour objectif principal d'optimiser les ressources utilisées et perdues par le protocole BACP. Il utilise comme BACP la technique de TDMA/ FDMA à base de balises en minimisant les risques d'interférence mais augmente le nombre de lecteurs actifs dans un cycle de lecture. De plus, ce protocole n'impose aucun matériel supplémentaire par rapport à BACP. Ce protocole est appelé **Beacon Analysis-based Collision Prevention more** (**BACP+**) permet d'augmenter les lectures et de réduire par conséquent la durée d'un cycle.

Afin de mieux décrire BACP+, nous reprenons l'illustration de BACP donné la section 5.2.5.

2.1. Résoudre les slots de temps perdus

Dans BACP tous les lecteurs choisissent aléatoirement un *time-slot*, ensuite l'algorithme BCAP va être déroulé pour voir s'il y'a des lecteurs qui interfèrent. Si tel est le cas alors ces lecteurs vont choisir aléatoirement des sous-slots de temps parmi les 16 disponibles dans le même slot. Ensuite

ils vont comparer leur préférence-code. Celui qui a le plus grande préference-code va garder le canal et les autres vont changer de canal et les intervalles de temps seront augmentés de 1. On constate que cela peut engendrer des intervalles de temps vides au début et d'autres surchargés car il se peut qu'aucun lecteur ne choisisse les slot de début dans la mesure où le choix se fait de manière aléatoire.

Pour remédier à cela, nous proposons dans BACP+ de régler très tôt les collisions de lecteurs. Dans ce cas tous les lecteurs doivent commencer à envoyer leur balise à k=1 dans le but de solder le réseau. S'il se trouve qu'un lecteur est en collision avec un ou des lecteurs alors ils comparent leur préference-code et celui qui en a le plus grand va lire les tags et les autres vont incrémenter leur time-slot de 1. Ainsi on voit bien que tous les intervalles de temps seront occupés. La figure 56 montre les slots de temps perdu dans BACP.

Figure 56:intervalle de temps perdu dans BACP

Dans BCAP+ tous les lecteurs vont tenter de communiquer à l'intervalle de temps k=1 pour éviter les perdus d'intervalles de temps, évidement il peut y avoir plusieurs collisions au début de l'intervalle temps mais elles seront réglées au fur et à mesure dans le tour comme dans la section 2.

2.2. Choisir un lecteur en cas de slot partagé dans une interférence de zones de lecture

Dans BCAP si plusieurs lecteurs ont choisi le canal et le même time-slot tel que la distance entre les lecteurs soit inférieure à 2 fois drt comme le cas de L4 et L9 dans la figure 57, alors ces lecteurs devront attendre le tour suivant et le canal est perdu car s'ils communiquent alors la réponse d'un tag peut amener une collision de lecteur-tag.

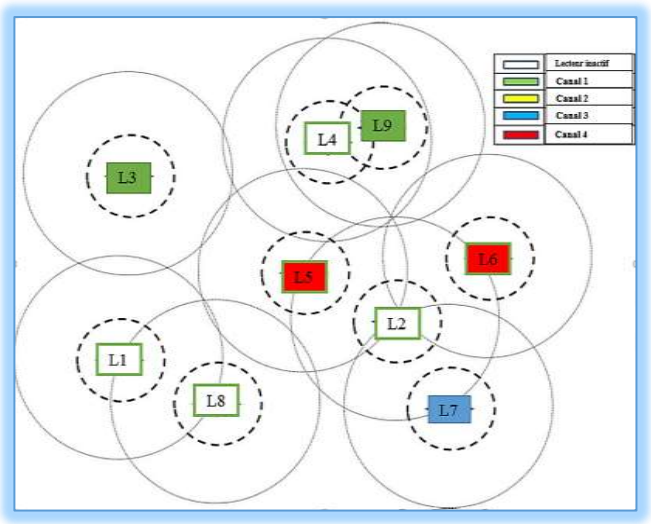


Figure 57 : Disposition de lecteurs dans l'espace

Ainsi dans notre solution BACP+ pour ne pas perdre le canal, nous allons comparer le preference_code des deux lecteurs, le plus prioritaire va garder le canal et l'autre attend le prochain AC pour ne pas brouiller la lecture du lecteur prioritaire comme s'est géré pour le cas de L4 et de L9 dans la figure 58 (b).

2.3. Ramener les éventuelles collisions vers les débuts de rounds

Dans BACP les collisions dans les slots supérieur sont fréquentes et cela fait que certains des lecteurs ne parviennent pas à être actifs dans le tour. Par exemple les lecteurs L2 et L4 ont choisi le dernier slot de temps k=6 comme le montre la figure 56. Donc si toute fois le lecteur L2 ne parvenait pas à lire alors il allait attendre le prochain AC. Cela pose des problèmes de lecteurs inactifs dans un cycle de lecture.

Ainsi, nous choisissons de communiquer très tôt en fixant au début du cycle k=1 pour tous les lecteurs comme dans la section 2.1 ci-dessus. De ce fait, L2 est parvenu à lire très tôt à k=3. Donc ce problème ne se pose pas dans BACP+ car les collisions sont réglées très tôt à cause du k que nous avons fixé au début de slot comme le montre la figure 58.

2.4. Activer un nombre maximum de lecteurs

Dans le BACP la priorité prime et remporte toujours le conflit à chaque fois qu'il y'a plusieurs lecteurs qui peuvent interférer dans un même canal et un même time-slot. Alors que l'objectif fixé par ces protocoles d'anticollisions est d'activer plus de lecteurs que possible dans un cycle de lecture et cette occasion est ratée si l'on prend le cas de L2, L5 et de L6 dans le canal 4 de la figure 55. Si L2 étais plus prioritaire que L5 et L6 alors les deux allaient abandonnés le canal et seule L2 va

l'occuper. Ainsi on perdrait deux activations en faveur de l'activation de lecteur L2. Donc c'est une insuffisance qui pourra trouver un mécanisme pour activer L5 et L6. Cela amènera L2 à changer de canal. De ce fait, le nombre de lecteurs activés l'emportera sur la priorité.

2.5. Faire un compromis entre la densité des lecteurs et le nombre de intervalle de temps

Si la densité des lecteurs est très élevée alors on aura beaucoup de collision dans les intervalles de temps. Ainsi, on peut prévoir une solution qui va faire un compromis entre les intervalles de temps et le nombre de lecteurs. Cela permettra de diminuer les collisions dans les intervalles de temps ainsi que le temps du cycle.

