ROYAUME DU MAROC
Université Mohammed V - RABAT -
جامعة محمد الخامس – الرباط –
Faculté des sciences
كلية العلوم
CENTRE D'ETUDES DOCTORALES - SCIENCES ET TECHNOLOGIES

N° d'ordre : 3751

THESE

En vue de l'obtention du : ***DOCTORAT***

Structure de Recherche *: Laboratoire de Recherche en Informatique et Télécommunications*
Discipline *: Sciences de l'ingénieur*
Spécialité *: Informatique et Télécommunications*

Présentée et soutenue le 25/02/2023 par :

MAFAMANE Rachid

Protocole anti-collision de la couche MAC pour les réseaux de capteurs RFID

JURY

Salma MOULINE	PES, Université Mohammed V, Faculté des Sciences, Rabat	Presidente
Khalid ZINE-DINE	PES, Université Mohammed V, Faculté des Sciences, Rabat	Rapporteur/Examinateur
Moulay Ahmed FAQIHI	PH, Université Mohammed V, ENSIAS, Rabat	Rapporteur/Examinateur
Yassin EL HILLALI	PU, Université Polytechnique Hauts-de-France, Valenciennes	Rapporteur/Examinateur
Mourad OUADOU	PA, Université Mohammed V, Faculté des Sciences, Rabat	Co-encadrant
Khalid MINAOUI	PES, Université Mohammed V, Faculté des Sciences, Rabat	Directeur de Thèse

Année Universitaire : 2022-2023

Je souhaite dédier ma thèse
à mes chers parents,
et mes frères.

REMERCIEMENTS

Les travaux de recherche présentés dans cette thèse ont été effectués à la Faculté des Sciences de l'Université Mohammed V, Rabat, au sein du Laboratoire de Recherche en Informatique et Télécommunications (LRIT), sous la direction de Monsieur **Khalid MINAOUI,** Professeur de l'Enseignement Supérieur et en co-encadrement avec Monsieur **Mourad OUADOU,** Professeur Assistant.

Je tiens tout d'abord à remercier mon directeur de thèse Monsieur **Khalid MINAOUI**, Professeur de l'Enseignement Supérieur à la Faculté des Sciences de Rabat, qui a été pour moi un guide précieux tout au long de mes études. Être son étudiant a été un privilège et un honneur, et je suis reconnaissant de la base solide qu'il m'a fournie pour poursuivre mes recherches dans ce domaine. J'apprécie les discussions fructueuses que nous avons eues, ainsi que son soutien et son dévouement inébranlables au fil des ans.

Je tiens à remercier chaleureusement Monsieur **Mourad OUADOU**, Professeur Assistant à la Faculté des Sciences de Rabat, pour son co-encadrement, sa patience et sa motivation tout au long de mes recherches. Je lui suis profondément reconnaissant pour le degré d'autonomie qu'elle m'a accordé tout en me donnant des conseils pertinents, pour les discussions stimulantes que nous avons eues et pour son soutien indéfectible. Je me réjouis à l'idée d'une future collaboration.

Je tiens à remercier chaleureusement Madame **Salma MOULINE**, Professeur de l'Enseignement Supérieur à la Faculté des Sciences de Rabat, qui a accepté de présider le comité de soutenance de ma thèse.

Je tiens également à remercier Monsieur **Khalid ZINE-DINE**, Professeur de l'Enseignement Supérieur à la Faculté des Sciences de Rabat, pour avoir accepté de rapporter cette thèse et pour avoir pris le temps d'évaluer soigneusement ce travail.

Je suis très reconnaissant à Monsieur **Moulay Ahmed FAQIHI**, Professeur Habilité à l'École Nationale Supérieure d'Informatique et d'Analyse des Systèmes (ENSIAS) de Rabat, d'avoir accepté de rapporter ce travail et pour ses précieux commentaires qui m'ont permis d'améliorer ce manuscrit.

Je tiens à remercier Monsieur **Yassin EL HILLALI**, Professeur des Universités à l'Université Polytechnique Hauts-de-France, Valenciennes, pour avoir accepté de rapporter également ce travail et de participer à la commission. Je le remercie sincèrement pour sa disponibilité et ses précieuses remarques afin d'améliorer mon travail.

RESUME

En vue de l'émergence de l'Internet des objets, le besoin d'une identification et d'une traçabilité efficaces a augmenté. L'identification par radiofréquence (RFID), une approche simple et favorable pour recueillir les informations, a donc attiré l'attention des communautés de recherche.
De nombreux domaines d'application nécessitent le déploiement un réseau RFID dense et une couverture efficace, ce qui risque d'engendrer des interférences entre les tags et les lecteurs RFID et par conséquent réduire les performances du système RFID.
Cependant, ce système souffre de problèmes causés par une densité élevée, tels que les collisions et les duplications. Le déploiement de la RFID est donc plus efficace dans un environnement dense où il peut améliorer les surcharges et les retards.
Plusieurs travaux proposent donc des protocoles de couche MAC pour résoudre ce problème de collision en se basant sur différentes méthodes d'accès au canal.
Notre travail de thèse propose dans ce contexte de nouvelles approches pour la gestion efficace des ressources de fréquence et de temps pour les lecteurs RFID déployés dans les réseaux de capteurs sans fil denses et mobiles à travers :

- Protocole général de la couche MAC FTSMAC dans lequel la fréquence du spectre est utilisée efficacement en divisant le signal en différents intervalles de temps via un mécanisme de messagerie distribué utilisé par les lecteurs RFID.
- Solution hybride FTSMAC-E améliorant le protocole anti-collision FTSMAC basé sur le TDMA-FDMA distribué.
- Protocole anti-collision basé sur le réseau neuronal artificiel de type feed-forward pour un apprentissage distribué entre les lecteurs RFID afin de prédire la présence de collisions et d'assurer une allocation efficace des ressources.
- Modèle (AIN-CA) d'anti-collision de lecteur en termes d'allocation de ressources utilisant un réseau immunitaire artificiel afin de minimiser les collisions.

Mots-clefs : Système RFID ; Internet des objets ; Réseau neuronal artificiel ; Réseau immunitaire artificiel ; Collision ; Couche MAC ; Réseau de capteurs sans fil ; Systèmes distribués ; Allocation de ressources.

ABSTRACT

Due to the emergence of the Internet of Things, the need for effective identification and traceability has increased. Radio-frequency identification (RFID), a simple and cheap approach for gathering information, has therefore drawn the attention of research communities.
Many application areas require a dense RFID network for efficient deployment and coverage, which causes interference between RFID tags and readers, thus reducing the performance of the RFID system.
However, this system suffers from problems caused by high density, such as collisions and duplication. Thus, the deployment of RFID is more effective in a dense environment where it may improve overage and delays.
Thus, several researchers propose MAC layer protocols to solve this collision problem based on different channel access methods.
Our thesis research offers new approaches to the efficient management of frequency and time resources for RFID readers deployed in dense and mobile wireless sensor networks through :

- General MAC layer protocol FTSMAC in which the spectrum frequency is efficiently used by dividing the signal into different time slots via a distributed messaging mechanism used by RFID readers.
- Hybrid solution FTSMAC-E improving FTSMAC based distributed TDMA-FDMA anti-collision protocol.
- An anti-collision protocol based on feed-forward artificial neural network methodology for shared learning between RFID readers to predict the presence of collisions and ensure an efficient resource allocation.
- Model (AIN-CA) of reader anti-collision in terms of resource allocation using artificial immune network in order to minimize collisions.

Key Words: System RFID; Internet of things; Artificial neural network; Artificial immune network; Collision; MAC layer; Wireless sensor network; Distributed systems; Resource allocation.

LISTE DES FIGURES

LISTE DES TABLEAUX

LISTE DES ALGORITHMES

LISTE DES ABREVIATIONS

A
AHAIS: Adaptive Hierarchical Artificial Immune System
AIN-CA: Artificial Immune Network Collision Avoidance
AINet-SL: Artificial Immune Network Social Learning
ANN: Artificial Neural Network
AVI: Automatic Vehicle Identification
B
BAN: Body Area Network
BAP: Battery-Assisted Passive
BAT: Battery-Assisted Tags
BSN: Body Sensor Networks
C
CC: Control Channel
CDMA: Code Division Multiple Access
CORA: Coverage Oriented Reader Anti-Collision
CSMA: Carrier Sense Multiple Access
D
DCNS: Distributed Color Non-Cooperative Selection
DCS: Distributed Color Selection
DEFAR: Distributed Efficient Fair Anti-Collision
DiMCA: Dimitted Multi-Channel Collision Avoidance
DMLAR: Distributed Machine Learning-Based Anti-Collision RFID
DRCA: Distance Reader Collision Avoidance
E
EMRCA: Efficient Multichannel Reader Collision Avoidance
EPC: Electronic Product Code
ETSI: European Telecommunications Standards Institute
F
FDMA: Frequency Division Multiple Access
FRCA: Fair Reader Collision Avoidance
FTSMAC: Frequency Time Scheme MAC
FTSMAC-E: Frequency Time Scheme MAC Extention
G
GDRA: Geometric Distribution Reader Anti-collision

H
HAMAC: High Adaptive MAC
HF: High Frequency
I
IoT: Internet of Things
L
LAN: Local Area Network
LF: Low frequency
M
MAC: Medium Access Control
MCMAC: Multi Channel MAC
MF: Medium Frequency
MWISBA: Maximum-Weight-Independent-Set-BAsed
N
NFRA: Neighbour Friendly Reader Anti-Collision
O
OEM: Original Equipment Manufacturer
OSI: Open Systems Interconnection
P
PA: Precision Agriculture
R
R2RCAM: Reader-to-Reader Collision Avoidance Model
RA-AIS: Reader Avoidance Artificial Immune System
RFID: Radio Frequency Identification
RRI: Reader to Reader Interference
RTI: Reader to Tag Interference
S
SDMA: Space Division Multiple Access
SHF: Super High Frequency
T
TCP: Transmission Control Protocol
TDMA: Time Division Multiple Access
TS: Time Slot
U
UHF: Ultra High Frequency
V
VRT: Variable Rate Technology
W
WBAN: Wireless Body Area Networks

LISTE DES PUBLICATIONS

- Mafamane, R., Ait Mansour, A., Ouadou, M., Minaoui, K. (2021). FTSMAC: A Multi-Channel Hybrid Reader Collision Avoidance Protocol for RFID Network. Journal of Sensor and Actuator Networks, 10(3), 46.
- Mafamane, R., Ouadou, M., Sahbani, H., Ibadah, N., Minaoui, K. (2022). DMLAR: Distributed Machine Learning-Based Anti-Collision Algorithm for RFID Readers in the Internet of Things. Computers, 11(7), 107.
- Mafamane, R., Ouadou, M., Minaoui, K. FTSMAC-Ext: A RFID Reader Anti-Collision Protocol for the WSN with a new TDMA distribution strategy
- Mafamane, R., Ouadou, M., Sahbani, H., Minaoui, K. AIN-CA: Artificial Immune Network Collision Avoidance protocol for a dense RFID
- Mafamane, R., Ouadou, M., Hassani, A. T. J., Minaoui, K. (2021, April). Study of the heterogeneity problem in the Internet of Things and Cloud Computing integration. In 2020 10th International Symposium on Signal, Image, Video and Communications (ISIVC) (pp. 1-6). IEEE.
- H. Belmajdoub, R. Mafamane, Y.Bekali Karfa, M.Ouadou and K.Minaoui. Face Recognition based on CNN, Hog and Haar Cascade methods using Raspberry Pi v4 Model B. Smart embedded system and applications book

SOMMAIRE

Introduction Générale

L'identification par radiofréquence (RFID) est une technologie d'identification automatique des objets, basée sur le principe du marquage des objets, humains ou animaux pour faciliter leur intégration dans des systèmes informatiques ou de données Juels [2006].

Les principaux composants de cette technologie sont les tags et lecteurs, et en raison de sa simplicité, l'avenir de la RFID est prometteur. En outre, de nombreuses applications ont adopté la technologie RFID comme base d'identification et de suivi Ahson and Ilyas [2017]. La technologie RFID a été appliquée dans un certain nombre de domaines, notamment les entrepôts intelligents Zhao et al. [2020], la santé Abuelkhail et al. [2021], la localisation intérieure Ma et al. [2018], la gestion de la chaîne d'approvisionnement Musa and Dabo [2016], les expériences de recherche sur le cerveau Al Ajrawi et al. [2018] et l'agriculture moderne Jyothi and Nandan [2020].

La gestion de la chaîne d'approvisionnement est l'un des exemples de domaines d'application de la technologie RFID. Ainsi, la RFID a été utilisée pour améliorer l'efficacité de la chaîne d'approvisionnement en permettant aux superviseurs de contrôler et de suivre les informations sur les produits. Cependant, malgré la demande croissante, les performances de la technologie RFID peuvent être remise en question par de nombreux facteurs, et notamment en raison de collisions entre noeuds Pal and Kant [2019], Shousong et al. [2018], Sidorov et al. [2019], Tao et al. [2018], Jiang [2019]. En effet, les tags Li et al. [2019] sont de petits composants constitués de circuits intégrés connectés à une antenne et d'une petite mémoire pour stocker les données. En pratique, les problèmes de collisions et d'interférences sont principalement liés au déploiement Hamid et al. [2018]. Par conséquent, les lecteurs doivent disposer de ressources adaptées pour gérer efficacement le processus de communication, en contrôlant l'accès au canal partagé. Ils doivent également être déployés de manière stratégique afin de couvrir une grande surface et de lire le plus grand nombre de tags possible. En général, le lecteur RFID utilise ces ondes radio pour alimenter les tags. Lorsque ceux-ci sont activées, ils peuvent communiquer leur contenu au lecteur.

L'un des principaux défis des réseaux RFID est d'améliorer le taux d'interrogation des tags par les lecteurs Ferrero [2019]. Dans un réseau RFID, une densité élevée de lecteurs Golsorkhtabaramiri et al. [2019] peut avoir un impact sur les performances du système en raison du nombre de collisions générées. En conséquence, le système peut souffrir d'une dégradation de collection des données, d'une augmentation du temps de communication et d'une forte consommation d'énergie. Les collisions sont ainsi un problème critique qui réduit considérablement les performances des systèmes RFID.

Le réseau RFID considéré dans ce document est associé aux réseaux de capteurs sans fil (RCSFs), sur lesquels les lecteurs et les tags sont distribués de manière aléatoire, et peuvent être déployés de manière fixe ou mobile. Les réseaux de capteurs sans fil utilisent les systèmes RFID pour créer une plateforme rechargeable performante. Plusieurs articles Landaluce et al. [2020],

Ji et al. [2018], Sobral et al. [2018], Adame et al. [2018], Alfian et al. [2017], Deng et al. [2017] définissent des architectures pour ce type de combinaison de réseaux de capteurs RFID.

Les collisions sont associées à la couche MAC du modèle OSI, chargée de contrôler l'accès au canal partagé Luo et al. [2021], Li et al. [2020b], Xuan and Li [2020], Cao et al. [2020]. Pour résoudre ce problème, plusieurs protocoles anti-collision ont été récemment proposés Kumar et al. [2021], Deng et al. [2019], Rezaie and Golsorkhtabaramiri [2018], Chuang and Tsai [2017], Su et al. [2017], Wang et al. [2019], Abbasian and Safkhani [2020], Zhou and Jiang [2021], Saia et al. [2019], Liu and Su [2018]. Les méthodes de base utilisées dans les systèmes RFID sont les suivantes : TDMA utilise un découpage temporel de la bande passante dont le principe est de répartir le temps disponible entre les différents noeuds. Alternativement, FDMA utilise les bandes de fréquences pour allouer dynamiquement une partie du spectre à chaque noeud. Alors que CSMA est utilisé pour détecter et éviter les collisions des trames lors des transmissions.

Ce travail est organisé en quatre chapitres. Tout d'abord, le chapitre 1 présente le sujet de recherche, notamment le contexte et les motivations qui ont permis de concevoir la thèse.

Dans le chapitre 2, nous présentons le problème des collisions dans les réseaux RFID et l'état de l'art des différents protocoles anti-collision. Le chapitre 3 est consacré à la résolution du problème de collision à partir de notre protocole hybride de contrôle des ressources multicanal FTSMAC et FTSMAC-E.Ces approches utilisent un nouveau système de notification efficace qui permet de créer des schémas de réutilisation des fréquences et des times slots. Dans le chapitre 4, nous avons réalisé deux protocoles anti-collision basés sur l'intelligence artificielle. Le protocole DMLAR permet un apprentissage indépendant à l'aide des modèles ANN artificiels et un système de distribution des ensembles de données et des modèles ANN résultants. Le second protocole de ce chapitre, AIN-CA, sert à distribuer les ressources aux lecteurs en utilisant un réseau immunitaire artificiel.

Chapter

1 Contexte et État de l'art

1.1 Systèmes d'Identification par Radio Frequence (RFID)

1.1.1 Les systèmes d'identification

Ces dernières années, les techniques d'identification automatique (Auto-ID) sont devenues très populaires dans de nombreuses industries de services, la logistique d'achat et de distribution, l'industrie, les entreprises de fabrication et les systèmes de flux de matériaux.

Des procédures d'identification automatique existent pour fournir des informations sur les personnes, les animaux et les produits. Les étiquettes à code-barres omniprésentes qui ont déclenché une révolution des systèmes d'identification il y a longtemps, se révèlent insuffisantes dans un nombre croissant de cas. Les points faibles des codes-barres sont leur faible capacité de stockage et le fait qu'ils ne peuvent pas être reprogrammés. La solution techniquement optimisée consiste à stocker les données dans une puce de silicium. La forme la plus courante de dispositifs électroniques porteurs de données utilisés dans la vie quotidienne est la carte à puce basée sur un champ de contact (carte à puce téléphonique, cartes bancaires). Cependant, le contact mécanique utilisé dans la carte à puce est souvent peu pratique. Un transfert de données sans contact entre le support de données et son lecteur est beaucoup plus flexible. Dans le cas idéal, la puissance nécessaire au fonctionnement du dispositif électronique de transport de données serait également transférée du lecteur à l'aide de la technologie sans contact. En raison des procédures utilisées pour le transfert d'énergie et de données, les systèmes d'identification sans contact sont appelés systèmes RFID (identification par radiofréquence).

La figure 1.1 présente un bref aperçu des différents systèmes d'identification automatique qui accomplissent des fonctions similaires à celles de la RFID.

1.1.2 Comparaison des systèmes d'identification

Une comparaison entre les systèmes d'identification décrits ci-dessus met en évidence les forces et les faiblesses de la RFID par rapport aux autres systèmes (tableau 1.1). Ici aussi, il existe une relation étroite entre les cartes à puce et les systèmes RFID ; cependant, ces derniers contournent tous les inconvénients liés au mauvais contact (sabotage, salissures, insertion unidirectionnelle, insertion chronophage, etc.).

1.1.3 Développement historique de la RFID

En 1935, la première notion de systèmes RFID a été inventée par un physicien écossais appelé Robert Alexander pour détecter les avions Harris [1960]. Ensuite, en 1950, le gouvernement britannique a développé le premier prototype du système RFID, connu sous le nom de système

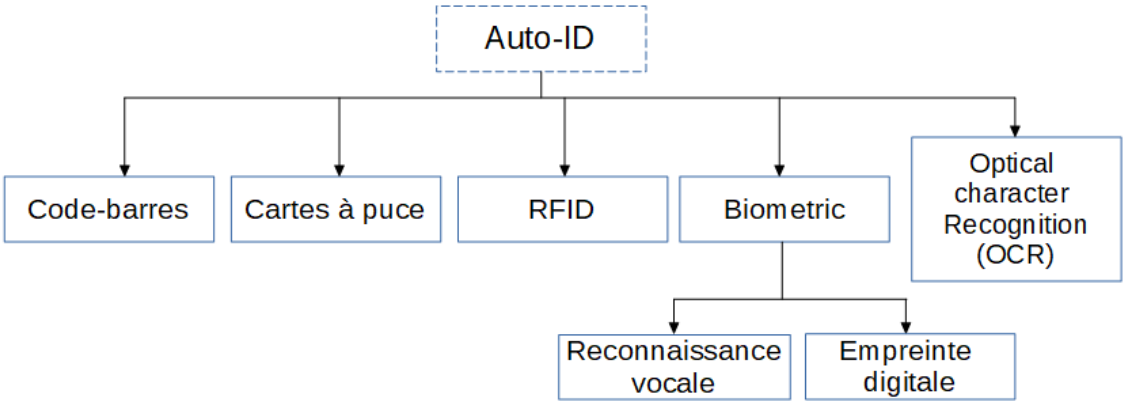

Figure 1.1: Aperçu des procédures d'auto-ID les plus importantes

Identification Friend or Foe (IFF) Charles [1973]. Ce système a été conçu pour des applications aéronautiques. Entre les années 1950 et 1960, il y a eu un grand développement dans le domaine de la RFID pour différentes applications, par ex. l'application des micro-ondes Vernon [1952] et des systèmes de transmission radio qui modulent les répondeurs passifs Harris [1960]. Dans les années 1970, la RFID a été intensivement appliquée à la logistique, au transport, au suivi des véhicules, au suivi du bétail ainsi qu'à l'automatisation industrielle. Le premier brevet américain dans ce domaine a été publié en 1973 pour l'invention d'un tag RFID active à mémoire réenregistrable Charles [1973]. En 2008, le département américain de la Défense a annoncé son intention d'utiliser la technologie du code de produit électronique (EPC) Want [2006] pour suivre les marchandises dans sa chaîne d'approvisionnement. En Europe, la RFID est destinée à améliorer les applications industrielles et de permettre aux systèmes à courte portée de contrôler les animaux Vernon [1952]. Au Japon, la RFID est utilisée pour les paiements sans contact dans les systèmes de transport Harris [1960].

1.1.4 Domaines d'application de la technologie RFID

Aujourd'hui, nous retrouvons la technologie RFID dans plusieurs domaines d'application y compris: **Transports** : La RFID est utilisée dans les infrastructures de transport intelligentes. Les étiquettes RFID sont utilisées pour percevoir les péages sur les autoroutes en inspectant une étiquette fixée à la voiture et pour payer les tarifs des bus, des trains ou des métros. Les cartes RFID peuvent être utilisées pour contrôler l'accès aux transports publics. Des étiquettes peuvent être attachées aux véhicules, ce qui leur permet d'entrer automatiquement dans les zones contrôlées.

Santé : L'adoption de la RFID dans le secteur médical permet de gérer les équipements médicaux. Dans les hôpitaux, les cartes étiquetées RFID peuvent être utilisées pour authentifier le personnel et lui permettre d'accéder aux dossiers médicaux sans porter atteinte à la vie privée. Les hôpitaux utilisent également des outils RFID pour mesurer les températures et surveiller l'hygiène des mains afin de lutter contre les infections. Au-delà de l'amélioration de la sécurité des patients, cette technologie peut aider les hôpitaux à faire des économies en permettant aux employés de travailler de manière plus productive et efficace. Outre la gestion des ressources, les cas d'utilisation de la RFID comprennent la fourniture d'un aperçu en temps réel de l'emplacement

Table 1.1: Comparaison des différents systèmes RFID

Paramètres du système	Code-barres	OCR	Reconnaissance vocale	Biométrie	Carte à puce	Systèmes RFID
Volume typique de données (octets)	1-100	1-100	-	-	16-64 k	16-64 k
Densité des données	Faible	Faible	Elevé	Elevé	Très élevé	Très élevé
Lisibilité par la machine	Bon	Bon	Coûteux	Coûteux	Bon	Bon
Lisibilité par les personnes	Limitée	Simple	Simple	Difficile	Impossible	Impossible
Influence de la saleté/ de l'humidité	Très élevé	Très élevé	-	-	Possible	Aucune influence
Influence de la couverture (op-tique)	Échec total	Échec total	-	Possible	-	Aucune influence
Influence de la direction et de la position	Faible	Faible	-	-	Unidirectionnel	Aucune influence
Dégradation/usure	Limitée	Limitée	-	-	Contacts	Aucune influence
Coût d'achat de lecture	Très faible	Moyen	Très élevé	Très élevé	Faible	Moyen
Coûts opérationnels (p. ex. imprimante)	Faible	Faible	None	None	Moyen	None
Copie/modification non autorisée	Léger	Léger	Possible	Impossible	Impossible	Impossible
Vitesse de lecture	Faible $\sim 4s$	Faible $\sim 3s$	Très faible >5s	Très faible >5-10s	Faible $\sim 4s$	Très rapide $\sim 0.5s$
Distance maximale de lecture	0-50 cm	<1 cm Scanner	0-50 cm	Direct contact	Direct contact	0-5m, microwave

des équipements médicaux et l'amélioration du flux de travail des patients en automatisant ce qui était auparavant un processus manuel de gestion et de programmation des procédures.

Chaînes d'approvisionnement : La RFID est de plus en plus déployée pour la gestion de la chaîne d'approvisionnement. Dans les chaînes d'approvisionnement, les étiquettes RFID sont utilisées à différents niveaux. De nombreux détaillants demandent à leurs fournisseurs d'étiqueter les objets avec des étiquettes RFID en utilisant le code produit électronique (EPC). Des géants du commerce de détail tels que Wal-Mart, Target et Philips Electronics ont adopté la technologie RFID. Outre l'utilisation de la RFID à des fins d'inventaire, elle peut être utilisée pour lutter contre le vol à l'étalage. Lorsque les marchandises arrivent au centre de distribution ou au magasin, des lecteurs RFID sont utilisés pour compter rapidement les expéditions au niveau de chaque article. Comme les centres de distribution ont un débit d'articles beaucoup plus élevé que les magasins, ils utilisent souvent des tunnels RFID automatisés. Les envois qui entrent dans le centre de distribution sont directement acheminés sur un convoyeur et sont comptabilisés lors de leur passage dans le tunnel.

Bibliothèques : La RFID a été utilisée pour remplacer les codes-barres sur les articles de bibliothèque tels que les livres ou les DVD. Elle peut être utilisée comme caisse de sortie en libre-service. Les bibliothèques peuvent améliorer leur efficacité, réduire les coûts de personnel et permettre le tri automatisé des livres. Des problèmes de confidentialité ont été soulevés concernant l'utilisation de la RFID par les bibliothèques. Un agent pourrait lire les étiquettes RFID de chaque personne quittant la bibliothèque.

Événements sportifs : Utilisation des systèmes RFID dans l'industrie des stades de sport De la gestion des événements à la surveillance des employés, la gestion d'un stade de sport est certainement une tâche complexe. La RFID peut contribuer à réduire les frictions à l'entrée d'un événement. Les fans n'ont plus besoin de porter des billets en papier, de saisir des informations ou même de transporter de l'argent liquide ; tout cela peut se faire d'un simple coup de poignet.

Figure 1.2: Intégration des technologies RFID dans un système de transport intelligent

Figure 1.3: L'identification positive des patients est le fondement de la sécurité des patients

La RFID contribue également à la prévention des fraudes : chaque bracelet est doté d'un code unique, ce qui le rend très difficile à contrefaire.

Suivi des animaux : À mesure que le commerce se mondialise, la tâche de suivre et de gérer les animaux destinés aux produits alimentaires devient de plus en plus critique et difficile. Les animaux peuvent être transportés sur de longues distances, se mêlant souvent à du bétail provenant de différents endroits. Les animaux de ferme et de zoo, ainsi que les animaux domestiques sont tous des porteurs potentiels de maladies menaçantes. La technologies RFID permet de gérer les animaux de ferme, avec des étiquettes d'oreille en basse fréquence ou UHF, des étiquettes en verre ou des bolus.

Figure 1.4: Gestion de la chaîne d'approvisionnement par RFID

Figure 1.5: Suivi automatisé et efficace des documents en temps réel, recherche de l'emplacement et de la disponibilité

1.1.5 Caractéristiques des systèmes RFID

1.1.5.1 Bandes de fréquences et spectre RFID

Le système RFID fonctionne dans des bandes spécifiques du spectre radio (tableau 1.2). Ces bandes sont normalement des bandes sans licence permettant à tout système de les utiliser. Bien que le spectre sans licence puisse être encombré dans certaines zones, la nature à courte portée de la RFID signifie que ces fréquences sont normalement très appropriées pour les applications RFID.

La bande particulière utilisée pour un système RFID est définie lors de sa conception et ce n'est pas un élément sélectionnable par l'utilisateur, bien que certaines bandes puissent être sélectionnées en fonction du pays dans lequel il est utilisé pour se conformer à la disponibilité du spectre sans licence. Ceci est normalement réglé en usine en fonction de la zone de vente connue. En règle générale, les différences de bande ne sont que relativement faibles et n'affectent pas les

Figure 1.6: Contrôle d'accès aux événements sportifs

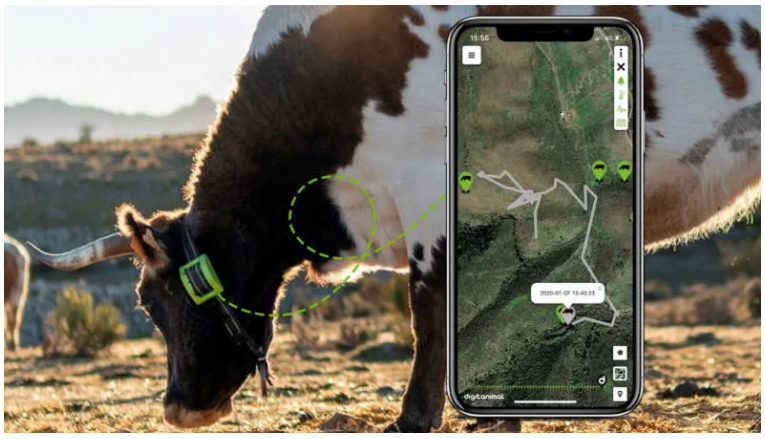

Figure 1.7: Système de gestion agricole et de suivi des animaux en utilisant la RFID

performances, et n'affectent que le spectre UHF.

La fréquence utilisée par le système RFID détermine de nombreuses caractéristiques de son fonctionnement. En conséquence, la détermination de la bande de fréquence RFID correcte est une décision importante dans le processus de développement. Il existe différentes bandes de fréquences RFID dans le spectre radio qui sont utilisées dans le monde entier. Ces bandes sont placées dans des zones très différentes du spectre radio, ce qui permet à la RFID de choisir les fréquences qui permettront d'obtenir les bons paramètres du système.

Les fréquences RFID UHF 858 - 930 MHz ne faisant pas l'objet d'une allocation globale, ces fréquences ne peuvent pas être utilisées à l'international. Lorsque l'accès est autorisé, il peut s'avérer qu'il existe différentes restrictions dans différents pays.

Étant donné que les bandes attribuées pour la RFID, en particulier dans la partie UHF du spectre, peuvent être différentes dans les régions du globe, il est nécessaire d'inclure une disposition à cet effet dans la conception. Heureusement, la différence dans les bandes de fréquences est relativement faible et peut souvent être prise en compte sans modification majeure de la conception RF.

Table 1.2: Les bandes de fréquences RFID et leurs applications

Bande de fréquence RFID	Bande	Gamme typique	Applications typiques de la RFID
125-134.2 kHz and 140-148.5 kHz	LF	Jusqu'à 1/2 mètre	Ces fréquences peuvent être utilisées dans le monde entier sans licence. Souvent utilisé pour l'identification des véhicules.
6.765 - 6.795 MHz	MF		Le couplage inductif est utilisé sur ces fréquences RFID.
13.553 - 13.567 MHz	HF	Jusqu'à 1 mètre	Ces fréquences RFID sont généralement utilisées pour le paiement sans contact,le contrôle d'accès, le suivi des vêtements, etc.
26.957 - 27.283 MHz	MF	Jusqu'à 1 mètre	Couplage inductif uniquement et utilisé pour des applications spéciales.
433 MHz	UHF		Ces fréquences RFID sont utilisées avec un couplage de rétrodiffusion, pour des applications telles que les clés de voiture à distance en Europe
858 - 930 MHz	UHF	1 a 10 mètres	Ces fréquences RFID ne sont pas accessibles à l'échelle mondiale et leur utilisation est soumise à des restrictions importantes. Lorsqu'ils sont utilisés, il est souvent utilisé pour la gestion des actifs, le suivi des conteneurs, le suivi des bagages, le suivi des travaux en cours, etc.
2.400 - 2.483 GHz	SHF		Couplage de rétrodiffusion, mais uniquement disponible aux États-Unis / Canada
2.446 - 2.454GHz	SHF	3 mètres vers le haut	Ces fréquences RFID sont utilisées pour le suivi à longue distance et avec des tags actifs, RFID et AVI (Automatic Vehicle Identification).
5.725 - 5.875 GHz	SHF		Couplage de rétrodiffusion. Peu utilisé pour la RFID.

- Amérique du Nord: Ici, la bande RFID UHF peut être utilisée sans licence dans les limites de 915 MHz (c'est-à-dire 902 - 928 MHz). Il exist des restrictions sur la puissance de transmission.
- Europe (moins d'exclusions): Dans cette région, les fréquences RFID (et d'autres applications radio de faible puissance) ont spécifié les recommandations ETSI EN 300 220 et EN 302 208, et la recommandation ERO 70 03. Celles-ci permettent le fonctionnement RFID dans la bande 865-868 MHz, mais avec certaines restrictions impliquées. Les lecteurs RFID doivent surveiller un canal avant de transmettre - "Listen Before Talk".
- France: La norme nord-américaine n'est pas acceptée en France car elle interfère avec les fréquences attribuées aux militaires.
- Chine et Japon: Il n'y a pas de bandes ou de fréquences RFID sans licence. Cependant, il est possible de demander une licence pour UHF RFID qui est accordée dans un site.
- Australie et New Zealand: Dans cette zone, la bande RFID existe entre 918 et 926 MHz car ces fréquences ne sont pas autorisées, mais il existe des restrictions sur la puissance de transmission.

La variété de bandes de fréquences disponibles pour la RFID offre aux développeurs un bon choix. La différence dans les propriétés ainsi que les façons dont elles peuvent être utilisées signifie qu'une variété de méthodes de couplage différentes peuvent être utilisées.

1.1.5.2 Les composants du système RFID

Les systèmes RFID sont produits par de nombreux fabricants et existent dans d'innombrables variantes. Cependant, un système RFID se compose principalement de trois composants ; le transpondeur/tag, le lecteur et le middleware RFID.

1.1.5.2.1 Lecteur RFID Un lecteur RFID est un dispositif de numérisation qui permet de lire les tags de manière fiable et communique les résultats au middleware. Un lecteur utilise ses antennes pour communiquer avec le tag en diffusant des ondes radio auxquelles répondront toutes les tags à portée. Les lecteurs peuvent traiter plusieurs composants à la fois, ce qui permet de minimiser les temps de traitement et de lecture. Ils peuvent être mobiles ou fixes et se différencient par leur capacité de stockage, leur capacité de traitement et la fréquence à laquelle ils peuvent lire (United States Government Accountability Office, 2005). Le lecteur RFID est composé des blocs fonctionnels suivants (figure 1.8) :

- Interface HF : la partie maître du lecteur qui possède les fonctionnalités suivantes :
  - Alimentation des transpondeurs RFID en générant de l'énergie à haute fréquence ;
  - Modulation du signal vers le transpondeur ;
  - Réception et démodulation des signaux des transpondeurs ;
- Unité de contrôle : la partie esclave du lecteur qui exécute les fonctionnalités suivantes :
  - Communication et exécution des commandes du logiciel d'application ;
  - Codage et décodage du signal ;
  - Contrôle de communication avec un transpondeur ;

Certains lecteurs RFID ont des fonctionnalités supplémentaires comme l'algorithme anti-collision, le chiffrement et le déchiffrement des données transférées et l'authentification lecteur-lecteur. Différentes conceptions de lecteurs existent, puisque chaque application a des exigences différentes. Les lecteurs RFID sont classés en trois types:

- Lecteurs OEM : les lecteurs OEM sont principalement utilisés pour les systèmes de capture de données, les systèmes de contrôle d'accès et les robots.
- Lecteurs à usage industriel : utilisés dans les usines d'assemblage et de fabrication
- Lecteurs portables : Ces lecteurs sont plus mobiles que les autres et sont dotés d'un écran LCD et d'un clavier. Ce type de lecteurs est utilisé dans les applications d'identification des animaux, de contrôle des dispositifs et de gestion des actifs.

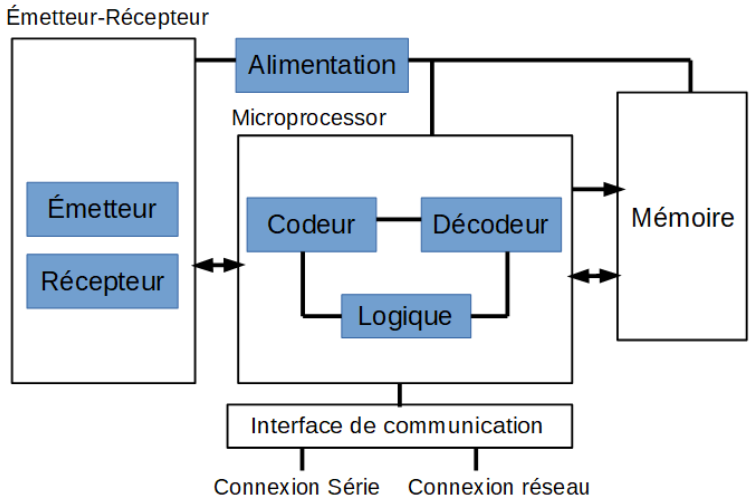

Figure 1.8: Circuit intégré de lecture

1.1.5.2.2 Tag RFID Un transpondeur RFID, ou tag, se compose d'une puce et d'une antenne. Une puce peut stocker un numéro de série unique ou d'autres informations basées sur le type de mémoire. Le type de mémoire de tag peut être en lecture seule, en lecture-écriture ou en écriture unique et en lecture multiple (United States Government Accountability Office, 2005). Les tags en lecture seule sont beaucoup moins chers à produire et sont utilisées dans la plupart des applications actuelles. Les tags en lecture-écriture sont utiles lorsque les informations doivent être mises à jour. L'antenne est utilisée pour transmettre des informations de la puce au lecteur, et plus l'antenne est grande, plus la portée de lecture est longue. Le tag RFID peut être soit attachée ou bien intégrée dans un objet à identifier, et peut être scannée par des lecteurs mobiles ou fixes à l'aide d'ondes radio (United States Government Accountability Office, 2005). Les tags RFID existent en trois versions différentes : tags passifs, tags actifs et tags semi-passifs/semi-actifs.

La structure générale du tag RFID (figure 1.9) : Alimentation d'antenne, Contrôle Logique, modulateur Tx, démodulateur Rx, Circuit intégré (IC) et Cellules de mémoire.

Un tag nécessite de l'énergie pour traiter les signaux reçus de l'interrogateur et pour renvoyer les signaux de données codés à l'interrogateur. Les signaux renvoyés peuvent être des signaux

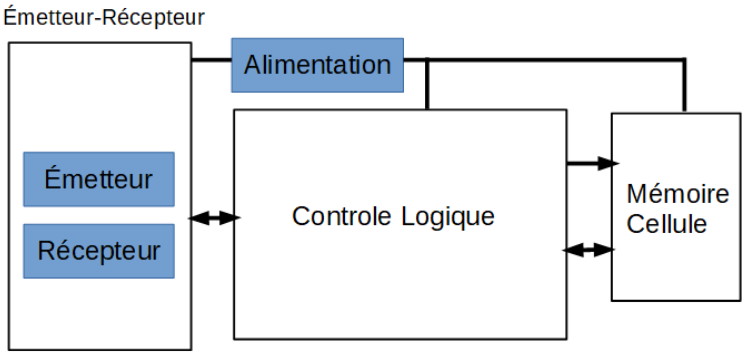

Figure 1.9: circuit intégré de tag

réfléchis ou des signaux générés par le tag. Selon la façon dont les tags obtiennent l'énergie, les tags sont classés comme suit :

Tags Passifs : Un tag passif n'a pas sa propre source d'alimentation ; il n'a pas de batterie à bord. Le tag est alimenté par les ondes radio reçues de l'interrogateur. La quantité d'énergie ainsi reçue est très faible, juste assez pour alimenter son circuit intégré. Par conséquent, les fonctionnalités de tag passive sont limitées. En raison d'un manque de puissance suffisante, il ne peut pas prendre en charge un émetteur actif pour communiquer avec l'interrogateur.

- Avantages: Petite taille Poids léger Pas cher (dépend de la quantité) N'ajoute pas du bruit radio Durée de vie plus longue (20 ans et plus) Résistance aux environnements difficiles
- Inconvénient: Nécessite la présence d'un interrogateur pour fonctionner Stockage de données en quantité limitée Exige des interrogateurs plus puissants Portée de lecture faible (quelques pouces à 20 pieds)

Tags Semi-Passifs : Les tags semi-passives sont également appelées tags semi-actives, passives assistées par batterie (BAP) ou tags assistés par batterie (BAT). Ce tag a une batterie intégrée pour alimenter son circuit intégré, mais, comme un tag passif, elle n'a pas d'émetteur actif. Il utilise la rétrodiffusion pour communiquer avec l'interrogateur. Il module la réflexion des ondes de l'interrogateur et nécessite un interrogateur pour envoyer des données.

- Avantages: Portée de lecture plus longue (100 pieds et plus) Puissance réduite des interrogateurs Peut avoir plus de mémoire, stocker plus de données Peut contenir des capteurs environnementaux N'ajoute pas du bruit radio
- Inconvénient: Sensible aux environnements difficiles Autonomie de la batterie limitée (2 à 7 ans) Coûte un peu plus cher que les tags passives Plus grande taille et poids Nécessite la présence d'un interrogateur pour fonctionner

Tags Actives: Le circuit intégré de ce tag peut contenir plus de puissance de traitement pour mettre en oeuvre des fonctionnalités supplémentaires telles que la manipulation de données. Ce tag (Figure 1.10) utilise la batterie pour alimenter son circuit intégré et son émetteur. Il n'a pas besoin de puissance émise ou de signaux radio de l'interrogateur pour transmettre ses données. En fait, il n'a même pas besoin d'un interrogateur. Un tag actif peut être configurée pour diffuser ses données à un instant prédéfinie, périodiquement ou lors de l'occurrence d'un certain événement. Sa plage de lecture typique est de 300 à 750 pieds. La portée de lecture dépend

de la puissance de la batterie et du type d'émetteur sur le tag. Un tag actif, comme un tag semi-passive, peut avoir des capteurs embarqués ou des capteurs externes qui lui sont connectés. Avec plus de puissance de traitement, le tag peut collecter des données auprès des capteurs et traiter localement les données avant diffusion.

- Avantages: Peut avoir plus de mémoire, stocker plus de données Puissance réduite des interrogateurs Portée de lecture plus longue (100 pieds et plus)
- Inconvénient: Contribue au bruit radio Sensible aux environnements difficiles Autonomie de la batterie limitée (2 à 7 ans) Coûte plus Plus grande taille et poids Nécessite la présence d'un interrogateur pour fonctionner

Figure 1.10: Tag Active

Les tags RFID ont différents types de mémoire (United States Government Accountability Office, 2005) :

Tags en lecture seule : ont une capacité de stockage minimale (généralement moins de 64 bits) et contiennent des données programmées en permanence qui ne peuvent pas être modifiées. Ces tags contiennent principalement des informations d'identification des articles et ils sont utilisées par exemple dans les bibliothèques et les magasins de location de vidéos.

Tags en lecture-écriture : en plus de stockage des données, elles peuvent permettre la mise à jour des données si nécessaire. Par conséquent, ils ont une plus grande capacité de mémoire et sont plus chers que les tags en lecture seule. Ces tags sont généralement utilisés lorsque les données doivent être modifiées tout au long du cycle de vie d'un produit, comme dans la fabrication ou la gestion de la chaîne d'approvisionnement.

Tags écriture unique, lecture multiple : permettent de stocker les informations une seule fois, mais ne permettent pas les mises à jour ultérieures des données. Ce tag fournit les fonctionnalités de sécurité d'un tag en lecture seule tout en ajoutant la fonctionnalité supplémentaire des tags en lecture-écriture.

1.1.5.2.3 Middleware RFID Middleware est un logiciel d'identification par radiofréquence (RFID), situé entre les lecteurs et les applications d'entreprise/métier. Le middleware a plusieurs fonctions et joue un rôle majeur dans le fonctionnement et la gestion du système RFID. Le middleware gère non seulement les lecteurs et les applications métier, mais gère, filtre, agrège et donne un sens aux données provenant des tags RFID.