3. Exemple d'exécution de BACP+

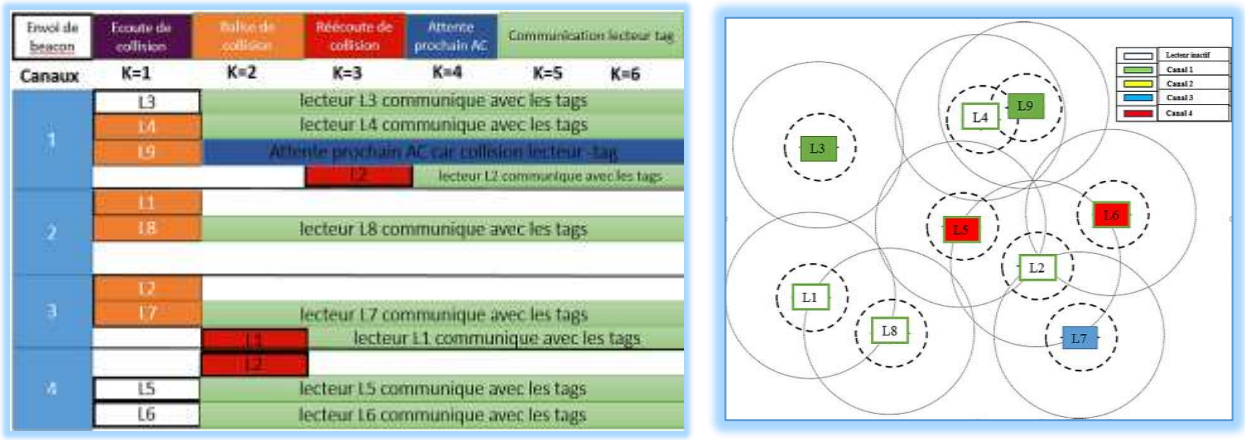
Nous reprenons le même scénario que dans le BACP pour afin faire une comparaison de gestion des collisions entre BACP et BACP+ dans un tour de lecture.
Les lecteurs choisissent au hasard des canaux de fréquence après l'envoi du message AC par le serveur central figure 58 (a). Après la sélection des canaux, les lecteurs sont répartis ainsi au hasard: Canal 1 = {L3, L9, L4}, Canal 2 = {L1, L8}, Canal 3 = {L2, L7} et Canal 4 = {L5, L6}.

Au début du premier time-slot (k=1) tous les lecteurs envoient leur preference_code respectivement dans leurs canaux contrairement à BCAP où les intervalles de temps choisis aléatoirement. Puis les lecteurs écoutent le canal jusqu'à la fin du time-slot k=1 et puisqu'ils ne reçoivent aucun preference_code des lecteurs voisins. Alors les lecteurs L3, L5 et L6 vont lire les tags respectivement dans leurs canaux.

Au canal 3, L2 et L7 s'interfèrent car s'entendent l'un à l'autre, puisque la distance entre les deux lecteurs est supérieure à 2 fois le rayon de lecture des lecteurs (drt). Ils comparent leur préference_code et comme L7 est plus prioritaire alors il va garder le canal et L2 va changer de canal en incrémentant son time-slot à 1.

Au canal 1, L4 et L9 s'interfèrent et dans BACP les deux lecteurs allaient entendre la prochaine AC (c'est-à-dire e prochain tour) car si la distance entre les deux lecteurs est inférieure à 2 fois drt. Donc, il n'y a pas de possibilité pour que les deux lecteurs communiquent avec les tags, même s'ils sont dans des canaux différents car une collision au niveau des tags sera notée et bloquera ainsi la communication de L4 et L9. C'est pourquoi, dans BCAP+ par soucis de perdre le canal, l'un des lecteurs va garder le canal. Les lecteurs L4 et L9 comparent leurs préference_code et puisque L9 est

plus prioritaire alors il va garder le canal et L4 va attendre le prochain tour (prochain AC). Le même processus est répété dans les intervalle de temps suivant.



(a) ***Figure 58: Illustration d'un tour du protocole BACP+*** *(b)*

Dans [40], il est démontré que selon la fonction Sift, la probabilité de collisions dans les slots supérieurs est plus élevée que dans les slots inférieurs. Ainsi, il est clair que BACP+ diminue significativement la probabilité d'interférence dans les intervalles de temps les plus élevés. Toutefois, le fait de ramener les tentatives de lecture de tous les lecteurs au début du round augmente la probabilité de collisions à ce début de round. Mais ces collisions auront l'avantage par rapport à BACP, d'être résolues dans les intervalles de temps suivants et avant la fin du round. Ce qui, par ailleurs pourrait réduire la durée d'un round. De surcroît, BACP+ pourrait dans certains cas, réduire également les intervalle de temps inutilisés ou activer le maximum de lecteurs dans un tour de lecteur comme nous le démontrerons dans 4.2.

4. Analyse et évaluation

Dans cette section nous procédons à l'analyse de BACP+ par rapport à BACP afin de déterminer et de justifier son efficacité. Pour ce faire, nous utilisons en premier lieu, le débit comme métrique de comparaison. Par la suite, nous essayerons de trouver un critère qui permettra de les évaluer dans des environnements de déploiement ou de dissimulation.

4.1. Comparaison des débits de lecture

Dans le scénario de la section 3, on peut constater que BACP+ augmente le débit de lecture par rapport à BACP. Ceci est globalement dû à l'exploitation des slots libres au départ qui permettra à tous les lecteurs de compétir pendant la phase de contention et éviter l'encombrement vers la fin du round qui oblige certains lecteurs à attendre le prochain AC au cas où ils ne gagnent pas le canal.

Si on sait que le temps d'un time slot est de 5ms et que la période de lecture des lecteurs sur les tags est de 0,46s, on peut quantifier le débit d de lecture de chaque solution en fonction du débit de lecture d'un lecteur par ms à l'aide de la formule ci-dessous : **D= d (T_slot * N_slot + T_com).**

D : débit de lecture d'un lecteur ;

d: débiter quantifier d'une solution (BACP ou BACP+) ;

T_slot : durée d'un intervalle de temps, elle est égale à 0,46s ;

N_slot : nombre d'intervalle de temps occupé par lecteur dans sa communication

T_com : durée de communication entre lecteur et tags.

Ainsi nous déterminons pour BACP et BACP+ le débit total de lecture :

- ✓ Pour BACP :
  - ✓ Débit du lecteur L5 : d (5.10-3 *5+ 0,46)= 0,485d bits/s ;
  - ✓ Débit du lecteur L6 : d (5.10-3 *3+ 0,46)= 0,475d bits/s ;
  - ✓ Débit du lecteur L7 : d (5.10-3 *0 + 0,46)= 0,46d bits/s ;
  - ✓ Débit du lecteur L1 : d (5.10-3 *3+ 0,46)= 0,475d bits/s ;
  - ✓ Débit du lecteur L2 : d (5.10-3 *3+ 0,46)= 0,475d bits/s ;
  - ✓ Débit du lecteur L3 : d (5.10-3 *3+ 0,46)= 0,475d bits/s ;
  - ✓ Débit du lecteur L4 : d (5.10-3 *5+ 0,46)= 0,485d bits/s ;
  - ✓ Débit du lecteur L9 : d (5.10-3 *1+ 0,46)= 0,466d bits/s ;
  - ✓ Débit du lecteur L8 : d (5.10-3 *2+ 0,46)= 0,47 d bits/s.

Donc le débit total de lecture dans BACP est égale à la somme des débits de lecture soit 4,266d bits/S.

- ✓ Pour BACP+ :
  - ✓ Débit du lecteur L5 : d (5.10-3 *5+ 0,46)= 0,485d bits/s
  - ✓ Débit du lecteur L6 : d (5.10-3 *5+ 0,46)= 0,485d bits/s
  - ✓ Débit du lecteur L7 : d (5.10-3 *5+ 0,46)= 0,485d bits/s
  - ✓ Débit du lecteur L1 : d (5.10-3 *5+ 0,46)= 0,485d bits/s
  - ✓ Débit du lecteur L2 : d (5.10-3 *5+ 0,46)= 0,485d bits/s
  - ✓ Débit du lecteur L3 : d (5.10-3 *5+ 0,46)= 0,485d bits/s
  - ✓ Débit du lecteur L4 : d (5.10-3 *5+ 0,46)= 0,485d bits/s

- ✓ Débit du lecteur L9 : d (5.10-3 *5+ 0,46)= 0,485d bits/s
- ✓ Débit du lecteur L8 : d (5.10-3 *5+ 0,46)= 0,485d bits/s

Donc le débit total de lecture dans BACP+ est égale à la somme des débits de lecture soit 4,365d bits/S. Ceci est obtenu par cette formule $\sum_{L=1}^{n} D$ avec n le nombre de lecteurs.

On peut constater en particulier que pour le scénario de la section 4.2.1 ci-dessous , le débit de BACP+ est supérieur de 0,099d bits/s à celui de BACP. De même, il a été constaté que le débit du BACP+ reste supérieur à celui du BACP dans les autres scénarios de la section 4.2.2 et 4.2.3.

4.2. Critère d'évaluation

Au delà du scénario (section 3) certes aléatoire mais par lequel, il reste insuffisant de décrire tout le comportement de BACP et BACP+ et de comparer leurs performances, nous avons jugé nécessaire de trouver des critères selon lesquels les performances de BACP et de BACP+ pourront être évaluées de façon consistante et pertinente.

4.2.1. Canaux sans interférence

Dans cette section, nous essayons de mettre en œuvre l'effet de déploiement des lecteurs sans interférence à travers les figures 60 et 61 afin de mesurer le comportement des deux solutions.

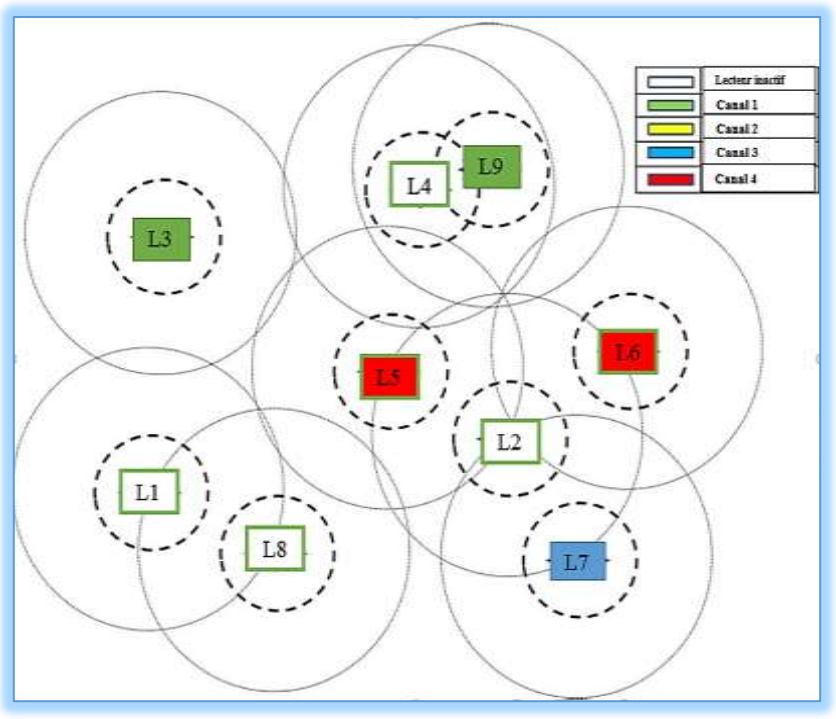


Figure 59 : Choix des canaux sans interférence avec BACP

Les lecteurs ont choisi aléatoirement des canaux comme suit :

Canal 1 = {L5, L6, L7}, Canal 2 = {L1, L2}, Canal 3 = {L3, L4} et Canal 4 = {L8, L9}.

Envoi de balise (be)	écoute de Collision (L)			Code de préférence faible			Réécoute (L)	Attend prochain AC	Communication lecteur tag
Canaux	K=1	K=2	K=3	K=4	K=5	K=6	Communication lecteur à tags		
1	L5	Lecteur L5 communique avec les tags							
			L6	L6	Lecteur L6 communique avec les tags				
					L7	L7	Lecteur L7 communique avec les tags		
2		L1	L1	Lecteur L1 communique avec les tags					
		L2	L2	Lecteur L2 communique avec les tags					
3		L3	L3	Lecteur L3 communique avec les tags					
	L4	Lecteur L7 communique avec les tags							
4				L9	L9	Lecteur L9 communique avec les tags			
			L8	L8	Lecteur L8 communique avec les tags				

Figure 60 : Choix des canaux sans interférence avec BACP

Envoi de balise (be)	écoute de Collision (L)			Code de préférence faible			Réécoute (L)	Attend prochain AC	Communication lecteur tag
Canaux	K=1	K=2	K=3	K=4	K=5	K=6	Communication lecteur à tags		
1	L5	Lecteur L5 communique avec les tags							
	L6	Lecteur L6 communique avec les tags							
	L7	Lecteur L7 communique avec les tags							
2	L1	Lecteur L1 communique avec les tags							
	L2	Lecteur L2 communique avec les tags							
3	L3	Lecteur L3 communique avec les tags							
	L4	Lecteur L7 communique avec les tags							
4	L9	Lecteur L9 communique avec les tags							
	L6	Lecteur L6 communique avec les tags							

Figure 61 : Choix des canaux sans interférence avec BACP+

Si le choix des canaux est tel qu'il n'est pas d'interférence alors BACP+ est plus performant que BACP car au début de slot tous les lecteurs ont lit sans collision. Cela contribue à diminuer le temps de cycle par rapport à celui du protocole BACP. Certes nous constatons qu'il y'a pas de collision de part et d'autres des deux protocoles mais en terme de délai de cycle nous constatons que BACP+ prend moins de temps que BACP. Cela est dû par le choix aléatoire des intervalles de temps dans BCAP. Ainsi nous avons un débit de lecture de **98,98% dans BACP+** et **96,73% dans BACP**. Ces pourcentages ont été obtenu par cette formule : $\% = \frac{\sum_{L=1}^{n} D \ X \ 100}{(D_{total}BACP+) \ + T\_l\_slot}$ avec

D_{total}BACP+ : le débit total de BACP+ ;

T_l_slot = **T_slot * nombre de lecteurs**.