1.1.6 Principe de communication RFID

Essentiellement, la communication RFID est effectuée lorsque le tag passive sans batterie reflète les ondes porteuses envoyées par le lecteur/enregistreur (figure 1.11). Le flux de communication est comme suit :

- Le lecteur émet des ondes radio.
- L'antenne à l'intérieur de tag reçoit les ondes radio du lecteur/enregistreur.
- Le courant électrique traverse le circuit intégré, convertissant les données de la puce en signaux.
- Les signaux sont transmis à partir de l'antenne imprimée par électrode sur le tag.
- L'antenne du lecteur reçoit les signaux renvoyés par le tag.

Le couplage par rétrodiffusion utilise des ondes électromagnétiques et le couplage inductif utilise un champ magnétique pour échanger des données entre le tag et lecteur.

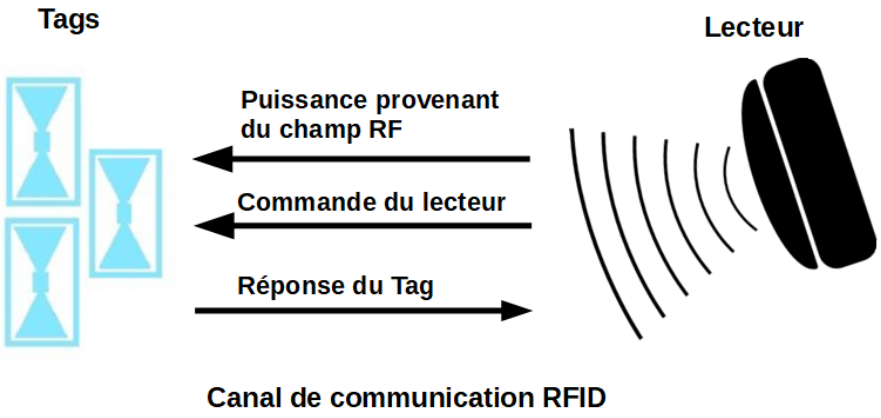

Figure 1.11: Communication RFID

1.1.6.1 Couplage inductif

Le processus de communication par couplage inductif (figure 1.12):

- Sur la base des données stockées, la micropuce de tag contrôle l'activation et la désactivation d'une résistance de charge qui influencera la tension dans l'antenne du lecteur.
- Ensuite, le lecteur peut détecter les changements de tension dans sa propre antenne.
- Le champ électromagnétique du lecteur pénètre dans la bobine de tag sur une distance plus courte.
- Par induction, une tension est générée dans la bobine d'antenne du tag.
- Cette tension est redressée et sert comme alimentation du tag.

1.1.6.2 Couplage de propagation

Le processus de communication par couplage de propagation (figure 1.13):

- Les ondes électromagnétiques sont réfléchies par des objets dont les dimensions sont supérieures à environ la moitié de la longueur d'onde de l'onde.

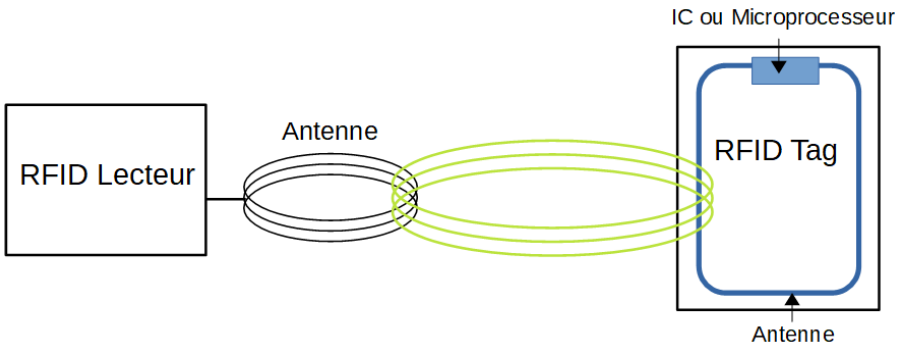

Figure 1.12: Couplage inductif RFID

- Une petite partie de la puissance électromagnétique du lecteur atteint le tag.
- Cette alimentation peut également être utilisée comme alimentation du tag (tag passif).
- Sur la base des données stockées, la micropuce modifie la charge connectée à l'antenne de tag, puis modifie les caractéristiques de réflexion de l'antenne.
- Ensuite, l'énergie RF réfléchie arrive à l'antenne du lecteur.

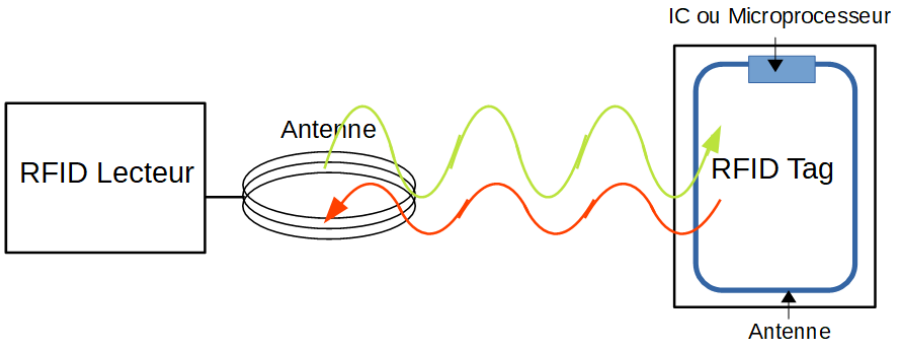

Figure 1.13: Couplage de propagation RFID

1.2 Intégration des Systèmes RFID dans les Réseaux de Capteurs Sans File

1.2.1 Les Réseaux de Capteurs Sans Fils

Un réseau de capteur sans fil (RCSF) Yick et al. [2008] (Figure 1.14) est un type de réseau sans fil constitué de dispositifs de capteurs répartis dans l'espace qui surveillent des informations physiques telles que la température, l'humidité, la lumière, l'acoustique, les vibrations et la pression. Les informations du capteur sont transmises à une ou plusieurs passerelles (puits) via des liaisons sans fil. Au cours de la dernière décennie, les RCSFs ont prouvé leur applicabilité

dans de nombreux scénarios, notamment la gestion des écosystèmes, les maisons et les bâtiments intelligents, la surveillance des risques naturels, les transports intelligents et la détection du comportement humain. La recherche sur les RCSFs a également motivé des domaines de recherche émergents, tels que l'Internet des objets (IoT) Atzori et al. [2010], les systèmes cyber physiques (CPS) Poovendran [2010] et les villes intelligentes et durables Badii et al. [2020], Reilly et al. [2019], Ogawa et al. [2019], Suri et al. [2018], Alrashdi et al. [2019], Singh et al. [2020a,b], Hassan et al. [2021], Shafiq et al. [2020], Zhang et al. [2020], Rahman et al. [2019], Khattak et al. [2019], Li et al. [2020a], Badii et al. [2019], Park et al. [2019], El Soussi et al. [2018], Cirillo et al. [2020], Basford et al. [2020].

En raison des portées de transmission limitées des noeuds de capteurs à faible puissance, les RCSFs adoptent normalement des topologies de communication multi-sauts, en particulier pour les applications qui nécessitent une large couverture de détection. Outre la transmission de ses propres données, un noeud de capteur dans un RCSF peut également relayer des données produites par des capteurs plus éloignés du puits. Les performances des applications de détection dépendent fortement des services réseau sous-jacents. Par exemple, les applications de surveillance des événements émergents telles que la détection d'incendie seraient sensibles au délai de transmission des données, tandis que les applications de collecte de données nécessitent un débit de réseau élevé et l'équité des lectures des capteurs. Par conséquent, la communication et la mise en réseau sans fil, y compris le contrôle du taux de détection, le routage, le contrôle d'accès au support (MAC) et le traitement du signal sans fil, jouent tous un rôle clé dans la conception globale du RCSF.

1.2.2 Défis pratiques des réseaux de capteurs sans fil

Les recherches actuelles démontrent les défis suivants dans les RCSFs :

Débit du réseau : En raison des interférences sans fil, des opérations cycliques et multi-sauts, et des débits de données limités des radios sans fil de faible puissance, la bande passante sans fil est une ressource rare dans les RCSFs. Un encombrement et une perte de paquets se produiraient lorsque les applications de détection produisent de lourd trafic de données. De plus, des études Bathula et al. [2009], Moeller et al. [2010] ont suggéré qu'il est essentiel de maximiser le débit de collecte de données. De plus, pour la réutilisation des ressources, plusieurs applications de détection peuvent coexister dans un même réseau physique (par exemple, l'Internet des objets Winter et al. [2012]), ce qui pose davantage de problèmes pour les communications réseau de bout en bout à haut débit sous-jacentes.

Équité de lecture du capteur : Les applications de collecte de données nécessitent généralement une répartition équitable des taux d'échantillonnage des capteurs (c'est-à-dire le taux auquel chaque noeud de capteur collecte des données d'environnement) Hou et al. [2008], Liu et al. [2010], Rangwala et al. [2006], Sridharan and Krishnamachari [2009]. Cependant, en raison du compromis fondamental entre le débit et l'équité Joe-Wong et al. [2013], la maximisation pure du débit entraînerait une mauvaise équité. Par exemple, dans un cadre de débit optimal, des taux de détection beaucoup plus faibles seraient alloués aux noeuds de capteurs éloignés du puits, par rapport à ceux proches du puits, ce qui entraînerait un biais potentiellement inacceptable dans les lectures provenant du réseau.

Énergie : En raison de leur capacité de stockage d'énergie limitée et de leur potentiel de déploiement à long terme, la pénurie d'énergie des noeuds de capteurs à faible coût et à faible consommation a été un problème clé pour le RCSF Joe-Wong et al. [2013], Sudevalayam and Kulkarni [2010]. Bien que le développement des technologies de récupération d'énergie (comme l'énergie solaire) puisse atténuer ce problème Sudevalayam and Kulkarni [2010], l'énergie reste une ressource de goulot d'étranglement. Cela est dû à la capacité de récupération d'énergie

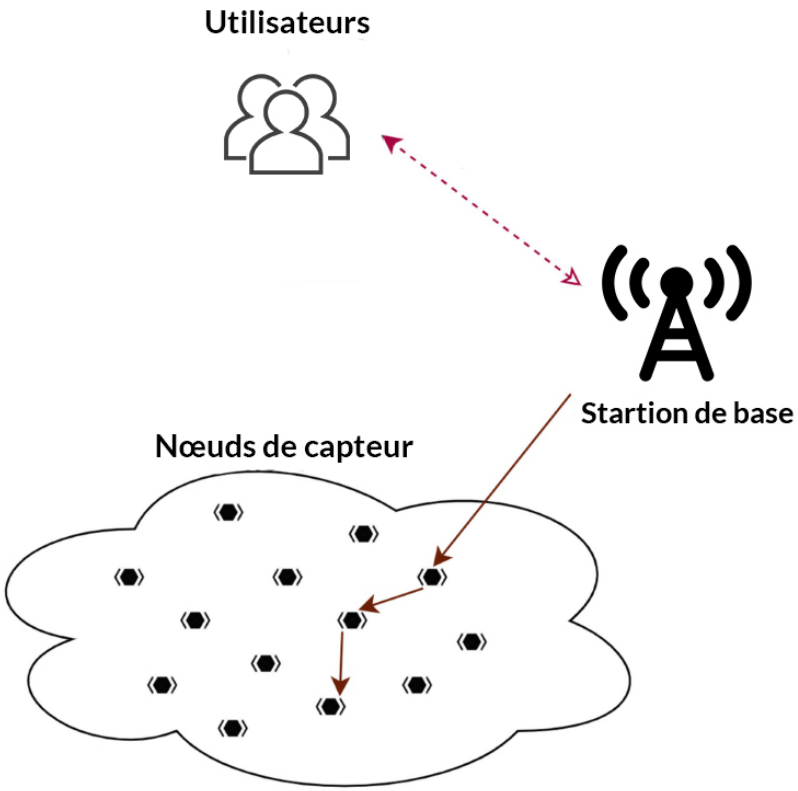

Figure 1.14: Structure de réseau de capteur sans fil

limitée (par exemple, les panneaux solaires équipés de minuscules noeuds de capteurs doivent être petits) et à la disponibilité intermittente de l'énergie environnementale (par exemple, il n'y a pas d'énergie solaire la nuit).

Capacité limitée des noeuds de capteurs : Les noeuds de capteurs adoptent normalement un système matériel simple et peu coûteux pour un déploiement potentiel à grande échelle. Un tel matériel à faible coût ne peut prendre en charge que des logiciels embarqués très efficaces et légers, qui nécessitent une faible complexité de calcul et de stockage des algorithmes RCSF.

Dynamique du système et incertitude : Les RCSFs sont de nature dynamique avec une qualité de liaison sans fil fluctuante Gnawali et al. [2009], Moeller et al. [2010], une dérive d'horloge locale Sivrikaya and Yener [2004] et des modèles de trafic de données hybrides (par exemple périodiques, basés sur des événements et basés sur des requêtes) Akkaya and Younis [2005]. De plus, la mobilité des noeuds est introduite dans les RCSFs, pour économiser de l'énergie Marta and Cardei [2009], pour assurer la connectivité Park and Heidemann [2011], ou pour satisfaire des exigences applicatives spécifiques Dyo et al. [2012]. De plus, les progrès récents dans les techniques de récupération d'énergie offrent des opportunités pour réaliser des opérations durables dans les RCSFs Sudevalayam and Kulkarni [2010]. Cependant, cela introduit également des ressources énergétiques variables dans le temps et incertaines. Ces dynamiques de réseau ont toutes des impacts significatifs sur les performances RCSFs et posent des défis pour la conception d'algorithmes RCSF.

Exigences des opérations réparties : En raison de leur évolutivité et de leur adaptabilité à la dynamique du réseau, les algorithmes distribués sont normalement préférés aux algorithmes centralisés dans les RCSFs. Contrairement aux approches centralisées qui résolvent les problèmes de réseau sur la base d'informations de réseau complètes, les algorithmes distribués nécessitent que des noeuds de capteurs individuels communiquent entre eux afin de résoudre de manière collaborative le problème de réseau global sur la base d'une connaissance du réseau local et incomplète, ce qui est donc plus difficile.

Prise en charge de la détection omniprésente : La détection devient omniprésente, des capteurs de température et de lumière dans les bâtiments intelligents à la détection des fuites d'eau dans les égouts et à la surveillance du bruit et de la qualité de l'air dans les rues. Certains capteurs sont capables de se connecter à Internet. Cependant, cela peut dans certains cas s'avérer prohibitif. Par exemple, les communications de données cellulaires 3G peuvent être coûteuses, tandis que les connexions à courte portée basées sur CSMA ne sont pas toujours disponibles. Une alternative intéressante consiste à utiliser des appareils mobiles transportés par des véhicules ou des individus pour collecter des données de capteurs de manière opportuniste, tirant ainsi parti à la fois des communications à courte portée peu coûteuses et des appareils mobiles omniprésents. Cependant, ce paradigme de détection et de communication opportuniste introduit de nouveaux défis tels que l'incitation à la participation des propriétaires d'appareils mobiles.

Les systèmes d'identification par radiofréquence (RFID) et les réseaux de capteurs sans fil (RCSFs) représentent deux technologies clés pour l'informatique omniprésente qui ont attiré une attention considérable ces dernières années puisque leur utilisation révolutionne divers domaines d'application. Cependant, ces deux technologies ont des domaines de recherche et développement distincts. L'intégration de la RFID et des réseaux de capteurs peut accroître leur utilité dans d'autres domaines scientifiques et techniques en exploitant les avantages des deux technologies. Dans ce chapitre, nous étudions pourquoi l'intégration des systèmes RFID et des RCSFs est importante et nous identifions les exigences clés pour parvenir à une intégration efficace. Nous présentons les architectures d'intégration de réseaux de capteurs RFID et sans fil et fournissons une liste détaillée d'exemples d'applications réelles.

1.2.3 Pourquoi intégrer les réseaux RFID et RCSFs ?

L'intégration des technologies RFID et RCSF maximisera leur efficacité, et permettra d'offrir de nouvelles perspectives à un large éventail d'applications utiles et comblera le fossé entre le monde réel et le monde de la recherche/universitaire. En effet, la technologie intégrée résultante aura des capacités étendues, une évolutivité et une portabilité ainsi que des coûts inutiles réduits Mitrokotsa and Douligeris [2009].

Parmi les avantages de cette intégration: Extension des capacités et des fonctionnalités : Compte tenu du fait que les réseaux RFID peuvent fournir des informations critiques, telles que l'identité et la localisation d'un objet, en fusionnant les RFID avec les RCSFs, des informations supplémentaires peuvent être récupérées, tandis que le potentiel d'exploitation de ces informations est multiplié. Par exemple, dans la gestion de la chaîne d'approvisionnement, nous sommes en mesure non seulement de suivre les produits alimentaires, mais également de surveiller leurs conditions environnementales.

Évolutivité-portabilité : Les systèmes RFID intégrés aux RCSFs bénéficient des avantages de la communication sans fil. La transmission et le traitement des données et informations critiques sont facilités sans la charge et les inconvénients des transactions filaires tout en économisant un temps précieux. Les lecteurs RFID portables peuvent encore accélérer la collecte de données et faciliter les procédures dans diverses applications. Par exemple, les applications de soins de santé, y compris la surveillance des médicaments quotidiens des personnes âgées ou la surveillance des

patients pour le diagnostic des décès, peuvent être extrêmement facilitées sans rendre les patients immobiles grâce à des câblages de données encombrants.

Réduction des coûts inutiles : La réduction du coût des services employés est un facteur critique dans de nombreuses applications, y compris les applications industrielles. L'exigence est d'atteindre l'objectif souhaité avec le coût minimum possible en prenant en charge des solutions de sauvegarde en cas de circonstances indésirables. Par exemple, les marchandises périssables peuvent être surveillées de sorte que, dans le cas où ils ne sont pas correctement stockés, leur transport puisse être interrompu, évitant ainsi des coûts de transport supplémentaires inutiles.

1.2.4 Exigences pour l'intégration des réseaux RFID et RCSFs

L'intégration des RFID et des RCSFs doit être effectuée de manière à répondre aux exigences spécifiques pour disposer d'une solution efficace. Certaines des exigences les plus importantes à prendre en considération sont les travaux suivants Cho et al. [2007], Mitrokotsa and Douligeris [2009]:

Communication précise et fiable : Dans les réseaux clients-serveurs traditionnels, de grands flux de données sont transférés des serveurs aux clients. Cependant, dans les systèmes RFID et RCSF intégrés, le flux de données est principalement transféré d'un grand nombre d'appareils (clients) vers quelques serveurs. Par la suite, les serveurs sont censés traiter toutes les informations reçues des RFID et des capteurs de manière fiable et permettre de prendre les mesures appropriées dans un court laps de temps. Fiabilité et précision sont également attendues pour les données transférées aux applications (ou utilisateurs) du système intégré dans une latence tolérable. La capacité du réseau de capteurs RFID intégrés à fournir des données à la destination requise avec fiabilité et à fournir une confirmation de la réussite d'une tâche est d'une importance considérable. La fiabilité et la précision d'un réseau de capteurs RFID intégrés dépendent également de la criticité de l'application spécifique. Dans les applications moins critiques, un degré de fiabilité inférieur est requis.

Efficacité énergétique : Compte tenu du fait que les noeuds de capteurs et les tags RFID actives présentent des ressources limitées, le réseau de capteurs RFID intégrés devrait prendre en compte cette limitation. Le système intégré doit être économe en énergie pour garantir une communication précise et fiable avec une consommation d'énergie minimale.

Survivabilité de la maintenance du réseau : Compte tenu du grand nombre d'appareils pouvant être utilisés dans un réseau de capteurs RFID intégrés, l'une des exigences les plus importantes pour un tel réseau est la capacité d'effectuer la configuration des appareils à distance et les mises à jour logicielles des appareils à distance. Ainsi, nous pouvons atteindre une capacité de survie élevée et une maintenance efficace du réseau avec un coût acceptable. De plus, il est important que le réseau intégré soit capable de récupérer en cas d'attaques possibles de périphériques ou de déni de service (DoS). Un moyen possible d'y parvenir serait l'adoption de mécanismes de tolérance aux intrusions ainsi que d'atténuation tels que l'utilisation de réplication de périphériques réseau critiques.

1.2.5 Architectures possibles des réseaux RFID et RCSFs intégrés

Les tags RFID intégrés à capteurs ou capteurs-tags, comme nous allons les désigner par la suite, peuvent être distingués en deux catégories principales : les capteurs-tags intégrés qui ne peuvent communiquer qu'avec les lecteurs RFID et les capteurs-tags intégrés qui sont capables de communiquer entre eux et de former un réseau ad hoc coopératif. Dans cette section, nous fournirons les principales caractéristiques de ces deux catégories de capteurs-tags intégrés et nous présenterons également un aperçu des recherches et propositions commerciales disponibles pour

chaque catégorie.

1.2.5.1 Tags RFID intégrées avec capteurs

1.2.5.1.1 Capteurs-Tags intégrés avec capacités de communication limitée

L'un des moyens les plus simples d'intégrer les réseaux RFID avec les RCSFs est l'intégration de capacités de détection dans les tags RFID. De nombreuses tags RFID a incorporé des capteurs dans leur conception et, ainsi, ils sont capables de prendre des lectures de capteurs et de les transmettre plus tard à un lecteur. Néanmoins, lorsque les tags RFID reçoivent des capacités de détection, la frontière entre les réseaux RFID et les réseaux de capteurs devient floue car les tags-capteurs utilisent les mêmes protocoles et mécanismes pour lire les identifiants des tags et pour collecter les données détectées. Dans cette architecture, les tags-capteurs intégrés fonctionnent comme des tags RFID normales et sont équipées d'une identification unique, tandis que les capteurs intégrés sont utilisés pour collecter des informations de détection liées à l'environnement, aux conditions existantes et aux objets associés (Figure 1.15). L'intégration des tags RFID avec des noeuds de capteurs est basée sur la conversion du signal analogique des capteurs par le module A/D tandis que les données résultantes sont transmises par les lecteurs à la station de base Bouhassoune et al. [2019].

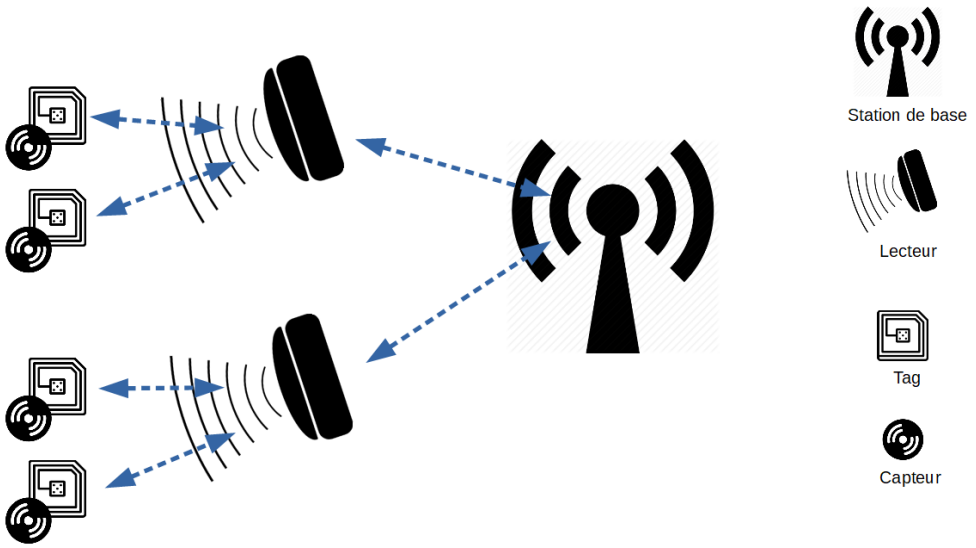

Figure 1.15: Architecture d'intégration de capteur-tag, lecteur RFID et station de base

1.2.5.1.2 Capteurs-Tags intégrés avec capacités de communication étendue

Les tags-capteurs intégrés qui ne peuvent communiquer qu'avec les lecteurs RFID peuvent être considérées comme des tags RFID avec des capacités de détection supplémentaires mais avec des capacités de communication limitées. Cependant, il est possible d'intégrer des noeuds de capteurs avec des tags RFID afin que les tags de capteurs intégrés puissent communiquer entre elles ainsi qu'avec d'autres appareils sans fil. Ainsi, cette catégorie comprend les capteurs-tags intégrés qui dépassent les limites d'une communication possible uniquement avec un lecteur RFID et sont capables de communiquer entre eux via un réseau ad hoc coopératif (Figure 1.16).

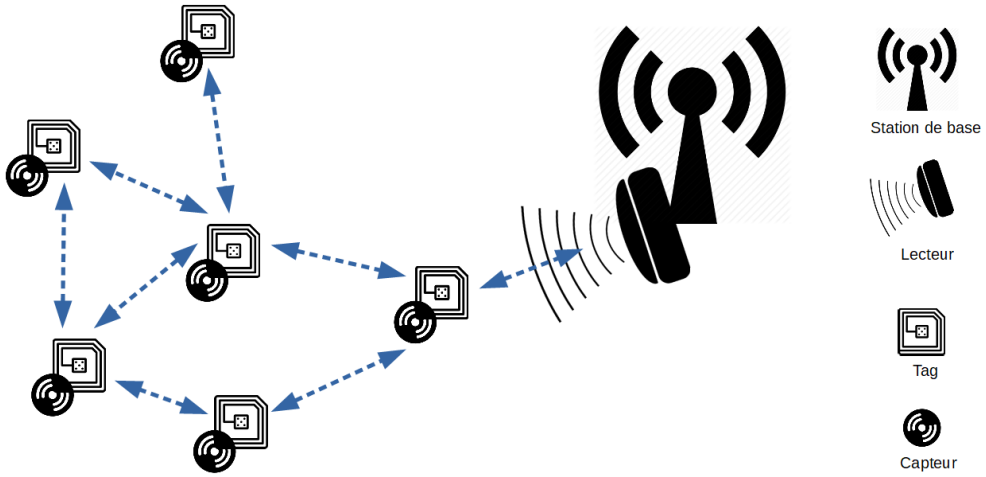

Figure 1.16: Architecture d'intégration de capteur-tag et de lecteur-station de base

1.2.5.2 Intégration de lecteurs RFID avec des noeuds de capteurs sans fil

Une autre stratégie possible d'intégration des systèmes RFID aux RCSF consiste à intégrer des lecteurs RFID aux noeuds de capteurs. Dans ce scénario d'intégration, l'existence de trois types d'appareils est supposée : les lecteurs/noeuds capteurs RFID intégrés, les tags RFID simples et le puits ou la station de base. Ce type d'intégration a été introduit pour la première fois par Zhang et al. Zhang and Wang [2006]. Ils ont qualifié le noeud de lecteur/capteur RFID intégré de noeud intelligent. Les noeuds intelligents intégrés peuvent être considérés comme des noeuds de capteurs pouvant être utilisés comme lecteurs RFID étendant leurs capacités de détection. Les noeuds intelligents sont capables de relayer des informations et d'être configurés en tant que noeuds relais d'un RCSF. Ils sont capables de communiquer entre eux en créant un réseau de communication ad hoc. Le noeud de lecteur/capteur RFID intégré est capable de fonctionner comme un routeur et de transmettre des messages à la bonne destination. Les noeuds intelligents sont chargés de collecter des données à partir de simples tags RFID dans leur portée et communiquent entre eux pour relayer les données vers la station de base où toutes les données sont collectées et traitées par un humain. L'architecture de ce réseau intégré, illustrée à la Figure 1.17, est similaire au RCSF à deux niveaux basés sur le clustering hiérarchique. Ce type de stratégie d'intégration ouvre de nouvelles perspectives dans les applications probables.

Les limites des lecteurs RFID traditionnels, notamment leur fonctionnement passif, leurs graves problèmes de mobilité en raison de leur volume important et la position de leurs antennes limitent leurs applications potentielles. Le noeud intelligent intégré est plus petit, moins coûteux et plus facile à déployer. Cependant, cette stratégie d'intégration présente également des inconvénients importants, car elle se caractérise par des modèles de trafic many-to-one et présente certains problèmes liés au déséquilibre énergétique entre les noeuds intelligents.

1.2.5.3 Architecture mixte

Dans l'architecture mixte, les tags RFID et les noeuds capteurs sont des dispositifs physiquement distincts, mais ils coexistent dans un réseau intégré et ils fonctionnent indépendamment. Le

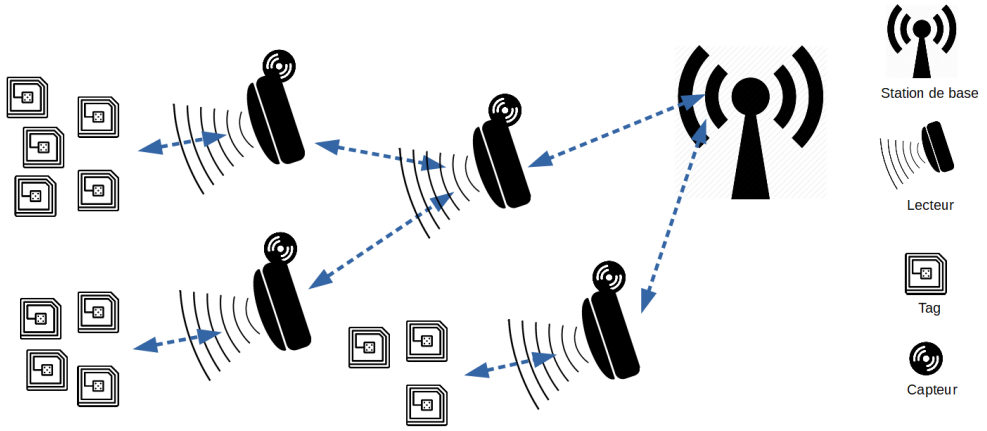

Figure 1.17: Intégration de lecteurs RFID avec des noeuds de capteurs sans fil

principal avantage d'une telle architecture mixte réside dans le fait qu'il n'est pas nécessaire de concevoir un dispositif matériel intégré. Cependant, il existe une possibilité d'interférence de communication entre les tags/lecteurs RFID et les noeuds capteurs car dans ce cas, les dispositifs physiquement sont distincts. Les procédures qui doivent être suivies pour éviter cette interférence peuvent entraîner une surcharge supplémentaire.

Initialement, l'architecture mix a été discutée par Zhang et al. Zhang and Wang [2006]. Selon Zhang et al. un réseau de capteurs RFID intégrés qui suit l'architecture mixte se compose de trois types de dispositifs : les stations intelligentes, les tags RFID normales et les noeuds de capteurs normaux (Figure 1.18). Une station intelligente est un appareil spécial composé d'un lecteur RFID, d'un microprocesseur et d'une interface réseau. Les stations intelligentes ne présentent pas de contraintes de puissance et elles sont capables d'agréger les informations des tags RFID et des noeuds capteurs et de les transmettre à un serveur local ou à un LAN distant. Les informations des tags RFID et des noeuds capteurs peuvent être transmises à la station de base. Parce que les stations intelligentes ne sont pas confrontées à des contraintes de puissance, l'architecture de protocole Internet traditionnelle peut également être déployée. Ainsi, les stations intelligentes sont capables d'effectuer non seulement des traitements de données mais également des protocoles de routage et des protocoles de transport tels que TCP. Un protocole de communication qui peut être utilisé dans un environnement aussi hétérogène est la technologie 802.11/WiFi.

1.2.6 Applications des technologies RFID et RCSFs dans l'Internet des objets

L'interconnexion entre les objets via Internet a beaucoup attiré l'attention des chercheurs et des entreprises du monde entier Gubbi et al. [2013], Atzori et al. [2010]. Dans ce contexte, le terme 'Internet des objets' (IoT) est largement utilisé pour désigner la présence de choses ou d'objets autour de personnes qui, grâce à un seul schéma d'adressage, sont capables d'interagir les uns avec les autres et de coopérer avec leurs voisins pour atteindre des objectifs communs Giusto et al. [2010]. Dans le rapport Hype Cycle for Emerging Technologies publié en 2014 par Gartner's, le loT est la technologie la plus en vogue en développement aujourd'hui Burton and Willis [2014]. Selon Campos and Cugnasca [2014] l'International Data Corporation (IDC), le nombre d'objets connectés à Internet a dépassé le nombre de personnes sur terre en 2008.

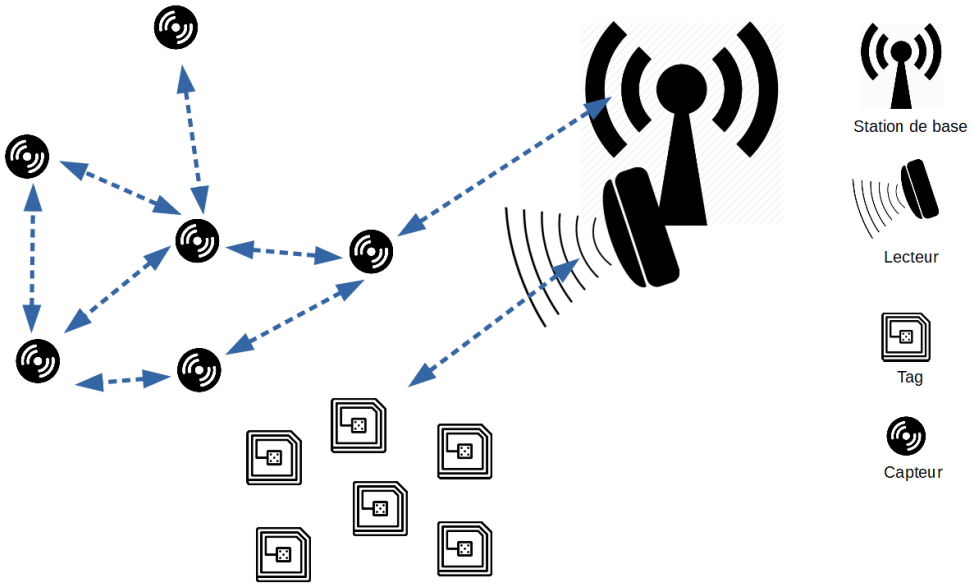

Figure 1.18: Architecture mixte de tags RFID et de noeuds de capteurs

Dans ce scénario, deux technologies ont permis l'avancement du loT : l'identification par radiofréquence (RFID) et les réseaux de capteurs sans fil (RCSF). La technologie RFID permet d'identifier des objets et de capturer des données sans avoir besoin d'un champ visuel entre le lecteur et l'identifiant Jia et al. [2012]. Les RCSFs permettent de surveiller les paramètres de l'environnement, tels que la température, l'humidité relative, le potentiel hydrique du sol, la lumière, la pression atmosphérique, etc. Mainetti et al. [2011]. Ainsi, un nombre croissant d'applications ont émergé sur la base du paradigme loT. Après un examen approfondi de la littérature, les applications des technologies RFID et RCSF pour IoT ont été regroupées en cinq catégories, comme suivants (figure 1.19): soins de santé, agriculture, logistique, villes intelligentes et maison intelligente.

Soins de santé : La plupart des applications se concentrent sur le réseau corporel (BAN), également appelé réseau de capteurs corporels (BSN) ou réseau corporel sans fil (WBAN). Des capteurs sont utilisés pour surveiller des paramètres, tels que la pression artérielle, la température corporelle, l'activité respiratoire. À cette fin, les capteurs peuvent être entièrement à l'intérieur, sur et à proximité immédiate d'un corps humain dans des poches, à la main, etc. Grâce à des passerelles, il est possible pour les professionnels de la santé d'accéder aux données des patients en ligne Pang et al. [2015]. Par conséquent, il existe des applications qui impliquent la surveillance des patients, la détection des chutes et les réfrigérateurs médicaux Pang et al. [2014].

Agriculture : Les applications dans le domaine de l'agriculture qui utilisent la RFID, les capteurs, les actionneurs et leur réseau sont aujourd'hui à un stade avancé Ruiz-Garcia and Lunadei [2011], Abbasi et al. [2014]. Cela a contribué à une augmentation des variétés de terminologies actuellement utilisées, telles que l'agriculture de précision (PA), l'agriculture intelligente, la technologie à taux variable (VRT), l'agriculture de précision, l'agriculture du système de positionnement global, l'agriculture par pouce, l'agriculture à forte intensité d'informations, spécifique au site. Gestion des cultures, etc. Srinivasan [2006]. Dans ce contexte, les domaines d'application suivants sont pris en considération : l'irrigation, la traçabilité alimentaire, l'identification et la

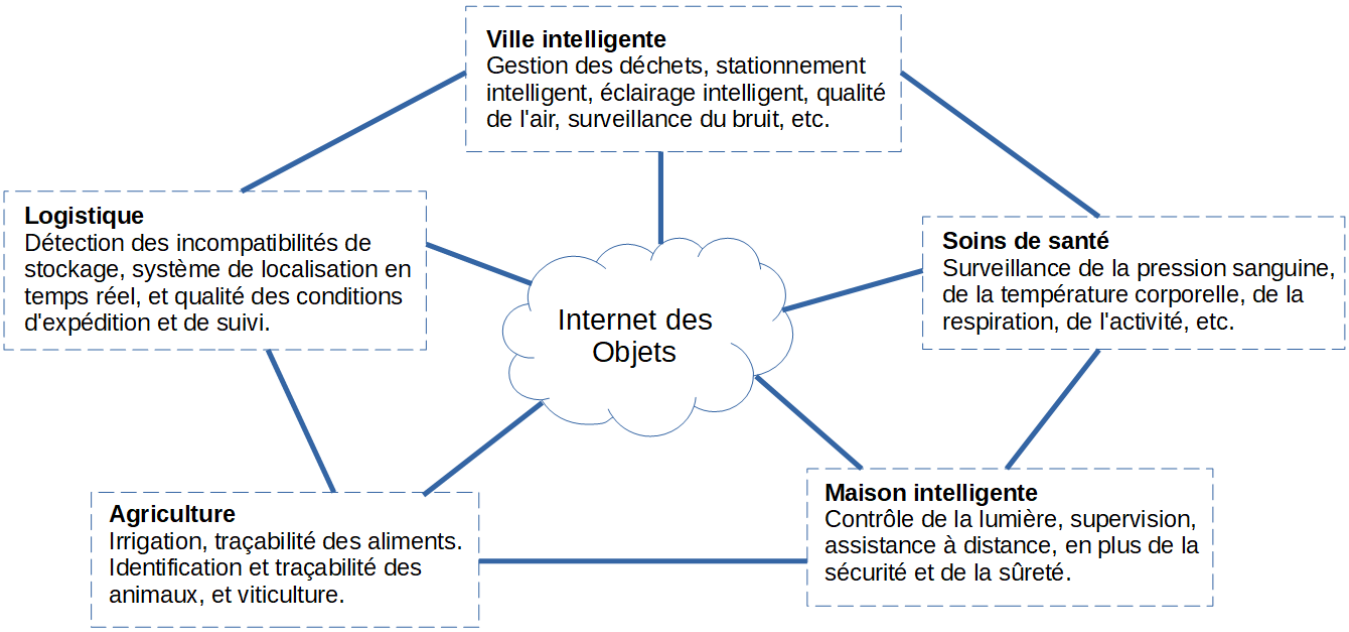

Figure 1.19: Application et connectivité des domaines de l'IoT

traçabilité des animaux Yan-e [2011], et la viticulture.

Logistique : L'utilisation des technologies RFID et RCSFs soutient la logistique dans un sens très positif Cheung et al. [2008]. La combinaison de la logistique et du loT permet une optimisation et des systèmes de distribution en temps réel. Presque tous les faits d'une entreprise, des identifiants aux capteurs omniprésents, sont disponibles instantanément. Les applications actuelles incluent, entre autres, la détection d'incompatibilité de stockage Atali et al. [2009], le système de localisation en temps réel (RTLS) Kamel Boulos and Berry [2012] et la qualité des conditions d'expédition et de suivi Mahlknecht and Madani [2007].

Villes intelligentes : L'adoption du paradigme à plus grande échelle trouve des applications dans de nombreux domaines et contextes différents d'une ville, Schaffers et al. [2011]. Dans un article Zanella et al. [2014], des applications loT dans les villes intelligentes sont présentées, comme suit : santé structurelle des bâtiments, gestion des déchets, qualité de l'air, surveillance du bruit, embouteillages, consommation d'énergie de la ville, stationnement intelligent, éclairage intelligent, et l'automatisation et la salubrité des bâtiments publics.

Maisons intelligentes : Les réseaux domotiques sans fil (WHAN) permettent des applications de surveillance et de contrôle pour le confort des utilisateurs à domicile et une gestion efficace de la maison. Les WHAN permettent une variété de cas d'utilisation, comme présenté dans Gomez and Paradells [2010], avec une liste d'exemples non exhaustive : contrôle de la lumière, télécommande, soins à distance, en plus de la sécurité et de la sûreté.

1.2.7 Le problème de collision lié à l'intégration des systèmes RFID dans les réseaux de capteurs sans fil

Les RCSFs-RFID suivent généralement diverses stratégies MAC qui leur permettent d'accéder aux canaux de communication sans fil. Cependant, les noeuds peuvent tenter d'accéder aux canaux sans fil en même temps, ce qui peut entraîner des collisions entre plusieurs noeuds. Les facteurs qui influencent ce problème sont les suivants:

Environnements denses: L'avènement des villes intelligentes et la nécessité d'améliorer la productivité, la traçabilité, la sécurité et l'agilité des installations occasionnelles ont entraîné un déploiement plus important de lecteurs pour assurer la couverture de la zone de déploiement. Si les déploiements denses sont censés améliorer la couverture et le délai, ils ont surtout pour effet de générer des collisions. Ces collisions se produisent à différents niveaux, mais dans notre these, nous nous concentrerons uniquement sur les collisions de lecture. Ces dernières se produisent lorsque plusieurs lecteurs tentent de lire simultanément une étiquette donnée. Comme les étiquettes sont des entités passives, sans capacité de calcul ou de dissociation de fréquence, elles sont incapables de différencier les différentes demandes provenant des lecteurs et identifieront les multiples demandes comme du bruit radioélectrique, ce qui fait que l'étiquette n'est pas lue.

Mobilité: dans le cas d'une ville intelligente où les tags sont fixées aux infrastructures urbaines, le système ne peut pas dépendre de lecteurs fixes, l'utilisation de véhicules de transport public ou de vélos publics pourrait aider à atteindre toutes les étiquettes déployées. Cependant, l'utilisation de lecteurs mobiles entraîne une augmentation des collisions. En effet, lorsque la mobilité n'est pas contrôlée pour gérer les collisions de plusieurs lecteurs qui scrutent le terrain, il en résulte une augmentation des collisions. les collisions de plusieurs lecteurs parcourant la même zone, cela induit des des problèmes d'étiquettes non lues et éventuellement non couvertes, ce qui va à l'encontre du l'objectif initial d'avoir des lecteurs mobiles.

Dans le chapitre suivant, nous présentons en détail le problème de collision des réseaux de capteurs RFID. Nous nous concentrons sur les collisions de lecteurs RFID et nous abordons les différents protocoles anti-collision proposés dans la littérature.

1.3 Problèmes de collision RFID

Dans les systèmes RFID, les lecteurs et les tags peuvent communiquer en utilisant la même fréquence. Ainsi, une transmission simultanée peut se produire, ce qui conduit à des collisions. Les collisions détruisent le numéro d'identification EPC de tag et peuvent également interférer avec les commandes de contrôle des lecteurs. De ce fait, le problème de collision est la principale source de retards dans le processus d'identification. Il existe deux types de collisions : les collisions de lecteurs et les collisions de tags. Les sections suivantes décrivent les deux types et leurs effets sur les performances du système.

1.3.1 Les collisions dans les systèmes RFID

1.3.1.1 Collision des Lecteurs

Dans un réseau RFID, une densité élevée des lecteurs peut avoir des répercussions sur les performances du système, en raison de nombreux collisions provoquées. En conséquence, le système peut subir une dégradation de l'efficacité de la collecte de données, une augmentation du temps de communication et une consommation d'énergie élevée. Ainsi, les collisions représentent un problème critique qui dégrade considérablement les performances des systèmes RFID.