Cette non-interférence de lecteurs se retrouve aussi dans les situations de très faible densité où la distance inter-lecteurs est supérieure à 2*(rayon de lecture).

Ainsi la règle 1 stipule qu'en situation de non-interférence des lecteurs, la durée d'un round est plus petite dans BACP+ que dans BACP.

4.2.2. Densité sans mobilité

Ici, nous essayons de mettre en œuvre la densité des lecteurs pour justifier le rendement des solutions. On constate que la tendance est globalement la même i.e. on a moins de lecture dans toutes les deux solutions. Cependant, dans les situations de forte densité où les zones de lecture de plusieurs lecteurs se chevauchent, comme le montre l'illustration des figures 63 et 64, BACP+ présente un débit de lecture meilleur que BACP. En effet, dans de telles circonstances, BACP empêche l'activation de tous ces lecteurs interférants alors que BACP+ choisit parmi ces lecteurs ceux qui pourront rester, ce qui augmente le taux de lecture dans BACP+.

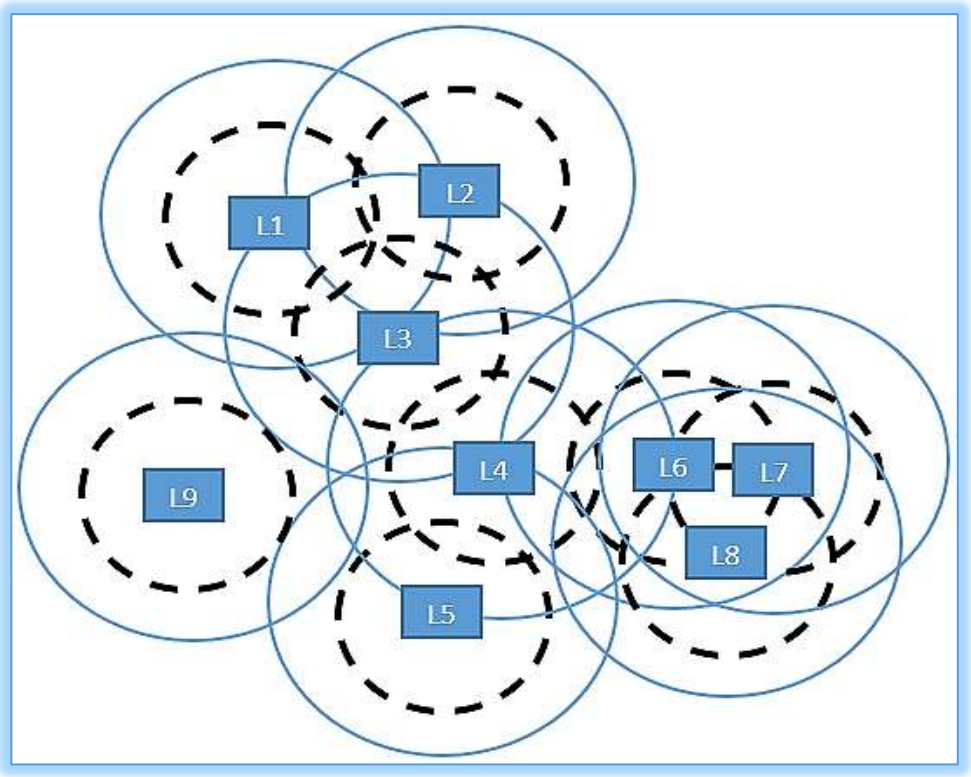


Figure 62 : environnement dense de lecteurs

Apres choix aléatoire des canaux les lecteurs sont répartis comme suit :

Canal 1 = {L6, L7, L8}, Canal 2 = {L1, L2}, Canal 3 = {L3, L4} et Canal 4 = {L5, L9}.