De plus, deux types de collisions de lecteur sont définis: Reader to Reader Interference (RRI)

et Reader to Tag Interference (RTI). La figure 1.20 représente deux lecteurs (R1 et R2) et trois tags (T, T1 et T2) avec le champ de lecture (rr1 et rr2) et le champ d'interférence (cr1 et cr2) de deux lecteurs successivement. DR1R2 représente la distance entre ces lecteurs.

1.3.1.1.1 RRI - Reader to Reader Interference

Le RRI montré dans la figure 1.20-a se produit lorsque plusieurs lecteurs dans un champ d'interférence (équation 1.1) communiquent simultanément utilisant la même fréquence.

$$rr1 + rr2 < d_{R1R2} < max(cr1, cr2) \tag{1.1}$$

Dans un premier temps, le lecteur R2 essaie d'interroger le tag T2, tandis que le tag T1 répond à la requête du lecteur R1 situé dans le champ d'interférence de R2 et utilisant la même fréquence, ce qui provoque une collision de type Reader to Reader. Pour éviter le RRI, les deux lecteurs doivent utiliser deux fréquences distinctes ou fonctionner dans des tranches de temps différentes.

1.3.1.1.2 RTI - Reader to Tag Interference

Concernant le RTI, deux types d'interférences peuvent être distingués. La première survient lorsque plusieurs lecteurs tentent d'interroger simultanément le même tag dans leur champ de lecture commune (équation 1.2), indépendamment de la fréquence utilisée. Une représentation de cette interférence est donnée dans la figure 1.20-b.

$$d_{R1R2} < rr1 + rr2 \tag{1.2}$$

Dans le cas où les lecteurs R1 et R2 tentent d'interroger le tag T simultanément, ce tag ne pourra pas décoder la requête des deux lecteurs, et l'interrogation ne sera pas effectuée. Ainsi, afin d'éviter la collision RTI, les deux lecteurs doivent fonctionner dans un intervalle de temp différente.

Le deuxième type de RTI se produit lorsqu'un tag se trouve dans le champ d'interférence d'un lecteur et dans le champ de lecture d'un autre lecteur (équation 1.3) qui fonctionne sur la même fréquence. Cette interférence est représentée sur la figure 1.20-c.

$$max(cr1, cr2) < d_{R1R2} < max(cr1 + rr2, cr2 + rr1) \tag{1.3}$$

Même si deux lecteurs n'interfèrent pas, le tag dans cette situation provoquera une collision. Ce type de collision est le plus étendu par rapport aux autres type précédents, ce qui complique davantage la convergence vers un déploiement sans collision. Dans la figure 1.20-c, RTI est déclenché lorsque le lecteur R1 essaie d'interroger le tag T1 située dans la zone d'intersection du champ de lecture de R1 et du champ d'interférence de R2 et qu'ils essaient simultanément de lire le tag T2, donc ce signal atteint également le tag T1 produisant une collision. Pour arrêter l'apparition de ce type de collision, les lecteurs concernés doivent opérer sur des fréquences différentes ou des intervalles de temps différents.

1.3.1.2 Collisions des Tags

Ce type de collision est le type de collision le plus courant dans les systèmes RFID denses Li et al. [2006], Pillai et al. [2005], Wang and Liu [2006], Liu and Lai [2006]. Dans de tels systèmes, il y a un seul lecteur RFID et plusieurs tags, comme le montre la figure 1.21. L'objectif principal est d'identifier toutes les tags dans la zone de lecture en un temps minimum.

Cependant, dans les réseaux denses, le nombre de collisions des tags augmente, ce qui diminue l'efficacité de lecture, et donc augmente le temps de lecture. Par conséquent, il existe différentes

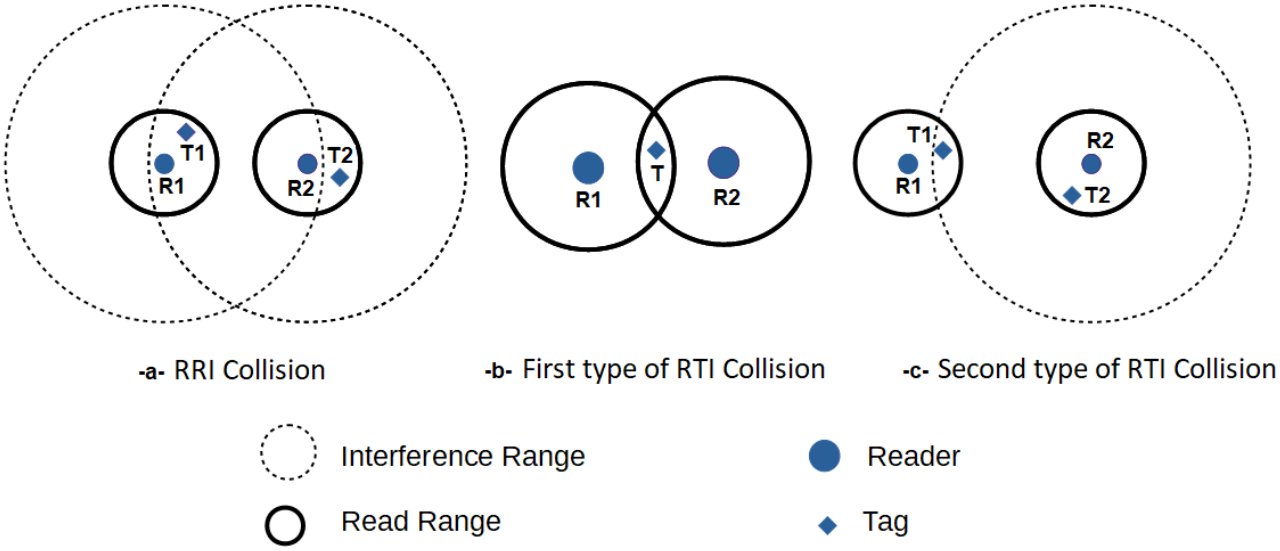

Figure 1.20: Collisions RFID. (a) Interférence entre lecteurs, (b) Interférence entre lecteurs et tags (1er type), (c) Interférence entre lecteurs et tags (2ème type)

propositions pour améliorer les protocoles anti-collision de la couche MAC en tenant compte des paramètres de la couche Physique.

1.3.2 Gestion centralisée ou distribuée des collisions entre lecteurs RFID ?

Dans cette thèse, nous nous concentrons pour la résolution des collisions côte lecteur de manière distribué. Plusieurs propositions ont été élaborées pour résoudre ces problèmes de collisions Reader to Reader et Reader to Tag et qui peuvent être classées en fonction de différents critères pour déterminer s'ils sont : Centralisé ou Distribué.

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

Centralisé : Dans cette configuration, les lecteurs communiquent avec une entité supérieure (serveur central) chargée de la programmation des opérations. Le serveur central est capable, après avoir rassemblé toutes les informations de la topologie des lecteurs, de calculer le schéma de lecture optimal réduisant les collisions. Cependant, en général, l'utilisation d'un serveur central restreint la mobilité des lecteurs au détriment d'un niveau de calcul et de latence plus élevé. Un lien de communication doit également être établi entre les lecteurs et cette entité supérieure. De plus, le fait que les lecteurs dépendent d'une entité supérieure pour toute opération rend les solutions moins réactives.

Distribué : Dans cette configuration, les lecteurs communiquent directement entre eux et localement (dans le temps et dans l'espace), s'accordent de manière paire à paire sur leurs schémas de fonctionnement pour réduire les collisions. Les lecteurs peuvent échanger avec leurs pairs dans l'étendue de leur portée de communication définissant leur voisinage, cela permet aux

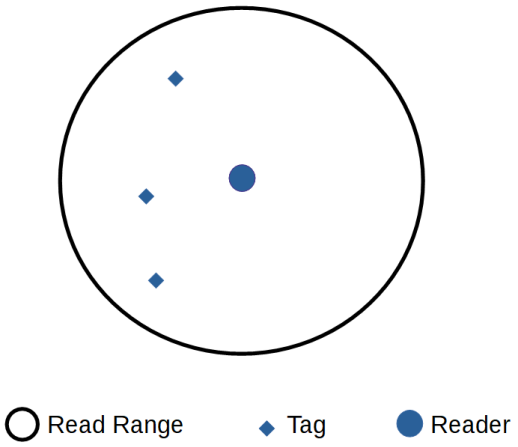

Figure 1.21: Collision entre plusieurs tags et un lecteur

solutions basées sur ce paradigme d'être évolutives et de supporter des changements dynamiques de topologie comme ce serait le cas avec les lecteurs mobiles. Chaque décision prise par un lecteur donné est dictée par sa connaissance de son voisinage à un instant donné.

1.3.3 La couche MAC anti-collision

Différents protocoles anti-collision de la couche MAC ont été développés pour séparer les signaux des lecteurs en collision sur la couche MAC, à savoir l'accès multiple par répartition en fréquence FDMA, l'accès multiple par répartition spatiale SDMA, l'accès multiple par répartition en code CDMA, l'accès multiple par répartition dans le temps TDMA et L'accès multiple à détection de porteuse CSMA.

FDMA : Dans ce protocole, la bande de fréquences est divisée en différentes sous-bandes de fréquences réparties entre différents lecteurs Myung [2007]. Cependant, cette technique ajoute de la complexité au système, car les lecteurs doivent pouvoir décoder différentes fréquences en même temps.

SDMA : Cette technique utilise l'étalement de tags sur la zone de lecture Kielstein et al. [2006]. Il fournit une forte augmentation de l'efficacité de lecture. Le principal inconvénient est le coût de mise en oeuvre du lecteur RFID à antennes multiples. De plus, dans les applications denses, les distances entre tags sont très faibles afin d'être réparties sur la zone de lecture.

CDMA : Ce protocole utilise des techniques de modulation à étalement de spectre pour transmettre les données sur l'ensemble du spectre Adachi et al. [2005]. Le CDMA est la procédure idéale pour de nombreuses applications, par exemple les systèmes de navigation. Cependant, le coût des tags augmente considérablement. De ce fait, ce n'est pas un protocole optimal pour les applications RFID denses.

TDMA : Dans ce protocole, une seule bande de fréquence est divisée en tranches de temps et attribuée aux lecteurs Ergen and Varaiya [2010]. Dans cette technique, chaque lecteur doit être synchronisée avec les Times Slots et envoie ses informations au début de la Times Slots sélectionnée. Cette technique peut être directement appliquée sur les systèmes RFID passifs. Dans de tels systèmes, la simplicité des tags transfère la complexité aux lecteurs, où le lecteur doit contrôler la synchronisation temporelle.

CSMA : Est un protocole de contrôle d'accès au support (MAC) Jiang and Walrand [2009]

dans lequel un noeud vérifie l'absence d'autre trafic avant de transmettre sur un support de transmission partagé, tel qu'un bus électrique ou une bande du spectre électromagnétique.

1.4 Protocoles anti-collision RFID: Etat de l'art

1.4.1 Protocoles distribués

Pour résoudre le problème de collision des lecteurs RFID, plusieurs chercheurs ont proposé des solutions pour la couche MAC. Dans cette section, nous mentionnons différents protocoles de la littérature selon l'architecture centralisée ou distribuée.

Pulse (A Survey of RFID Readers Anticollision Protocols) Birari and Iyer [2005] : Ce protocole tout comme le LBT, a des lecteurs qui écoutent le médium avant d'interroger les tags. Cependant, dans ce cas, pour éviter les problèmes d'écoute, les lecteurs 'pulse' constamment un signal pour alerter leurs voisins pendant le fonctionnement. Ainsi, lorsqu'un lecteur reçoit les balises pulsantes, il se désactive et attend que le support soit libre. Cela avait l'avantage de s'assurer qu'un et un seul lecteur interroge les tags dans un voisinage donné. Néanmoins, dans un environnement mobile dense, les lecteurs qui envoient une 'pulse' peuvent finir par désactiver un grand nombre de leurs voisins, ce qui a un impact considérable sur le débit et l'efficacité du système.

Comme Pulse, **Dica** Hwang et al. [2006] utilise également un canal de contrôle basé sur l'évitement de collision distribué CSMA. Dans cet algorithme, le lecteur diffuse un paquet "BRD_WHO" pour définir s'il y a un lecteur actif dans son champ d'interférence. Si le paquet "BUSY" est reçu, cela signifie que le canal de données est occupé. Sinon, si le paquet reçu est "BRD_END", le lecteur peut commencer à interroger les tags. Même si ce protocole peut résoudre le RTI en utilisant de nombreux intervalles de temps, il ne peut pas détecter le RRI.

Contrairement à PULSE et Dica qui n'utilisent qu'un seul canal de donne, **MCMAC** Olaleye et al. [2018] est un protocole de couche MAC multicanal distribué pour les réseaux RFID qui utilise plusieurs canaux de données pour interroger les tags et un canal de contrôle pour la communication lecteur-lecteur. Dans cette solution, chaque lecteur calcule son backoff de manière aléatoire et s'éteint. A la réception d'un message de contrôle, le lecteur sélectionne une fréquence libre et annonce de nouveaux canaux occupés. S'il n'y a pas de fréquence libre, il faut attendre le cycle suivant. Ce protocole souffre du RTI, car la lecture simultanée d'un même tag par deux lecteurs provoque des collisions même s'ils utilisent des fréquences différentes, puisque le seul canal de contrôle peut juste résoudre le RRI.

Dimitted Multi-Channel Collision Avoidance (**DiMCA**) Safa et al. [2015] : légèrement différent des algorithmes CSMA présentés précédemment, le protocole DiMCA propose aux lecteurs d'échanger des messages sur deux canaux de contrôle divers fonctionnant à des distances différentes. Le premier couvre le champ de lecture du lecteur où sont envoyés les messages contenant l'ID du lecteur et le second canal couvre le champ d'interférence où sont envoyés les messages contenant à la fois l'ID du lecteur et le canal choisi. Avant d'interroger les tags, un lecteur attend un temps aléatoire pendant lequel il peut recevoir des messages sur les canaux de contrôle. Ainsi, selon le type de message reçu, un lecteur conserve deux files d'attente de voisins interférents : ceux pour lesquels il peut opérer en même temps mais sur une fréquence différente et ceux pour lesquels il doit opérer différemment à la fois. Avant de commencer son opération d'interrogation, un lecteur vérifie sa file d'attente et en fonction de l'état, soit il choisit un autre canal et le diffuse à ses voisins au préalable, soit il attend un signal END de ses voisins pour opérer dans un autre cycle. Bien que cette solution améliore à la fois le débit et l'efficacité du système RFID, elle repose sur un surcoût créé par les messages échangés qui peut avoir un impact sur le délai.

Efficient Multichannel Reader Collision Avoidance (**EMRCA**) Jiang et al. [2016] prendre en compte l'aspect multicanal. Les auteurs identifient deux types de collisions en fonction de champ d'interrogation et d'interférence des lecteurs. Les lecteurs commencent par détecter le canal de contrôle commun utilisé par tous les noeuds pour se communiquer. Si aucune activité n'est détectée pendant une période donnée, le lecteur commence la phase de contention. Sinon, selon la source d'activité, soit démarré une nouvelle session d'écoute à la fin de l'activité en cours, soit poursuit le chronomètre avant la contention. Pendant la phase de contention, les lecteurs attendent un backoff aléatoire. Si un lecteur reçoit un beacon lors de ce délai d'attenteil revient à la détection du canal de contrôle, sinon si le délai s'achève sans aucune réception de beacon, le lecteur passe à l'interrogation des tags. Il occupe alors le canal de donne choisi et émet périodiquement un beacon d'annonce sur le canal de contrôle commun. Ce protocole améliore l'équité et l'efficacité globales de Pulse mais souffre toujours de la mobilité et de la forte drensité de déploiement des lecteurs.

Distributed Efficient Fair Anti-Collision (**DEFAR**) Mitton et al. [2016], est un protocole distribué basé sur TDMA, dont le but est de sélectionner au moins un lecteur dans un domaine de collision en échangeant des tags entre les lecteurs. Un lecteur est sélectionné en fonction de son identification et de son niveau de priorité. Cette méthode répartit différents niveaux de priorité entre ces lecteurs en fonction de leur comportement antérieur. Au moins un lecteur gagne un tour parmi d'autres. Cela signifie qu'une fois toutes les phases achevées, une meilleure couverture sera obtenue.

Coverage Oriented Reader Anti-Collision (**CORA**) Mbacke et al. [2016], est une solution pour les réseaux RFID avec un déploiement mobile et critique. Le lecteur effectue un apprentissage local de son voisinage. Pour cela, chaque lecteur commence par sélectionner un Time Slot, puis, renseigne ses voisins dans le domaine de collision. La collecte de ces informations par les lecteurs, permet à chacun de calculer le nombre de lecteurs en collision (même Time Slot) et non-collision (Time Slot différente) en fonction de leur Time Slot utilisée. Le lecteur peut s'activer et lire les tags si le nombre de lecteurs voisins non collisionnés est supérieur au nombre de lecteurs en collision.

High Adaptive MAC (**HAMAC**) Amadou and Mitton [2015], est un protocole dédié aux réseaux RFID mobiles et à grande échelle. Basé sur CSMA, ce protocole est utilisé pour atteindre une valeur d'attente maximale afin d'éviter plus de collisions. Pour ce faire, le lecteur met à jour dynamiquement sa Contention Windows (CW) en fonction du niveau de contention sur le canal partagé dans le réseau RFID. Chaque fois que le lecteur constate que tous les canaux sont occupés, il divise son CW en deux et sélectionne un nouveau backoff. Cela augmente encore sa priorité. Une fois que le lecteur atteint un nombre minimum de CW sans avoir de canal libre, le lecteur recommence avec la CW par défaut.

Distributed Color Selection (**DCS**): En utilisant DCS Waldrop et al. [2003], les lecteurs réservent périodiquement des Time Slots (ici appelées couleurs) en choisissant aléatoirement parmi la gamme de couleurs disponibles. Ces intervalles de temps sont ensuite utilisés pour interroger les tags. Ainsi, si deux ou plusieurs lecteurs voisins choisissent les mêmes couleurs, leurs signaux entrent en collision et les balises couvertes sont manquées. En cas de collision, les lecteurs concernés sélectionnent une nouvelle couleur parmi celles disponibles et envoient un message de kick aux voisins pour réserver le Time Slot pour le tour d'interrogation suivant. Tous les lecteurs de la couleur correspondante doivent changer de Time Slot pour le tour suivant. Le nombre de couleurs disponibles au choix est fixe et donné au départ. Selon le nombre maximum de couleurs disponibles, le système RFID est fortement affecté. En effet, si la valeur max couleurs est trop faible, un grand nombre de lecteurs finissent par choisir les mêmes couleurs et se heurtent, tandis que si la valeur est trop élevée, certains Time Slots ne sont pas occupés et le débit et délai de couverture sont impactés.

Colorwave Lee and Lee [2006] : Egalement connu sous le nom de DCS à maximum variable, cet algorithme résout le problème principal de DCS. Comme son nom l'indique, il permet de modifier le nombre maximum de couleurs disponibles tout au long de la vie du système RFID. Afin de fixer la valeur maximale de la couleur en fonction de l'état du réseau, 2 seuils variables sont introduits UpSafe DnSafe. Chaque lecteur surveille son nombre d'interrogations réussies, selon qu'elles atteignent la valeur de UpSafe ou DnSafe, elles augmentent ou diminuent respectivement leur valeur locale de couleurs maximales disponibles et envoient un message de kick. Dans un voisinage proche où plusieurs lecteurs entrent en collision, une fois qu'ils atteignent une valeur seuil, ils envoient tous des messages de kick pour réserver leurs couleurs d'où le nom Colorwave.

Distributed Color Non-Cooperative Selection (**DCNS**) : Gandino et al. [2012] est un algorithme dérivé de Colorwave. La première différence avec Colorwave est que les lecteurs ici n'envoient pas de messages de kick mettant à jour leur valeur de couleur maximale. Un autre paramètre introduit est qui détermine la probabilité pour un lecteur d'interroger les tags une fois à son intervalle de temps. Les lecteurs sont classés en 3 types différents : killer pour $\mu = 2$, avec une gamme de couleurs si faible, ces lecteurs interrogent fréquemment les tags, ils n'envoient donc pas de kicks ni ne changent de canal pour éviter les collisions avec les killers voisins ; normal pour $2 < \mu < seuil$, ces lecteurs agissent comme des lecteurs occasionnels dans Colorwave ; killer pour $\mu > seuil$, ces lecteurs envoient constamment des messages kick et interrogent rarement les tags, ils augmentent leur valeur de η afin d'augmenter leurs chances d'interrogation.

1.4.2 Protocoles centralisés

Neighbour Friendly Reader Anti-Collision (**NFRA**) : En utilisant NFRA Eom et al. [2009], les interrogations sont organisées en rondes coordonnées par un serveur. Ce coordinateur envoie au début de chaque tour de lecture une Commande d'Arrangement (AC) annonçant le nombre maximum de Time Slots de beacon parmi lesquelles choisir. A la réception, chaque lecteur sélectionne au hasard un Time Slot et attend la commande correspondante (OC) du serveur. Ils envoient alors un beacon pour alerter les lecteurs voisins de leur intention d'interroger les tags. Si aucune collision n'est observée pendant la période de beacon, le lecteur envoie alors un Overriding Frame (OF) pour désactiver tous les lecteurs voisins pour le tour en cours. Une fois qu'un lecteur reçoit un OF, il attend le prochain AC du coordinateur pour concourir à nouveau. Dans les déploiements très denses, cet algorithme induit un nombre élevé de lecteurs désactivés à cause des OF. De plus, les lecteurs avec une valeur de Time Slot élevée ont plus de chances d'être désactivés par leurs homologues à Time Slots faibles. Suivant le protocole NFRA, de telles variantes sont proposées en modifiant les procédures de contention, NFRA++ Ferrero et al. [2011], NFRA-C Nawaz and Jeoti [2015], Xia-NFRA Xia et al. [2015].

NFRA+ NFRA++: Ces propositions Ferrero et al. [2011] sont des versions améliorées de NFRA comme leur nom l'indique. Le premier NFRA+, corrige l'inconvénient des valeurs de Time Slots élevées. Cet algorithme tente d'améliorer l'équité en augmentant la priorité des lecteurs qui passent un long temps d'attente sans interroger les tags. Cette augmentation de priorité renforce la probabilité pour le lecteur de choisir une valeur d'intervalle de temps faible et vice-versa pour les lecteurs de faible priorité avec un temps d'attente faible. Cela affecte l'équité de l'algorithme mais pas le nombre élevé de lecteurs désactivé à chaque tour. NFRA++ essaie de corriger ce problème en offrant une seconde chance aux lecteurs précédemment en collision. Dans cet algorithme, après avoir envoyé tous les OC correspondants au tour en cours, le coordinateur envoie ensuite un autre OC aux lecteurs qui avaient auparavant des tags en collision. Les lecteurs déterminent une probabilité T d'envoyer un tag dans cet ultime OC. Cela donne une chance de heurter les lecteurs dans le tour en cours pour rivaliser à nouveau avec une probabilité T. La couche supplémentaire d'équité et de seconde chance combinées permet à cet algorithme d'avoir

des performances élevées.

NFRA-C Nawaz and Jeoti [2015], est un autre protocole anti-collision qui améliore le débit des systèmes RFID. Efficace pour les réseaux denses en utilisant un compteur pour stocker les journaux de communication réussis de chaque lecteur. Le lecteur diffuse son message via beacon pour informer les voisins c collisions prédéfinies.

Xia-NFRA Xia et al. [2015], est un protocole anti-collision haute performance adapté aux réseaux RFID denses et mobiles. Pour atteindre cet objectif, l'algorithme permet au lecteur d'utiliser une nouvelle sous-trame dans la trame de transmission du protocole NFRA. Pour améliorer la précision de la transmission et une amélioration du backoff est mise en oeuvre.

Pour améliorer les performances de NFRA en réduisant les collisions de lecteur à lecteur, **GDRA** Bueno-Delgado et al. [2012] (Geometric Distribution Reader Anti-collision) est un protocole basé sur l'algorithme de distribution géométrique Sift. En utilisant cette distribution géométrique aléatoire, les lecteurs sélectionnent la valeur du Time Slot plutôt que la distribution uniforme classique qui réduira la surcharge des messages de beacon. Cette proposition reste faible dans le cas de réseaux RFID denses qui conduisent à désactiver suffisamment de lecteurs.

D'autre part, **DRCA** Golsorkhtabaramiri and Issazadehkojidi [2017] est un protocole TDMA centralisé basé sur la distance, qui écoute le canal et utilise différents Time Slots pour éviter les collisions. Il améliore le protocole GDRA en permettant un débit plus élevé à l'aide de la fonction Sift pour choisir au hasard des Time Slots. Le lecteur qui choisit les TS précédentes, écoute le canal. Si le canal est libre, le lecteur peut interroger les tags. Sinon, le lecteur augmente son nombre de Time Slots si cette distance est suffisamment longue. Sinon, une collision entre le lecteur et tags peut apparaître.

Fair Reader Collision Avoidance **FRCA**, Rezaie and Golsorkhtabaramiri [2018] est une version améliorée de GDRA. Ce protocole basé sur TDMA propose deux algorithmes, FRCA1 pour réduire les collisions lecteur-lecteur et FRCA2 pour tous les types de collisions entre lecteurs. Les lecteurs sélectionnent des Time Slots aléatoirement à l'aide de la fonction Tamiser.

1.4.3 Protocoles basés sur l'apprentissage machine

Dans un réseau RFID, il est nécessaire d'activer des lecteurs pour lire autant de tags que possible. Mais dans un déploiement réel, tous les tags ne peuvent pas être interrogés en raison du problème de collision. Le problème de reader-coverage collision avoidance arrangement (RCCAA) est donc abordé pour étudier comment activer les lecteurs et ajuster leurs champs de lecture pour interroger plus de tags sans collision.

L'algorithme **MWISBA** (maximum-weight-independent-set-based) Liu et al. [2015] est un protocole qui permet de résoudre ce problème en utilisant un champ de lecture multiple et propose une méthode heuristique basée sur le maximum-weight independent-set pour définir la portée de lecture des lecteurs redondants. MWISBA permet donc de résoudre l'interférence lecture-tag en ajustant le champ de lecture, cependant, l'interférence lecture-lecture n'est pas prise en compte.

MWISBAII Meddeb and Jaballah [2017] est proposé pour améliorer et résoudre le problème RRI de MWISBA en permettant de résoudre les différents types de collision. Ce protocole convertit le problème de reader-coverage collision avoidance arrangement (RCCA) en un problème MWIS. Il utilise ensuite la théorie des graphes pour résoudre le MWIS. Enfin, la solution MWIS peut être traduite en une solution pour le problème RCCA. Cette proposition est centralisée et la transformation graphique du problème MWIS pourrait être énorme pour le calcul du serveur central.

Puisque, MWISBA et MWISBAII sont des protocoles centralisés. Le but du nouveau proto-

Table 1.3: Comparaison des protocoles anti-collision

Attributs	PULSE	CORA	MCMAC	DIMAC	NFRA-C	BACP	DRCA	MWISBA	MWISBAII	Distributed -MWISBAII
RRI	√	√	√	√	√	√	√	–	√	√
RTI	√	√	–	–	√	√	√	–	√	√
Distribué	√	√	√	√	–	–	–	–	–	√
Centralisé	–	–	–	–	√	√	√	√	√	–
Apprentissage machine	–	–	–	–	–	–	–	–	–	–
Multi data channel	–	√	√	√	–	–	√	–	–	–
CSMA	√	–	√	√	√	–	√	–	–	–
FDMA	–	–	√	√	–	√	–	–	–	
TDMA	–	√	√	√	√	√	√	–	–	–

cole **Destribued-MWISBAII** Yan et al. [2020] qui représente la version distribuée de MWISBAII, est d'attribuer à chaque lecteur le processus de calcul et de prise de décision et de les communiquer ensuite à leurs voisins.

Pour résoudre le probleme reader-to-reader collision avoidance model (R2RCAM), un réseau immunitaire artificiel **RA-AIS** Li et al. [2015] est proposé pour optimiser l'allocation des ressources. L'anticorps candidat correspondant aux ressources optimales Fréquentielle et Temporelle, l'antigène représentant les ressources allouées pour le modèle R2RCAM et la phase de mutation correspond à l'ajustement dynamique efficace du champ d'interrogation des lecteurs.

Le système immunitaire artificiel hiérarchique adaptatif (**AHAIS**) Li et al. [2014] augmente le taux de convergence et l'efficacité du système RFID. Dans cet algorithme, les antibadys sont classés en deux niveaux, Common Swarm (CS) avec une affinité plus faible au niveau supérieur et un Elitist Swarm (ES) avec une affinité plus élevée au niveau inférieur. Dans l'opérateur de mutation, l'ES antibady utilise l'auto-apprentissage et la recherche locale, et le CS antibady met l'accent sur l'apprentissage de l'ES et la recherche globale.

Un réseau immunitaire artificiel avec apprentissage social (**AINet-SL**) Li et al. [2013] Inspiré du comportement social des animaux. Comme AHAIS, cet algorithme classe également les anticorps en deux groupes : ES et CS. Les deux subissent successivement la stratégie d'auto-apprentissage et de mutation par apprentissage social. La phase de mutation utilise deux stratégies d'apprentissage, l'apprentissage social stochastique (SSL) et l'apprentissage social heuristique (HSL).

1.4.4 Comparaison des protocoles anti-collision RFID

Comme déjà mentionné, les protocoles sont classés en fonction de leur déploiement centralisé ou distribué. Dans le tableau 1.3, nous faisons intervenir d'autres attributs pour différencier clairement les protocoles. Ces attributs sont : la capacité à résoudre les RRI et RTI, le nombre canal de données utilisés pour l'interrogation des tags, l'architecture de communication entre lecteurs et la méthode d'accès au canal utilisée.

CHAPTER

2 PROTOCOLES ANTI-COLLISION DISTRIBUÉS POUR LES LECTEURS RFID

L'évitement des collisions est l'un des piliers les plus décisifs pour améliorer les performances des réseaux sans fil RFID. La compréhension des caractéristiques de déploiement (Architecture, densité, mobilité, ressources, délai) des réseaux RFID est essentielle pour la conception d'un protocole anti-collision efficace pour tous ces réseaux. Jusqu'à présent, divers protocoles de lecteurs RFID ont été proposés, qui ne tiennent pas compte de toutes ces caractéristiques. Afin d'obtenir une méthode améliorée qui surmonte de telles limitations, nous proposons dans cette étude un nouveau protocole hybride FTSMAC et son extension FTSMAC-E. Nos nouvelles contributions utilisent un nouveau concept de partage efficace des ressources fréquentielles et temporelles entre les lecteurs de manière distribuée. Ce système de notification permet de créer des schémas d'allocation de fréquences et de Times Slot qui permettent à un maximum de lecteurs d'interroger les tags sans collisions et dans des intervalles de temps réduits.

2.1 Contribution 1: Protocole hybride multicanal de prévention des collisions entre lecteurs des réseaux RFID - FTSMAC

2.1.1 Introduction

Dans cette section, nous décrivons notre premier protocole hybride FTSMAC proposé basé sur les méthodes de contrôle d'accès aux canaux CSMA, TDMA et FDMA. Pour éviter les collisions entre lecteurs, cette stratégie utilise un système de notification qui permet aux lecteurs, selon certains critères de sélectionner des voisins. Par conséquent, la réutilisation des fréquences et Times Slots par le voisinage permettra aux lecteurs de gérer efficacement les ressources.

2.1.2 Principe de base du protocole proposé

Pour comprendre l'environnement de nos réseaux RFID sur la figure 2.1, nous désignons le lecteur Rx représenté par le petit cercle noir. Tous les lecteurs sont uniformes utilisent plusieurs canaux de données pour interroger les tags, et qu'un seul canal de contrôle est utilisé pour la communication entre eux.

Les lecteurs en collision Ri (petits cercles rouges) sont les concurrents avec Rx pour l'accès au canal puisqu'ils sont situés dans son champ d'interférence, où Ri est un lecteur de l'ensemble des voisins et cr est la longueur du champ d'interférence du canal de données. Les lecteurs situés dans cette zone doivent fonctionner sur des fréquences et dans des intervalles de temps différents pour éviter les collisions RRI et RTI. Les lecteurs voisins Rj (en bleu) réutilisent la même fréquence de Rx sans collision, et crr représente le champ de lecture du canal de contrôle. Dans ce contexte, dxj représente la distance entre Rx et son voisin. En utilisant le canal de contrôle, le but de Rx est de

sélectionner un lecteur parmi les voisins Rj pour réutiliser sa fréquence. Nous appelons l'ensemble des lecteurs réutilisant la même ressource de Fréquence et Time Slot, 'FTDMA_Scheme'.

Table 2.1: Structure proposée pour les messages de contrôle

Message type	READER_SENDER	READER_RECEIVER	READER_IN_CHAIN	AFFECT_FREQ	AFFECT_TS
REQUEST1	√	–	√	–	–
REQUEST2	√	–	–	–	–
RESPONSE	√	√	–	–	–
ADD_TO_CHAIN	–	√	–	√	√
NEW_CHAIN	–	√	–	√	√

Table 2.2: Structure de la table mémoire utilisée

USED_PROTOCOL	READER_IN_CHAIN	AFFECT_FREQ	AFFECT_TS

Chaque lecteur a une mémoire 'Table de contrôle' (tableau 2.2) avec quatre champs :

- USED_PROTOCOL : Les méthodes d'accès au canal utilisées, FTDMA ou CSMA.
- READER_IN_CHAIN : Les lecteurs constituent le FTDMA_Scheme auquel appartient ce lecteur.
- AFFECT_FREQ : La fréquence à réutiliser.
- AFFECT_TS : Le Time Slot à réutiliser.

Comme illustré dans (tableau 2.1), le message de contrôle est constitué de six champs :

- TYPE : Le type de message (REQUEST1, REQUEST2, RESPONSE, ADD_TO_CHAIN).
- READER_SENDER : L'identification de lecteur source.
- READER_RECEIVER : L'identification de lecteur destination.
- READER_IN_CHAIN : L'ensemble des identifiants des lecteurs utilisant la même fréquence.
- AFFECT_FREQ : La fréquence à réutiliser par le lecteur destinataire.
- AFFECT_TS : Le Time Slot à réutiliser par le lecteur destinataire.

A la réception d'une demande d'assignation d'un lecteur au groupe de coalition Rx, le lecteur compare les informations de sa table de contrôle (tableau 2.2) avec celles de la demande reçue via le canal de contrôle, pour décider d'accepter ou refuser de rejoignez le groupe FTDMA_Scheme de Rx.

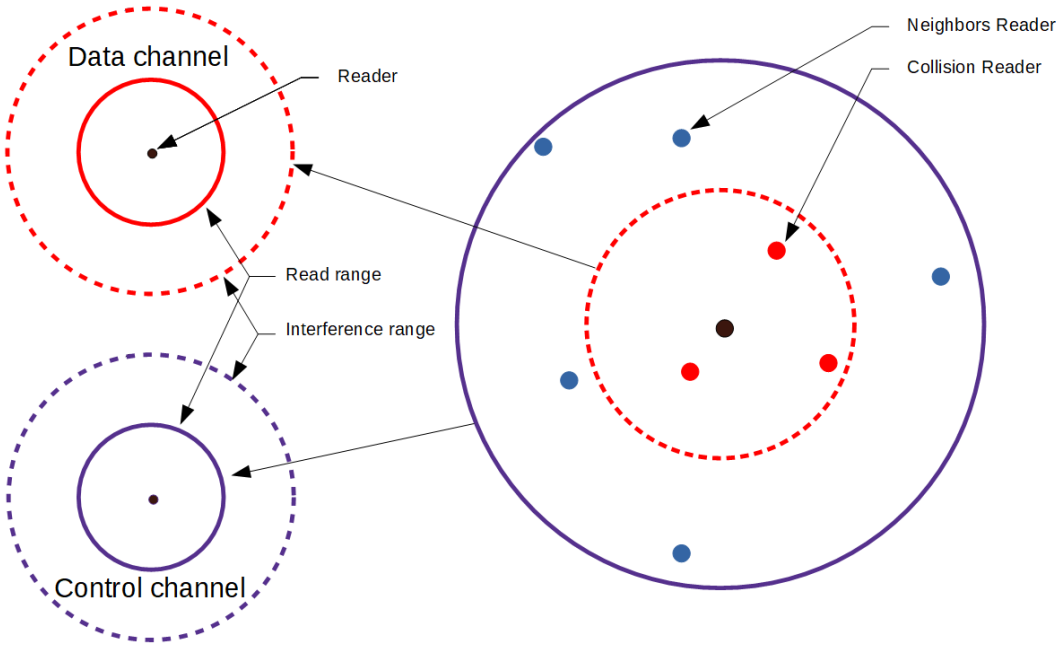

Figure 2.1: Architecture de base proposée pour les lecteurs RFID

2.1.3 Description de l'algorithme FTSMAC

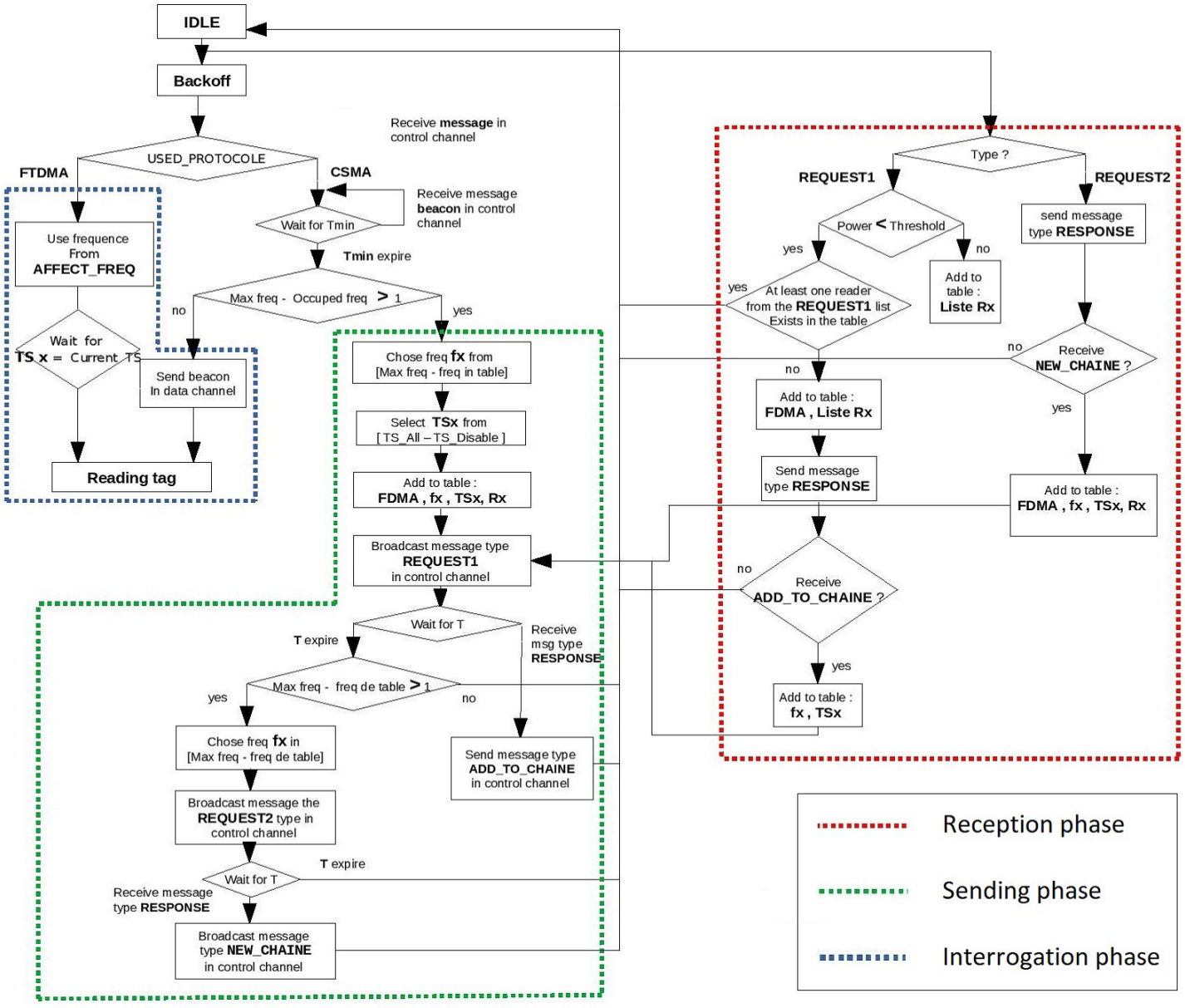

Figure 2.2: Structure de l'algorithme proposé

Avant de commencer l'interrogation des tags, tous les lecteurs doivent connaître leurs ressources de fréquence appropriées pour éviter les collision RRI, et de Time Slot pour éviter les collision RTI. Nous allouons les ressources selon certains critères définis. Comme illustré dans la figure 2.2, le lecteur attend un temps Backoff aléatoire dans la plage avec un pas CW (Contention Window)

Golsorkhtabaramiri et al. [2015] égal au temps de convergence nécessaire aux lecteurs pour créer les FTDMA_Scheme. On peut donc s'assurer qu'aucun autre lecteur ne tente d'envoyer une requête lors de la phase de création des FTDMA_Scheme. Les étapes des différents phase de notre algorithme sont détaillés dans ce qui suit:

2.1.3.1 Phase d'interrogation

Après le réveil du lecteur Rx, il commence par vérifier sa table mémoire (tableau 2.2). Si le champ USED_PROTOCOL contient FDMA, alors il exécutera la partie bleue de l'algorithme ; par conséquent, il peut utiliser la fréquence du champs AFFECT_FREQ et le Time Slot dans du champ AFFECT_TS pour commencer l'interrogation des tags.

Sinon, le champ USED_PROTOCOL avec la valeur CSMA. Dans ce cas, le lecteur écoute le canal de données pendant un temps Tmin Finkenzeller [2010]. Si Tmin expire sans avoir reçu de beacon, le lecteur commence à utiliser la fréquence libre.

2.1.3.2 Phase d'émission

Selon la phase précédente, s'il n'y a qu'une seule fréquence disponible à l'usage, le lecteur Rx utilise le protocole CSMA. Cependant, s'il y a plus de fréquences, le lecteur effectue le traitement de la partie verte (Figure 2.2). Ainsi, le lecteur sélectionne et ajoute une fréquence et un Time Slot libres à sa table. Il remplace alors CSMA par FTDMA et enregistre son ID. Ces informations représentent le point de départ du premier FTDMA_Scheme. Le lecteur donc cherche en utilisant REQUEST1 un nouveau Neighbor Reader Rj (Figure 2.1) et l'intègre dans son FTDMA_Scheme via le message ADD_TO_CHAIN.

Si le temps expire sans recevoir aucune réponse, le lecteur diffuse une REQUEST2 (aux lecteurs voisins Rj et aux lecteurs en collision Ri) pour trouver le lecteur qui initialisera un nouveau FTDMA_Scheme.

2.1.3.3 Phase de réception

Si le lecteur reçoit un message (REQUEST1 ou REQUEST2) lors du Backoff, il exécute la partie rouge de l'algorithme (Figure 2.2). Dans le cas d'un message REQUEST1, le lecteur compare la puissance du signal reçu Pr avec la puissance seuil ($Seuil = Pr \mid di = cc$), où Pr est la puissance du signal reçu, dont di est la distance entre les deux lecteurs, et cc est le rayon du champ de collision du canal de données. Si $Pr > Seuil$, ces lecteurs sont classés comme lecteurs de collision Ri. Ensuite, les lecteurs en collision Ri enregistrent le message READER_IN_CHAIN. Sinon, le lecteur voisin Rj vérifie s'il y a des interférences avec les lecteurs constituant le FTDMA_Scheme en cours.

Cependant, le lecteur Rj effectue les actions suivantes : remplacement de CSMA par FTDMA, mettre à jour le champ READER_IN_CHAIN, et attendre l'allocation de ressources à la réception dans un message ADD_TO_CHAIN.

Dans l'autre cas, après avoir reçu un message REQUEST2, le lecteur envoie un message RESPONSE à l'expéditeur Rx et quitte l'état IDLE. Sinon, il reçoit un message NEW_CHAIN, remplace CSMA par FTDMA et ajoute les nouvelles ressources dans sa table pour commencer à créer le nouveau FTDMA_Scheme.