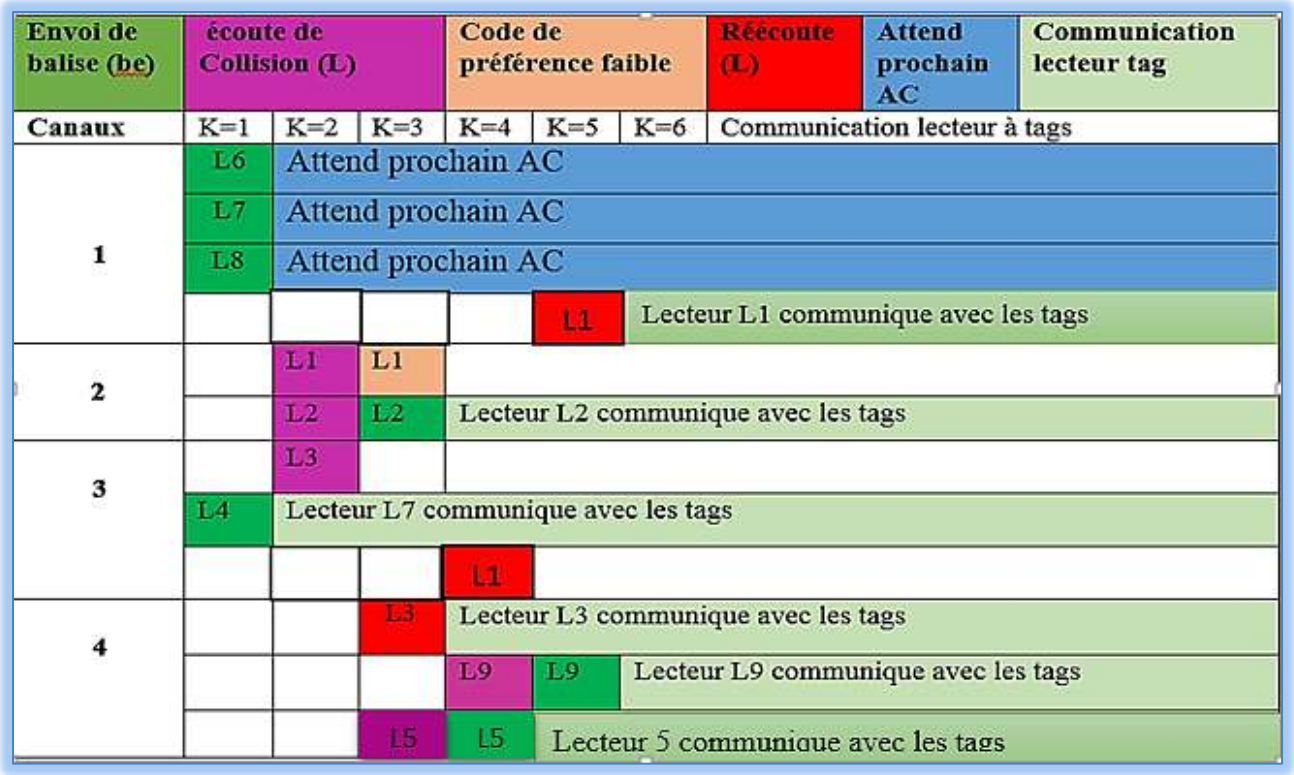


Figure 63 : densité sans mobilité des lecteurs avec BACP

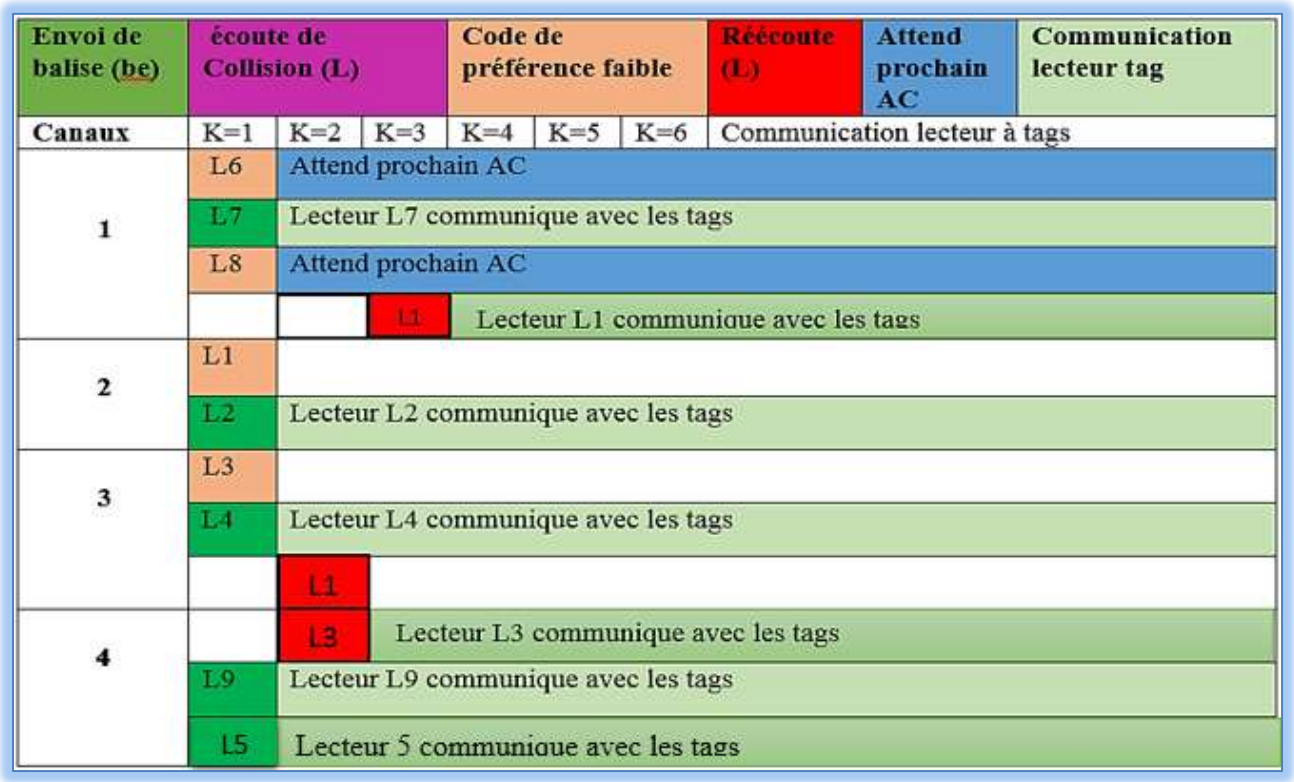


Figure 64 : densité sans mobilité des lecteurs avec BACP+

Ainsi la règle 2 stipule que si le système est dense alors BACP+ active plus de lecteurs que BACP avec un temps inférieur à celui du BACP.

Ainsi nous déterminons pour BACP et BACP+ le débit total de lecture :

- ✓ Pour BACP+ :
  - ✓ Débit du lecteur L5 : d (5.10-3 *5+ 0,46)= 0,485d bits/s ;
  - ✓ Débit du lecteur L6 =0 ;
  - ✓ Débit du lecteur L7 : d (5.10-3 *5 + 0,46)= 0,485d bits/s ;
  - ✓ Débit du lecteur L1 : d (5.10-3 *3+ 0,46)= 0,475d bits/s ;
  - ✓ Débit du lecteur L2 : d (5.10-3 *5+ 0,46)= 0,485d bits/s ;
  - ✓ Débit du lecteur L3 : d (5.10-3 *3+ 0,46)= 0,475d bits/s ;
  - ✓ Débit du lecteur L4 : d (5.10-3 *5+ 0,46)= 0,485d bits/s ;
  - ✓ Débit du lecteur L9 : d (5.10-3 *5+ 0,46)= 0,485d bits/s ;
  - ✓ Débit du lecteur L8 = 0.

Donc le débit total de lecture dans BACP est égale à la somme des débits de lecture soit 2,9d bits/S.

- ✓ Pour BACP :
  - ✓ Débit du lecteur L5 : d (5.10-3 *2+ 0,46)= 0,47d bits/s
  - ✓ Débit du lecteur L6 =0
  - ✓ Débit du lecteur L7 =0
  - ✓ Débit du lecteur L1 : d (5.10-3 *1+ 0,46)= 0,466d bits/s
  - ✓ Débit du lecteur L2 : d (5.10-3 *3+ 0,46)= 0,475d bits/s
  - ✓ Débit du lecteur L3 : d (5.10-3 *3+ 0,46)= 0,475d bits/s
  - ✓ Débit du lecteur L4 : d (5.10-3 *5+ 0,46)= 0,485d bits/s
  - ✓ Débit du lecteur L9 : d (5.10-3 *1+ 0,46)= 0,466d bits/s
  - ✓ Débit du lecteur L8 =0

Donc le débit total de lecture dans BACP est égale à la somme des débits de lecture soit 2,837d bits/S.

Nous pouvons constater en particulier que dans ce scénario, le débit de BACP+ est supérieur de 0,063d bits/s à celui de BACP. Ainsi nous avons un débit de lecture de **98,47% dans BACP+** et **96,33% dans BACP**.

4.2.3. Densité avec mobilité

Ici, nous tentons de mettre en œuvre la mobilité des lecteurs pour justifier le rendement des solutions. On constate que la tendance est globalement la même car il y'a beaucoup de lecteurs qui attendent le prochain AC. Cependant, dans les situations de forte mobilité où les zones de lecture de plusieurs lecteurs se chevauchent, comme le montre l'illustration la figure 65, BACP+ présente un débit de lecture meilleur que BACP. En effet, dans de telles circonstances, BACP empêche l'activation de tous ces lecteurs interferants, alors que BACP+, choisit un parmi ces lecteurs.

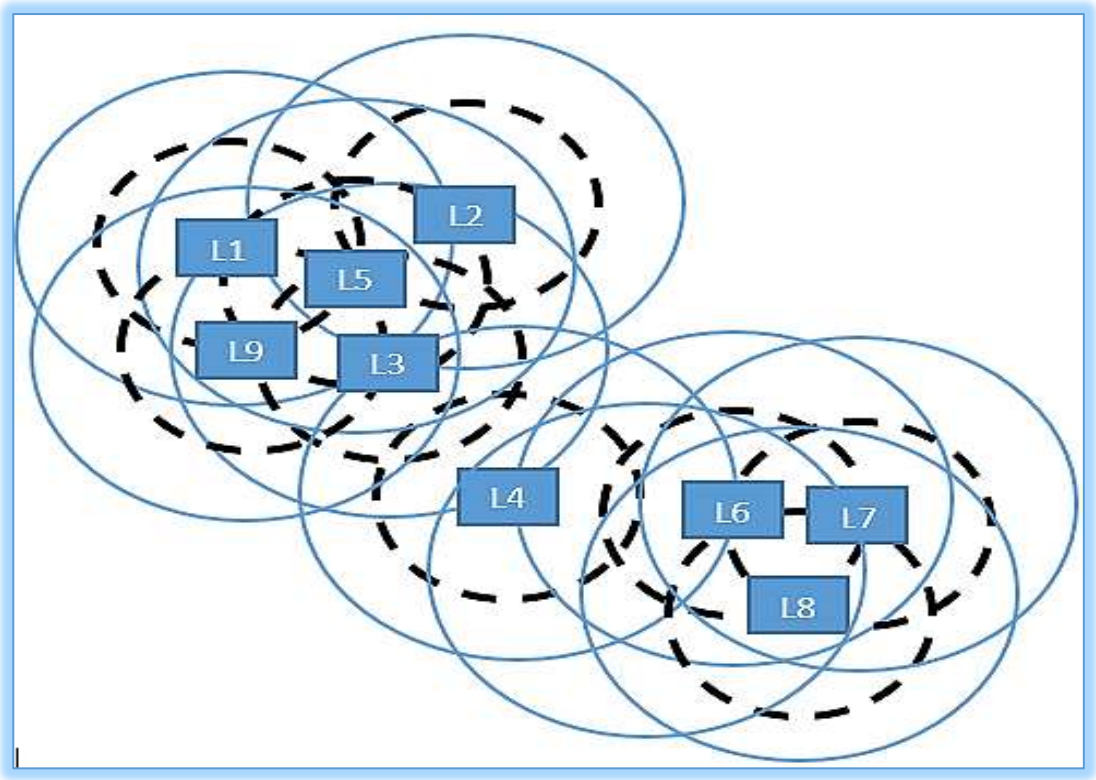


Figure 65 : environnement dense avec mobilité des lecteurs

Apres choix aléatoire des canaux les lecteurs sont répartis comme suit :

Canal 1 = {L9, L5, L1, L2}, Canal 2 = {L3, L4}, Canal 3 = {L6, L7} et Canal 4 = {L8}

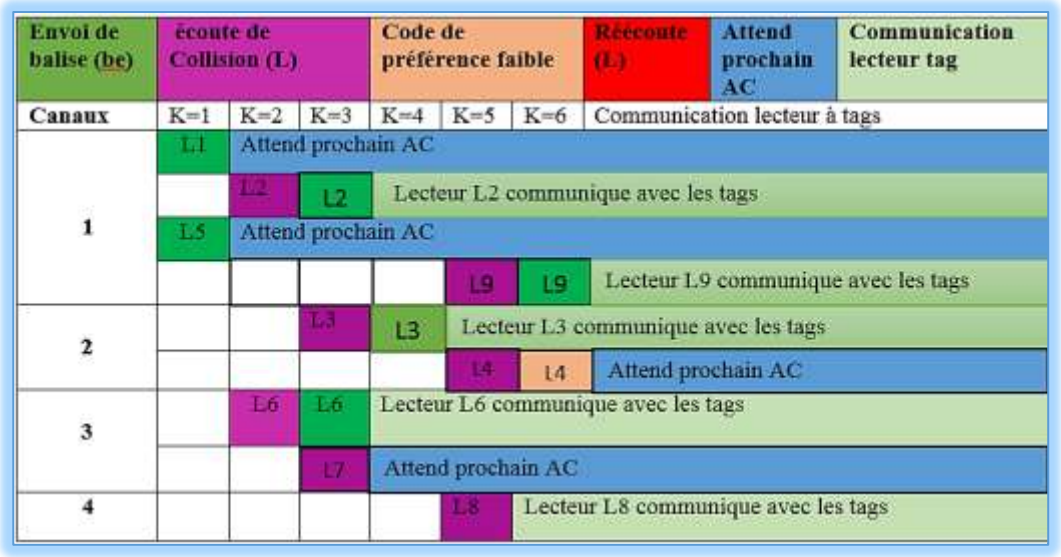


Figure 66 : densité avec mobilité des lecteurs avec BACP

Figure 67 : densité avec mobilité des lecteurs avec BACP+

Dans le cas de la densification avec des lecteurs mobiles, nous constatons que le protocole BACP+ active plus de lecteurs que le protocole BACP dans un tour de lecture. Car dans BACP le lecteur L4 se trouve en fin de cycle même s'il peut changer de canal il ne pourra pas car il est dans le dernier time-slot. Dans BACP+ ce problème ne se pose pas car L4 a participé très tôt dans le cycle donc il aura le temps de changer de canal et d'être activé. De plus, le temps de cycle et plus court dans BACP+ que dans BACP.

Conclusion

Basé sur BACP dont il reprend le principe fondamental de fonctionnement, notamment l'utilisation du multicanal et le changement de canal relativement à la distance inter-lecteur, BACP+ propose deux améliorations principales par rapport à BACP, à savoir l'optimisation des débits de lecture et la réduction de la durée des rounds. L'analyse théorique de cette proposition s'est faite suivant différents scénarii qui montrent la performance de BACP+ par rapport à BACP comme le montrent les figures de la section 4. Toutefois, une validation ne peut être exacte et pertinente sur la base de quelques scénarios mais sur des situations générales. C'est la raison pour laquelle, des critères d'évaluation ont été établis pour permettre de dégager des assertions quant à la performance de l'un ou l'autre protocole c'est-à-dire BACP et BACP+. C'est ainsi qu'il est montré qu'en cas de choix de canaux tels qu'il n'y a pas d'interférence entre les lecteurs, BAC+ offre une durée de round plus réduite. La seconde règle est définie dans un contexte de densité où il est prouvé une meilleure performance en terme de débit de lecture.