2.1.4 Exemple illustratif

Pour bien comprendre le fonctionnement de l'algorithme FTSMAC, nous discutons ci-dessous un cas d'étude d'un réseau RFID aléatoire (Figure 2.3) et une illustration du processus de commu-

nication entre les lecteurs constituant ce réseau (Figure 2.4).

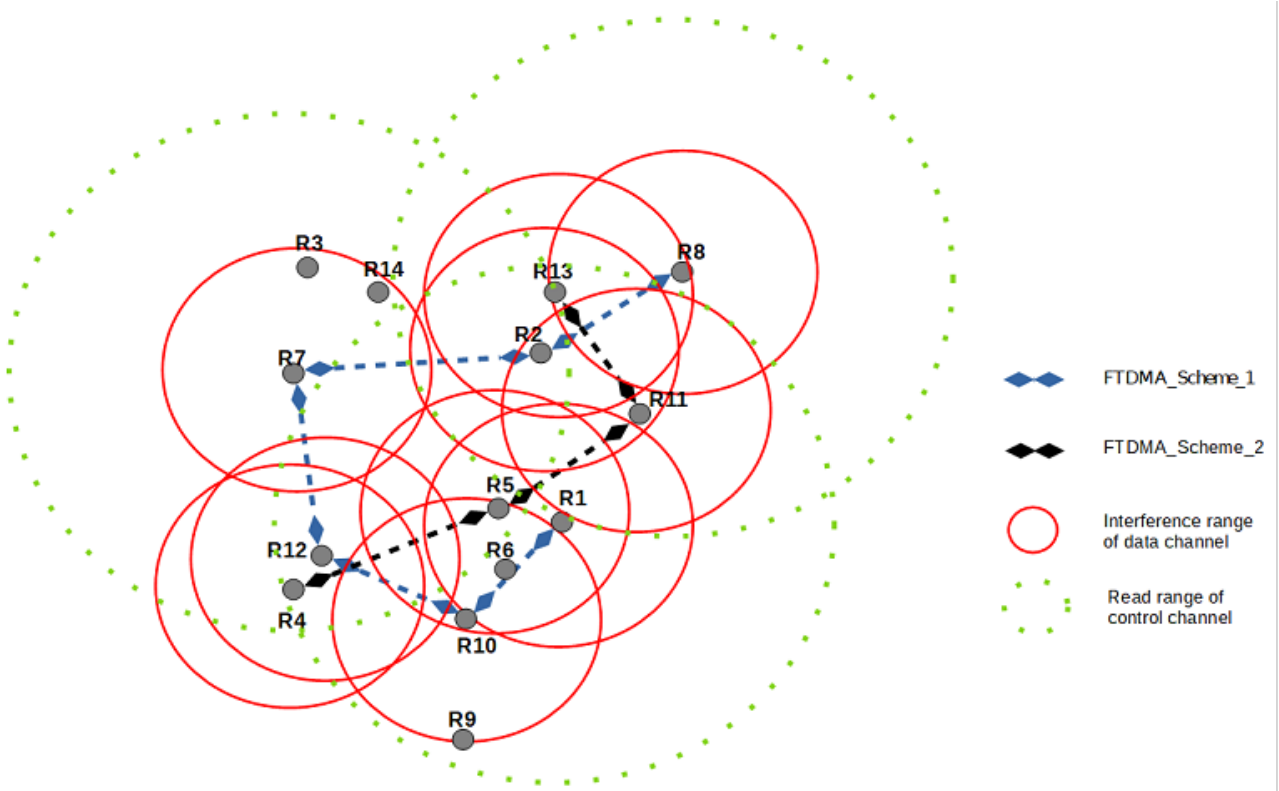

Figure 2.3: Application de l'algorithme sur un réseau RFID

Grâce à notre algorithme, dans cet exemple nous disposons de trois fréquences et Time Slot. En conséquence, nous définissons FTDMA_Scheme_1 comme l'ensemble des lecteurs R1, R10, R12, R7, R2 et R8 utilisant la première paire de ressources (freq1 et TS1). FTDMA_Scheme_2 est composé de R13, R11, R5 et R4 utilisent la deuxième paire de ressources (freq2 et TS2). Les lecteurs qui n'arrive pas a rejoindre FTDMA_Scheme_2 partagent la dernière fréquence utilisant CSMA.

La figure 2.4 décrit le processus de communication utilisé par le protocole dans cet exemple (figure 2.3). Nous présentons le schéma de l'algorithme pour les différentes situations de chaque lecteurs (R1, R2, R3, R8, R10, R13) sur l'annexe A.

Premièrement, tous les lecteurs sont dans l'état d'attente. R1 (Rx) est le lecteur avec le Backoff minimal, donc le premier à se réveiller peut démarrer le processus de création FTDMA_Scheme. Ensuite, il diffuse REQUEST1 sur le canal de contrôle pour annoncer sa présence et de demander aux lecteurs voisins (lecteurs bleus Rj) de réutiliser sa ressource (fréquence et TS). Les lecteurs reçoivent des demandes et mise à jour leurs tableaux. Les lecteurs en collision R5 et R6 (lecteurs rouges Ri) reçoivent une puissance de seuil bas. Par conséquent, ils ne répondent pas à la demande. Parmi les lecteurs voisins, R10 (lecteurs bleus Rj) répond en premier à la requête R1. Donc, il sera sélectionné comme nouveau voisin et confirmera en envoyant un message ADD_TO_CHAIN. Ensuite, R10 (nouveau Rx) continue le processus de création du

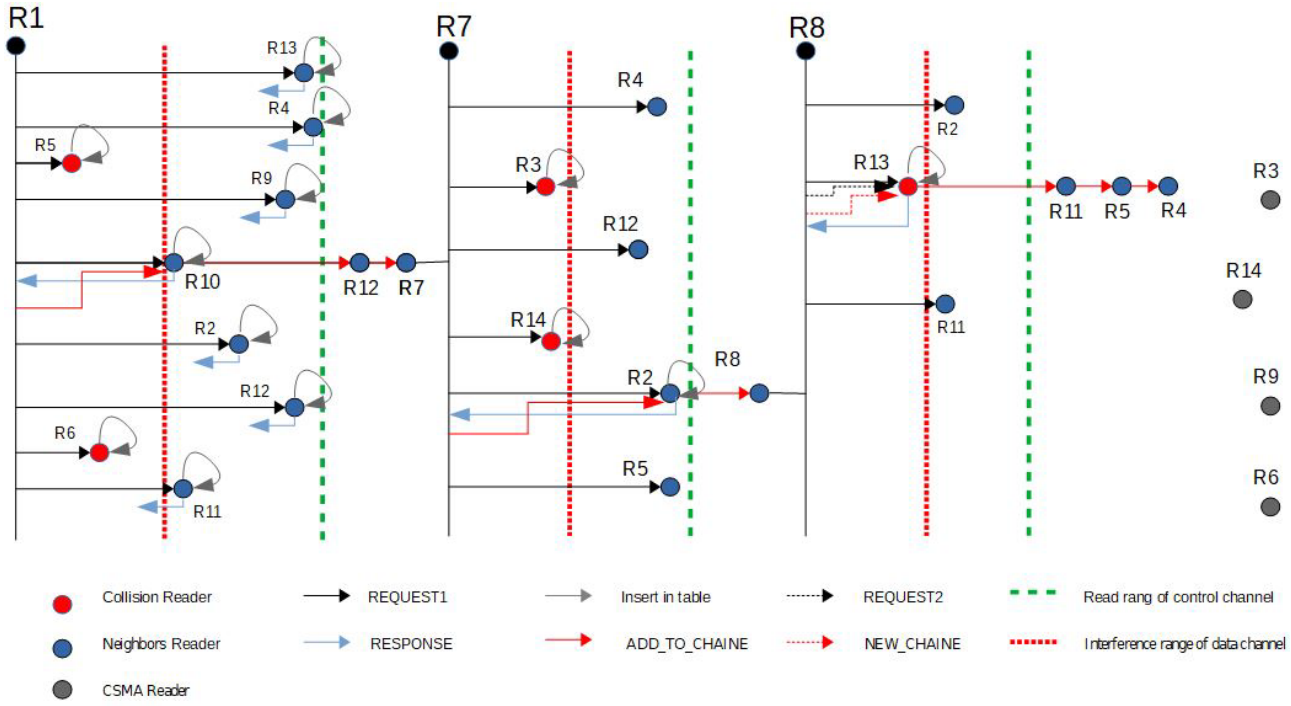

Figure 2.4: Processus de création des schémas FTDMA

FTDMA_Scheme en ajoutant R12 et R7.

Selon le messageREQUEST1 du R7, le lecteur R2 sera le nouveau membre du FTDMA_Scheme courant. Les lecteurs R3 et R14 ne répondent pas au message REQUEST1 car ils sont déjà dans le champ d'interférence de R7. Le lecteur R12 ne répond pas à la requête puisqu'il est membre du FTDMA_Scheme courant (AFFECT_FREQ = f1 et AFFECT_TS = TS1). Les lecteurs R4 et R5 ne répondent pas à la requête car ils entrent en collision avec les autres lecteurs du FTDMA_Scheme courant. Par conséquent, R7 accepte la demande de R2.

Ensuite, le lecteur R2 sélectionne son voisin R8 (figure 2.4). Ce dernier a son tour tente de trouver un voisin, mais ne reçoit pas de réponse après avoir envoyé un message REQUEST1 car le champ READ-ER_IN_CHAIN du message reçu des voisins R2 et R11 contient des identifiants de lecteur qui existent déjà dans leurs tables. Donc, R8 envoie un nouveau message REQUEST2 pour sélectionner le lecteur initiateur du nouveau FTDMA_Scheme. Puisque le lecteur R3 est le plus proche, il répond en premier. Ensuite, R8 envoie un message NEW_CHAIN pour transférer les nouvelles ressources au lecteur R13, qui lancera à son tour le prochain FTDMA_Scheme inclue R11, R5 et R4.

Enfin, il ne reste qu'une fréquence qui sera réservée aux lecteurs R3, R6, R9 et R14 en dehors du domaine de collision. Suite à la suspension de leur tentative de création du FTDMA_Scheme, ces lecteurs passeront au CSMA basé sur le principe Listen Before Talking (LSB).

Table 2.3: Paramètres de simulation

Paramètre	Valeur
Surface de simulation	300 $\times 300m$
Nombre de lecteurs (cas 1)	10, 20, 30, 40, 50
Nombre de lecteurs (cas 2)	50
Temps de simulation (cas 1)	300
Temps de simulation (cas 2)	0, 50, 100, 150, 200, 250, 300
Nombre de tags (cas 2)	20, 40, 60, 80, 100
Position du lecteur et de tag	Random
Type d'antenne	Omni-directional
Portée de lecture du canal de données (rr)	3.5 m
Portée de collision du canal de données (cr)	8 m
Portée de lecture du canal de contrôle (crr)	2 $\times cr$
Portée de collision du canal de contrôle (crc)	30 m
Nombre de canaux de données (cas 1)	3
Nombre de canaux de données (cas 2)	1, 2, 3, 4, 5
Nombre de TS (cas 1)	3
Nombre de TS (cas 2)	1, 2, 3, 4, 5
Nombre de canaux de contrôle	1
Nombre d'échantillons pour l'évaluation	10
protocoles comparés	PULSE, MCMAC
Backoff	(ReaderID-1) $\times CW$
CW	Temps de convergence de tous les lecteurs
Tmin	5 ms (Standard EPC)

2.1.5 Simulations et résultats

Dans cette section, nous présentons les performances et les résultats obtenus en simulant le réseau RFID à base de notre algorithme FTSMAC. Dans cette simulation, nous avons utilisé les protocoles anti-collision distribuée PULSE, MCMAC et CORA pour comparer notre méthode avec les approches existantes.

À cette fin, nous avons utilisé la plate-forme MATLAB pour simuler un réseau sans fil utilisant la technologie de communication RFID, y compris les problèmes de collision RRI et RTI, en comparant avec les protocoles de la littérature. Nous avons également développé les modèles de lecteurs et tags RFID. Pour communiquer entre les entités, nous avons simulé une communication de lecteur à lecteur et de lecteur à tag. Les paramètres de simulation sont présentés dans le tableau 2.3. Le déploiement des lecteurs a été randomisé dans un espace de $300m \times 300m$. Tous les lecteurs sont uniformes et utilisent trois Time Slots avec un champ de lecture de 3,5 m et un champ d'interférence de 8 m, et un canal de contrôle avec un champ de lecture de 16 m et un champ d'interférence de 30 m.

Dans cette étude, quatre scénarios ont été définis. Dans le premier scénario, la simulation a été appliquée en fonction du nombre de lecteurs (10, 20, 30, 40, 50), tandis que le second a été appliqué en fonction de la durée de simulation (50, 100, 150, 200, 250, 300). Le troisième scénario a été appliqué en fonction du nombre de tags (20, 40, 60, 80, 100). Le scénario final a été appliqué en fonction du nombre de fréquences et de TS (1, 2, 3, 4, 5). Dans ces scénarios, nous avons étudié les performances du système et le nombre de lecteurs actifs.

Un protocole anti-collision doit garantir un nombre élevé de lectures réussies dans un environ-

nement de collision, ce qui est un critère important pour mesurer les performances du protocole. On considère une interrogation réussie si le lecteur reçoit la réponse de la requête par les tags dans son champ de lecture.

Nous définissons les performances du système (lecture moyenne réussit) comme suit (equation 2.1) :

$$SystemPerformance(\%) = \frac{Total\_Success \times 100}{Total\_Interrogations} \tag{2.1}$$

Où Total_success représente le nombre d'interrogations de lecteur-tag réussies et Total_interrogation représente le nombre total d'interrogations de lecteur-tag.

Sur la base de la figure 2.5, nous avons le nombre d'interrogation succès utilisant notre algorithme est plus élevé. Il dépasse 80% dans le cas de 50 lecteurs car il permet à un maximum de lecteurs d'exploiter les ressources fréquentielles disponibles. MCMAC est moins performant car il gère des ressources individuelles, ce qui rend difficile l'utilisation des fréquences. Le protocole Pulse est le plus faible parmi les autres. On note le même résultat avec CORA car il ne peut gérer qu'un seul canal de données.

La figure 2.6 illustre la moyenne des interrogations réussies en fonction de la variation du temps de simulation. Notre protocole est plus rapide puisqu'il ne demande pas de temps supplémentaire pour obtenir un meilleur résultat, et se stabilise à 82% de l'efficacité de lecture pour le temps de simulation supérieurs à 150, alors que MCMAC atteint 66%. Les résultats pour CORA et MAC sont similaires, mais ces approches se stabilisent à 70 %. Pulse nécessite plus de temps pour interroger les tags car un seul canal de données est partagé par tous les lecteurs dans le domaine de collision.

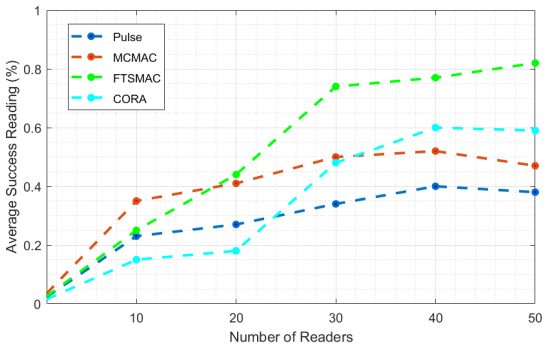

Figure 2.5: Performances du système en fonction du nombre de lecteurs

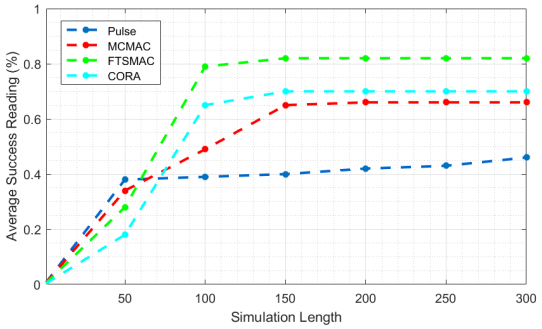

Figure 2.6: Performances du système en fonction de la durée de la simulation

Le paramètre des lecteurs actifs représente le nombre de lecteurs qui réussissent l'interrogation des tags. C'est un facteur important pour l'évaluation de la performance du système. Pour obtenir le nombre de lecteurs actifs dans chaque simulation, nous calculons le nombre de lecteurs pouvant interroger les tags sans interférer avec les lecteurs voisins. Sur la figure 2.7, l'évolution du protocole Pulse ne dépasse pas 10 lecteurs actifs, alors que les autres algorithmes augmentent le nombre de lecteurs actifs. Dans un réseau de plus de 40 lecteurs, MCMAC et CORA arrêtent leur évolution. En revanche, notre proposition poursuit l'évolution du nombre de lecteurs actifs et obtient de meilleurs résultats car elle permet au nombre maximum de lecteurs du réseau d'obtenir les ressources afin d'éviter les collisions en réutilisant intelligemment les schémas FTSMAC.

La figure 2.8 illustre la moyenne des interrogations réussies des protocoles FTSMAC, CORA, MCMAC et Pulse en termes de nombre de tags (20 à 100) lus par 30 lecteurs. Les performances de Pulse sont généralement faibles car un seul canal de données ne permet pas une interrogation bien réussie. MCMAC et CORA atteignent environ 60% de performances, alors que notre protocole dépasse 70%. Les résultats montrent que notre protocole peut lire une plus grande gamme de tags. Par conséquent, en termes d'efficacité de lecture des tags, FTSMAC est plus stable et plus efficace par rapport aux autres protocoles.

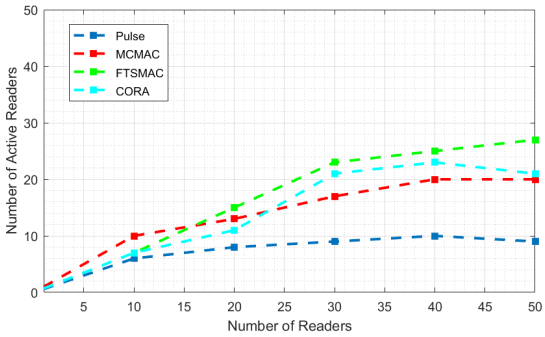

Figure 2.7: Nombre de lecteurs actifs par rapport au nombre de lecteurs

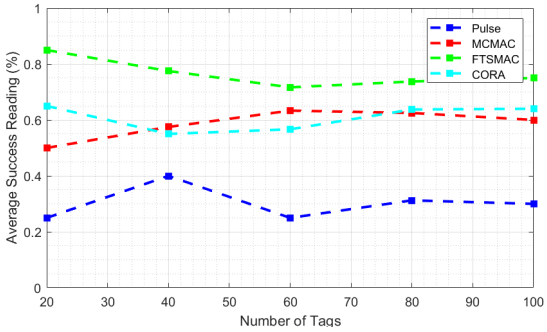

Figure 2.8: Performances du système en fonction du nombre de tags

La figure 2.9 illustre l'évolution du protocole FTSMAC en fonction du nombre de fréquences et de Time Slots disponibles pour les lecteurs de 10 à 50. Le principe de notre approche est basé sur la génération du FTDMA_scheme. Le schéma utilise les deux paires de ressources de fréquence et de Time Slots. La création de ces schémas permet à un grand nombre de lecteurs de s'intégrer dans l'un des schémas et d'obtenir des ressources pour l'interrogation des tags. Comme le montre la figure 2.9, cela permet au réseau RFID d'utiliser plus de ressources pour créer davantage de schémas FTDMA, et donc plus de lecteurs actifs peuvent communiquer sans collision, augmentant ainsi les performances du système. L'utilisation d'une seule fréquence et TS a permit d'atteindre 42 % de l'efficacité du système, tandis que l'augmentation des paramètres, en utilisant cinq paire de ressources, a augmenté les résultats à 88 % de l'efficacité du système.

Les différents apports techniques de cet article qui le distinguent des autres solutions pour atteindre ces résultats sont les suivants :

- Un mécanisme de notification est utilisé pour échanger la fréquence et les paquets d'allocation de ressources temporaires via le canal de contrôle en mode distribué par les lecteurs pour créer les différents FTDMA_Schemes.

- FTDMA_Scheme peut inclure et activer un maximum de lecteurs pour obtenir les ressources disponibles et interroger les tags sans collision.

- Utilisation d'une solution hybride basée sur les méthodes d'accès aux canaux partagés de la couche MAC : FDMA, TDMA et CSMA.

- FDMA est utilisé pour l'allocation permanente des fréquences aux lecteurs afin de résoudre le problème de collision RRI.

- TDMA est utilisé pour l'allocation temporaire des fréquences aux lecteurs afin de résoudre le problème de collision RTI. Le nombre de périodes TDMA est égal au nombre de FTDMA_Schemes générés.

- CSMA est utilisé par les lecteurs qui n'appartiennent pas à aucun FTDMA_Scheme pour

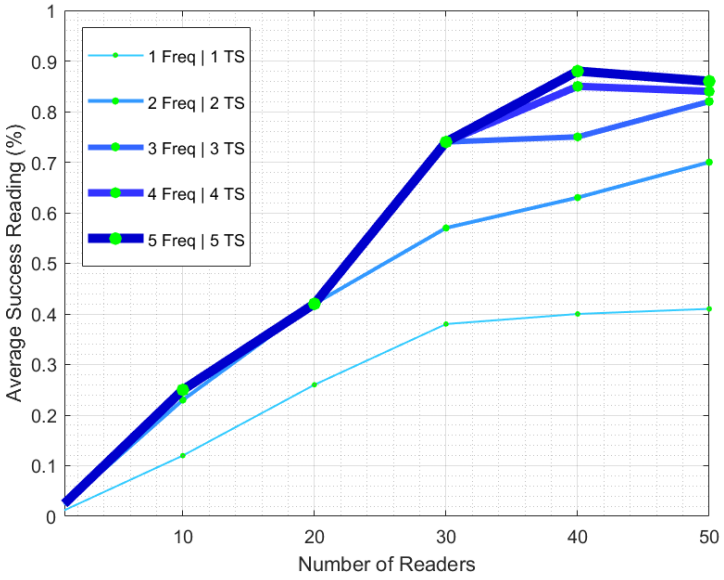

Figure 2.9: Performance du système en fonction du nombre de lecteurs et ressources utilisé

gérer les accès concurrents au canal de données.

- L'utilisation d'un Backoff adapte le temps de création du FTDMA_Scheme en fonction du nombre de lecteurs pour éviter les collisions d'accès au canal de contrôle.

2.1.6 Conclusions

Dans cette première contribution, nous avons proposé un protocole robuste qui évite les collisions de lecteurs RTI et RRI dans les réseaux RFID denses multicanal. Ce protocole est basé sur un système de notification qui distribue les ressources à l'aide d'un FTDMA_Scheme.

A cet effet, les lecteurs attendent un temps aléatoire de backoff pour éviter les collisions au niveau de canal de contrôle. Le lecteur avec la temporisation minimale se réveille en premier et démarre le processus de création FTDMA_Scheme.

Dans l'étape suivante, les lecteurs utilisent le canal de contrôle pour attribuer des fréquences et des Time Slots aux lecteurs les plus proches en dehors du domaine de collision. Chaque lecteur qui reçoit le message de contrôle mémorise les deux ressources dans sa table et commence plus tard le processus de création du FTDMA_Scheme.

L'approche proposée implique tous les lecteurs qui reçoivent une notification sur le canal de contrôle pour créer les FTDMA_Scheme. Par conséquent, le nombre maximum de lecteurs peut être atteint en utilisant la fréquence et les intervalles de temps comme ressources pour l'interrogation des tags.

Pour prouver l'efficacité de notre protocole, nous avons utilisé la simulation pour illustrer la capacité des lecteurs RFID à traiter les interférences de lecteur à lecteur et de lecteur à tag en utilisant cette stratégie distribuée en augmentant l'efficacité de lecture et le nombre de lecteurs actifs avec un minimum de de ressources.

L'avantage de notre algorithme par rapport à d'autres solutions est qu'il utilise une nouvelle

méthode de distribution de ressources basée sur un schéma qui permet une allocation et une gestion efficaces et plus rapides des ressources aux lecteurs RFID.

La méthode utilisée par le protocole FTSMAC est très efficace en termes de gestion des fréquences alors que la gestion des TS reste basique et dépend toujours des schémas de distribution des fréquences. Pour cela, nous découvrirons dans la deuxième contribution une extension de FTSMAC utilisant un nouveau système de notification TDMA entre lecteurs.

2.2 Contribution 2: Protocole anti-collision distribué basé sur les schémas FDMA-TDMA utilisés pour les lecteurs RFID - FTSMAC-E

2.2.1 Introduction

Afin d'améliorer les performances et d'obtenir un système stable et efficace du protocole FTSMAC. Dans cette partie, nous allons présenter notre nouvelle stratégie de distribution des ressources temporelles FTSMAC-E (TDMA) pour résoudre les problèmes de collision RTI. Nous avons gardé la partie gestion des ressources fréquentiel du protocole FTSMAC (FDMA) pour résoudre les problèmes de collision RRI.

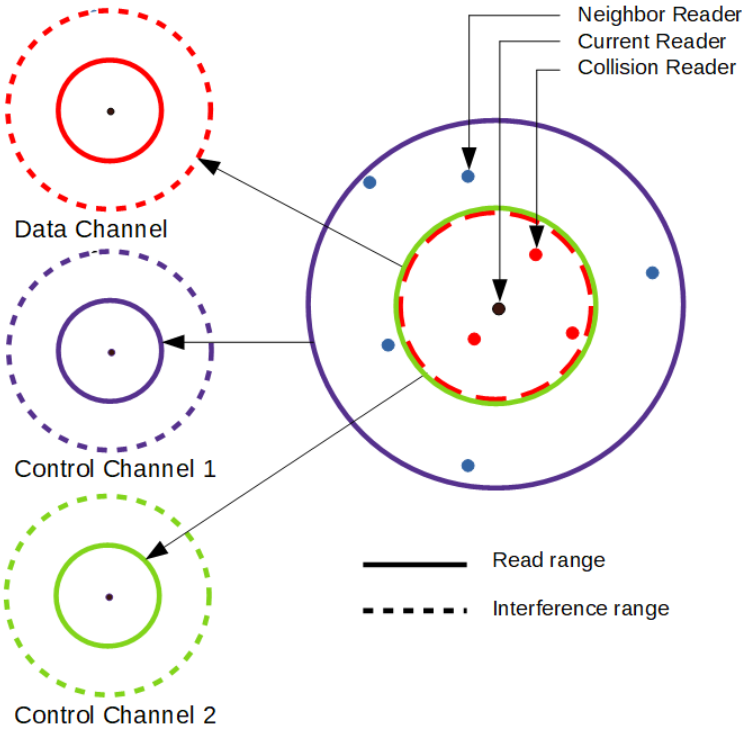

Figure 2.10: Architecture de base proposée pour les lecteurs RFID

2.2.2 Principe de base

Notre protocole FTSMAC-E utilise un système de notification pour la communication entre les lecteurs via un canal de contrôle. Nous utilisons deux canaux de contrôle différents décrits dans

Table 2.4: Structure proposée pour les messages de contrôle

Type de Message	READER_SENDER	READER_RECEIVER	ELIMINATE_TS
REQUEST1	√	–	√
REQUEST2	√	–	–
RESPONSE1	√	√	–
RESPONSE2	√	√	–
TS_select	√	–	–

la figure 2.10 pour contrôler l'allocation des ressources. Le canal de contrôle CC1 est utilisé pour distribuer les fréquences à réutiliser et le canal de contrôle CC2 pour gérer les Times Slots. Le lecteur vise les lecteurs de collisions situés dans son champ d'interférence du canal de données pour gérer les TS en utilisant le canal de contrôle CC2 afin d'éviter les collisions RTI et utilise le canal de contrôle CC1 pour distribuer les fréquences aux lecteurs voisins afin d'éviter les collisions RRI.

Le système de notification pour contrôler l'attribution des Times Slots utilise les structures de trame et les tables suivantes.

Le tableau 2.4 décrit les différents champs de chaque trame :

- READER_SENDER : Identification du lecteur source.
- READER_RECEIVER : Identification du lecteur destination.
- ELIMINATE_TS : TS utilisé par le lecteur source.

Ces paquets sont reçus et stockés dans la table des lecteurs (tableau 2.5) :

- TS_Enable : TS autorisé à l'utilisation.
- TS_Disable : TS non autorisé à l'utilisation.

Table 2.5: Structure de la table mémoire

TS_Disable	TS_Enable

2.2.3 Processus de l'algorithme

L'objectif de cet algorithme (figure 2.11) est d'établir un système distribué qui empêche les lecteurs d'utiliser des TS pouvant provoquer une RTI. Au début, tous les lecteurs sont dans l'état Backoff. Le lecteur qui se réveille le premier, commence le processus de notification avec les lecteurs voisins. Ainsi, le lecteur exécute la phase de réception (zone verte) lorsqu'il reçoit un message de contrôle. Sinon, le lecteur exécute la phase d'envoi et de lecture (zone bleue).

2.2.3.1 Phase d'émission et de lecture

Le lecteur peut commencer à interroger les tags en utilisant le canal de données s'il y a un TS dans sa table $IsEmpty(TSEnable) = 0$ et s'activer à son tour. S'il n'y a pas de TS, $IsEmpty(TSEnable) = 1$, le lecteur choisit l'un des TS disponibles, $TSAvailable = TSAll -$

$TSDisable$ et le mémorise $TSEnable = TS$ dans sa table. A ce stade, le lecteur émet un message REQUEST1 en utilisant le canal de contrôle pour découvrir le plus proche voisin concerné par la RTI et l'avertir d'éviter d'utiliser sa propre TS. Après un délai Tmin, si le lecteur reçoit un message RESPONSE1 des lecteurs cibles, il conserve le premier message reçu et active son propriétaire via le message TS_select pour lui permettre de sélectionner son TS et de commencer le processus de découverte suivant. Si le lecteur ne reçoit pas de réponse pendant Tmin, cela implique soit qu'il n'y a pas de voisin dans le RTI, soit que tous les voisins ont déjà sélectionné leur propre TS. Dans ce cas, et pour étendre le champ de vision, le lecteur émet un nouveau message REQUEST2 pour découvrir d'autres lecteurs en utilisant les voisins comme relais. Si le lecteur ne reçoit pas de réponse, le processus est déclenché. Si un message RESPONSE1 est reçu, le lecteur conserve le premier et envoie un message TS_select au nouveau voisin pour choisir son TS et commencer le processus suivant.

2.2.3.2 Phase de réception

Un lecteur peut recevoir deux types de messages REQUEST1 ou REQUEST2 sur le canal de contrôle mentionné dans le paragraphe précédent. Si un lecteur reçoit le REQUEST1, il ajoute la valeur TS du champ ELIMINATE_TS de la trame 'RESPONSE1(TS)' à la colonne TS_Disable de sa table, $TSDisable = TSDisable + RESPONSE1(TS)$. Ensuite, le lecteur envoie un message RESPONSE1 s'il n'y a pas de TS enable $IsEmpty(TSEnable) = 0$ dans sa table pour l'utiliser. Le lecteur doit choisir un des TS disponibles et le mémoriser dans le champ TS_Enable $TSEnable = TS$. Sinon, le lecteur n'est pas concerné et quitte le processus. Ainsi, le premier lecteur ayant répondu peut choisir sa propre TS via le message d'autorisation TS_select. Ensuite, le lecteur sélectionne un TS parmi ceux disponibles et le mémorise dans le champ TS_Enable de sa table. Si le lecteur reçoit un message REQUEST2, il peut réagir comme un relai s'il n'est pas concerné puisqu'il possède déjà un TS, $IsEmpty(TSEnable) = 0$. Par conséquent, il rediffuse la trame à ses voisins. Ensuite, s'il reçoit un message RESPONSE2, il l'envoie à l'expéditeur de REQUEST2 et attend la réponse contenant le TS pour le transférer. Si le lecteur qui a reçu le REQUEST2 est concerné car il n'a pas de TS, $IsEmpty(TSEnable) = 1$. Il envoie un message RESPONSE2 et attend la réponse TS_select.

2.2.3.3 Exemple illustratif

Dans cette section, nous présentons un exemple illustratif pour comprendre le fonctionnement de l'algorithme. Considérons un déploiement aléatoire de 31 lecteurs RFID. Les figures 2.12 et 2.13, montrent successivement le processus de distribution des Fréquences (FTSMAC) et des Time Slots (FTSMAC-E) sur les lecteurs du réseau (tableau 2.6). Le lien virtuel entre les lecteurs regroupe les lecteurs réutilisant la même ressource et les champs attachés aux lecteurs représentent leur table de mémoire. Tous les lecteurs, à l'exception du lecteur R11, ont réussi à obtenir leur propre fréquence (figure 2.12). Ainsi, 6 fréquences sont suffisantes pour couvrir ce réseau et éviter les collisions RRI. En ce qui concerne la gestion des ressources temporelles (TS), la figure 2.13 montre que tous les lecteurs du réseau ont reçu leur Time Slots. Par conséquent, 4 TS sont suffisants pour éviter la collision RTI. La figure 2.14, illustre les deux cas particuliers qui peuvent être rencontrés dans cette partie de l'algorithme.

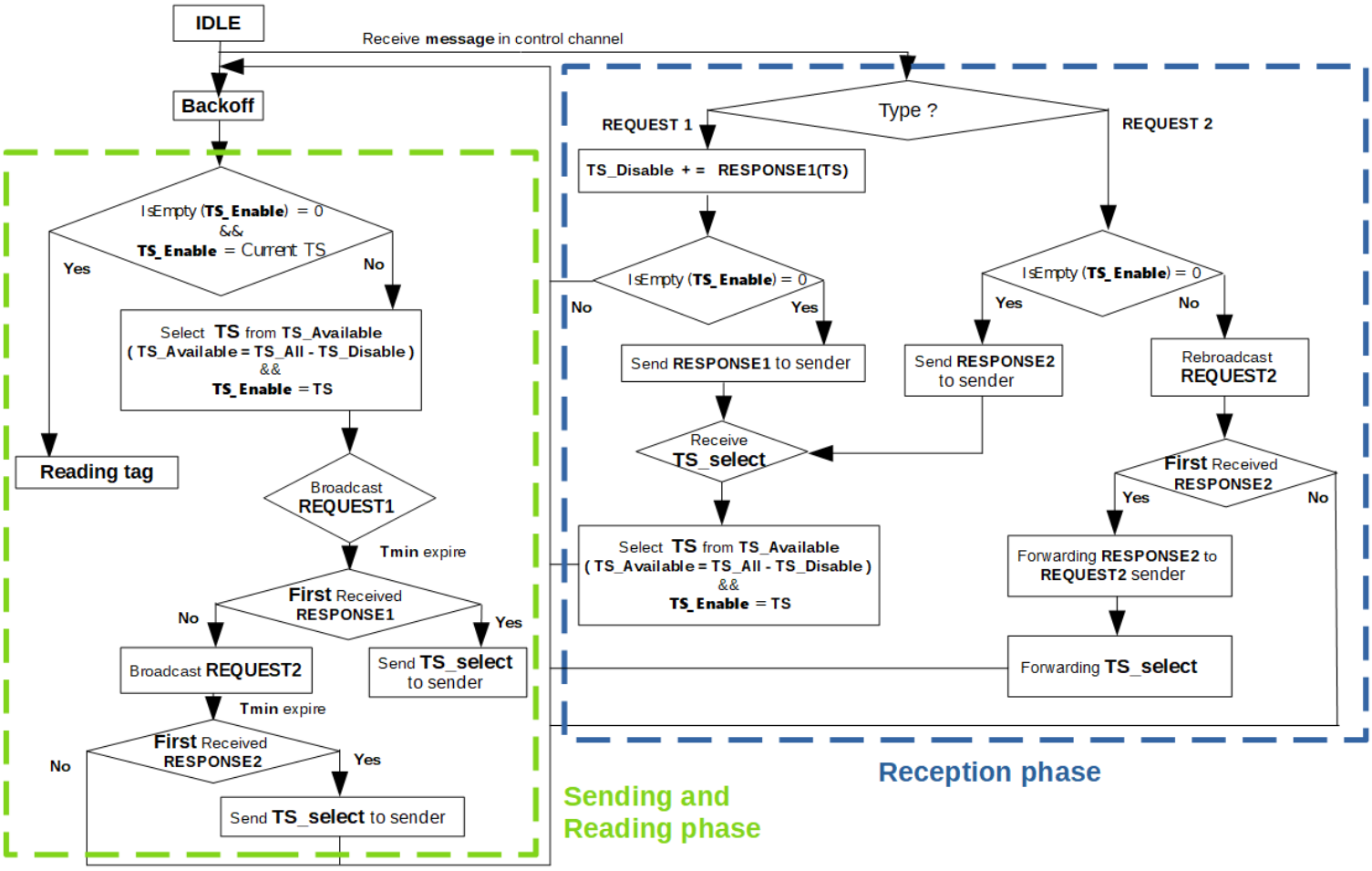

Figure 2.11: Structure de l'algorithme proposé

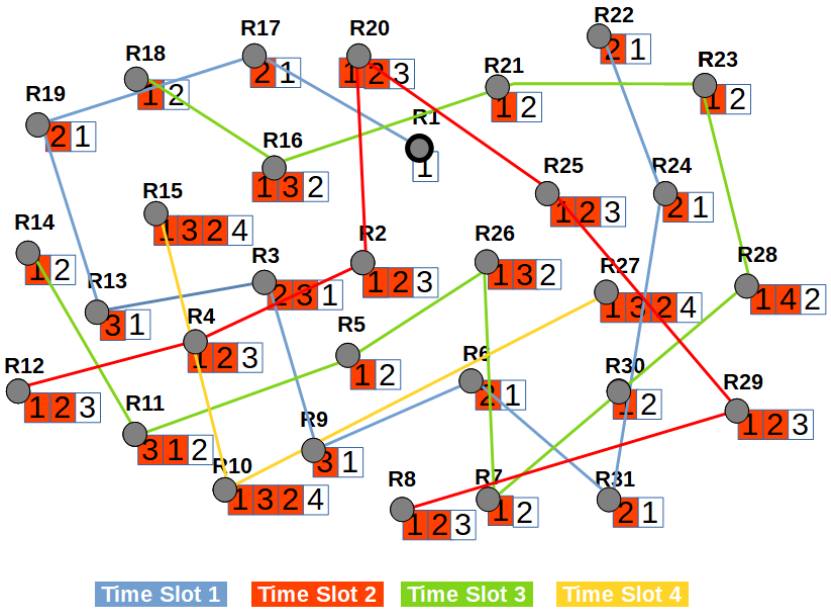

Figure 2.13: Processus de distribution des Time Slots (FTSMAC-E)

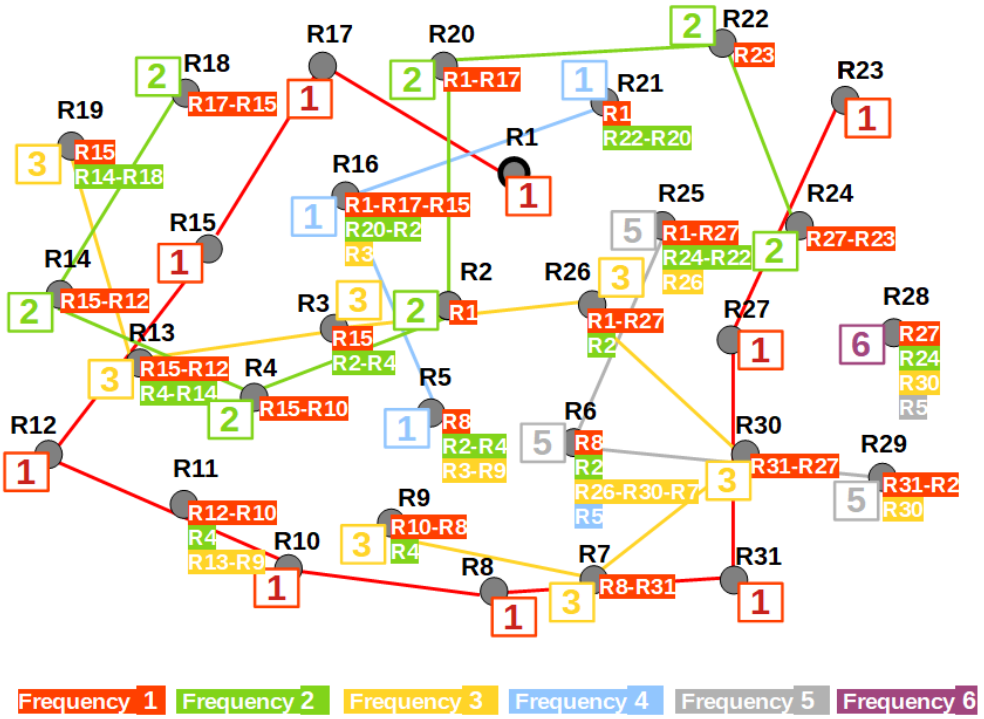

Figure 2.12: Processus de distribution des Fréquences (FTSMAC)

- Cas 1:

Dans la figure 2.14, R1 se réveille en premier (Backoff min). Il commence par sélectionner TS1 et le mémorise dans sa table $TSEnable = TS1$. Ensuite, le lecteur annonce à ses voisins dans RTI d'éviter TS1 en diffusant le message REQUEST1. Les lecteurs voisins mémorisent TS1 dans leurs tables $TSDisable = TS1$ et envoient des messages RESPONSE1 à R1. Ce lecteur ne considère que la première réponse provenant du lecteur le plus proche dans RTI, R21. Ainsi, R1 envoie un TS_select à R21 lui permettant de choisir son TS parmi les TS_Available $TSAvailable = TSAll - TSDisable$, il sélectionne donc TS2 $TSEnable = TS2$ et continue le processus.

- Cas 2:

Dans la figure 2.14, le lecteur R15 vérifie sa table $TS\_Disable = [TS1, TS2, TS3]$ et choisit

Table 2.6: Ressources assignées aux lecteurs utilisant FTSMAC-E

	TS1	TS2	TS3	TS4
Canal1	R1, R17, R31	R23	R12, R8	R15, R10, R27
Canal2	R24, R22	R14, R18	R20, R2, R4	–
Canal3	R19, R13, R3, R9	R26, R30, R7	–	–
Canal4	–	R5, R16, R21	–	–
Canal5	R6	–	R25, R29	–
Canal6	–	R28	–	–

$TS\_Enable = TS4$. A ce stade, R15 informe les voisins dans RTI en diffusant un message REQUEST1. Mais aucun message RESPONSE1 n'est reçu car tous les voisins ont déjà leur propre TS. Donc, afin d'éviter d'être bloqué à ce stade, R15 décide de chercher un lecteur ailleurs pour continuer le processus. R15 diffuse donc un nouveau message REQUEST2 en utilisant les voisins de RTI comme relais de message pour atteindre les autres lecteurs. Le voisin R13 détecte le premier message RESPONSE2 de R12 et l'envoie à R15 qui autorisera via le message TS_select ce nouveau lecteur non voisin à sélectionner son TS et à poursuivre le processus.