Conclusion générale et perspectives

Le principal défi des systèmes RFID est la gestion des collisions générées lors des lectures de tags surtout dans des environnements de fortes densités comme les ports ou les grands entrepôts. Pour résoudre ce problème, trois catégories de collisions ont été distinguées parmi lesquelles les collisions lecteur-lecteur dont l'étude fait l'objet de ce mémoire.

Après avoir élaboré un état de l'art où sont présentées et étudiées les deux familles qui composent les protocoles anti-collisions de lecteurs à savoir la famille distribuée et celle des protocoles centralisés et après avoir fait une étude comparative et approfondie des protocoles centralisés, nous nous sommes orientés vers les protocoles multicanal parce qu'ils offrent un débit de lecture plus élevé car permettant plus de lectures simultanées mais ils présentent néanmoins plus d'interférences que les protocoles monocanal. Beaucoup de protocoles parmi lesquels GDRA, DRCA ou BACP permettent gérer ces interférences,

BACP qui est une des dernières solutions proposées est plus performante que les autres mais présente néanmoins quelques limites qui peuvent être améliorées. C'est ainsi que nous avons proposé BACP+, une amélioration de BACP qui essaie de garder tous ses avantages tout en augmentant son débit de lecture. Des scénarios de simulation manuelle basée sur des exemples concrets et précis nous ont permis de déceler quelques critères de tendance liés à l'interférence, à la densité et à la mobilité. Nous avons pu déterminer que si les lecteurs voisins choisissent des canaux différents de telle sorte qu'ils n'interfèrent pas, alors même si le nombre de lecture est la même pour BACP que pour BACP+ mais la durée de lecture est plus réduite dans BACP+ que dans BACP. Ainsi dans ce cas, la perspective est de trouver un algorithme de sélection ou d'allocation de canaux de manière à empêcher les interférences entre voisins. Nous avons également montré que plus la densité des lecteurs augmente plus le débit de lecture est faible dans tous les deux protocoles. Cependant, le débit sera moins faible dans BACP+. Nous avons pu constater que la mobilité favorise les collisions de lecteur-tag. Par conséquent, une attente du prochain AC par les lecteurs est fréquente dans ces cas.

Par ailleurs, nous avons constaté un degré d'activité plus élevé dans BACP+ que dans BACP en début de la période de contention, ce qui peut impacter la consommation énergétique. Il sera alors question de faire le compromis entre débit de lecture et préservation de l'énergie.

Nos futurs travaux vont dans le sens de prendre en compte d'autres éléments qui permettront non seulement d'améliorer les performances de nos propositions mais également de les rendre encore plus adaptées aux environnements de déploiement. Nous continuons à travailler sur l'analyse théorique afin de mieux justifier la performance de notre contribution BACP+ par rapport au BACP. Nous voulons également mener dans BACP+ une politique de réutilisation du canal libéré avant la fin du round.

Nous envisageons également de faire de la simulation en tenant en compte d'autres paramètres tels que la consommation énergétique afin de mieux justifier les performances de chaque solution.

Table des matières

Bibliographie

[1] Englund, C., & Wallin, H. (2004). *RFID in the wireless sensor network* (Doctoral dissertation, Chalmers University of Technology).

[2] HAUET, J. P. (2006). L'identification par radiofréquence (RFID) technique et perspectives. *REE. Revue de l'électricité et de l'électronique* (10), 79-88.

[3] Commerce, D. (2005). Radio Frequency Identification: Opportunities and Challenges in Implementation.

[4] Nasri, N., Kachouri, N., Samet, M., & Andrieux, L. (2008, July). Radio Frequency Identification (RFID) working, design considerations and modelling of antenna. In *Systems, Signals and Devices, 2008. IEEE SSD 2008. 5th International Multi-Conference on* (pp. 1–6). IEEE.

[5] Garfinkel, S., & Holtzman, H. (2006). Understanding RFID technology. *RFID*, 15-36.

[6] Yasri, M. (2016). *Capteur de corrosion passif et sans contact* (Doctoral dissertation, Brest).

[7] Schill, F., Zimmer, U. R., & Trumpf, J. (2004, December). Visible spectrum optical communication and distance sensing for underwater applications. In *Proceedings of ACRA* (pp. 1–8).

[8] Nasri, N. (2010). *Étude, simulation et caractérisation électronique et protocolaire de modules RFID dédiés à une communication en milieu aquatique* (doctoral dissertation, Toulouse 2).

[9] Shih, D. H., Sun, P. L., Yen, D. C., & Huang, S. M. (2006). Taxonomy and survey of RFID anti-collision protocols. *Computer communications*, *29* (11), 2150–2166.

[10] ETSI, E. 302,208-2 v1. 1.1, September 2004. *CTAN: http://www. Etsi. Org* .

[11] Leong, K. S., Ng, M. L., & Cole, P. H. (2005, August). The reader collision problem in RFID systems. In *Microwave, Antenna, Propagation and EMC Technologies for Wireless Communications, 2005. MAPE 2005. IEEE International Symposium on* (Vol. 1, pp. 658–661). IEEE.

[12] Klair, D. K., Chin, K. W., & Raad, R. (2010). A survey and tutorial of RFID anti-collision protocols. *IEEE Communications Surveys & Tutorials*, *12* (3), 400–421.

[13] Safa, Haidar, Wassim El-Hajj, and Christine Meguerditchian. "A distributed multi-channel reader anti-collision algorithm for RFID environments." *Computer Communications* 64 (2015): 44–56.

[14] Ko, Doohyun, Bumjin Kim, and Sunshin An. "Research on Anti-Reader Collision Protocols for Integrated RFID-WSNs." *KSII Transactions on Internet & Information Systems* 4.5 (2010).

[15] Kim, Sung Won, and Gyanendra Prasad Joshi. "Reducing interference in RFID reader networks." *RFID SYSTEMS* (2010): 297.

[16] Hoffman, Alwyn, Johann Holm, and Henri-Jean Marais. "A Comparison of TTF and RTF UHF RFID Protocols." *RFID SYSTEMS* (2010): 231.

[17] Garcia-Alfaro, Joaquin, and Guillermo Navarro-Arribas. "Foreword from the program chairs of DPM 2010." (2011).

[18] Qin, Hang, and Yi Liu. "A Secure Lightweight Mutual Authentication for RFID Systems." *Applied Mechanics and Materials*. Vol. 644. Trans Tech Publications, 2014.