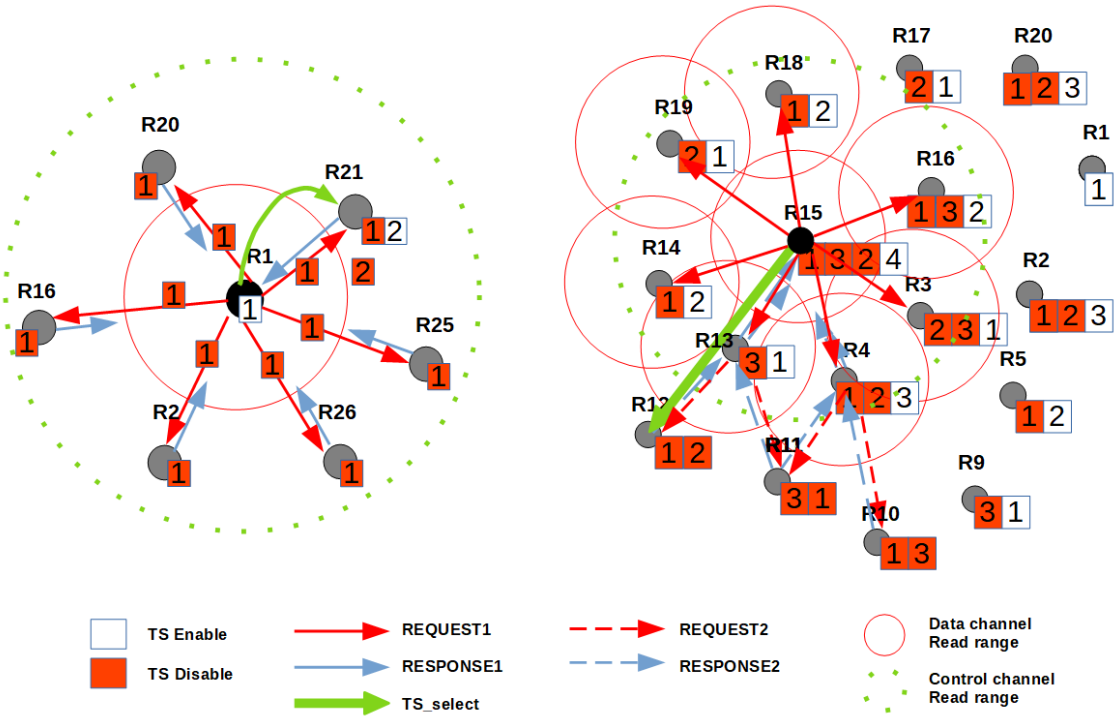

Figure 2.14: Utilisation des messages de contrôle par FTSMAC-E

2.2.4 Simulation et résultats

Dans cette section, nous présentons les résultats obtenus à partir de la simulation d'un réseau RFID constitué de lecteurs et tags RFID mobiles distribuées aléatoire. Afin d'étudier un environnement de collision RFID, le tableau 2.7 comprend les différents paramètres de simulation. Nous avons comparé les résultats obtenus avec les protocoles de la littérature FTSMAC, Pulse, MCMAC et CORA.

La figure 2.15 montre l'évolution supérieure de FTSMAC-E par rapport à FTSMAC pour un nombre différent de déploiements de lecteurs. L'efficacité de lecture peut atteindre presque 100%. La technique de distribution des ressources de temps et fréquence utilisée par FTSMAC-E et FTSMAC permet d'obtenir des performances système très élevées par rapport aux protocoles Pulse, MCMAC et CORA.

Table 2.7: Paramètres de simulation

Paramètre	Valeur
Nombre de lecteurs (réseau sparse)	10, 20, 30, 40, 50
Nombre de lecteurs (réseau dense)	50, 100, 150, 200, 250
Nombre de tags	100
Position du lecteur et de tags	Random
Type d'antenne	Omni-directional
Portée de lecture du canal de données (rr)	3,5 m
Portée de lecture du canal de contrôle (crr)	2 x rr
Nombre de canaux de données	7
Nombre de TS (cas 1)	7
Nombre de TS (cas 2)	1, 2, 3, 4, 5, 6, 7
Nombre de canaux de contrôle	1
protocoles comparés	FTSMAC, Pulse, MCMAC, CORA
Backoff	$(ReaderID - 1) \times CW$
CW	emps de convergence de tous les lecteurs
Tmin	5 ms (Standar EPC)
T	Temps de réponse des lecteurs voisins

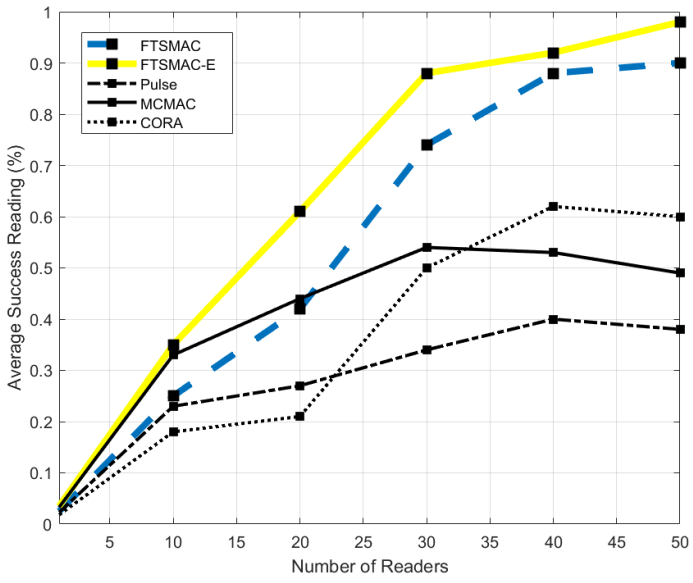

Figure 2.15: Moyenne de lecture réussie par rapport au nombre de lecteurs

Dans les figures suivantes, nous comparons notre protocole FTSMAC-E avec FTSMAC qui est le plus proche en termes de performance comme le montre la figure précédente. La figure 2.16 confirme les performances de FTSMAC-E en termes de nombre de lecteurs actifs, permettant à presque tous les lecteurs de la simulation d'être activés et d'utiliser le canal de données sans collision. Lorsque l'on atteint 50 lecteurs, ce qui correspond à la valeur maximale de lecteurs, la

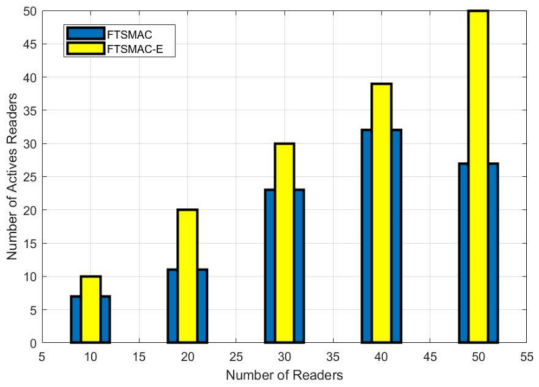

Figure 2.16: Nombre de lecteurs actifs en fonction de nombre de lecteurs

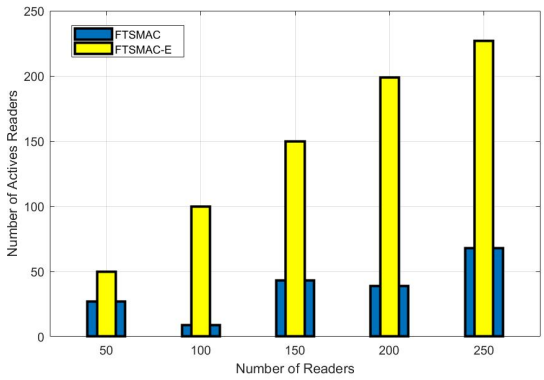

Figure 2.17: Nombre de lecteurs actifs en fonction de nombre de lecteurs pour les réseaux dense

différence devient déviante entre les deux approches. Cela montre que notre approche a minimisé d'avantage les collisions, en conservant le même traitement puissant des RRI que l'approche FTSMAC et en améliorant le processus de résolution des collisions RTI.

Dans le second scénario figure 2.17, nous étudions le cas d'un réseau RFID dense pour un nombre de lecteurs variant de 50 à 250, en utilisant 7 canaux de données et time slots. Nous obtenons des résultats très intéressants en termes de nombre de lecteurs actifs avec une grande différence entre les deux protocoles par rapport au résultat précédent pour le réseau sparse. Cela montre que FTSMAC-E est plus adapté aux systèmes RFID denses.

Le dernier scénario représente une simulation avec plusieurs configurations. Dans la figure 2.18, nous avons étudié l'efficacité du système pour différents nombres de lecteurs (10 à 50 lecteurs) en fonction des Time Slots utilisés (1 à 7 TS). Pour la simulation avec 10 lecteurs, FTSMAC-E est supérieur à FTSMAC avec une différence de 12% et se stabilise à 36% à partir de 2 TS. Pour 20 lecteurs, toujours à partir de 2 TS, FTSMAC-E est supérieur (62%) avec une différence de 18%. Pour 30 lecteurs, notre protocole atteint 88% de performance dépassant FTSMAC à partir de 4 TS avec une différence de 15%. Pour 40 lecteurs, moins de 5 TS affectent la performance de notre approche par rapport à FTSMAC, mais à partir de 5 TS, FTSMAC-E atteint 92% de performance. Enfin, pour un déploiement de 50 lecteurs est presque similaire à celui de 40 lecteurs, mais dans ce cas, les lecteurs ont besoin de plus de 5 TS pour dépasser FTSMAC et donc atteindre la valeur de performance la plus élevée de 98%.

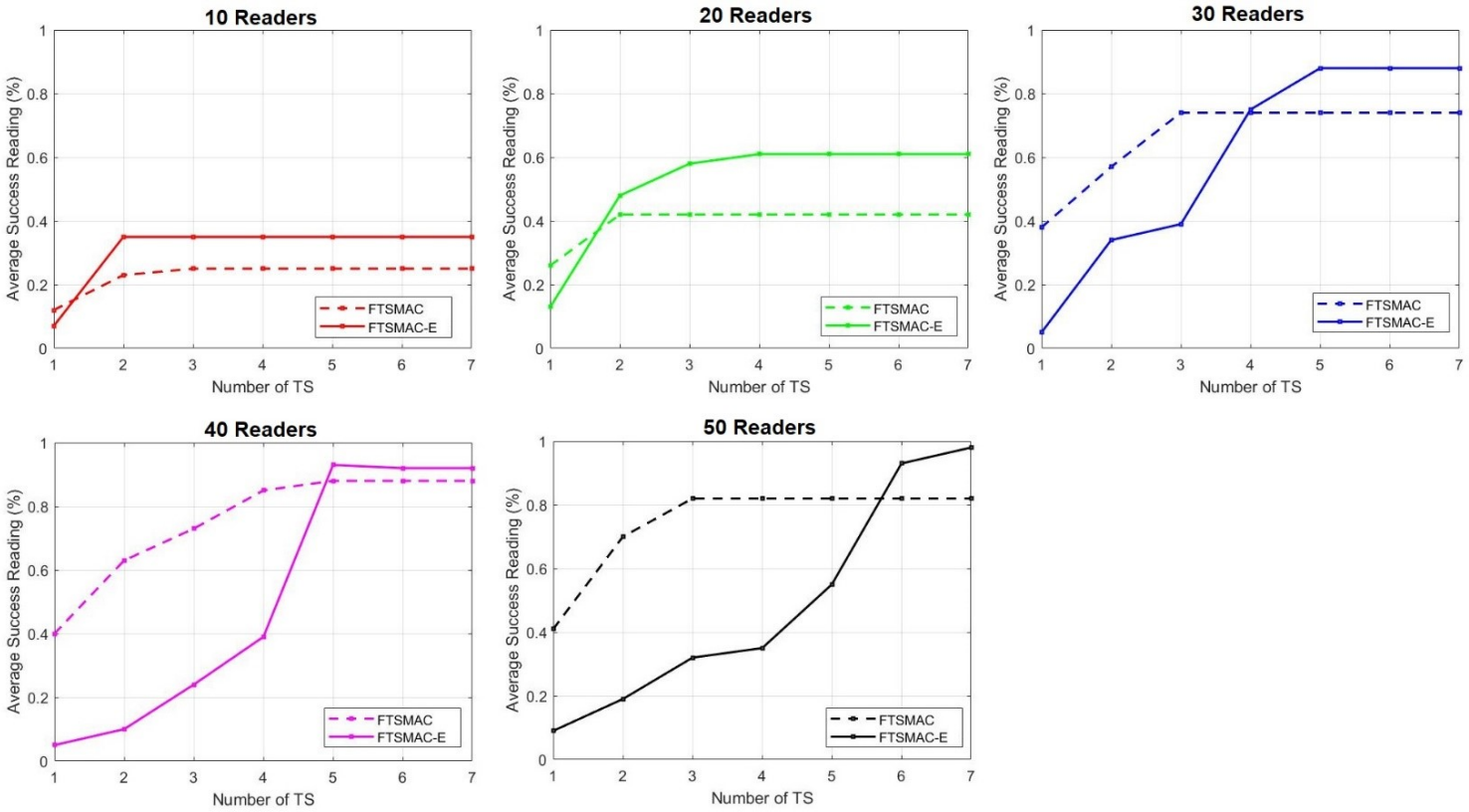

Figure 2.18: Moyenne de lecture réussie par rapport au nombre de TS

2.2.5 Conclusion

Dans cet article, nous avons proposé un protocole de couche MAC pour résoudre le problème de collision RRI et RTI dans les réseaux RFID multicanaux denses. Notre nouvel algorithme distribué FTSMAC-E fournit deux mécanismes de notification différents pour distribuer les fréquences et les Time Slots. Les résultats de la simulation du réseau RFID montrent l'évolution du protocole et l'amélioration du processus de protection contre les collisions RRI et RTI. Ce protocole permet d'activer le maximum de lecteurs possibles pour les réseaux denses.

Afin de rendre les lecteurs RFID indépendants et sans l'intervention des lecteurs voisins ou du serveur central au niveau de la gestion des ressources, dans le chapitre suivant nous permettons à chaque lecteur d'apprendre les scénarios de déploiement dans son réseau pour prédire la fréquence et la TS qui convient pour chaque période. Pour ce faire, nous nous orientons vers le concept d'intelligence artificielle en utilisant deux différentes contributions basées sur les réseaux de neurones artificiels et les réseaux immunitaires artificiels.

Chapter

3 Protocoles anti-collision des lecteurs RFID basé sur l'Intelligence Artificielle

Aujourd'hui, la progression vers l'intelligence artificielle devient plus exigeante pour la nouvelle génération de réseaux de capteurs RFID qui nécessitent un nombre considérable d'entités de lecture RFID, une mobilité accrue et des temps de transfert d'informations plus critiques. Les protocoles anti-collision classiques ne permettent plus une gestion efficace des ressources pour ces réseaux. La solution consiste à rendre les lecteurs RFID plus intelligents en déployant des modèles d'apprentissage pour chaque lecteur. Cela permettra aux différents lecteurs de réagir de manière autonome pour choisir les fréquences et les ressources temporelles adaptées à chaque situation durant leur cycle de vie sans coordination avec une entité centrale ou un lecteur voisin. Dans ce chapitre, nous avons réussi à rendre les lecteurs RFID indépendants et plus intelligents contre les collisions. Les deux contributions proposées reposent sur des concepts d'apprentissage différents : La première utilise les réseaux neuronaux artificiels tandis que la suivante est basée sur les réseaux immunitaires artificiels.

3.1 Contribution 3: Algorithme anti-collision basé sur les réseaux de neurones artificiels distribué pour les lecteurs RFID - DMLAR

3.1.1 Introduction

Un réseau RFID est généralement composé d'un grand nombre de lecteurs répartis dans l'espace. Il est donc difficile et peu pratique de gérer les ressources des lecteurs pendant leur déploiement. Par conséquent, un algorithme qui détermine de façon autonome la fréquence et la TS des lecteurs est nécessaire. Une nouvelle stratégie de gestion des ressources des noeuds lecteurs basée sur un réseau de neurones est proposée ici.

En général, les concepteurs de RCSF considèrent l'apprentissage machine comme une collection d'outils et d'algorithmes utilisés pour créer des modèles de prédiction. Cependant, les experts de l'apprentissage machine reconnaissent qu'il s'agit d'un domaine riche avec de très nombreux schémas et modèles. La compréhension de ces thématiques sera bénéfique à certains chercheurs à déployer l'apprentissage machine aux réseaux RFID. Appliqué à de nombreuses applications de RCSF, les algorithmes d'apprentissage machine seront des avantages considérables pour les réseaux RFID afin de résoudre les problèmes de collision.

Les réseaux de neurones artificiels (ANN) pour l'apprentissage supervisé sont généralement utilisé pour résoudre les problèmes de régression et de classification. Pour résoudre les collisions RRI et RTI, nous proposons que les lecteurs RFID utilisent un réseau neuronal artificiel comme méthode d'apprentissage. Cela permettra aux lecteurs de contrôler indépendamment la sélection de leurs ressources sans l'intervention d'un serveur central ou d'autres lecteurs. Les modèles ANN sont générés sur la base du scénario de déploiement du réseau RFID et du domaine d'application.

En tant que système de régression logistique étendu, le ANN incorpore des couches supplémentaires de combinaisons de caractéristiques. Grâce à ces couches supplémentaires, nous pouvons apprendre davantage et obtenir de meilleurs performances. Nous avons choisi le ANN au lieu de la régression logistique sur la base de la comparaison entre l'utilisation de deux modèles de collision (RRI et RTI) et le seul modèle RRI-RTI multiclasse (4 sorties) (voir tableau 3.1).

Table 3.1: Comparaison des performances

ANN model	RRI-RTI	RRI	RTI
Performance	0,21	0,85	1,74

Les entrées et les sorties sont utilisées par le réseau ANN pour apprendre et former un modèle adapté aux différents scénarios de déploiement et de déplacement des lecteurs RFID. En général, un réseau neuronal comporte trois couches de neurones interconnectés : la couche d'entrée, les couches cachées et la couche de sortie.

- La couche d'entrée: introduit les données collectées par le lecteur lors de chaque transaction.
- Les couches cachées: constituent le coeur de notre perception, où les relations entre les variables seront mises en évidence.
- La couche de sortie: prédit la présence ou l'absence de chacun des types de collision.

Dans cette section, nous allons présenter notre système de prédiction et son application sur le réseau RFID mobile.

3.1.2 Algorithme d'apprentissage

La méthodologie proposée est décrite dans la figure 3.1. L'objectif de notre algorithme est le suivant : Les données de prévision sont générées, collectées et partagées par les lecteurs RFID afin de les utiliser dans leur réseau neuronal artificiel pour l'auto-apprentissage, et les lecteurs diffusent leur modèle d'apprentissage sur le réseau pour sélectionner le meilleur.

3.1.2.1 Phase de collection

3.1.2.1.1 Construction de Dataset Avant de passer à la phase d'apprentissage utilisant l'ANN, nous allons réaliser différents scénarios de communication RFID dans lesquels chaque lecteur collecte et détecte la présence ou l'absence de collisions à chaque période (mouvement) des lecteurs (Algorithme 1). Ainsi, dans la phase de collecte (figure 3.1. Alloction), chaque lecteur Rx prépare son Dataset tout au long de la simulation pour la phase d'apprentissage. Les lecteurs mettent à jour leurs dataset Dx à chaque mouvement représenté par une instance de période 'p'. Ainsi, le nombre de lignes de données sera égal au nombre de périodes de simulation. Après la simulation, tous les lecteurs R1, ... ,Rn diffusent et mettent à jour leurs datasets (Algorithme 2). Ainsi, la taille de dataset devient :

$$dsatasetSize = nbrR \times p \tag{3.1}$$

avec, nbrR : nombre de lecteurs et p : nombre de périodes.

Une entrée de dataset se compose de deux parties, l'entrée et la sortie :

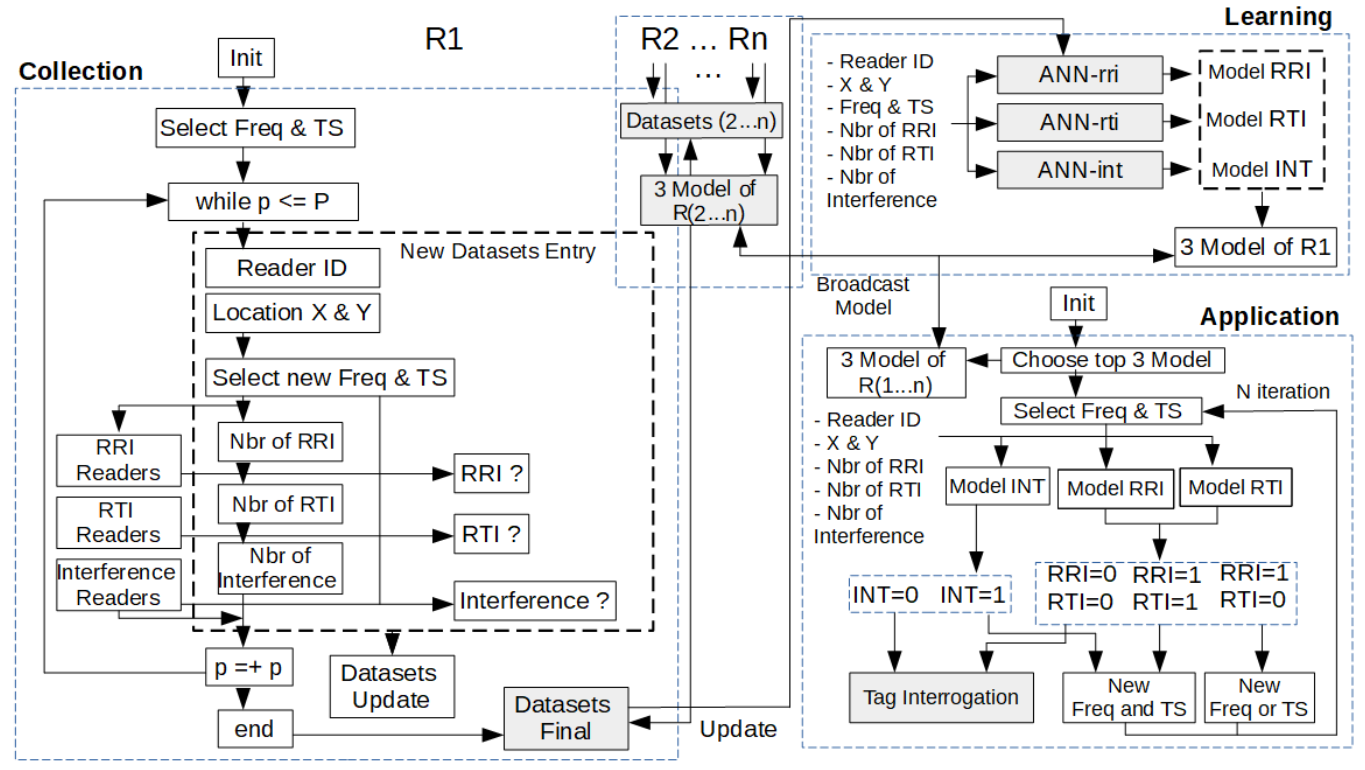

Figure 3.1: Schéma de l'algorithme proposé

$$datasetInput(Rx, pi) = [ReaderID, Location, NewFreq, NewTS, NbrRRI, NbrRTI, NbrINT] \tag{3.2}$$

Alors que, Rx est le xième lecteur et pi est la iième période.
Les paramètres d'entrée du dataset sont:

- Reader ID : Identifiant unique du lecteur.
- Location : Les coordonnées X et Y.
- New Freq : Le canal est choisi aléatoirement et utilisé pour la lecture des tags.
- New TS : Le Time Slot choisit aléatoirement et utilise pour la lecture des tags.
- Nbr RRI : Le nombre de lecteurs dans le domaine Reader to Reader Interférence.
- Nbr RTI : Le nombre de lecteurs dans le domaine Read to Tag Interférence.
- Nbr INT : Le nombre de lecteurs dans le domaine d'interférence.

$$datasetOutput(Rx, pi) = [RRI, RTI, INT] \tag{3.3}$$

avec, Rx est le xième lecteur et pi est la iième période.
Les paramètres de sortie du dataset sont:

- RRI : Détection d'interférence de lecture à lecture.
- RTI : Détection d'interférence de lecture à tag.
- INT : Détection d'interférence.

3.1.2.1.2 Calcul du nombre de lecteurs interférents et détection des interférences (Algorithme 1)

Afin de collecter les informations externes pour l'entrée (NbrRRI, NbrRTI et NbrINT) et la sortie (RRI, RTI et INT), un système de notification (Algorithme 1) a été développé. A chaque période de simulation, tous les lecteurs du réseau attendent le Backoff Golsorkhtabaramiri et al. [2015]. Le premier lecteur à se réveiller, Ri, écoute le canal de contrôle CC pendant une période T afin d'éviter les collisions sur ce canal Golsorkhtabaramiri et al. [2015]. Ensuite, le lecteur Ri diffuse un MsgD dans son champ d'interférence du canal de données égal au champ de lecture du canal de contrôle. Les lecteurs situés dans ce champ répondent par une trame MsgR pour indiquer les ressources utilisées. A ce stade, le lecteur Ri compare la puissance reçue des trames pour calculer le nombre de lecteurs qui sont susceptibles d'être en RRI (receiveP $<$ CCP) ou en RTI (receiveP $>$ CCP). Ainsi, Ri va vérifier s'il y a au moins une collision RRI (MsgR.Freq = Ri.Freq) ou RTI (MsgR.Freq = Ri.Freq et MsgR.TS = Ri.TS).

3.1.2.1.3 Processus de diffusion des datasets par les lecteurs (Algorithme 2)

Afin de partager les datasets sans collisions, nous utilisons une stratégie de communication efficace après la phase de collecte. Le lecteur Ri qui se réveille le premier (Backoff = 0) Golsorkhtabaramiri et al. [2015] commence à diffuser le MsgM contenant son dataset (Di). Ce message est reçu par les lecteurs dans le champ de lecture du canal de contrôle de Ri. Chaque lecteur compare le nombre de lecteurs reçus le MsgM (MsgM.nbrReader) avec le nombre total de lecteurs afin d'éviter une boucle de diffusion. Ensuite, il transmet le nouveau MsgM aux voisins suivants jusqu'à ce que tous les lecteurs mettent à jour leur dataset.

Pour une simulation longue et un réseau RFID dense, en fin de cette phase, tous les lecteurs disposeront de plus de données provenant de tous les lecteurs du réseau pour effectuer l'apprentissage dans la phase suivante.

3.1.2.2 Phase d'apprentissage

Dans la phase d'apprentissage, les lecteurs utilisent le réseau neuronal artificiel (ANN) Bartman et al. [2015] pour le protocole de la couche MAC. Chaque lecteur doit préparer trois modèles indépendants. Notre modèle ANN est composée d'une entrée de 7 neurones et d'une sortie d'un seul neurone et de 3 couches cachées, constituées successivement de 7,10 et 3 neurones (figure 3.3).

Les trois modèles utilisés par les lecteurs RFID (figure 3.2) :

- MxRRI : modèle de prédiction RRI, utilise le dataset avec entrée (Reader ID, Location, New Freq, Nbr RRI) et sortie (RRI).
- MxRTI : Modèle de prédiction RTI, utilise le dataset avec entrée (Reader ID, Location, New Freq, New TS, Nbr RTI) et sortie (RTI).
- MxINT : Modèle de prédiction d'interférence, utilise le dataset avec entrée (Reader ID, Location, New Freq, New TS, Nbr INT) et sortie (INT).

Algorithm 1 Calcul du nombre de lecteurs interférents et détection des interférences

CCP puissance du canal de contrôle
receiveP puissance reçue
MsgD = [senderID] message de découverte
Freq = random[freq1...freqN] choisir une fréquence aléatoire
TS = random[ts1...tsN] sélectionner un Time Slot aléatoire
MsgR = [receiverID, Freq, TS] message de réponse
RRI, RTI, INT = 0 Détection des interferences
Wait (Backoff) attendre un backoff aléatoire pour éviter les collisions au niveau du canal de contrôle
Rx broadcast MsgD chaque lecteur diffuse un message MsgD pour détecter les lecteurs dans le champ de contrôle
if receive = MsgD réception du message MsgD
send MsgR réponse au message MsgR du lecteur expéditeur
elseif receive = MsgR reception du message MsgR
// ——— RRI section——-
- if MsgR.receiveP < CCP puissance du signal reçu inférieure à la puissance du canal de contrôle
nbrRRI = nbrRRI + 1 nouveau lecteur de RRI
– if MsgR.Freq = this.Freq Le lecteur RRI utilise la même fréquence
RRI = 1 Détection de collision RRI
// ——— RTI section——-
- elseif
nbrRTI = nbrRTI + 1 nouveau lecteur dans RTI
– if MsgR.Freq = this.Freq and MsgR.TS = this.TS Le lecteur RRI utilise la même fréquence et TS
RTI = 1 Détection de collision RTI
- end
end
// —— Interference section ——
nbrINT = nbrRRI + nbrRTI nouveau lecteur en Interférence
if RRI=1 or RTI=1 Il existe une collision RRI ou RTI
INT = 1 Interférence détecté
else
INT = 0 Interférence non détecté

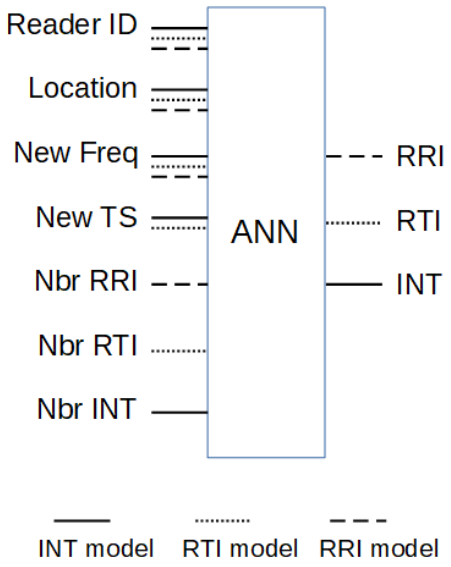

Figure 3.2: Modèles proposés par l'ANN

Après la phase d'apprentissage, chaque lecteur diffuse les trois modèles (Algorithme 2) à tous les lecteurs du réseau RFID. L'objectif est d'exploiter le choix multiple en profitant de la variété des expériences de chaque lecteur. Ainsi, tous les lecteurs recevront l'ensemble des modèles suivants :

$$receivedModel = [[M1RRI, M1RTI, M1INT]...[MiRRI, MiRTI, MiINT]...[MnRRI, MnRTI, MnINT]] \tag{3.4}$$

Où i est le ième lecteur et n est le nombre de lecteurs dans le réseau.

3.1.2.3 Phase d'application

Dans la phase d'application et au début de la simulation, tous les lecteurs sélectionnent les meilleurs modèles MxRRI, MxRTI et MxINT en fonction de leurs performances. Ainsi, tous les lecteurs utiliseront les mêmes modèles. Ensuite, et à chaque phase de la simulation (mouvement des lecteurs), le lecteur doit préparer l'entrée pour lancer ses modèles ANN afin de prédire la présence d'une collision. Pour cela, le lecteur ajoute son ID et sa position (x, y) puis choisit aléatoirement une Fréquence et un Time Slot et calcule le nombre de lecteurs en RRI, RTI et INT. Les modèles peuvent alors prédire la présence de collisions et effectuer l'action appropriée pour N itération selon le tableau 3.2.

3.1.2.4 Exemple illustratif

Afin de comprendre le fonctionnement de notre algorithme, la figure 3.4 illustre un exemple d'utilisation des modèles d'apprentissage RRI, RTI et INT par le lecteur R1 pendant sa durée de vie.

Après que le lecteur R1 construit le dataset et les modèles ANN. Il lance le premier test a la période p1 en sélectionnant la fréquence f1 et le Time slot ts1 et détecte ensuite les lecteurs qui

Algorithm 2 Diffusion de Datasets et de modèles

Dx Dataset du lecteur Rx
MxRRI Rx reader RRI model
MxRTI Rx reader RTI model
MxINT Rx reader Interference model
nbrReader nombre de lecteurs qui ont reçu MsgM pour éviter la boucle de diffusion infinie
modelID model identification
MsgM = [modelID, nbrReader, MxRRI, MxRTI, MxINT] model message
ModelSet model list
Reader.size nombre de lecteurs dans le réseau de simulation
Rx broadcast MsgM chaque lecteur a diffusé un MsgM dans le canal de contrôle
-if receive = MsgM recevoir le message MsgM
– while MsgM.nbrReader < Reader.size tant que les lecteurs du réseau n'ont pas tous reçu le message MsgM
— if MsgM.modelID not existe ModelSet Le MsgM du lecteur ID n'est pas reçu
update ModelSet ajouter les nouveaux modèles à la liste des modèles
MsgM.nbrReader = MsgM.nbrReader + 1 un nouveau lecteur reçoit le message MsgM
broadcast MsgM diffuser un message MsgM dans le canal de contrôle
– end
-end

Table 3.2: Les résultats de la prédiction et les actions correspondantes

	Prediction			Action		
Model	RRI	RTI	Interference	New Freq	New TS	Tag Interrogation
MxRRI and MxRTI	0	0	-	x	x	√
	1	0	-	x	√	x
	1	1	-	√	x	x
	1	1	-	√	√	x
MxInterference	-	-	0	x	x	√
	-	-	1	√	√	x

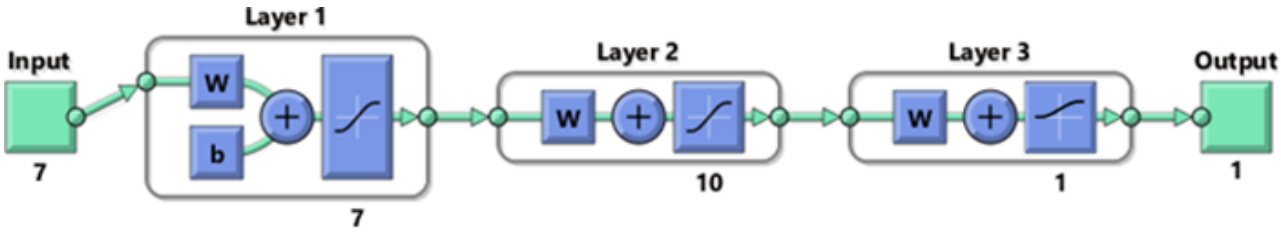

Figure 3.3: Architecture de réseau neuronal artificiel pour les lecteurs RFID

peuvent être dans le RRI et le RTI (Tableau 3.3). Ainsi, le résultat du modèle ne détecte aucune collision et commence à interroger les tags. À l'étape suivante (p2), le lecteur R1 sélectionne une nouvelle fréquence f3 et intervalle de temps ts1, puis détecte deux lecteurs qui peuvent être en RRI et RTI (tableau 3.3). Le résultat du modèle réussi prévoit la présence d'une collision RRI. À ce stade, le lecteur tente une nouvelle fréquence pendant N itérations. Dans les autres périodes p3, p4 et p5, le modèle de lecteur R1 prédit la présence de collisions RRI et RTI (Tableau 3.3). Par conséquent, le lecteur essaie une nouvelle fréquence et Time Slot pour N itérations.

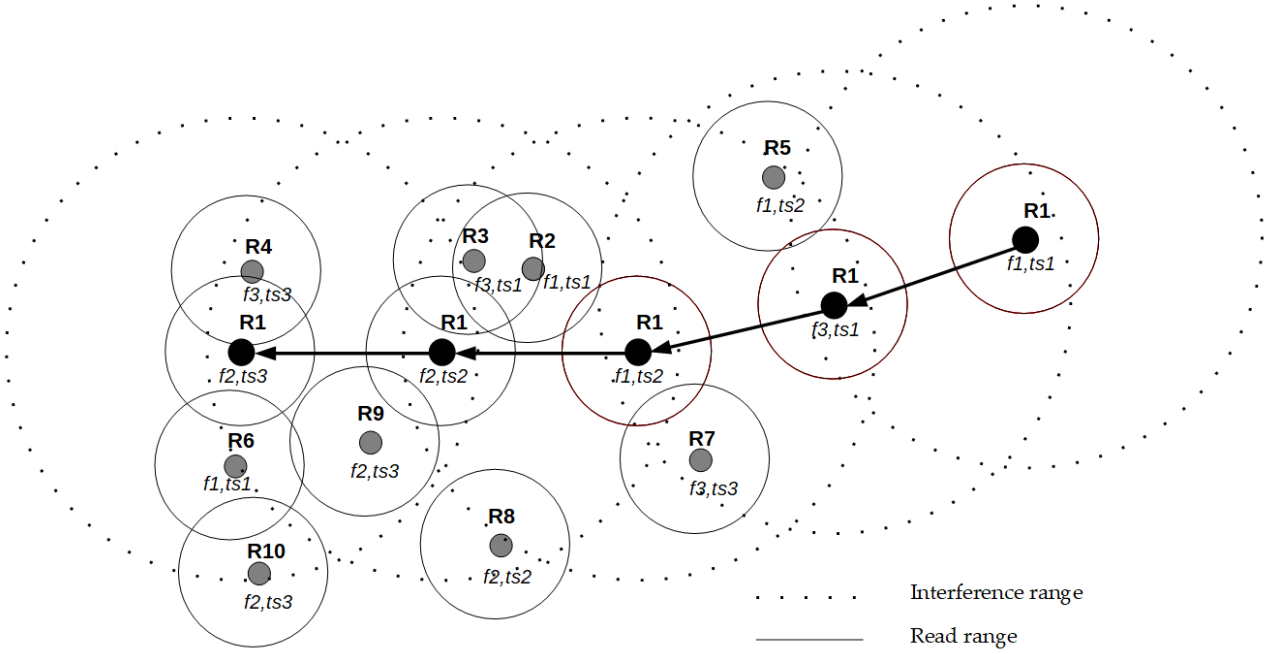

Figure 3.4: Scénario d'un lecteur mobile dans un réseau RFID

Les contributions suivantes sont apportées à notre système de détection des collisions :

- Exécution de différents scénarios de simulation pour le réseau RFID en utilisant plusieurs lecteurs et un temps de simulation plus long.

Table 3.3: L'entrée/sortie du modèle ANN du lecteur durant son mouvement

	ANN Input							ANN Output		
period	Reader ID	Location	New Freq	New TS	Nbr RRI	Nbr RTI	Nbr INT	RRI	RTI	INT
p1	1	x1,y1	f1	ts1	-	-	-	0	0	0
p2	1	x2,y2	f3	ts1	2	-	2	1	0	0
p3	1	x3,y3	f1	ts2	4	2	4	1	1	1
p4	1	x4,y4	f2	ts2	7	3	7	1	1	1
p5	1	x5,y5	f2	ts3	4	2	4	1	1	1

- Collecte de données par les lecteurs à chaque mouvement et diffusion du résultat des datasets à la fin de la simulation à tous les lecteurs du réseau.
- Création et configuration des objets du réseau neuronal par les lecteurs.
- Entraînement du réseau de neurones pour obtenir les trois modèles requis et les diffuser aux autres lecteurs du réseau.
- Choix et validation du meilleur modèle à utiliser pour la prédiction des collisions.

3.1.3 Simulations et résultats

3.1.3.1 Environnement et paramètres de simulation

Dans cette section, nous présentons les résultats obtenus en appliquant le modèle considéré (figure 3.3). Le réseau RFID est déployé dans le domaine de la santé sur le site d'un hôpital. Le réseau RFID est combiné avec le réseau de capteurs où les tags-capteurs sont attachés aux patients et les lecteurs RFID sont portées par les infirmières. Nous avons réalisé trois modèles de mobilité pour les lecteurs : mobilité free (figure 3.5), mobilité semi-free (figure 3.6) et mobilité directed (figure 3.7).

Nous avons réalisé plusieurs simulations de réseaux RFID sur MATLAB en utilisant notre algorithme anti-collision selon différents critères de mobilité, de ressource et de densité. Un réseau neuronal nécessite un grand nombre de données pour l'apprentissage et le test. Le dataset dans cette proposition est préparé durant les simulations.

Les paramètres de simulation sont présentés dans le tableau 3.4. Les lecteurs mobiles (10, 20 ... 50 lecteurs) sont répartis sur une surface de $600m \times 600m$ et tous les lecteurs peuvent communiquer entre eux par un canal de contrôle. Ces lecteurs peuvent utiliser les canaux de données disponibles (1,2 ... 10 fréquences) et chaque canal peut supporter chaque trame de Time Slots (1,2 ... 10 TS). L'ANN utilisé pour les modèles RRI, RTI et INT est constitué de 7 noeuds d'entrée, de 3 couches cachées de 7, 10 et 1 noeuds en succession, et d'un noeud de sortie. Les données d'entrée et de sortie du réseau neuronal sont présentées comme suit :

- Reader ID: échelles à l'intervalle [0-10]
- Location X and Y: échelles à l'intervalle [0-10]
- New Freq: [2,4,6,8,10]
- New TS: [2,4,6,8,10]

Table 3.4: Paramètres de simulation

Paramètre	Valeur
Surface de simulation	600m x 600m
Nombre de lecteurs	10, 20, 30, 40, 50
Nombre de tags	1000
Position du lecteur et de tag	Random
Type d'antenne	Omni-directional
Portée de lecture du canal de données (rr)	3 m
Portée d'interférence du canal de données (cr)	562 m
Portée de lecture du canal de contrôle (crr)	6 m
Nombre de canaux de données	2, 4, 6, 8, 10
Nombre de Time Slot	2, 4, 6, 8, 10
Nombre de canaux de contrôle	1
Taille de la couche d'entrée des ANN	7
Taille de la couche de sortie des ANN	1
Nombre de couche cachée des ANN	3
Fonction d'entraînement	trainlm
Nombre maximum d'époques à entraîner	1000
Fonction de transfert	Tansig, logsig
Nombre de périodes	1000
Taille de dataset	nbr periods * nbr readers
Division des données pour l'apprentissage	70 %
Division des données pour la validation	15 %
Division des données pour les tests	15 %

- Nbr RRI, Nbr RTI and Nbr INT: échelles à l'intervalle [0-10]

- RRI, RTI and INT: Booléen [0,1]

Nous avons utilisé la fonction d'apprentissage trainlm basée sur l'optimisation de Levenberg-Marquardt pour mettre à jour les valeurs de poids et de biais. Pour un tel réseau de capteurs RFID, trainlm est souvent l'algorithme de rétropropagation le plus rapide et le plus recommandé pour les algorithmes supervisés car il nécessite moins de mémoire que les autres algorithmes Karatas and Sahingoz [2018].

Nous avons choisi les protocoles anti-collision suivants qui utilisent le principe de communication distribuée (similaire à notre approche) : Pulse, CORA, MCMAC et FTSMAC pour comparer les performances.

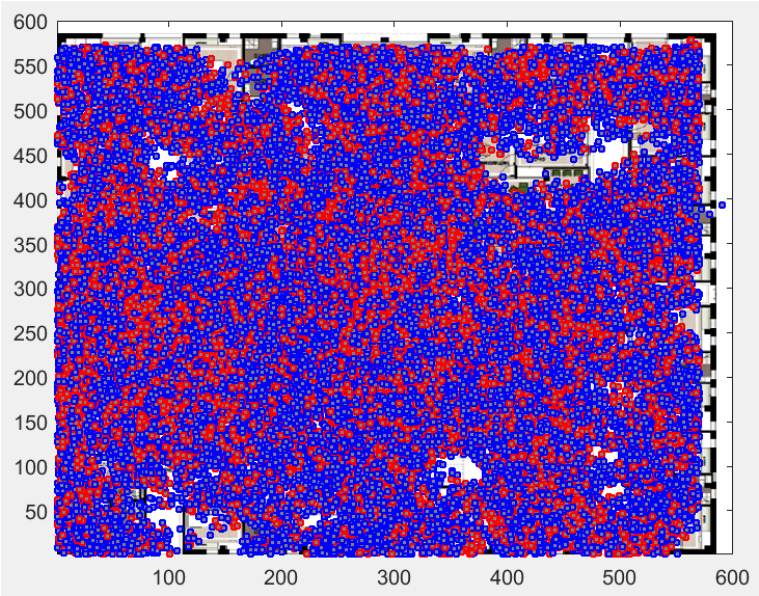

Figure 3.5: Réseau de lecteurs RFID pour free mobility

La performance de l'algorithme anti-collision du lecteur a été évaluée selon différents critères, la prédiction des collisions (equation 3.5) et la performance du système (equation 2.1).

Nous définissons la prédiction de collision comme suit :

$$CollisionPrediction(\%) = TP + TN \tag{3.5}$$

Où TP est une matrice de confusion vrai-positif et TN est une matrice de confusion vrai-négatif de l'ANN.