[19] Lijun Gao et Zhang Lu, « RFID authentication protocol for low-cost tags », Cross Strait Quad-Regional Radio Science and Wireless Technology Conference (CSQRWC), 2011 (Volume : 2), 26-30 juin 2011.

[20] Chae Hoon Lim et Taekyoung Kwon, *Strong and Robust RFID Authentication Enabling Perfect Ownership Transfer*, 2006.

[21] Sindhu Karthikeyan et Mikhail Nesterenko, "*RFID security without extensive cryptography*", *SASN '05 Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*, 2005.

[22] ang D, Wang J, Zhao JY (2006) A novel solution to the reader collision problem in RFID system. In: Proceedings of IEEE international conference on wireless communications, networking and mobile computing, pp 1–4

[23] Waldrop J, Engels DW, Sarma SE (2003) Colorwave: a MAC for RFID reader networks. In: Proceedings of IEEE conference on wireless communications and networking, vol 3, pp 1701–1704

[24] Bueno-Delgado, M. Victoria, and Pablo Pavón-Mariño. "A maximum likelihood-based distributed protocol for passive RFID dense reader environments." *The Journal of Supercomputing*64.2 (2013): 456–476.

[25] Waldrop J, Engels DW, Sarma SE (2003) Colorwave: an anticollision algorithm for the reader collision

problem. In: Proceedings of IEEE international conference on communications, pp 1206–1210

[26] Mbacke, Abdoul Aziz, Nathalie Mitton, and Herve Rivano. "RFID reader anticollision protocols for dense and mobile deployments." *Electronics* 5.4 (2016): 84.

[27] Gandino, Filippo, et al. "Probabilistic DCS: An RFID reader-to-reader anti-collision protocol." *Journal of Network and Computer Applications* 34.3 (2011): 821–832.

[28] Mbacke, Abdoul Aziz, Nathalie Mitton, and Herve Rivano. "RFID reader anticollision protocols for dense and mobile deployments." *Electronics* 5.4 (2016): 84.

[29] Gandino, Filippo, et al. "Probabilistic DCS: An RFID reader-to-reader anti-collision protocol." *Journal of Network and Computer Applications* 34.3 (2011): 821–832.

[30] Golsorkhtabaramiri, Mehdi, et al. "Comparison of energy consumption for reader anti-collision protocols in dense RFID networks." *Wireless Networks* (2018): 1–14.

[31] Waldrop, James, Daniel W. Engels, and Sanjay E. Sarma. "Colorwave: A MAC for RFID reader networks." *Wireless Communications and Networking, 2003. WCNC 2003. 2003 IEEE*. Vol. 3. IEEE, 2003.

[32] Alesii, Roberto, et al. "Backscattering UWB/UHF hybrid solutions for multi-reader multi-tag passive RFID systems." *EURASIP Journal on Embedded Systems* 2016.1 (2016): 10.

[33] Olaleye, Oladiran G., et al. "Modeling and performance simulation of PULSE and MCMAC protocols in RFID-based IoT network using OMNeT++." *RFID (RFID), 2018 IEEE International Conference on*. IEEE, 2018.

[34] Birari, Shailesh M., and Sridhar Iyer. "PULSE: a MAC protocol for RFID networks." *International Conference on Embedded and Ubiquitous Cosmputing*. Springer, Berlin, Heidelberg, 2005.

[35] Garcia-Alfaro, Joaquin, and Guillermo Navarro-Arribas. "Foreword from the program chairs of DPM 2010." (2011)

[36] Dai, Hongyue, Shengli Lai, and Hailong Zhu. "A multi-channel MAC protocol for RFID reader networks." *Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007. International Conference on*. IEEE, 2007.

[37] Meguerditchian, C., Safa, H., & El-Hajj, W. (2011, December). New reader anti-collision algorithm for dense rfid environments. In *Electronics, Circuits and Systems (ICECS), 2011 18th IEEE International Conference on* (pp. 85–88). IEEE.

[38] Assarian, Ali, et al. "A beacon analysis-based RFID reader anti-collision protocol for dense reader environments." *Computer Communications* 128 (2018): 18–34.

[39] Nawaz, F., & Jeoti, V. (2015). NFRA-C, neighbor friendly reader to reader anti-collision protocol with counters for dense reader environments. *Journal of Network and Computer Applications, 49*, 60–67.

[40] Bueno-Delgado, M. V., et al. (2013). A geometric distribution reader anti-collision protocol for RFID dense
reader environments. IEEE Transactions on Automation Science and Engineering, 10 (2), 296–306.

[41] ueno-Delgado, M. V., & Vales-Alonso, J. (2011). On the optimal frame-length configuration on real passive RFID systems. Journal of Network and Computer Applications, 34 (3), 864–876.

[42] Khandelwal, G., Lee, K., Yener, A., & Serbetli, S. (2007). ASAP: a MAC protocol for dense and timeconstrained RFID systems. EURASIP journal on Wireless Communications and Networking,
2007 (2), 3-3.

[43] ETSI, EN. (2011). 302,208-1 version 1.4. 1. Available: http://www.etsi.org. Jan 2015.

[44] Amadou, I., & Mitton, N. (2015, September). HAMAC: High adaptive MAC protocol for dense RFID readerto-reader networks. In International Conference on AdHoc Networks (AdHocNets).

[45] Golsorkhtabaramiri, M., & Issazadehkojidi, N. (2017). A distance based RFID reader collision avoidance protocol for dense reader environments. Wireless Personal Communications, 95(2), 1781-1798

[46] Assarian, A., Khademzadeh, A., HosseinZadeh, M., & Setayeshi, S. (2018). A beacon analysis-based RFID reader anti-collision protocol for dense reader environments. *Computer Communications*, *128*, 18-34.

[47] Yi Jiang et al. « An efficient multi-channel reader collision avoidance protocol in RFID systems ». In : Proceedings of Wireless Communications and Networking Conference (WCNC). IEEE. 2016.

[48] Zhang YuJing et Cui Yinghua. « EDMC : An enhanced distributed multichannel anti-collision algorithm for RFID reader system ». In : Proceedings of American Institute of Physics Conf. 2017.

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

[50] M Victoria Bueno-Delgado et Pablo Pavón-Mariño . « A maximum likelihoodbased distributed protocol for passive RFID dense reader environments ». In : *The Journal of Supercomputing* 64 (2013).

[51] Filippo Gandino et al. « DCNS : An adaptable high throughput RFID reader-to-reader anticollision protocol ». In : *IEEE Transactions on Parallel and Distributed Systems* 24.5 (2013).

[52] Mbacké, A. A. (2018). *Collecte et remontée multi-sauts de données issues de lecteurs RFID pour la surveillance d'infrastructures urbaines* (Doctoral dissertation, Université de Lille).

[53] Kyle Jamieson, Hari Balakrishnan et YC Tay . « Sift : A MAC protocol for event-driven wireless sensor networks ». In : Wireless Sensor Networks.Springer, 2006.