Selon la norme européenne Borisov and Zuev [2017], la puissance de sortie autorisée est de 2 W, ce qui donne une couverture de lecture de 10 m pour le lecteur. Pour calculer le Path Loss entre le lecteur et le tag et vice versa pour une distance de lecture de 3m, nous utilisons l'équation 3.6

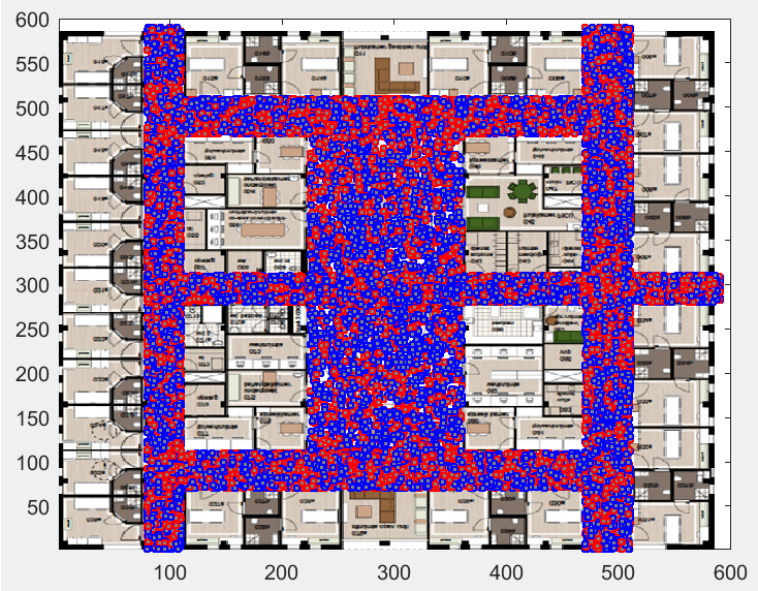

Figure 3.6: Réseau de lecteurs RFID pour semi-free mobility

$$\begin{cases} PL = 35 + 25 \times log(\frac{d}{1}) & \text{if } 0 < d < 8 \\ PL = 35 + 25 \times log(\frac{3}{1}) = 43,92db \end{cases} \tag{3.6}$$

Pour alimenter un tag passif, une puissance d'entrée de 13 dB est nécessaire, donc la perte est de : $PL + PL + 13 = 100,85dB$

La distance nécessaire entre deux lecteurs pour éviter la collision est calculée comme suit :

$$\begin{cases} PL = 35 + 25 \times log(\frac{d}{1}) = 100,85 \\ d = 562m \end{cases} \tag{3.7}$$

3.1.3.2 Performances et prédiction des collisions

Dans cette section, nous allons étudier et appliquer les trois modèles obtenus dans la phase d'apprentissage pour la prédiction de collision.

Les figures 3.5, 3.6 et 3.7 présentent l'historique des prédictions pour tous les mouvements des lecteurs dans un réseau RFID constitué de 50 lecteurs utilisant 4 fréquences et 4 TS. La couleur rouge définit la position (1000 mouvements pour chaque lecteur) où la prédiction de collision est fausse, alors que la couleur bleue correspond à la prédiction vraie. D'après les figures, nous pouvons remarquer que les prédictions correctes sont les plus nombreuses pour les différents modèles de mobilité. La densité varie selon les modèles de déploiement. Les lecteurs sont plus denses et par conséquent plus de prédictions fausses dans la figure 3.7 qui représente le modèle de mobilité directed suivi par la mobilité semi-free et la mobilité free successivement.

Les résultats de Best Validation Performance pour le modèle ANN décrit ci-dessus en utilisant différents datasets (taille de datasets : $50 \times 1000 = 50000$ lignes) dans le tableau 3.5 montrent

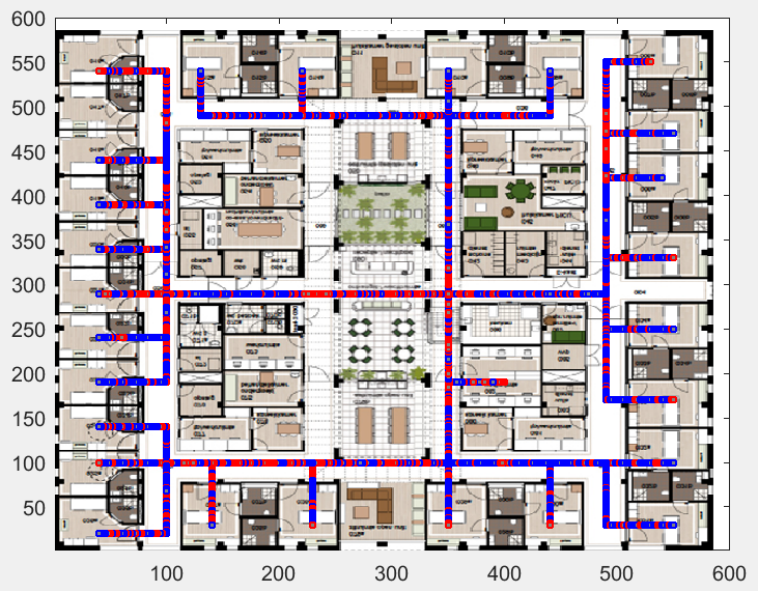

Figure 3.7: Réseau de lecteurs RFID pour directed mobility

Table 3.5: Performance du modèle pour différents Datasets

	Modèle RRI	Modèle RTI
Dataset 1	0.092179	0.10571
Dataset 2	0.094731	0.10626
Dataset 3	0.086352	0.10309
Dataset 4	0.090341	0.10636
Dataset 5	0.088141	0.10927
Dataset 6	0.087115	0.10341
Dataset 7	0.089247	0.10869

la cohérence et la stabilité de la performance pour différentes expériences. Les figures 3.8 et 3.9 illustrent les performances des modèles RRI et RTI pour différents datasets liés au déploiement de lecteurs utilisant 10 fréquences et TS. Les résultats du modèle RRI sont similaires autour de 0,08, alors qu'ils diffèrent pour le modèle RTI entre 0,04 et 0,11.

3.1.3.3 *Évolution de la prédiction des collisions*

Les figures 3.10, 3.11 et 3.12 montrent l'évolution de la valeur de la prédiction de collision pour chaque modèle de mobilité en fonction du nombre de lecteurs, de fréquence et TS utilisés par chaque lecteur.

Dans la figure 3.10, les résultats de la prédiction de collision RTI sont toujours supérieurs au modèle RRI et INT, quel que soit le nombre de lecteurs dans le réseau. Le modèle RTI atteint son maximum et dépasse les autres modèles pour un réseau de 50 lecteurs (presque 100%) indépendamment de la disponibilité des ressources. Les modèles RRI et INT obtiennent des résultats proches dans les déploiements de 50, 40 et 30 lecteurs avec un avantage du modèle RRI. Ainsi, nous constatons que ce modèle de déploiement peut prédire efficacement la présence de

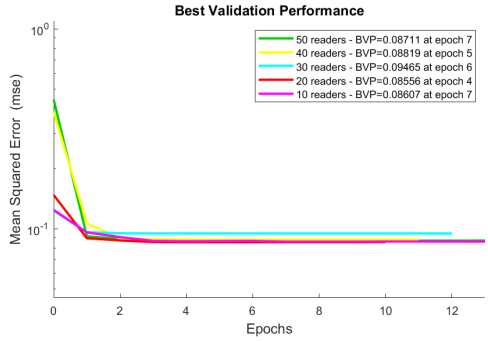

Figure 3.8: Best Validation Performance de modele RRI

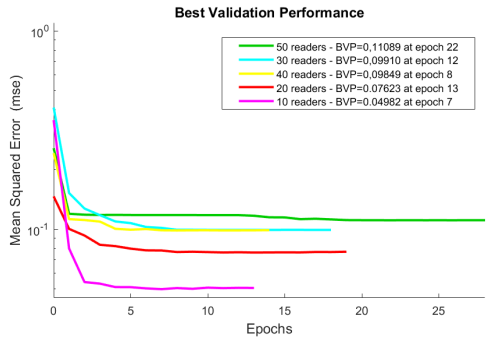

Figure 3.9: Best Validation Performance de modele RTI

collisions RRI pour les réseaux RFID denses, indépendamment de la disponibilité des ressources. Alors que les collisions RTI peuvent être prédites efficacement (jusqu'à 90% pour 10 fréquences et TS) en fonction de la disponibilité des ressources.

Dans la figure 3.11, le modèle RRI reste supérieur aux autres modèles pour les réseaux de 50 et 40 lecteurs et indépendamment des ressources disponibles. En revanche, le modèle RRI rejoint le modèle RTI pour le déploiement de 10 et 20 lecteurs de 4 fréquences et TS. Selon ces résultats, le modèle de prédiction de collision RRI peut être déployé dans les réseaux RFID denses indépendamment des ressources, tandis que pour les réseaux sparse, les collisions RRI et RTI peuvent être prédites efficacement avec l'avantage du RRI pour 2 fréquences et TS.

Dans le dernier déploiement (figure 3.12), on remarque que les trois modèles se rapprochent. Le modèle de prédiction RTI reste supérieur de l'autre modèle pour les réseaux denses (40 et 50 lecteurs), pour un réseau moyen (30 lecteurs) les modèles RRI et RTI sont similaires, alors que dans un réseau sparse (10 et 20 lecteurs) le modèle RRI devient supérieur au modèle RTI.

D'après l'analyse des trois scénarios précédents, vous remarquerez que nous n'avons pas abordé le modèle de prédiction de collision INT en raison de sa faiblesse. Nous ne pouvons donc pas utiliser ce modèle général de prédiction des collisions. Nous utilisons donc deux modèles différents (RRI et RTI), chacun étant chargé de prédire l'un des types de collision RRI et RTI.

Dans les figures 3.13 et 3.14, nous avons comparé les performances des différents modèles RRI, RTI et INT déployés pour le modèle de mobilité diricted en fonction du nombre de fréquences dans la figure 3.13 (10 TS fixes) et du nombre de TS dans la figure 3.14 (10 TS fixes) pour un déploiement de 50 lecteurs. Dans la figure 3.13, le modèle de prédiction RTI est le plus fort et le plus stable en fonction du nombre de TS disponibles, tandis que l'évolution du modèle de prédiction RRI dépend de la disponibilité des TS en se rapprochant du modèle RRI en utilisant 10 TS. Dans la figure 3.14, les modèles RRI et RTI sont presque similaires avec un petit avantage pour le modèle RRI en utilisant les basses fréquences (2 à 4 fréquences) et un avantage pour le modèle RTI dans les hautes fréquences (8 à 10 fréquences).

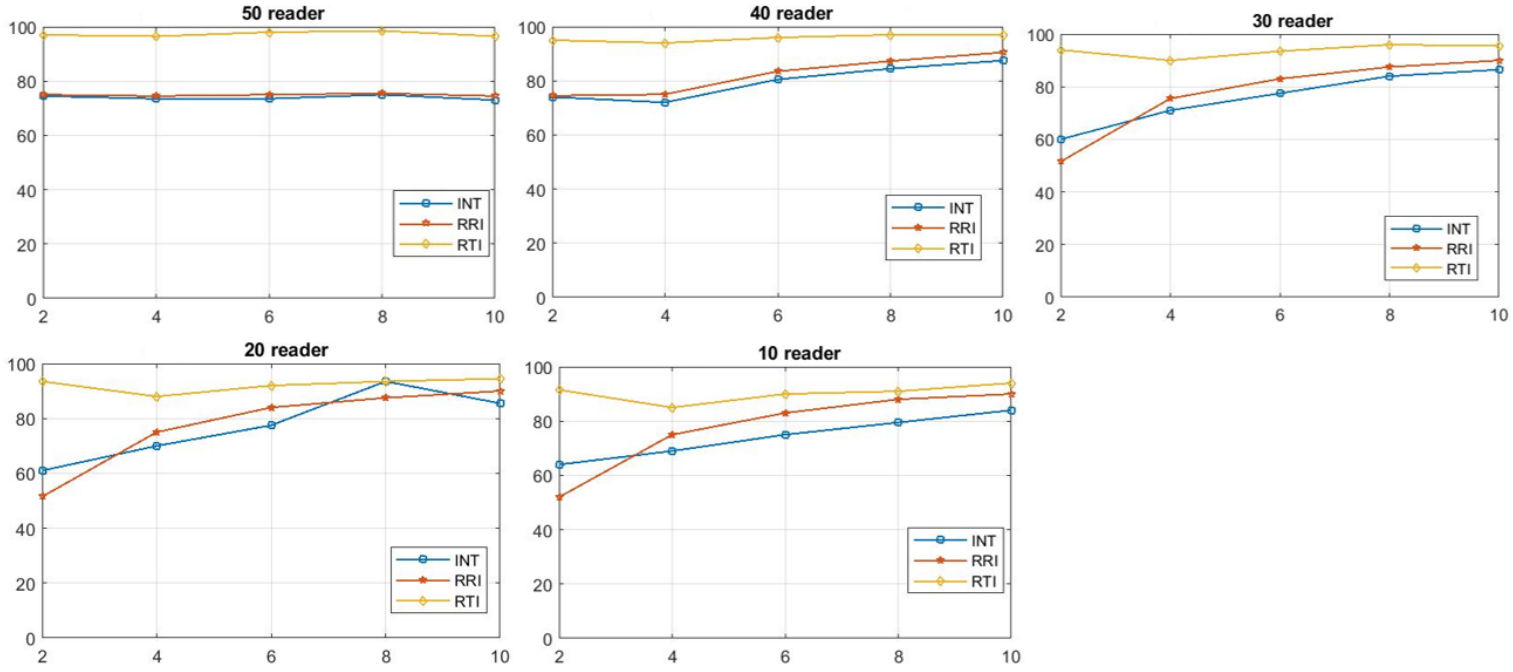

Figure 3.10: Prédiction des collisions en fonction du nombre de fréquences et Time Slot utilisés pour le modèle de mobilité free.

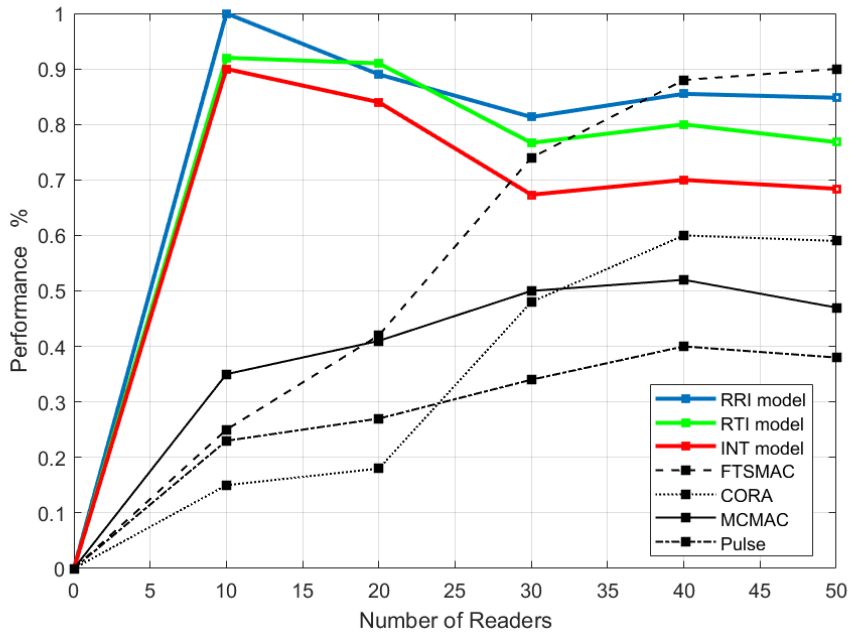

Figure 3.15: Performance en fonction du nombre de lecteurs

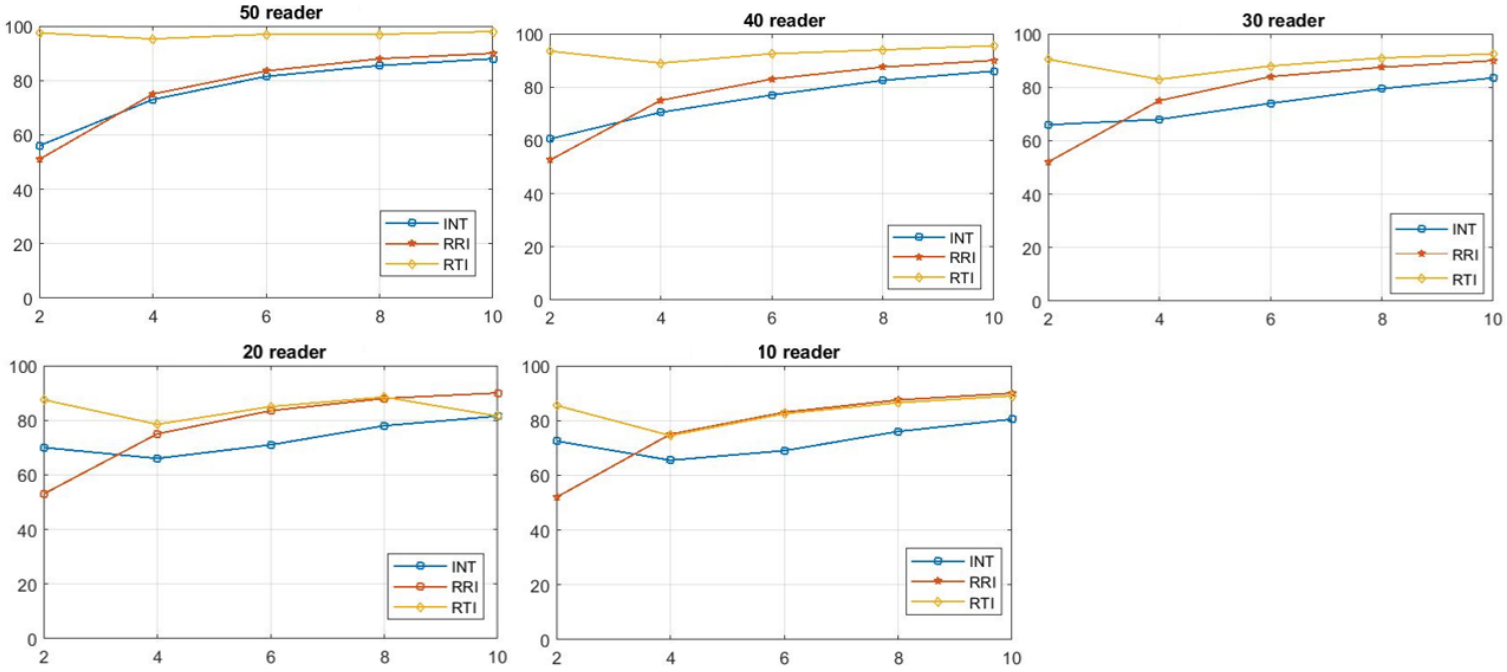

Figure 3.11: Prédiction des collisions en fonction du nombre de fréquences et Time Slot utilisés pour le modèle de mobilité semi-free

Dans la figure 3.15, nous avons comparé notre protocole utilisant les différents modèles d'apprentissage avec les solutions de la littérature Pulse, MCMAC, CORA et FTSMAC pour un déploiement de 10 à 50 lecteurs utilisant 3 fréquences et Time Slots. La simulation montre que notre protocole obtient les meilleurs résultats indépendamment du nombre de lecteurs RFID. Il atteint son maximum (90% à 100%) pour un réseau de 10 à 20 lecteurs, après la chute à 30 lecteurs, les résultats se stabilisent entre 77% et 85% pour les modèles RRI et RTI.

3.1.4 Comparaison des coûts - (10 fréquences et 10 TS)

Dans le domaine de la santé, les données recueillies auprès des patients sont extrêmement importantes et critiques. La figure 3.16 illustre le nombre d'interrogations ayant échoué en fonction du nombre de lecteurs déployés. Les protocoles CORA et MCMAC suivent une évolution similaire du nombre d'interrogations ayant échoué. CORA ne prent pas en charge davantage de ressources, alors que MCMAC ne couvre que le problème de collision RRI.

La surcharge du réseau représente le nombre de paquets de contrôle échangés entre les lecteurs. Nous constatons que notre méthode DMLAR présente le plus faible taux de surcharge comme le montre la figure 3.17. Alors que ce paramètre augmente pour MCMAC. De plus, NFRA utilise un serveur pour diffuser les commandes de contrôle aux lecteurs ce qui augmente le nombre d'octets échangés.

Le délai global de lecture des lecteurs est déterminé comme le temps nécessaire au lecteur pour interroger toutes les tags. La figure 3.18 montre que NFRA consomme plus de temps en raison de la communication lecteur-serveur. FTSMAC et MCMAC nécessitent un délai raisonnable en

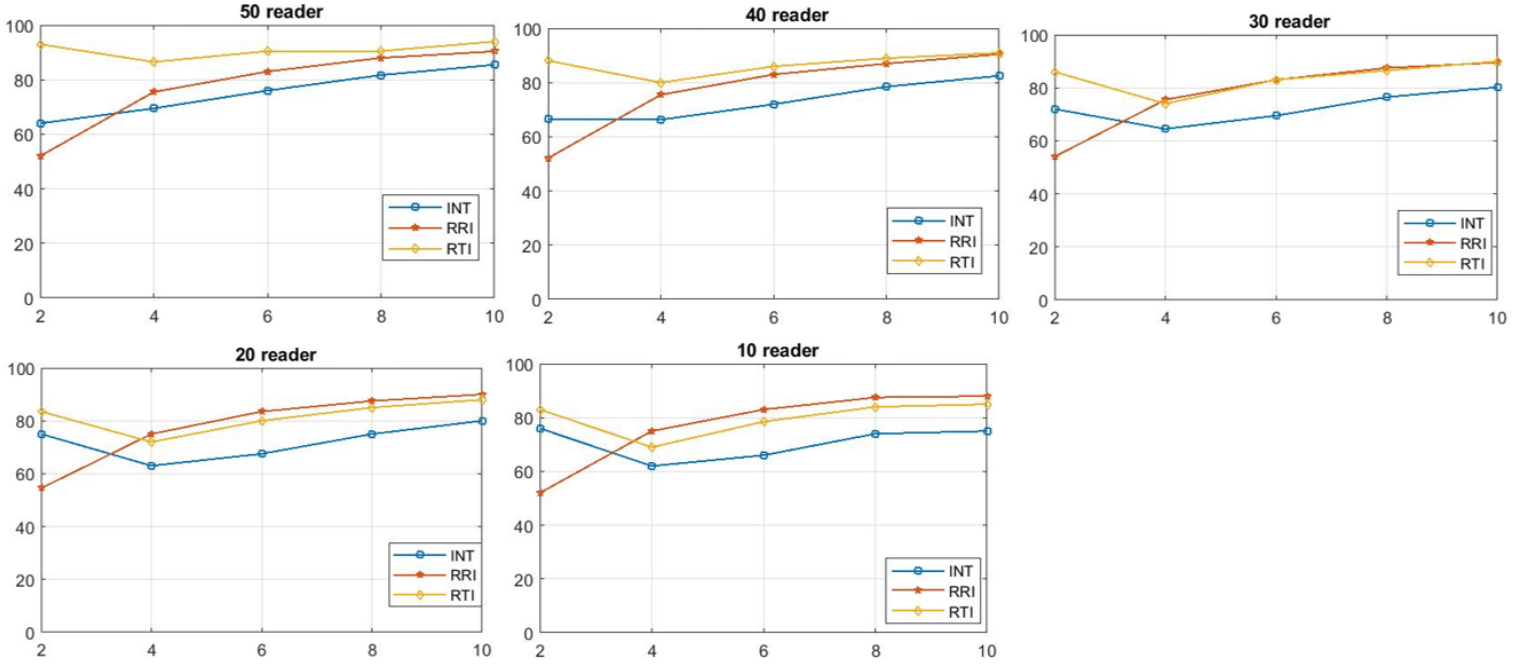

Figure 3.12: Prédiction des collisions en fonction du nombre de fréquences et Time Slot utilisés pour le modèle de mobilité directed

utilisant des systèmes de notification avancés. En revanche, l'approche DMLAR nécessite un délai plus faible puisqu'elle utilise ce délai pour prédire les collisions au moyen de modèles ANN au lieu d'utiliser un système de notification.

L'efficacité énergétique est spécifiée comme l'énergie totale requise par le lecteur pour interroger les tags. Comme le montre la figure 3.19, NFRA a une consommation d'énergie élevée car il utilise un serveur central pour gérer toutes les interactions. MCMAC et FTSMAC suivent un développement parallèle avec une différence de presque 15 w en utilisant 40 et 50 lecteurs. D'autre part, le DMLAR consomme le minimum d'énergie en raison de l'absence d'un système de notification qui nécessite plus d'énergie consommée par ses modules de communication.

3.1.5 Conclusion

Cette partie propose un nouvel algorithme anti-collision pour la gestion des ressources fréquentiels et temporels des lecteurs RFID dans les environnements mobiles. Ce protocole permet aux lecteurs de contrôler individuellement leurs ressources en fonction du modèle de prédiction de collision sélectionné par les lecteurs du réseau RFID après la phase d'apprentissage. Les lecteurs utilisent un modèle de prédiction de collision pour chaque type d'interférence, soit entre lecteurs ou entre lecteurs et tags pour une plus grande précision et une prédiction correcte. Le dataset utilisé pour l'apprentissage des lecteurs est mis à jour à chaque mouvement au cours duquel les lecteurs changent de position et les ressources utilisées. À la fin de la simulation, tous les lecteurs diffusent leur datasets afin d'obtenir une dataset plus importante pour un apprentissage efficace. L'objectif de cette proposition est de permettre au plus grand nombre de lecteurs possible d'interroger les tags sans collision afin d'augmenter les performances des réseaux RFID

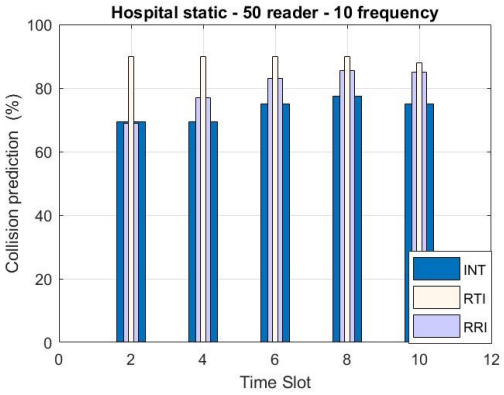

Figure 3.13: Prédiction des collisions en fonction du nombre de TS (50 lecteurs 10 fréquences)

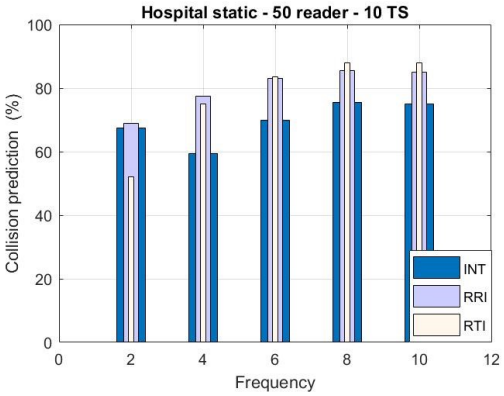

Figure 3.14: Prédiction des collisions en fonction du nombre de fréquences (50 lecteurs 10 TS)

mobiles de manière autonome et plus intelligente.

3.2 Contribution 4: Protocole de prévention des collisions utilisant les réseaux immunitaires artificiels pour les réseaux RFID dense - AIN-CA

3.2.1 Introduction

Dans cette contribution, nous proposons une innovation en introduisant un algorithme d'apprentissage issue de la nature, base sur le système immunitaire biologique. Ce dernier est un système évolutif fondamental que les êtres humains possèdent et qui nous permet de protéger notre organisme contre l'invasion de virus ou de bactéries grâce à des mécanismes tels que la reconnaissance des antigènes, l'évolution, la mémoire et l'ajustement cellulaire.

Pour être précis (figure 3.20), dès qu'un pathogène/antigène pénètre dans notre corps, la réponse immunitaire du réseau immunitaire est activée et commence à fonctionner. Si l'agent pathogène/antigène est détecté pour la première fois, les cellules lymphatiques B activés produisent un certain nombre d'anticorps qui seront répliqués pour tenter de détruire l'agent pathogène/antigène a l'aide des cellules lymphocytes T. Dans ce processus de développement biochimique, les anticorps se multiplient et se multiplient. Au cours de ce processus de développement biochimique, ces anticorps deviennent à plusieurs reprises somatiquement hypermutés et déconcentrés, à un taux élevé, à chaque fois que. Au fur et à mesure que cette réponse biochimique progresse, ces anticorps deviennent progressivement matures et se transforment ainsi en cellules mémoires qui ont des cycles de vie plus longs. Ce processus est généralement appelé la réponse primaire. Plus tard, cependant, les cellules mémoire répondront rapidement au même antigène ou à un antigène similaire. Ce processus est souvent appelé la réponse secondaire, qui est beaucoup plus rapide et plus puissante que la réponse primaire.

Comme des méthodes d'optimisation intelligentes pour résoudre des problèmes scientifiques tels que la détection des intrusions et la manipulation des données, le système immunitaire artificiel a été développé sur la base des principes du système immunitaire biologique. Un système

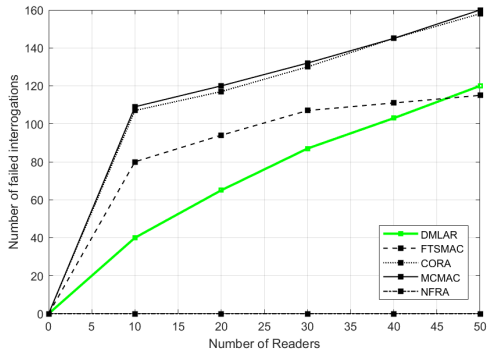

Figure 3.16: Interrogations échouées vs Nombre de lecteurs

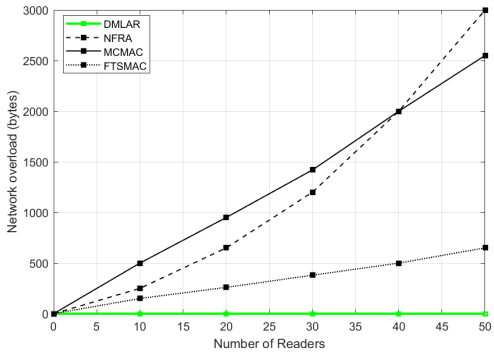

Figure 3.17: Surcharge du réseau vs Nombre de lecteurs

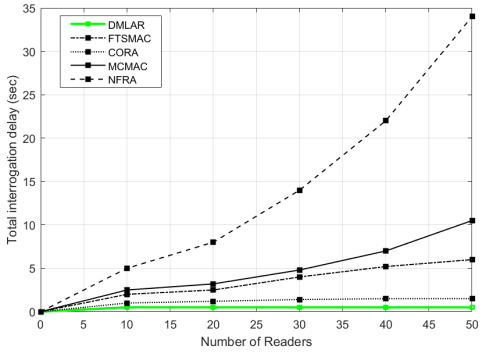

Figure 3.18: Temps total d'interrogation vs Nombre de lecteurs

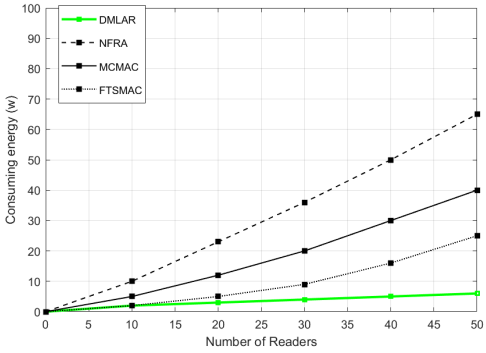

Figure 3.19: Consommation d'énergie vs Nombre de lecteurs

immunitaire artificiel est classé en plusieurs groupes : Série de sélection négative, série de sélection de clones, série de théorie du danger et série de réseau immunitaire. Pour comprendre la représentation artificielle, certains concepts des systèmes immunitaires biologiques et des réseaux immunitaires artificiels sont les suivants :

Systèmes immunitaires biologiques est constitué de:

- Antigène : Macromolécule reconnue par les anticorps ou les cellules du système immunitaire d'un organisme, capable de déclencher une réponse immunitaire chez celui-ci.
- Anticorps : Molécule complexe propagée par les cellules B utilisée par le système immunitaire adaptatif pour détecter et neutraliser spécifiquement les agents pathogènes.
- Affinité : Attraction spécifique entre un anticorps et un antigène (figure 3.21).

Réseaux immunitaires artificiels constitue de;

- Antigène : Question objective à résoudre, y compris les conditions de contrainte.
- Anticorps : Solution candidate qui satisfait la question projective.

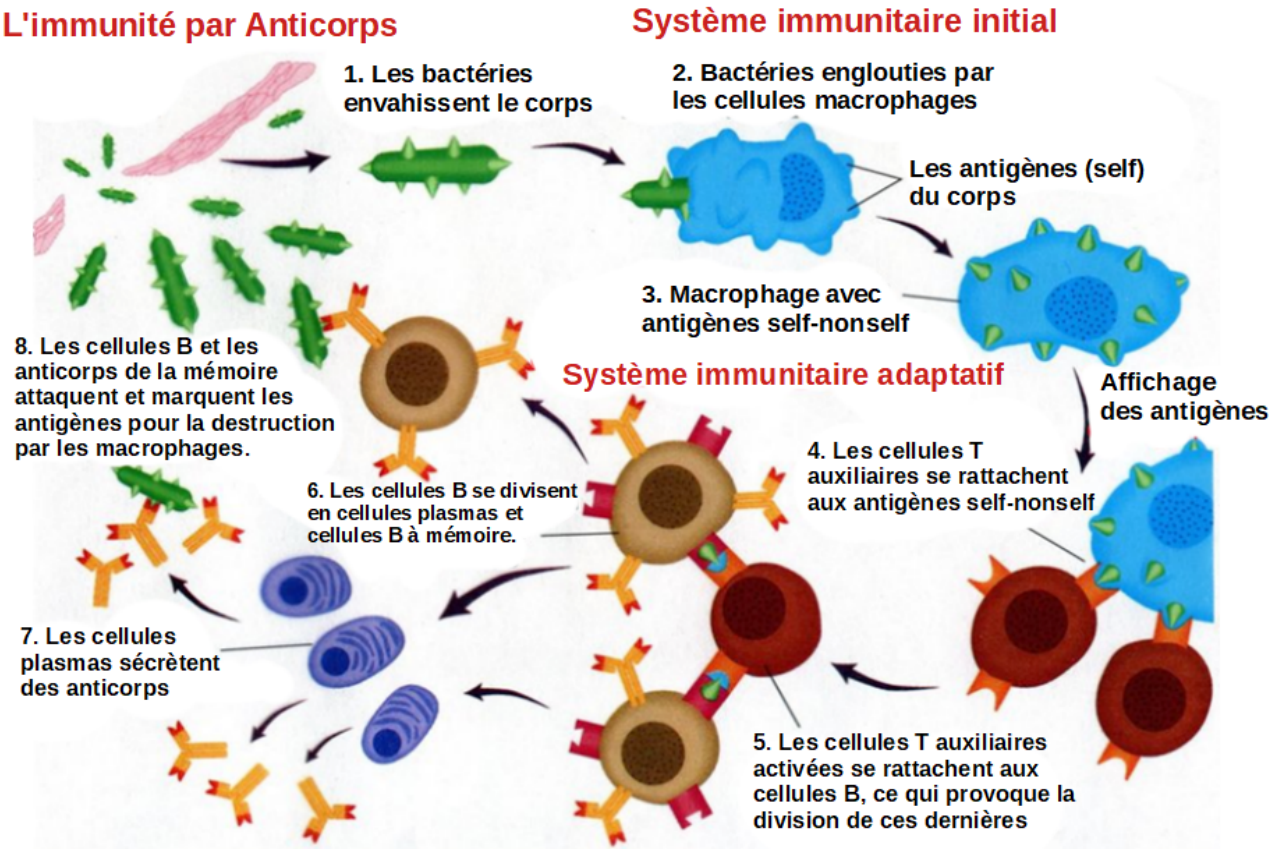

Figure 3.20: Processus du système immunitaire

- Affinité : Valeur de finesse du problème objectif correspondant à la solution.

3.2.2 Modèle anti-collision lecteur-lecteur RFID

L'efficacité de l'identification des tags par les lecteurs RFID peut être mesurée par le nombre de tags que les lecteurs sont capables d'interroger dans leurs champs d'interrogation en évitant les collisions (figure 1.20). Pour simplifier, nous formulons le problème des collisions sous la forme de l'expression mathématique suivante en termes de ressources de fréquence et de temps utilisées:

$$N_{Collision} = \sum_{r=1}^{NR} \sum_{ts=1}^{NTS} \alpha_r(ts) OR \beta_r(ts) \tag{3.8}$$

On note que,

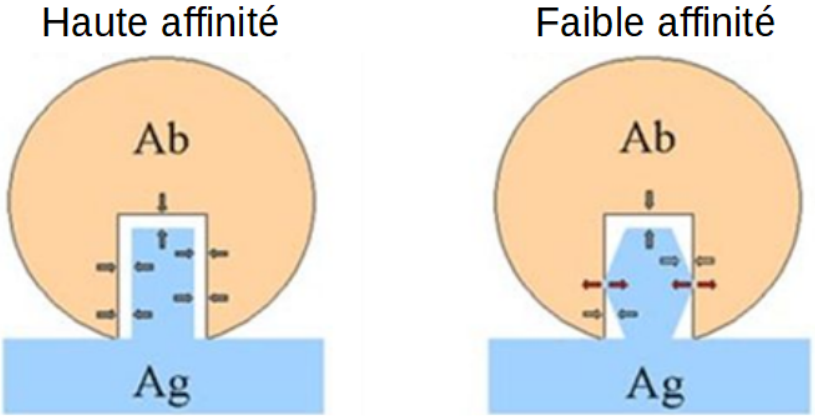

Figure 3.21: Concept d'affinité

$\alpha_j(k)$ représente le nombre de collisions RRI détectées par le lecteur j au k th Time Slot :

$$\alpha_j(k) = \begin{cases} 1 & \text{if } F_j(k) = F_m(k) \text{ and } TS_j = TS_m \\ 0 & \text{Otherwize} \end{cases} \tag{3.9}$$

$\beta_j(k)$ représente le nombre de collisions RTI détectées par le lecteur j au k th Time Slot :

$$\beta_j(k) = \begin{cases} 1 & \text{if } F_j(k) = F_i(k) \text{ or } TS_j = TS_i \\ 0 & \text{Otherwize} \end{cases} \tag{3.10}$$

Où, $F_x(k) \in NF$, $k \in NTS$, $x \in NR$, $NR = 1, 2, ..., N_{Reader}$, $NTS = 1, 2, ..., N_{TS}$ et $NF = 0, 1, 2, ..., N_{Frequency}$.

Par conséquence, compte tenu de l'ordonnancement des ressources (fréquences et Time Slots) et de la position des lecteurs, le modèle d'évitement des collisions RRI et RTI peut être présenté comme le problème d'optimisation suivant :

$$\begin{cases} minimise & \mathrm{N}_{Collision} = \sum_{r=1}^{NR} \sum_{ts=1}^{NTS} \alpha_r(ts) OR \beta_r(ts) \\ s.t. & f \in NF, ts \in NTS \text{ and } r \in NR \end{cases} \tag{3.11}$$

3.2.3 Réseau immunitaire artificiel pour l'allocation des ressources

Dans cette partie, nous allons présenter notre protocole anti-collision basé sur le réseau immunitaire artificiel pour gérer l'allocation des ressources aux lecteurs RFID (fréquence et TS) afin d'éviter les problèmes de collision RRI et RTI.

Ce protocole AIN-CA sert à décroître l'Antigène considéré ici comme le problème à minimiser représenté par l'équation 3.8. Alors que l'Anticorps représente l'ensemble des ressources (Fréquence et TS) à attribuer aux lecteurs du réseau RFID afin de minimiser le nombre de collisions (Antigène) (4). L'affinité entre l'anticorps et l'antigène est déterminée par la valeur de la fonction du problème objectif, qui est le nombre de collisions RRI et RTI détectées par les lecteurs.

Par conséquence, les opérateurs immunitaires suivants, le format des anticorps, l'affinité,

l'initialisation, le clonage, la mutation et la suppression doivent être adaptés à chaque type de déploiement de réseau RFID. Voir plus de détails ci-dessous.

3.2.3.1 Format de codage des anticorps

Une solution réalisable pour l'équation 3.8 est représentée par un anticorps Ab(t) dont le format d'encodage proposé est illustré dans la figure 3.22. Un anticorps candidat Ab(t) consiste en une chaîne de segments (nombre de segments = NReader) dont chacun correspond à un lecteur RFID du réseau. Un segment $Ab_u(i,t)$ est constitué de deux bits, le Time Slot TS(i) et la Fréquence Fi(TS(i)) à allouer au i ème lecteur au TS(i) i ème Time Slot et à la position (xi,yi). Notre système génère dynamiquement un nouvel anticorps Ab(t) à chaque nouvelle position (période) t des lecteurs du réseau. Ainsi, la longueur de l'anticorps Ab à la fin de la simulation est $N_{Reader} \times t_{max}$, où t_{max} est le nombre de périodes de simulation.

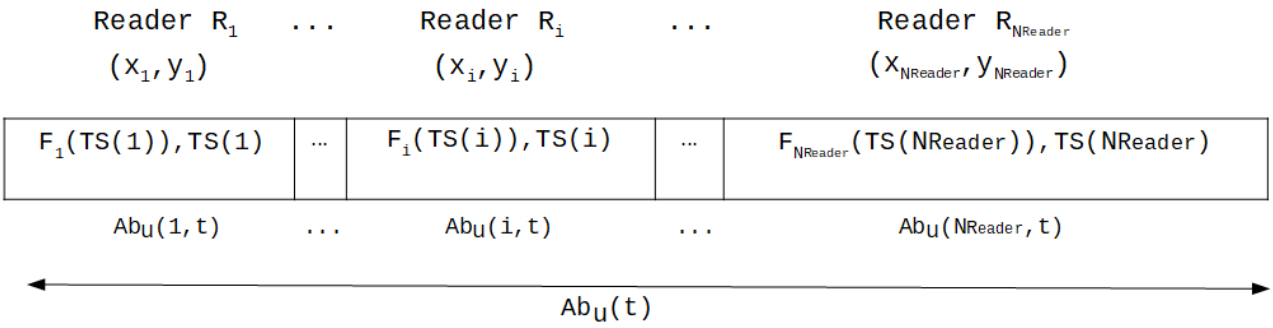

Figure 3.22: Format de codage des anticorps

3.2.3.2 Fonction d'affinité

Notre réseau immunitaire propose une fonction d'affinité pour mesurer et tester l'efficacité de l'anticorps à minimiser la fonction objective (4). Une valeur d'affinité est calculée pour chaque anticorps candidat figure 3.22. En considérant la fonction objective, nous formons la fonction d'affinité par rapport à l'anticorps Ab correspondant.

$$\begin{cases} Aff(Ab_u(t)) = \sum_{r=1}^{NR} \sum_{ts=1}^{NTS} \dfrac{1}{A.\alpha_r(ts) + B.\beta_r(ts)} \\ \text{ts} \in NTS \text{ and } r \in NR \text{ et A,B dans l'intervalle [0,1].} \end{cases} \tag{3.12}$$

Cette valeur d'affinité permettra à notre réseau immunitaire artificiel de guider l'évolution de la population d'anticorps candidats en permettant une sélection plus efficace.

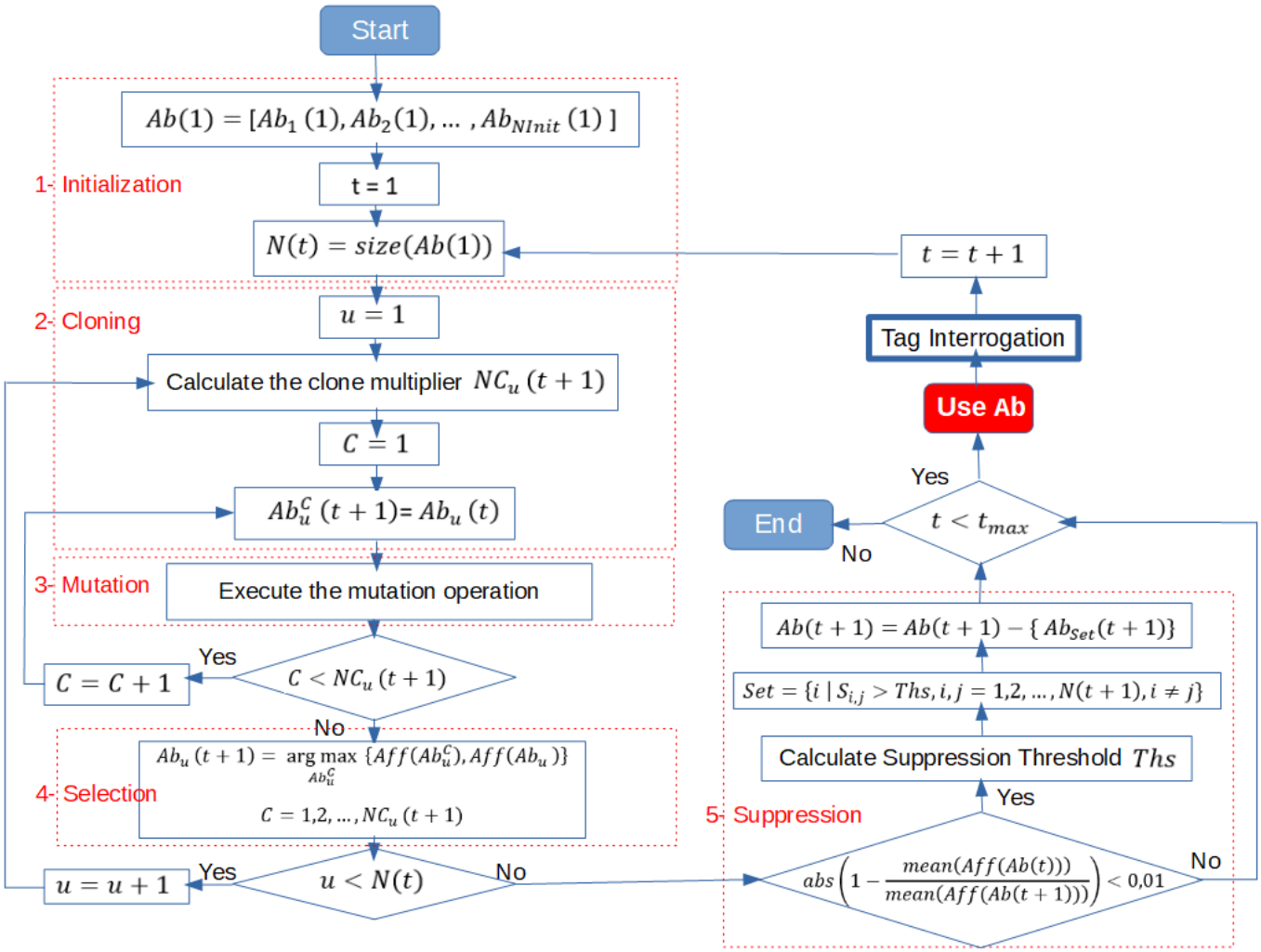

Figure 3.23: Le Réseau immunitaire artificiel proposé

3.2.3.3 *Phase d'initialisation*

Au début de chaque période de simulation ti, dans la partie Initialisation. Le réseau immunitaire génère aléatoirement Nini anticorps candidats equation 3.13 pour former une population qui peut alimenter notre algorithme figure 3.23.

$$Ab(ti) = [Ab_1(ti), Ab_2(ti), ..., Ab_{NInit}(ti)] \tag{3.13}$$

L'anticorps candidat généré doit satisfaire les conditions de l'équation 3.8 selon un premier test sur le tableau RFID. Ensuite, nous classerons les anticorps en fonction de leur affinité obtenue comme suit : les anticorps à forte affinité HAff et les anticorps à faible affinité LAff, $LAff = N - HAff$.

3.2.3.4 Phase de clonage

Après la génération de l'anticorps. Le réseau immunitaire effectue une opération de clonage à chaque anticorps parent Ab_u pour produire ces anticorps fils Ab_u^C. Le processus de reproduction des fils peut dépendre de l'affinité des parents, ce qui permettra d'avoir une nouvelle génération d'anticorps avec plus de possibilités d'évolution. Le nouvel anticorps clone continuera à l'opération d'affinité suivante en excluant le parent. Notre algorithme utilise différentes stratégies de clonage pour chaque classe d'anticorps. Dans cette étape, nous allons rediviser chaque groupe HAff et LAff en deux sous-groupes selon le type de collision dominé par chaque anticorps : HAff-RRI, HAff-RTI, LAff-RRI et LAff-RTI. Nous avons défini dynamiquement le nombre de clones en fonction du nombre de lecteurs déployés dans le réseau et de la valeur de l'affinité de l'anticorps parent comme suit :

$$\begin{cases} \mathrm{NC}_u(t+1) = min(N_{Reader} \times \alpha_j(k)) \times Aff(Ab_u(t)), NC_{max}) & \text{for } Ab_u(t) \in HAff - RRI \\ \mathrm{NC}_u(t+1) = min(N_{Reader} \times \alpha_j(k)) \times Aff(Ab_u(t)), NC_{max}) + NC_0 & \text{for } Ab_u(t) \in LAff - RRI \\ \mathrm{NC}_u(t+1) = min(N_{Reader} \times \beta_j(k)) \times Aff(Ab_u(t)), NC_{max}) & \text{for } Ab_u(t) \in HAff - RTI \\ \mathrm{NC}_u(t+1) = min(N_{Reader} \times \beta_j(k)) \times Aff(Ab_u(t)), NC_{max}) + NC_0 & \text{for } Ab_u(t) \in LAff - RTI \end{cases} \tag{3.14}$$

Où, NC_{max} est le nombre maximum de clones et NC_0 est un nombre entier qui appuie la 1ere évolution des anticorps avec une affinité inférieure.

3.2.3.5 Phase de mutation

La mutation est la partie du réseau immunitaire qui va préciser la solution du problème de collision RFID et également influencer la vitesse de convergence de notre réseau RFID. Nous utilisons le format de codage dans la figure 3.22 sur lequel nous effectuons soigneusement l'opération de mutation.

D'après l'équation d'optimisation 3.11, l'occurrence des collisions entre lecteurs dépend du TS et de la fréquence sélectionnés pour interroger les tags sur une distance spécifique. Par conséquent, un mécanisme d'allocation de ces ressources est proposé. Le format d'encodage utilisé est basé sur le segment N_{Reader} avec deux bits pour chacun d'eux afin de distribuer les ressources à chaque lecteur.

Au début de notre processus de mutation de figure 3.23, nous définissons le nombre de bits existants qui correspond au nombre de ressources supportées par un anticorps candidat. Le nombre de bits à muter dans ce processus dépendra de l'affinité de l'anticorps et chaque bit muté est mémorisé dans la liste MB. Nous commençons par sélectionner aléatoirement un bit d'anticorps bit(i,t) qui représente Fr(i,t) ou bien TS(i,t) et qui n'existe pas dans la liste MB. Ensuite, nous définissons le nombre de solutions faisables FS à proposer pour chaque bit en mutation. Le nombre de FS dans notre processus est égal au nombre de collisions RRI rencontrées par le lecteur i si l'utilisation de ce bit permet d'obtenir plus de collisions RRI que RTI. Dans le cas contraire, le nombre de FS sera égal au nombre de collisions RTI. Ensuite, le FS à chaque itération représente un bit de même nature (Fréquence ou TS) dont bit(i,t) égal à la valeur d'un autre bit différent bit(j,t) du format de codage. Enfin, on choisie aléatoirement un élément du FS pour chaque bit afin d'obtenir un bit muet bit'(i,t). La liste MB reçoit le bit(i,t) pour éviter sa remutation.

Algorithm 3 PROCEDURE Mutation_strategy()

$N_{bit} = 2 \times N_{reader}$
Déterminer le nombre de bits d'anticorp a muter
$N_{mutat} = min(N_{bit} \times Aff(Ab_u^c(i,t)), N_{bit})$
Liste de mute
$MB = []$
for $m = 1 : N_{mutat}$
Sélection aléatoire d'un anticorp $Ab_u^c(i,t)$ bit a muter
$bit(i,t) = random\{Fr(i,t)|TS(i,t)\}$
if $bit(i,t)$ not exist in MB
if $\alpha_i(k) > \beta_i(k)$ then $N = \alpha_i(k)$ else $N = \beta_i(k)$
for $n = 1 : N$
Déterminer l'ensemble des solutions réalisables
$FS(n) = C_u\{Fr(j,t)|j \in [1...N], j \neq i\}$ if $bit(i,t) = Fr(i,t)$
$FS(n) = C_u\{TS(j,t)|j \in [1...N], j \neq i\}$ if $bit(i,t) = TS(i,t)$
end
Selectionner aleatoirement un element dans FS(i) comme resultat mute bit'(i,t)
$Fr'(i,t) = random(FS(i))$ if $bit(i,t) = Fr(i,t)$
$TS'(i,t) = random(TS(i))$ if $bit(i,t) = TS(i,t)$
Ajouter le bit anticorps a la liste des bits mute
add bit(i,t) to MB
end

3.2.3.6 Phase de suppression

Pour obtenir une meilleure diversité d'anticorps Ab. Une mesure de la concentration de ces Ab est effectuée par l'opérateur de suppression. Nous utilisons l'opérateur de suppression lorsque l'affinité moyenne de la génération actuelle t+1 et l'affinité moyenne de la génération précédente t ne sont pas sensiblement différentes.

Dans ce cas, nous utiliserons une technique de suppression dynamique dont le seuil est ajusté dynamiquement et lié à la similarité des anticorps candidats pendant leur processus d'évaluation. Le seuil de suppression est calculé comme suit [1] :

$$Ths = min\{D_{ij} \mid i \neq j\} + \varphi \times (max\{D_{ij} \mid i \neq j\} - min\{D_{ij} \mid i \neq j\}) \tag{3.15}$$

Où, D_{ij} représente la distance euclidienne entre le i th et le j th Ab, et $\varphi \in (0,1)$[27].

La similarité S_{ij} utilisée dans l'algorithme (figure 3.23) est calculée en utilisant l'entropie de l'information [1].

Après cette dernière phase de notre réseau immunitaire artificiel, l'anticorps candidat résultant est prêt à être injecté dans les lecteurs RFID pour l'interrogation des tags. Dans la période suivante, après le déplacement des lecteurs dans le réseau, l'anticorps candidat précédent Ab(t+1) sera exploité pour initialiser une nouvelle génération d'anticorps candidats Ab(t+2). Cette dépendance est due à la proximité d'un lecteur dans deux positions successives par rapport à l'état du réseau.

Table 3.6: Paramètres de simulation

Paramètre	Valeur
de simulation	600m x 600m
Nombre de lecteurs (réseau sparce)	10,20,30,40,50
Nombre de lecteurs (réseau dense)	50,100,150,200
Nombre de tags	1000
Position des lecteurs et tags	Random
Type d'antenne	Omni-directional
Portée de lecture du canal de données	3 m
Portée d'interférence du canal de données	562 m
Nombre de canaux de données	2, 4, 6, 8, 10
Nombre de TS	2, 4, 6, 8, 10
Nombre de périodes	100
A, B (Paramètres d'affinité)	10-100
t_{max} (Nombre de génération)	Nombre de périodes
NC_{max} (Nombre max de clonage Ab)	1000
NC_0 (Nombre de référence de clonage Ab)	100

3.2.4 Simulations et résultats

Dans cette section, nous allons examiner les performances de notre algorithme basé sur le réseau immunitaire artificiel pour résoudre le problème de collision RFID. Une série de simulations sont réalisées sur différents scénarios en fonction des ressources fréquentielles (1,2, 4, 6, 8, 10) temporelles (1,2, 4, 6, 8, 10) utilisées et de la mobilité des lecteurs. Le réseau RFID et notre algorithme anti-collision sont réalisés sur Matlab. Ce réseau RFID est déployé sur un environnement hospitalier dont le but est d'interroger les tags injectées ou attachées au patient par les lecteurs portés par les infirmières. Les paramètres de simulation sont présentés dans le tableau 3.4. Les lecteurs (10, 20, 30, 40, 50 lecteurs) sont déployés selon différents modèles de mobilité dans un hôpital couvrant $600m \times 600m$ (figure 3.5-3.7).

Les performances de notre réseau immunitaire artificiel pour éviter les collisions avec les lecteurs sont évaluée selon plusieurs critères, la formule pour mesurer ces performances est la suivante :

Pour la capacité du système à éviter les collisions avec les lecteurs :

$$RTI_{performance} = 1 - \frac{1}{N_{period} \times N_{reader}} \sum_{p=1}^{N_{period}} \sum_{r=1}^{N_{reader}} N_{RTI_{collision}}(p, r) \tag{3.16}$$

Pour la capacité du système à éviter les collisions avec les RRI :

$$RRI_{performance} = 1 - \frac{1}{N_{period} \times N_{reader}} \sum_{p=1}^{N_{period}} \sum_{r=1}^{N_{reader}} N_{RRI_{collision}}(p, r) \tag{3.17}$$

Où $N_{Readerest}$ est le nombre de lecteurs du réseau RFID,N_{period} est le nombre de périodes de simulation, $N_{RTI_{collision}}$ est le nombre de collisions RTI et $N_{RRI_{collision}}$ est le nombre de collisions RRI.

Nous étudions d'abord la performance de notre algorithme en fonction des ressources disponibles.

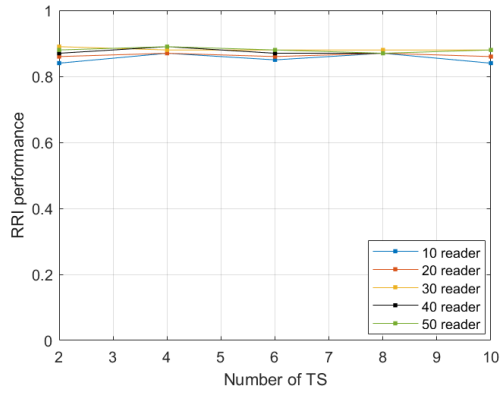

Figure 3.24: Performance RRI vs Nombre TS en fonction du nombre de lecteurs

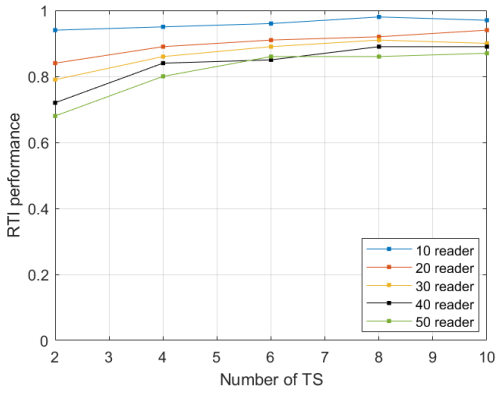

Figure 3.25: Performance RTI vs Nombre TS en fonction du nombre de lecteurs

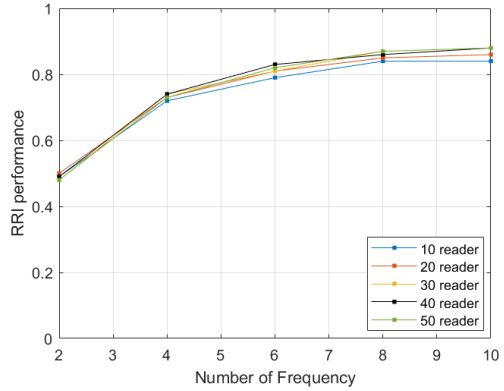

Figure 3.26: Performance RRI vs Nombre Fréquence en fonction du nombre de lecteurs

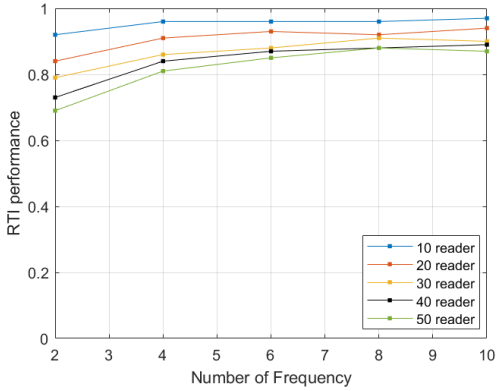

Figure 3.27: Performance RTI vs Nombre Fréquence en fonction du nombre de lecteurs

La figure 3.24 montre l'évolution des performances de RRI en fonction du nombre de Time Slots utilisés par différents déploiements des lecteurs. Que ce soit le nombre de lecteurs dans le réseau, l'évolution des performances dépasse 80% et suit une évolution quasi stable. Pour évaluer les performances de RTI, la figure 3.25 montre une évolution constante pour tous les déploiements de lecteurs. Un réseau de 10 lecteurs s'approche de 100% tout au long de son évolution tandis que les autres atteignent plus de 80% après 4 TS. Pour évaluer l'effet des ressources fréquentielles disponibles sur la performance RRI, la figure 3.26 montre une évolution croissante presque similaire pour les différents nombres de lecteurs et à partir de 6 fréquences, les lecteurs dépassent 80% de la performance RRI. La figure 3.27 concernant les performances de RTI en fonction du nombre de fréquences suit une évolution proche de celle de la figure 3.25 en ce qui concerne le TS. En étudiant ces 4 figures, on peut noter les points suivants :

- Les performances RRI ne dépend pas du nombre de TS disponibles.

- Les performances RTI suivent presque la même évolution croissante que ce soit en fonction des fréquences ou des TS.

- Quel que soit le nombre de lecteurs déployés, les performances RRI suivent une évolution similaire.

Dans cette partie nous allons étudier l'évolution des performances de notre algorithme en fonction du nombre de lecteurs déployés et des ressources disponibles pour les différents modèles de mobilité. Les figures 3.28 et 3.29 représentent les performances en fonction des TS utilisés. La performance RRI de la figure 3.28 se stabilise à 89% avec une petite différence sur 8 TS pour tous les modèles de mobilité. Alors que la performance RTI dans la figure 3.29 suit une évolution croissante, en particulier pour le modèle free moins dense qui peut atteindre 93% de la performance en utilisant 10 TS, tandis que les modèles semi-free et directed dépassent 80% en utilisant 4 et 8 TS successivement. Les figures 3.30 et 3.31 montrent les performances en fonction des fréquences disponibles. Les différentes performances RRI évoluent de manière croissante dans la figure 3.30. Les modèles free et semi-free de mobilités sont similaires, dépassant de 88% le modèle à mobilité directed. La performance RTI en fonction de la fréquence dans la figure 3.31 suit la même évolution que la figure 3.29 en fonction du TS à l'exception du modèle à mobilité directed qui augmente constamment autour de 82%. Les deux autres figures 3.32 et 3.33 évaluent les performances en fonction du nombre de lecteurs déployés en utilisant 10 Fréquence et TS. Comme vous pouvez le constater sur la figure 3.32, les différentes performances RRI suivent une évolution croissante similaire pour les différents modèles de déploiement, atteignant 87%. La figure 3.33 montre un développement croissant de la performance RTI pour tous les modèles de mobilité. Le modèle free atteint 93% des performances RTI à 50 lecteurs tandis que les deux autres modèles atteignent plus de 80%.

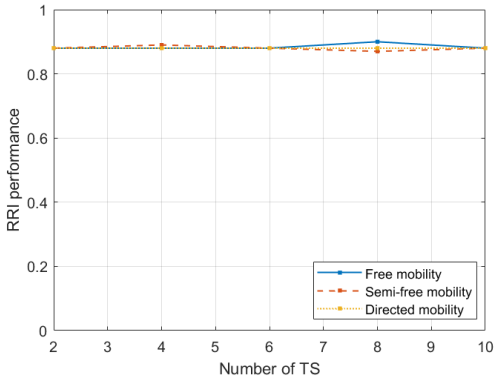

Figure 3.28: Performance RRI vs nombre TS selon le modèle de mobilité

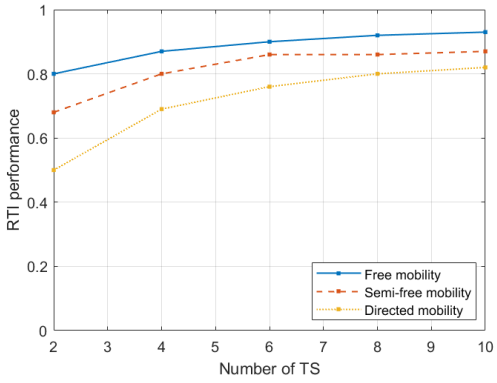

Figure 3.29: Performance RTI vs nombre TS selon le modèle de mobilité

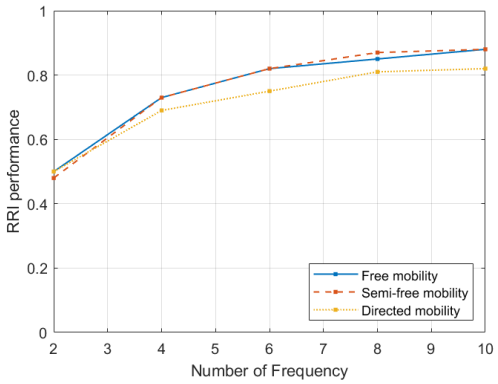

Figure 3.30: Performance RRI vs nombre Frequence selon le modèle de mobilité

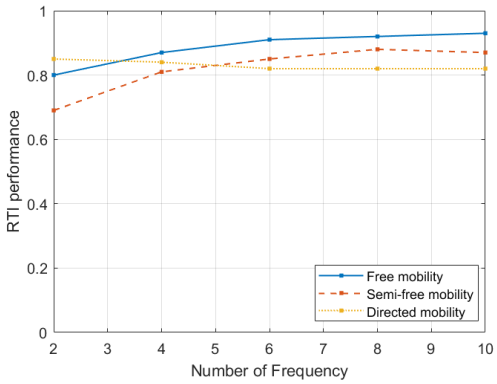

Figure 3.31: Performance RTI vs nombre Frequence selon le modèle de mobilité

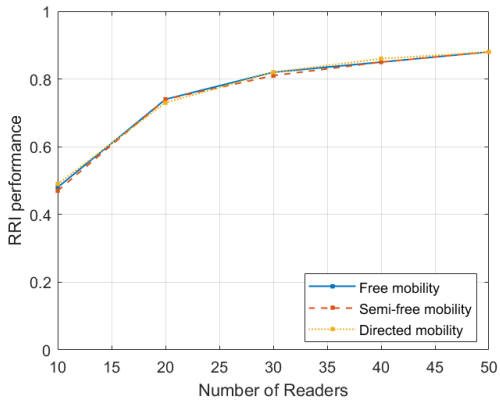

Figure 3.32: Performance RRI vs nombre Lecteur selon le modèle de mobilité

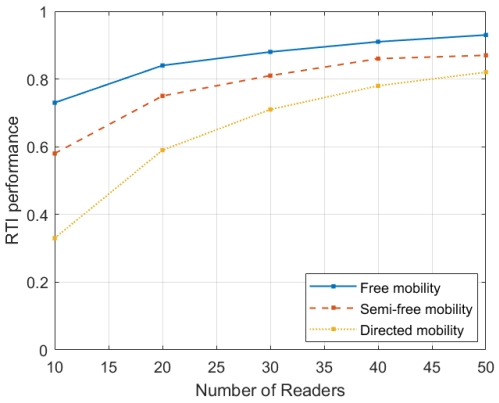

Figure 3.33: Performance RTI vs nombre Lecteur selon le modèle de mobilité

Finalement, nous étudions la différence entre les performances RRI et RTI en fonction du nombre de lecteurs pour les différents modèles de mobilité. La figure 3.34 montre que la performance RTI est supérieure à la performance RRI dans le modèle de mobilité free. De même, sur la figure 3.35, la performance RTI est supérieure à la performance RRI pour le modèle de mobilité semi-free avant de se croiser et la performance RRI devient la plus élevée. Contrairement à la figure 3.34, la performance RRI est supérieure à la performance RTI pour le modèle de mobilité directed dans la figure 3.36. Enfin, les performances sont évaluées pour un réseau dense de lecteurs (figure 3.37) pour le modèle de mobilité semi-free. Les performances de RRI sont supérieures à celles de RTI jusqu'à ce que nous atteignions le point de croisement de 200 lecteurs où les performances de RTI dépassent ensuite celles de RRI.

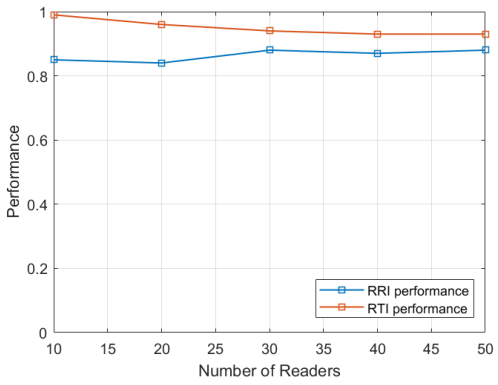

Figure 3.34: Performance vs nombre Lecteur pour le modèle de mobilité free

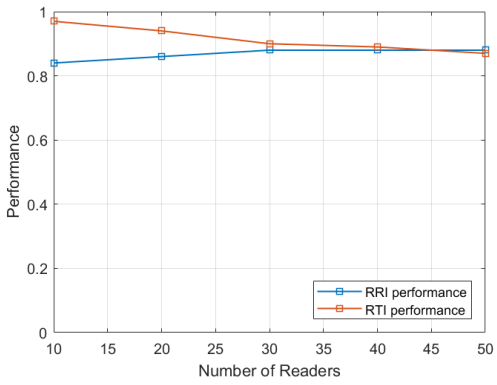

Figure 3.35: Performance vs nombre Lecteur pour le modèle de mobilité semi-free

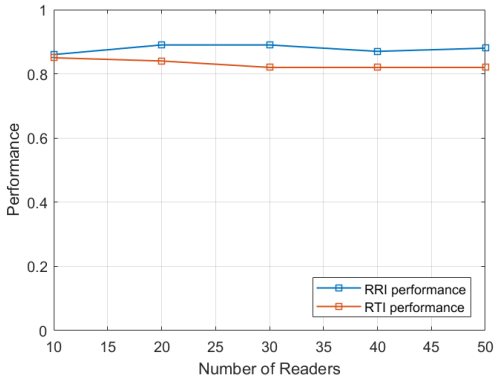

Figure 3.36: Performance vs nombre Lecteur pour le modèle de mobilité directed

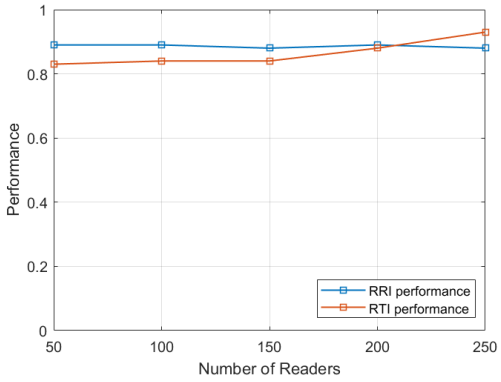

Figure 3.37: Performance RTI vs nbr lecteur (50,100,150,200) pour le modèle de mobilité semi-free

3.2.5 Conclusion

Dans cet partie, nous avons proposé un protocole basé sur le réseau immune artificiel dont le principe est de générer une population d'anticorps à chaque période de simulation. Cet anticorps constitue la ressource fréquentielle et temporelle à utiliser par chaque lecteur du réseau RFID. Notre algorithme utilise une stratégie de mutation basée sur le nombre de collisions RRI et RTI détectées par les lecteurs déployés à chaque période. Cela permet aux lecteurs d'obtenir les ressources les plus adéquates à leur situation. Notre réseau immunitaire artificiel génère une nouvelle génération d'anticorps basée sur l'état de déploiement précédent des lecteurs, ce qui permet d'obtenir de meilleurs résultats de performance face aux collisions RRI et RTI.

.

Conclusion Général et Perspectives

Dans cette thèse, nous avons abordé le défi de collision relatif à l'intégration des systèmes RFID et RCSF dans un contexte d'Internet des objets. De nos jours, la RFID présente un intérêt important en raison du nombre d'applications utilisées dans ce domaine. Les systèmes RFID fournissent des mécanismes d'identification et de suivi des objets à faible coût et à faible consommation. C'est la condition essentielle pour différentes applications ultra-denses, par exemple la logistique, la santé et les villes intelligentes. Dans ces applications, un nombre important des lecteur et tags sont nécessaires, pour une identification plus efficace. Par conséquent, l'identification souffre du problème de collision. L'objectif principal de cette thèse est d'augmenter le taux de lecture des tags dans le champ du lecteur en minimisant le nombre de collisions. La communication des lecteurs est planifiée au niveau de la couche MAC au moyen de nos différents protocoles anti-collision: FTSMAC, FTSMAC-E, DMLAR et AIN-CA.

Tout d'abord, dans le premier chapitre, nous avons discuté les motivations principales et présenté le contexte de cette thèse. Nous avons également introduit les principales caractéristiques des systèmes d'identification par Radio Fréquence RFID. L'intégration des deux techniques prometteuses de la technologie RFID et du RCSF permettra de renforcer leur efficacité, de générer de nouvelles possibilités pour un ensemble important d'applications. La technologie combinée aura une fonctionnalité étendue et réduira les coûts inutiles. Dans un tel réseau RFID-RCSF, une forte densité de lecteurs peut affecter les performances du système à cause des multiples collisions possibles. En effet, le système risque de subir une baisse au niveau de collection des données, une prolongation du temps de transmission et une forte consommation d'énergie. Les collisions constituent par conséquent un problème essentiel qui réduit de manière significative les performances des systèmes RFID. Pour assurer la synchronisation des lecteurs afin d'éviter les collisions, une certaine méthodes de communication est nécessaire entre les lecteurs ou avec une entité centrale pour la gestion des ressources fréquentiel et temporel.

Au début, nous avons aborde le problème de collision RFID et l'état de l'art des différents protocoles anti-collision de la couche MAC de la littérature. Nous avons classifie les algorithmes en centralise et distribue. Les algorithmes centralisés dont les lecteurs communiquent avec un serveur central chargé de gérer les ressources des lecteurs. Pour les algorithmes distribués, les lecteurs peuvent communiquer entre eux de manière directe et en se coordonnant sur leur modèle de gestion des ressources, afin de réduire les collisions. Enfin, pour les algorithmes basés sur l'apprentissage automatique, les lecteurs prédisent leur fréquence et leurs ressources temporelles à l'aide des modèles d'apprentissage générés.

Nous avons proposé un nouveau protocole anti-collision FTSMAC et son extension FTSMAC-E pour la gestion des ressources entre les lecteurs de manière distribuée. Le protocole hybride FTSMAC est une solution basée sur les méthodes de gestion d'accès au canal CSMA, TDMA et FDMA. Cette stratégie utilise, pour éliminer les collisions entre lecteurs, un processus de notification par lequel les lecteurs peuvent en respectant certains critères de déterminer leurs

voisins. Le principe repose sur la réutilisation des TS et fréquence par les lecteurs voisins, permettant une gestion efficace des ressources. Dans le but de renforcer les capacités et de mettre en place un mécanisme fiable et efficace du protocole FTSMAC, une approche de distribution des ressources temporelles TDMA est proposée FTSMAC-E pour résoudre les problèmes de collision RTI. Nous avons conservé la partie concernant la gestion des fréquences du protocole FTSMAC (FDMA) pour minimiser les collisions RRI.

Après nous avons présenter nos méthodes basées sur l'apprentissage machine DMLAR et AIN-CA. Nous avons mis en évidence pour la première fois un modèle ANN d'apprentissage pour chaque lecteur du réseau RFID. Notre algorithme DMLAR poursuit le principe suivant : Les données de prédiction sont créées, collectées et diffusées par les lecteurs RFID pour les intégrer aux réseaux neuronaux artificiels ANNs. Les lecteurs communiquent les modèles d'apprentissage entre eux afin de déterminer le modele le plus performant. AIN-CA présente notre protocole anti-collision basé sur le réseau immunitaire artificiel permettant de contrôler la répartition des ressources entre les lecteurs RFID (fréquence et TS) pour éviter les collisions RRI et RTI. Ce protocole AIN-CA est utilisé pour diminuer l'Antigène qui représente ici le problème à minimiser. L'Anticorps correspond à une série de ressources (Fréquence et TS) à allouer aux lecteurs RFID pour réduire le nombre de collisions (Antigène). L'affinité est déterminée par le nombre de collisions RRI et RTI détectées par les lecteurs.

Chaque chapitre comporte un certain nombre de contributions, qui constituent différentes perspectives de travaux futurs pouvant dériver de cette thèse.

Contribution 2 : L'objectif des travaux futurs est de s'assurer que la solution est complète et robuste. Par conséquent, nous adapterons cette méthode FTSMAC-E afin d'améliorer les performances du schéma FTDMA_Scheme en utilisant un algorithme qui permet une distribution efficace des ressources dans le but d'activer le maximum de lecteurs dans le cas de réseaux RFID denses.

Contribution 3 : Dans les travaux futurs, nous essayerons d'améliorer les performances de ce système d'apprentissage pour les réseaux RFID à haute densité. Pour ce faire, nous optimiserons notre système de notification distribué pour prendre en charge le grand nombre de datasets fournis par les lecteurs. En outre, nous utiliserons la contrainte de temps comme élément d'entrée du modèle ANN pour contrôler le mouvement temporaire des lecteurs. Dans la phase de mise en uvre de notre algorithme, nous intégrerons un réseau immunitaire artificiel pour le processus d'allocation des ressources après la prédiction des collisions par ANN.

Contribution 4 : Au cours de prochains travaux, nous allons nous concentrer sur l'augmentation de l'efficacité de ce système immunitaire pour sélectionner les ressources appropriées afin d'éviter les collisions. À cette fin, nous adapterons un modèle de réseau neuronal artificiel pour prédire les ressources pour la "phase de mutation " de cet algorithme.

APPENDIX

A

ANNEXE

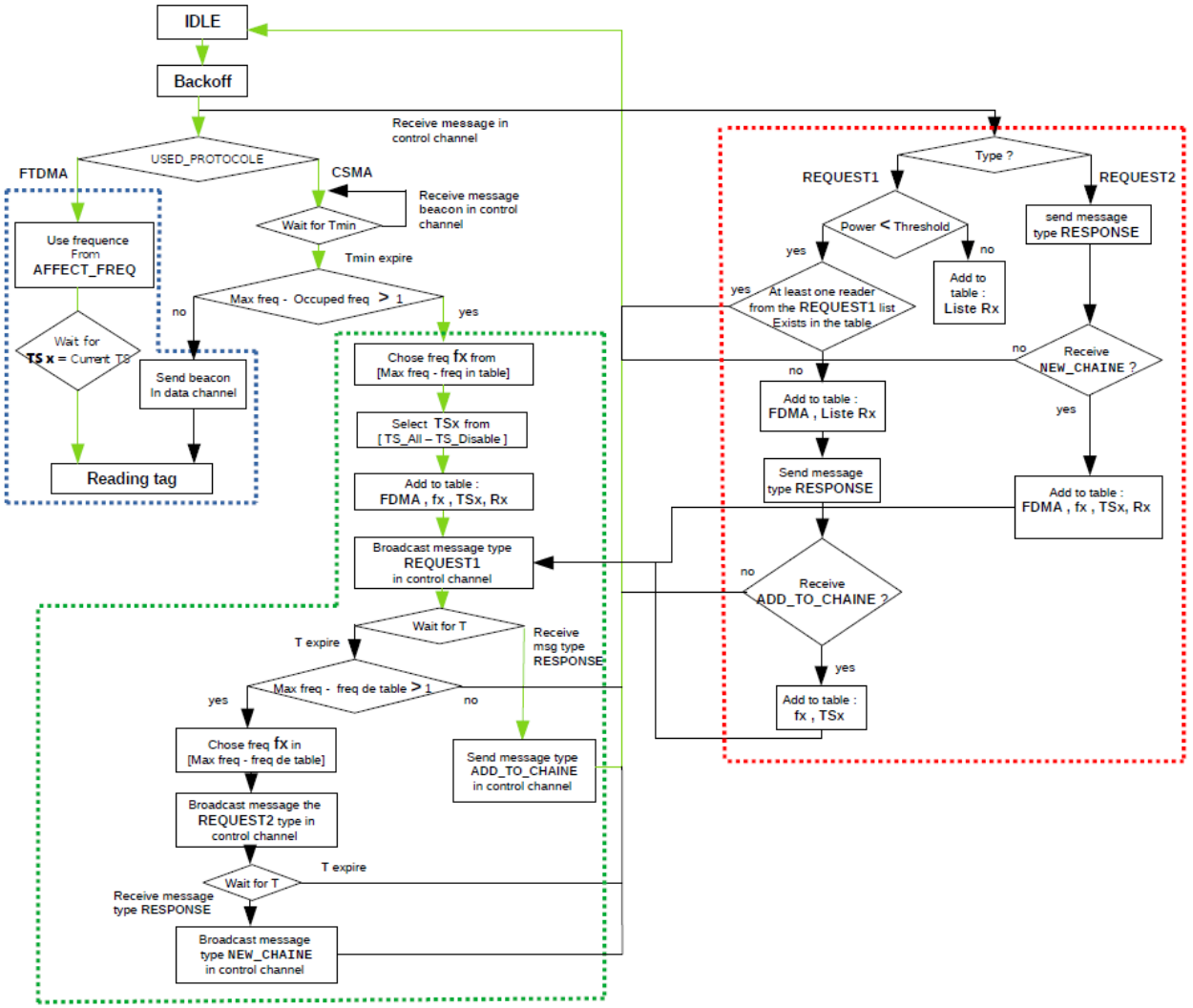

Figure A.1: Processus R1

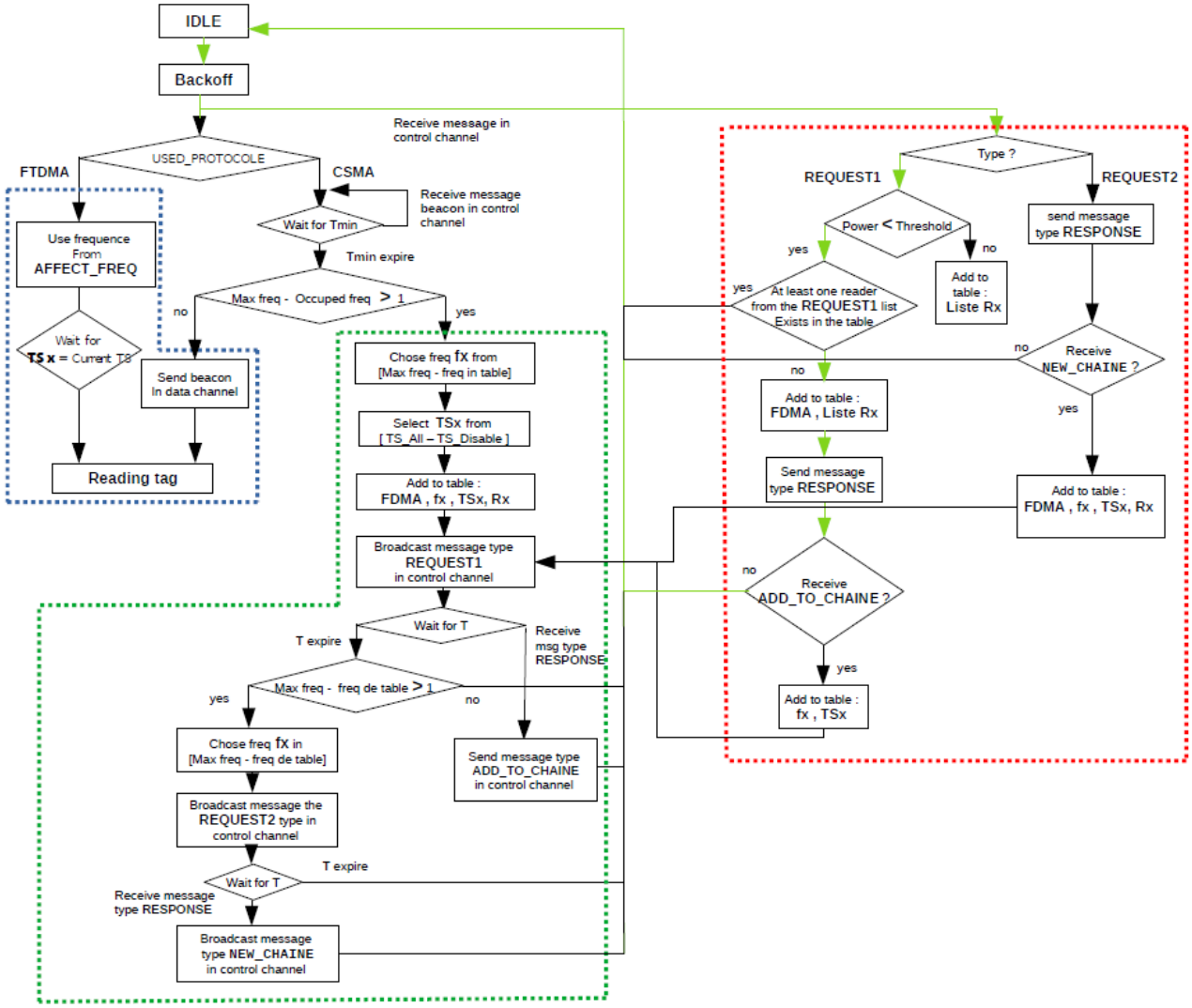

Figure A.2: Processus R2

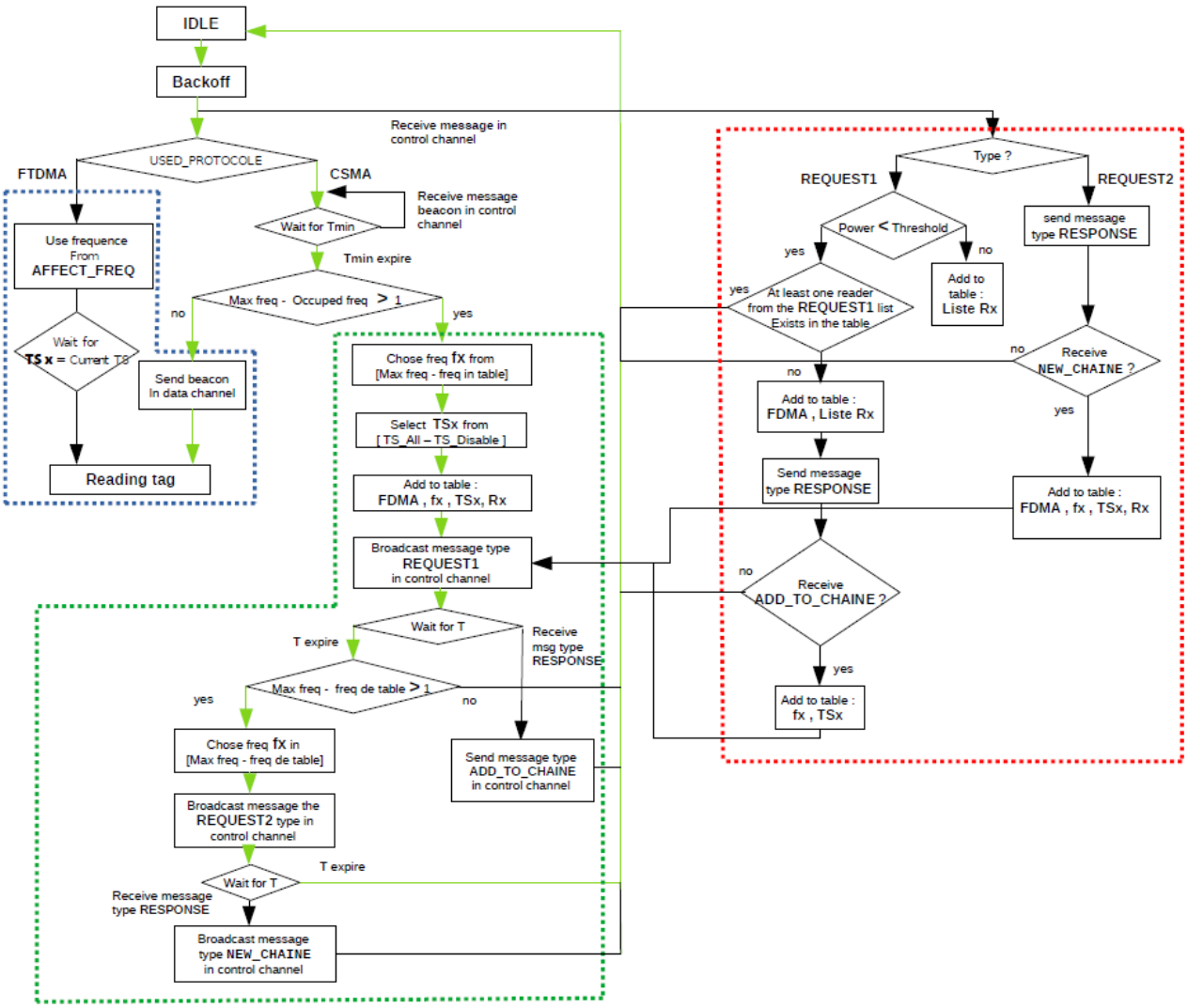

Figure A.3: Processus R3

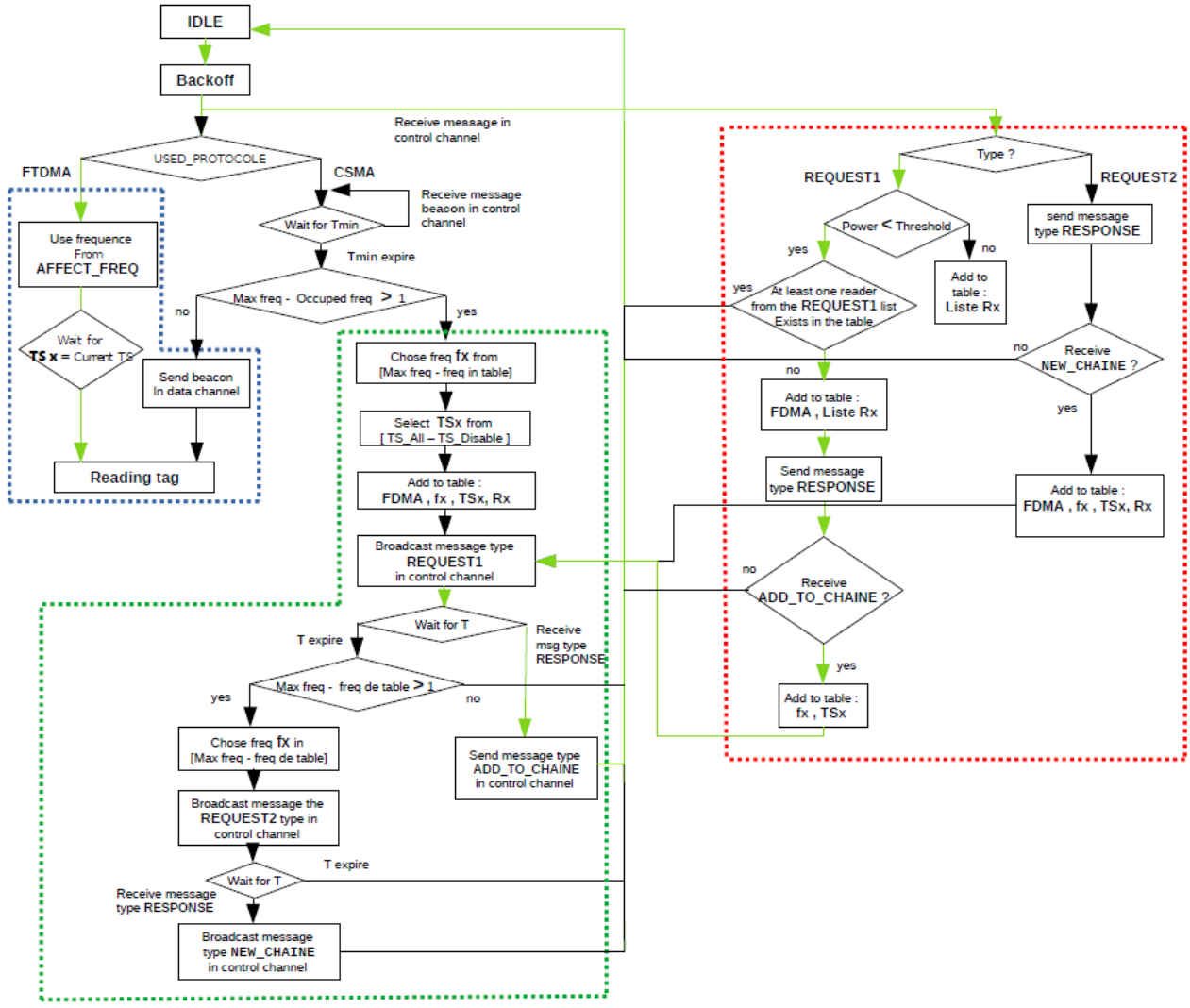

Figure A.4: Processus R10

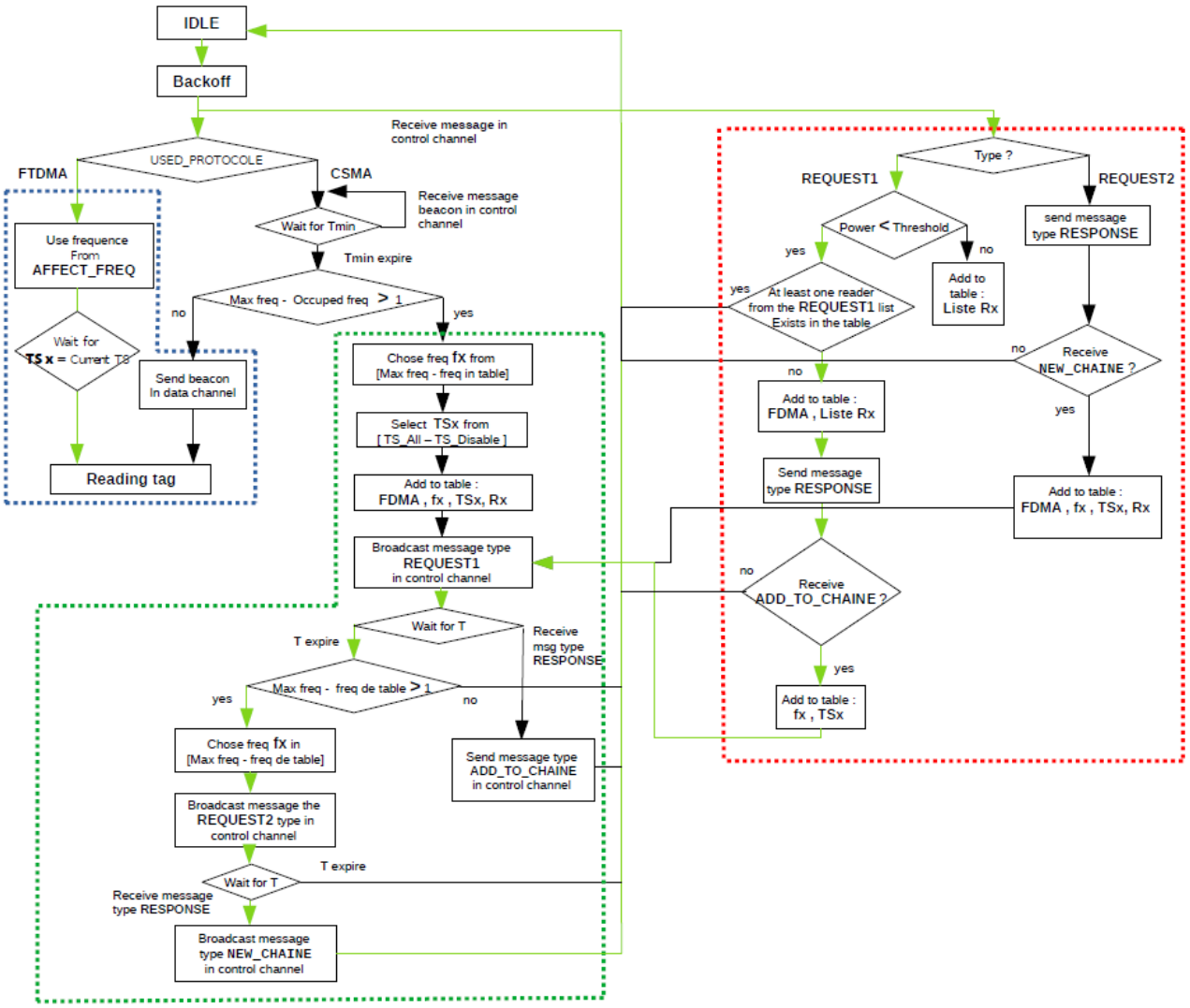

Figure A.5: Processus R8

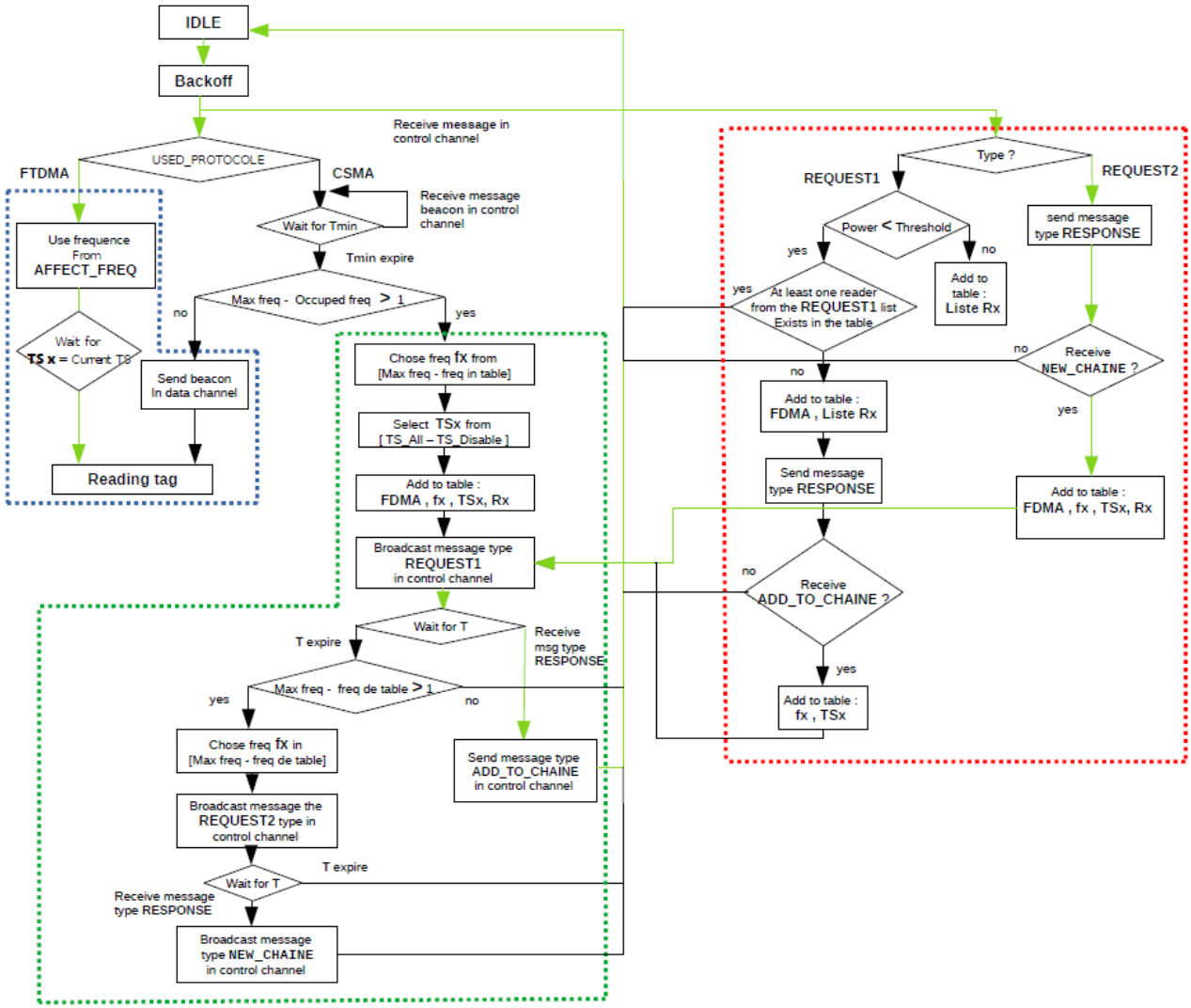

Figure A.6: Processus R13

BIBLIOGRAPHIE

https://www.ruddersoft.com/solution-apps/rfid-based-file-tracking-system.

https://www.nxp.com.cn/company/blog/traffic-congestion-addressing-one-of-the-biggest-smart-city-challenges-with-secure-rfid-technology:bl-smart-city-challenges-secure-rfid.

https://www.mecalux.fr/blog/supply-chain-manager.

https://www.smarttracksl.com/rfid-farm-management-animal-tracking/.

https://synergie.com.br/2021/03/29/gestao-hospitalar-4-0/.

https://www.yourfid.top/rfid-technology-applications-for-sports-events/.

A. Z. Abbasi, N. Islam, Z. A. Shaikh, et al. A review of wireless sensors and networks' applications in agriculture. *Computer Standards & Interfaces*, 36(2):263–270, 2014.

A. Abbasian and M. Safkhani. Cncaa: A new anti-collision algorithm using both collided and non-collided parts of information. *Computer Networks*, 172:107159, 2020.

A. Abuelkhail, U. Baroudi, M. Raad, and T. Sheltami. Internet of things for healthcare monitoring applications based on rfid clustering scheme. *Wireless Networks*, 27(1):747–763, 2021.

F. Adachi, D. Garg, S. Takaoka, and K. Takeda. Broadband cdma techniques. *IEEE Wireless communications*, 12(2):8–18, 2005.

T. Adame, A. Bel, A. Carreras, J. Melia-Segui, M. Oliver, and R. Pous. Cuidats: An rfid–wsn hybrid monitoring system for smart health care environments. *Future Generation Computer Systems*, 78:602–615, 2018.

S. A. Ahson and M. Ilyas. *RFID handbook: applications, technology, security, and privacy*. CRC press, 2017.

K. Akkaya and M. Younis. A survey on routing protocols for wireless sensor networks. *Ad hoc networks*, 3(3):325–349, 2005.

S. Al Ajrawi, H. Bialek, M. Sarkar, R. Rao, and S. H. Ahmed. Bi-directional channel modeling for implantable uhf–rfid transceivers in brain–computer interface applications. *Future Generation Computer Systems*, 88:683–692, 2018.

G. Alfian, J. Rhee, H. Ahn, J. Lee, U. Farooq, M. F. Ijaz, and M. A. Syaekhoni. Integration of rfid, wireless sensor networks, and data mining in an e-pedigree food traceability system. *Journal of Food Engineering*, 212:65–75, 2017.

I. Alrashdi, A. Alqazzaz, E. Aloufi, R. Alharthi, M. Zohdy, and H. Ming. Ad-iot: Anomaly detection of iot cyberattacks in smart city using machine learning. In *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, pages 0305–0310. IEEE, 2019.

I. Amadou and N. Mitton. High adaptive mac protocol for dense rfid reader-to-reader networks. In *International Conference on Ad Hoc Networks*, pages 82–93. Springer, 2015.

G. Anastasi, M. Conti, M. Di Francesco, and A. Passarella. Energy conservation in wireless sensor networks: A survey. *Ad hoc networks*, 7(3):537–568, 2009.

A. Atali, H. L. Lee, and Ö. Özer. If the inventory manager knew: Value of visibility and rfid under imperfect inventory information. *Available at SSRN 1351606*, 2009.

L. Atzori, A. Iera, and G. Morabito. The internet of things: A survey. *Computer networks*, 54 (15):2787–2805, 2010.

B. Bacheldor. Oil refineries to test sensor tags. *RFID Journal*, 2007.

C. Badii, P. Bellini, A. Difino, and P. Nesi. Sii-mobility: An iot/ioe architecture to enhance smart city mobility and transportation services. *Sensors*, 19(1):1, 2019.

C. Badii, P. Bellini, A. Difino, and P. Nesi. Smart city iot platform respecting gdpr privacy and security aspects. *IEEE Access*, 8:23601–23623, 2020.

J. Bartman, Z. Gomółka, and B. Twaróg. Ann training–the analysis of the selected procedures in matlab environment. *Computing in science and technology*, pages 88–101, 2015.

P. J. Basford, F. M. Bulot, M. Apetroaie-Cristea, S. J. Cox, and S. J. Ossont. Lorawan for smart city iot deployments: A long term evaluation. *Sensors*, 20(3):648, 2020.

M. Bathula, M. Ramezanali, I. Pradhan, N. Patel, J. Gotschall, and N. Sridhar. A sensor network system for measuring traffic in short-term construction work zones. In *International Conference on Distributed Computing in Sensor Systems*, pages 216–230. Springer, 2009.

S. M. Birari and S. Iyer. Pulse: a mac protocol for rfid networks. In *International Conference on Embedded and Ubiquitous Computing*, pages 1036–1046. Springer, 2005.

D. N. Borisov and S. A. Zuev. Modeling microstrip antennas for uhf rfid tags. In *2017 XI International Conference on Antenna Theory and Techniques (ICATT)*, pages 261–263. IEEE, 2017.

I. Bouhassoune, R. Saadane, and A. Chehri. Wireless body area network based on rfid system for healthcare monitoring: progress and architectures. In *2019 15th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS)*, pages 416–421. IEEE, 2019.

M. V. Bueno-Delgado, R. Ferrero, F. Gandino, P. Pavon-Marino, and M. Rebaudengo. A geometric distribution reader anti-collision protocol for rfid dense reader environments. *IEEE Transactions on Automation Science and Engineering*, 10(2):296–306, 2012.

B. Burton and D. A. Willis. Gartner?s hype cycle special report for 2014. *Gartner, Inc., Tech. Rep.*, 2014.

L. B. Campos and C. E. Cugnasca. Applications of rfid and wsns technologies to internet of things. In *2014 IEEE Brasil RFID*, pages 19–21. IEEE, 2014.

B. Cao, Y. Gu, Z. Lv, S. Yang, J. Zhao, and Y. Li. Rfid reader anticollision based on distributed parallel particle swarm optimization. *IEEE Internet of Things Journal*, 8(5):3099–3107, 2020.

W. Charles. Portable radio frequency emitting identifier, us, 1973.

Y. Cheung, K. Choy, C. Lau, and Y. Leung. The impact of rfid technology on the formulation of logistics strategy. In *PICMET'08-2008 Portland International Conference on Management of Engineering & Technology*, pages 1673–1680. IEEE, 2008.

J. Cho, Y. Shim, T. Kwon, Y. Choi, S. Pack, and S. Kim. Sarif: A novel framework for integrating wireless sensor and rfid networks. *IEEE Wireless Communications*, 14(6):50–56, 2007.

P.-J. Chuang and W.-T. Tsai. Switchtable: An efficient anti-collision algorithm for rfid networks. *Iet Communications*, 11(14):2221–2227, 2017.

F. Cirillo, D. Gómez, L. Diez, I. E. Maestro, T. B. J. Gilbert, and R. Akhavan. Smart city iot services creation through large-scale collaboration. *IEEE Internet of Things Journal*, 7(6): 5267–5275, 2020.

J. Collins. Bp tests rfid sensor network at uk plant. *RFID Journal*, 2006.

R. Deng, S. He, P. Cheng, and Y. Sun. Towards balanced energy charging and transmission collision in wireless rechargeable sensor networks. *Journal of Communications and Networks*, 19(4):341–350, 2017.

W. Deng, Z. Li, Y. Xia, K. Wang, and W. Pei. A widely linear mmse anti-collision method for multi-antenna rfid readers. *IEEE Communications Letters*, 23(4):644–647, 2019.

W. Ding. Minimizing wsn energy and cost by embedding rfid tags. In *2013 IEEE Global High Tech Congress on Electronics*, pages 50–55. IEEE, 2013.

V. Dyo, S. A. Ellwood, D. W. Macdonald, A. Markham, N. Trigoni, R. Wohlers, C. Mascolo, B. Pásztor, S. Scellato, and K. Yousef. Wildsensing: Design and deployment of a sustainable sensor network for wildlife monitoring. *ACM Transactions on Sensor Networks (TOSN)*, 8(4): 1–33, 2012.

M. El Soussi, P. Zand, F. Pasveer, and G. Dolmans. Evaluating the performance of emtc and nb-iot for smart city applications. In *2018 ieee international conference on communications (icc)*, pages 1–7. IEEE, 2018.

C. Englund and H. Wallin. *RFID in wireless sensor network*. PhD thesis, Citeseer, 2004.

J.-B. Eom, S.-B. Yim, and T.-J. Lee. An efficient reader anticollision algorithm in dense rfid networks with mobile rfid readers. *IEEE Transactions on industrial electronics*, 56(7):2326–2336, 2009.

S. C. Ergen and P. Varaiya. Tdma scheduling algorithms for wireless sensor networks. *Wireless networks*, 16(4):985–997, 2010.

R. Ferrero. Evaluation of throughput of tdma anti-collision protocols in static and mobile rfid networks. In *2019 4th International Conference on Smart and Sustainable Technologies (SpliTech)*, pages 1–7. IEEE, 2019.

R. Ferrero, F. Gandino, B. Montrucchio, and M. Rebaudengo. A fair and high throughput reader-to-reader anticollision protocol in dense rfid networks. *IEEE Transactions on Industrial Informatics*, 8(3):697–706, 2011.

K. Finkenzeller. *RFID handbook: fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication*. John wiley & sons, 2010.

F. Gandino, R. Ferrero, B. Montrucchio, and M. Rebaudengo. Dcns: An adaptable high throughput rfid reader-to-reader anticollision protocol. *IEEE Transactions on Parallel and Distributed Systems*, 24(5):893–905, 2012.

D. Giusto, A. Iera, G. Morabito, and L. Atzori. *The internet of things: 20th Tyrrhenian workshop on digital communications*. Springer Science & Business Media, 2010.

O. Gnawali, R. Fonseca, K. Jamieson, D. Moss, and P. Levis. Collection tree protocol. In *Proceedings of the 7th ACM conference on embedded networked sensor systems*, pages 1–14, 2009.

M. Golsorkhtabaramiri and N. Issazadehkojidi. A distance based rfid reader collision avoidance protocol for dense reader environments. *Wireless Personal Communications*, 95(2):1781–1798, 2017.

M. Golsorkhtabaramiri, M. Hosseinzadeh, M. Reshadi, and A. M. Rahmani. A reader anti-collision protocol for rfid-enhanced wireless sensor networks. *Wireless Personal Communications*, 81(2):893–905, 2015.

M. Golsorkhtabaramiri, N. Issazadehkojidi, N. Pouresfehani, M. Mohammadialamoti, and S. M. Hosseinzadehsadati. Comparison of energy consumption for reader anti-collision protocols in dense rfid networks. *Wireless Networks*, 25(5):2393–2406, 2019.

C. Gomez and J. Paradells. Wireless home automation networks: A survey of architectures and technologies. *IEEE Communications Magazine*, 48(6):92–101, 2010.

J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami. Internet of things (iot): A vision, architectural elements, and future directions. *Future generation computer systems*, 29(7):1645–1660, 2013.

S. A. Hamid, W. Ismail, C. Z. Zulkifli, and S. Abdullah. Dual band rfid-based blood glucose monitoring system in wireless sensor network platform. *Wireless Personal Communications*, 103(3):2229–2244, 2018.

D. B. Harris. Radio transmission systems with modulatable passive responder, Mar. 1 1960. US Patent 2,927,321.

R. J. Hassan, S. R. Zeebaree, S. Y. Ameen, S. F. Kak, M. A. Sadeeq, Z. S. Ageed, A.-Z. Adel, and A. A. Salih. State of art survey for iot effects on smart city technology: challenges, opportunities, and solutions. *Asian Journal of Research in Computer Science*, pages 32–48, 2021.

Y. T. Hou, Y. Shi, and H. D. Sherali. Rate allocation and network lifetime problems for wireless sensor networks. *IEEE/ACM Transactions on networking*, 16(2):321–334, 2008.

K.-i. Hwang, K.-t. Kim, and D.-s. Eom. Dica: Distributed tag access with collision-avoidance among mobile rfid readers. In *International Conference on Embedded and Ubiquitous Computing*, pages 413–422. Springer, 2006.

W. Ji, L. Li, and W. Zhou. Design and implementation of a rfid reader/router in rfid-wsn hybrid system. *Future Internet*, 10(11):106, 2018.

X. Jia, Q. Feng, T. Fan, and Q. Lei. Rfid technology and its applications in internet of things (iot). In *2012 2nd international conference on consumer electronics, communications and networks (CECNet)*, pages 1282–1285. IEEE, 2012.

L. Jiang and J. Walrand. A distributed csma algorithm for throughput and utility maximization in wireless networks. *IEEE/ACM Transactions on Networking*, 18(3):960–972, 2009.

W. Jiang. An intelligent supply chain information collaboration model based on internet of things and big data. *IEEE Access*, 7:58324–58335, 2019.

Y. Jiang, R. Zhang, W. Cheng, and W. Sun. An efficient multi-channel reader collision avoidance protocol in rfid systems. In *2016 IEEE Wireless Communications and Networking Conference*, pages 1–6. IEEE, 2016.

C. Joe-Wong, S. Sen, T. Lan, and M. Chiang. Multiresource allocation: Fairness–efficiency tradeoffs in a unifying framework. *IEEE/ACM Transactions on Networking*, 21(6):1785–1798, 2013.

A. Juels. Rfid security and privacy: A research survey. *IEEE journal on selected areas in communications*, 24(2):381–394, 2006.

P. M. S. Jyothi and D. Nandan. Utilization of the internet of things in agriculture: Possibilities and challenges. In *Soft Computing: Theories and Applications*, pages 837–848. Springer, 2020.

M. N. Kamel Boulos and G. Berry. Real-time locating systems (rtls) in healthcare: a condensed primer. *International journal of health geographics*, 11(1):1–8, 2012.

G. Karatas and O. K. Sahingoz. Neural network based intrusion detection systems with different training functions. In *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, pages 1–6. IEEE, 2018.

H. A. Khattak, H. Farman, B. Jan, and I. U. Din. Toward integrating vehicular clouds with iot for smart city services. *IEEE Network*, 33(2):65–71, 2019.

J. T. Kielstein, S. R. Salpeter, S. M. Bode-Boeger, J. P. Cooke, and D. Fliser. Symmetric dimethylarginine (sdma) as endogenous marker of renal function?a meta-analysis. *Nephrology Dialysis Transplantation*, 21(9):2446–2451, 2006.

A. Kumar, A. Aggarwal, and K. Gopal. A novel and efficient reader-to-reader and tag-to-tag anti-collision protocol. *IETE Journal of Research*, 67(3):301–312, 2021.

H. Landaluce, L. Arjona, A. Perallos, F. Falcone, I. Angulo, and F. Muralter. A review of iot sensing applications and challenges using rfid and wireless sensor networks. *Sensors*, 20(9): 2495, 2020.

S.-R. Lee and C.-W. Lee. An enhanced colorwave reader anti-collision algorithm in rfid system. *Journal of the Institute of Electronics Engineers of Korea TC*, 43(2):27–38, 2006.

C. Li, L. Mo, and D. Zhang. Review on uhf rfid localization methods. *IEEE Journal of Radio Frequency Identification*, 3(4):205–215, 2019.

D. Li, L. Deng, W. Liu, and Q. Su. Improving communication precision of iot through behavior-based learning in smart city environment. *Future Generation Computer Systems*, 108:512–520, 2020a.

N. Li, X. Duan, Y. Wu, S. Hua, and B. Jiao. An anti-collision algorithm for active rfid. In *2006 International Conference on Wireless Communications, Networking and Mobile Computing*, pages 1–4. IEEE, 2006.

Z. Li, C. He, and H.-Z. Tan. Ainet-sl: artificial immune network with social learning and its application in fir filter designing. *Applied Soft Computing*, 13(12):4557–4569, 2013.

Z. Li, C. He, J. Li, and H.-Z. Tan. Adaptive hierarchical artificial immune system and its application in rfid reader collision avoidance. *Applied Soft Computing*, 21:119–138, 2014.

Z. Li, J. Li, C. He, C. Tang, and J. Zhou. Rfid reader-to-reader collision avoidance model with multiple-density tag distribution solved by artificial immune network optimization. *Applied Soft Computing*, 30:249–264, 2015.

Z. Li, G. He, D. Xu, and S. Wang. Evaluation of centralized reader anti-collision protocols for mobile rfid system based on maximum independent set: A simulation study. *IEEE Access*, 8: 123381–123397, 2020b.

B. Liu and X. Su. An anti-collision algorithm for rfid based on an array and encoding scheme. *Information*, 9(3):63, 2018.

B.-H. Liu, N.-T. Nguyen, V.-T. Pham, and Y.-H. Yeh. A maximum-weight-independent-set-based algorithm for reader-coverage collision avoidance arrangement in rfid networks. *IEEE Sensors Journal*, 16(5):1342–1350, 2015.

L. Liu and S. Lai. Aloha-based anti-collision algorithms used in rfid system. In *2006 International Conference on Wireless Communications, Networking and Mobile Computing*, pages 1–4. IEEE, 2006.

R.-S. Liu, K.-W. Fan, Z. Zheng, and P. Sinha. Perpetual and fair data collection for environmental energy harvesting sensor networks. *IEEE/ACM Transactions on Networking*, 19(4):947–960, 2010.

Z. Luo, C. Jing, Y. Chen, and X. Xiong. A new underdetermined nmf based anti-collision algorithm for rfid systems. *ISA transactions*, 2021.

Y. Ma, B. Wang, S. Pei, Y. Zhang, S. Zhang, and J. Yu. An indoor localization method based on aoa and pdoa using virtual stations in multipath and nlos environments for passive uhf rfid. *IEEE Access*, 6:31772–31782, 2018.

S. Mahlknecht and S. A. Madani. On architecture of low power wireless sensor networks for container tracking and monitoring applications. In *2007 5th IEEE International Conference on Industrial Informatics*, volume 1, pages 353–358. IEEE, 2007.

L. Mainetti, L. Patrono, and A. Vilei. Evolution of wireless sensor networks towards the internet of things: A survey. In *SoftCOM 2011, 19th international conference on software, telecommunications and computer networks*, pages 1–6. IEEE, 2011.

M. Marta and M. Cardei. Improved sensor network lifetime with multiple mobile sinks. *Pervasive and Mobile computing*, 5(5):542–555, 2009.

A. A. Mbacke, N. Mitton, and H. Rivano. Rfid reader anticollision protocols for dense and mobile deployments. *Electronics*, 5(4):84, 2016.

A. Meddeb and A. Jaballah. Algorithm for readers arrangement without collision in rfid networks. In *2017 18th international conference on parallel and distributed computing, applications and technologies (PDCAT)*, pages 316–321. IEEE, 2017.

A. Mitrokotsa and C. Douligeris. Integrated rfid and sensor networks: architectures and applications. In *RFID and Sensor Networks*, pages 531–556. CRC press, 2009.

N. Mitton, A. A. Mbacke, and H. Rivano. Distributed efficient & fair anticollision for rfid protocol. In *2016 IEEE 12th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pages 1–8. IEEE, 2016.

S. Moeller, A. Sridharan, B. Krishnamachari, and O. Gnawali. Routing without routes: The backpressure collection protocol. In *Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks*, pages 279–290, 2010.

A. Musa and A.-A. A. Dabo. A review of rfid in supply chain management: 2000–2015. *Global Journal of Flexible Systems Management*, 17(2):189–228, 2016.

H. G. Myung. Introduction to single carrier fdma. In *2007 15th European signal processing conference*, pages 2144–2148. IEEE, 2007.

F. Nawaz and V. Jeoti. 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, 2015.

K. Ogawa, K. Kanai, K. Nakamura, H. Kanemitsu, J. Katto, and H. Nakazato. Iot device virtualization for efficient resource utilization in smart city iot platform. In *2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pages 419–422. IEEE, 2019.

O. G. Olaleye, A. Ali, D. Perkins, and M. Bayoumi. Modeling and performance simulation of pulse and mcmac protocols in rfid-based iot network using omnet++. In *2018 IEEE International Conference on RFID (RFID)*, pages 1–5. IEEE, 2018.

A. Pal and K. Kant. Internet of perishable logistics: Building smart fresh food supply chain networks. *IEEE Access*, 7:17675–17695, 2019.

Z. Pang, J. Tian, and Q. Chen. Intelligent packaging and intelligent medicine box for medication management towards the internet-of-things. In *16th international conference on advanced communication technology*, pages 352–360. IEEE, 2014.

Z. Pang, L. Zheng, J. Tian, S. Kao-Walter, E. Dubrova, and Q. Chen. Design of a terminal solution for integration of in-home health care devices and services towards the internet-of-things. *Enterprise Information Systems*, 9(1):86–116, 2015.

J.-h. Park, M. M. Salim, J. H. Jo, J. C. S. Sicato, S. Rathore, and J. H. Park. Ciot-net: a scalable cognitive iot based smart city network architecture. *Human-centric Computing and Information Sciences*, 9(1):1–20, 2019.

U. Park and J. Heidemann. Data muling with mobile phones for sensornets. In *Proceedings of the 9th ACM Conference on Embedded Networked Sensor Systems*, pages 162–175, 2011.

V. Pillai, R. Martinez, J. Bleichner, K. Elliot, S. Ramamurthy, and K. Rao. A technique for simultaneous multiple tag identification. In *Fourth IEEE Workshop on Automatic Identification Advanced Technologies (AutoID'05)*, pages 35–38. IEEE, 2005.

R. Poovendran. Cyber–physical systems: Close encounters between two parallel worlds [point of view]. *Proceedings of the IEEE*, 98(8):1363–1366, 2010.

M. A. Rahman, M. M. Rashid, M. S. Hossain, E. Hassanain, M. F. Alhamid, and M. Guizani. Blockchain and iot-based cognitive edge framework for sharing economy services in a smart city. *IEEE Access*, 7:18611–18621, 2019.

S. Rangwala, R. Gummadi, R. Govindan, and K. Psounis. Interference-aware fair rate control in wireless sensor networks. *ACM SIGCOMM Computer Communication Review*, 36(4):63–74, 2006.

E. Reilly, M. Maloney, M. Siegel, and G. Falco. A smart city iot integrity-first communication protocol via an ethereum blockchain light client. In *Proceedings of the International Workshop on Software Engineering Research and Practices for the Internet of Things (SERP4IoT 2019), Marrakech, Morocco*, pages 15–19, 2019.

H. Rezaie and M. Golsorkhtabaramiri. A fair reader collision avoidance protocol for rfid dense reader environments. *Wireless Networks*, 24(6):1953–1964, 2018.

L. Ruiz-Garcia and L. Lunadei. The role of rfid in agriculture: Applications, limitations and challenges. *Computers and Electronics in Agriculture*, 79(1):42–50, 2011.

A. G. Ruzzelli, R. Jurdak, and G. M. O'Hare. On the rfid wake-up impulse for multi-hop sensor networks. In *The 1st ACM Workshop on Convergence of RFID and Wireless Sensor Networks and their Applications (SenseID) at the 5th ACM International Conference on Embedded Networked Sensor Systems (ACM SenSys 2007), Sydney, Australia, November 04-09, 2007*, 2007.

H. Safa, W. El-Hajj, and C. Meguerditchian. A distributed multi-channel reader anti-collision algorithm for rfid environments. *Computer Communications*, 64:44–56, 2015.

R. Saia, S. Carta, D. R. Recupero, and G. Fenu. Internet of entities (ioe): A blockchain-based distributed paradigm for data exchange between wireless-based devices. In *SENSORNETS*, pages 77–84, 2019.

H. Schaffers, N. Komninos, M. Pallot, B. Trousse, M. Nilsson, and A. Oliveira. Smart cities and the future internet: Towards cooperation frameworks for open innovation. In *The future internet assembly*, pages 431–446. Springer, Berlin, Heidelberg, 2011.

M. Shafiq, Z. Tian, Y. Sun, X. Du, and M. Guizani. Selection of effective machine learning algorithm and bot-iot attacks traffic identification for internet of things in smart city. *Future Generation Computer Systems*, 107:433–442, 2020.

C. Shousong, W. Xiaoguang, and Z. Yuanjun. Revenue model of supply chain by internet of things technology. *IEEE Access*, 7:4091–4100, 2018.

M. Sidorov, M. T. Ong, R. V. Sridharan, J. Nakamura, R. Ohmura, and J. H. Khor. Ultra-lightweight mutual authentication rfid protocol for blockchain enabled supply chains. *IEEE Access*, 7:7273–7285, 2019.

S. Singh, P. K. Sharma, B. Yoon, M. Shojafar, G. H. Cho, and I.-H. Ra. Convergence of blockchain and artificial intelligence in iot network for the sustainable smart city. *Sustainable Cities and Society*, 63:102364, 2020a.

S. K. Singh, Y.-S. Jeong, and J. H. Park. A deep learning-based iot-oriented infrastructure for secure smart city. *Sustainable Cities and Society*, 60:102252, 2020b.

F. Sivrikaya and B. Yener. Time synchronization in sensor networks: a survey. *IEEE network*, 18(4):45–50, 2004.

J. V. Sobral, J. J. Rodrigues, R. A. Rabelo, J. C. Lima Filho, N. Sousa, H. S. Araujo, and R. Holanda Filho. A framework for enhancing the performance of internet of things applications based on rfid and wsns. *Journal of Network and Computer Applications*, 107:56–68, 2018.

A. Sridharan and B. Krishnamachari. Explicit and precise rate control for wireless sensor networks. In *Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems*, pages 29–42, 2009.

A. Srinivasan. *Handbook of precision agriculture: principles and applications*. CRC press, 2006.

J. Su, Z. Sheng, and L. Xie. A collision-tolerant-based anti-collision algorithm for large scale rfid system. *IEEE Communications Letters*, 21(7):1517–1520, 2017.

S. Sudevalayam and P. Kulkarni. Energy harvesting sensor nodes: Survey and implications. *IEEE communications surveys & tutorials*, 13(3):443–461, 2010.

N. Suri, Z. Zielinski, M. Tortonesi, C. Fuchs, M. Pradhan, K. Wrona, J. Furtak, D. B. Vasilache, M. Street, V. Pellegrini, et al. Exploiting smart city iot for disaster recovery operations. In *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, pages 458–463. IEEE, 2018.

Q. Tao, C. Gu, Z. Wang, J. Rocchio, W. Hu, and X. Yu. Big data driven agricultural products supply chain management: A trustworthy scheduling optimization approach. *IEEE Access*, 6: 49990–50002, 2018.

F. Vernon. Application of the microwave homodyne. *Transactions of the IRE professional Group on Antennas and Propagation*, pages 110–116, 1952.

J. Waldrop, D. W. Engels, and S. E. Sarma. Colorwave: An anticollision algorithm for the reader collision problem. In *IEEE International Conference on Communications, 2003. ICC'03.*, volume 2, pages 1206–1210. IEEE, 2003.

L.-C. Wang and H.-C. Liu. A novel anti-collision algorithm for epc gen2 rfid systems. In *2006 3rd International Symposium on Wireless Communication Systems*, pages 761–765. IEEE, 2006.

X. Wang, L. T. Yang, H. Li, M. Lin, J. Han, and B. O. Apduhan. Nqa: A nested anti-collision algorithm for rfid systems, 2019.

R. Want. An introduction to rfid technology. *IEEE pervasive computing*, 5(1):25–33, 2006.

T. Winter, P. Thubert, A. Brandt, J. W. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J.-P. Vasseur, R. K. Alexander, et al. Rpl: Ipv6 routing protocol for low-power and lossy networks. *rfc*, 6550:1–157, 2012.

M. Xia, Q. Yu, and Z. Li. Relative density based anti-collision algorithm in rfid networks with dense readers. In *TENCON 2015-2015 IEEE Region 10 Conference*, pages 1–5. IEEE, 2015.

X. Xuan and K. Li. Efficient anti-collision algorithm for rfid epc generation-2 protocol based on continuous detection. *International Journal of Wireless Information Networks*, 27(1):133–143, 2020.

P. Yan, S. Choudhury, and R. Wei. A machine learning auxiliary approach for the distributed dense rfid readers arrangement algorithm. *IEEE Access*, 8:42270–42284, 2020.

D. Yan-e. Design of intelligent agriculture management information system based on iot. In *2011 Fourth International Conference on Intelligent Computation Technology and Automation*, volume 1, pages 1045–1049. IEEE, 2011.

G. Yang, M. Xiao, and C. Chen. A simple energy-balancing method in rfid sensor networks. In *2007 International Workshop on Anti-Counterfeiting, Security and Identification (ASID)*, pages 306–310. IEEE, 2007.

J. Yick, B. Mukherjee, and D. Ghosal. Wireless sensor network survey. *Computer networks*, 52 (12):2292–2330, 2008.

A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi. Internet of things for smart cities. *IEEE Internet of Things journal*, 1(1):22–32, 2014.

H. Zhang, M. Babar, M. U. Tariq, M. A. Jan, V. G. Menon, and X. Li. Safecity: Toward safe and secured data management design for iot-enabled smart city planning. *IEEE Access*, 8: 145256–145267, 2020.

L. Zhang and Z. Wang. Integration of rfid into wireless sensor networks: architectures, opportunities and challenging problems. In *2006 Fifth international conference on grid and cooperative computing workshops*, pages 463–469. IEEE, 2006.

K. Zhao, M. Zhu, B. Xiao, X. Yang, C. Gong, and J. Wu. Joint rfid and uwb technologies in intelligent warehousing management system. *IEEE Internet of Things Journal*, 7(12):11640–11655, 2020.

W. Zhou and N. Jiang. Research on hybrid of aloha and multi-fork tree anti-collision algorithm for rfid. *Procedia Computer Science*, 183:389–394, 2021.

Résumé

En vue de l'émergence de l'Internet des objets, le besoin d'une identification et d'une En vue de l'émergence de l'Internet des objets, le besoin d'une identification et d'une traçabilité efficaces a augmenté. L'identification par radiofréquence (RFID), une approche simple et bon marché pour recueillir les informations, a donc attiré l'attention des communautés de recherche.
De nombreux domaines d'application nécessitent un réseau RFID dense pour un déploiement et une couverture efficace, ce qui provoque des interférences entre les tags et les lecteurs RFID et par conséquent réduit les performances du système RFID.
Cependant, ce système souffre de problèmes causés par une densité élevée, tels que les collisions et les duplications. Le déploiement de la RFID est donc plus efficace dans un environnement dense où il peut améliorer les surcharges et les retards.
Plusieurs chercheurs proposent donc des protocoles de couche MAC pour résoudre ce problème de collision en se basant sur différentes méthodes d'accès au canal.
Notre recherche de thèse propose de nouvelles approches pour la gestion efficace des ressources de fréquence et de temps pour les lecteurs RFID déployés dans les réseaux de capteurs sans fil denses et mobiles à travers :
- Protocole général de la couche MAC FTSMAC dans lequel la fréquence du spectre est utilisée efficacement en divisant le signal en différents intervalles de temps via un mécanisme de messagerie distribué utilisé par les lecteurs RFID.
- Solution hybride FTSMAC-E améliorant le protocole anti-collision FTSMAC basé sur le TDMA-FDMA distribué.
- Protocole anti-collision basé sur le réseau neuronal artificiel de type feed-forward pour un apprentissage distribué entre les lecteurs RFID afin de prédire la présence de collisions et d'assurer une allocation efficace des ressources.
- Modèle (AIN-CA) d'anti-collision de lecteur en termes d'allocation de ressources utilisant un réseau immunitaire artificiel afin de minimiser les collisions.

Mots-clefs : Système RFID ; Internet des objets ; Réseau neuronal artificiel ; Réseau immunitaire artificiel ; Collision ; Couche MAC ; Réseau de capteurs sans fil ; Systèmes distribués ; Allocation de ressources.

Abstract

Due to the emergence of the Internet of Things, the need for effective identification and traceability has increased. Radio-frequency identification (RFID), a simple and cheap approach for gathering information, has therefore drawn the attention of research communities.
Many application areas require a dense RFID network for efficient deployment and coverage, which causes interference between RFID tags and readers, thus reducing the performance of the RFID system.
However, this system suffers from problems caused by high density, such as collisions and duplication. Thus, the deployment of RFID is more effective in a dense environment where it may improve overage and delays.
Thus, several researchers propose MAC layer protocols to solve this collision problem based on different channel access methods.
Our thesis research offers new approaches to the efficient management of frequency and time resources for RFID readers deployed in dense and mobile wireless sensor networks through:
- General MAC layer protocol FTSMAC in which the spectrum frequency is efficiently used by dividing the signal into different time slots via a distributed messaging mechanism used by RFID readers.
- Hybrid solution FTSMAC-E improving FTSMAC based distributed TDMA-FDMA anti-collision protocol.
- An anti-collision protocol based on feed-forward artificial neural network methodology for shared learning between RFID readers to predict the presence of collisions and ensure an efficient resource allocation.
- Model (AIN-CA) of reader anti-collision in terms of resource allocation using artificial immune network in order to solve this problem.

Key Words: System RFID; Internet of things; Artificial neural network; Artificial immune network; Collision; MAC layer; Wireless sensor network; Distributed systems; Resource allocation.