Titre: Title:	RFID : L'attaque sangsue est-elle réalisable à plus de 30 cm d'un transpondeur HF?
Auteur: Author:	Simon Guigui
Date:	2015
Type:	Mémoire ou thèse / Dissertation or Thesis
Référence: Citation:	Guigui, S. (2015). RFID : L'attaque sangsue est-elle réalisable à plus de 30 cm d'un transpondeur HF? [Mémoire de maîtrise, École Polytechnique de Montréal]. PolyPublie. https://publications.polymtl.ca/2036/

URL de PolyPublie: PolyPublie URL:	https://publications.polymtl.ca/2036/
Directeurs de recherche: Advisors:	Jose Manuel Fernandez, & J. M. Pierre Langlois
Programme: Program:	Génie informatique

UNIVERSITÉ DE MONTRÉAL

RFID : L'ATTAQUE SANGSUE EST-ELLE RÉALISABLE À PLUS DE 30 CM D'UN TRANSPONDEUR HF ?

SIMON GUIGUI
DÉPARTEMENT DE GÉNIE INFORMATIQUE ET GÉNIE LOGICIEL
ÉCOLE POLYTECHNIQUE DE MONTRÉAL

MÉMOIRE PRÉSENTÉ EN VUE DE L'OBTENTION
DU DIPLÔME DE MAÎTRISE ÈS SCIENCES APPLIQUÉES
(GÉNIE INFORMATIQUE)
DÉCEMBRE 2015

UNIVERSITÉ DE MONTRÉAL

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

Ce mémoire intitulé :

RFID : L'ATTAQUE SANGSUE EST-ELLE RÉALISABLE À PLUS DE 30 CM D'UN TRANSPONDEUR HF ?

présenté par : GUIGUI Simon
en vue de l'obtention du diplôme de : Maîtrise ès sciences appliquées
a été dûment accepté par le jury d'examen constitué de :

M. BOYER François-Raymond, Ph. D., président
M. FERNANDEZ José M., Ph. D., membre et directeur de recherche
M. LANGLOIS J.M. Pierre, Ph. D., membre et codirecteur de recherche
M. DAVID Jean-Pierre, Ph. D., membre

Mais vous savez, moi je ne crois pas qu'il y ait de bonnes ou de mauvaises situations. Moi, si je devais résumer ma vie, aujourd'hui avec vous, je dirais que c'est d'abord des rencontres, des gens qui m'ont tendu la main peut-être à un moment où je ne pouvais pas, où j'étais seul chez moi. Et c'est assez curieux de se dire que les hasards, les rencontres forgent une destinée. Parce que quand on a le goût de la chose, quand on a le goût de la chose bien faite, le beau geste, parfois on ne trouve pas l'interlocuteur en face, je dirais le miroir qui vous aide à avancer.

Otis, Astérix & Obélix : Mission Cléopâtre (2002),

REMERCIEMENTS

Je tiens tout d'abord à remercier mes directeurs de recherche M. Fernandez et Pierre Langlois pour m'avoir donné l'opportunité de faire cette maîtrise, pour leurs conseils et leur rigueur et enfin pour leur financement.

Je voudrais remercier Tatu Serioja Ovidiu de l'INRS pour sa disponibilité et son expertise précieuse dans le domaine des communications radiofréquences.

Mes remerciements vont aussi à tous les anciens et nouveaux étudiants du laboratoire de sécurité informatique SecSI que j'ai pu côtoyer pendant ma maîtrise : Joan Calvet, Sabrine Jdaida, François Labrèche, Fanny Lalonde Lévesque, Antoine Lemay, Pierre Brun-Murol. Leur motivation et leur bonne humeur ont contribué à former une ambiance de travail stimulante et chaleureuse.

Merci à mes parents Jean Guigui et Catherine Jean, et à ma famille entière pour son soutien. Je souhaite enfin remercier mes amis Jérôme Gaveau, Mahmoud Ghorbel, Adrien Larbanet, Alexandre Leuliet, Thomas Jan Mahamad, et Aurélien Salomon.

RÉSUMÉ

La technologie RFID (Radio Frequency IDentification) permet l'identification sans fil de transpondeurs qui souvent ne contiennent pas de source d'alimentation propre. La technologie NFC (Near Field Communication) vient prolonger cette première solution en ne se limitant plus seulement à l'identification, mais plus généralement à la communication sans fil. Ces deux technologies sont de plus en plus présentes dans notre quotidien. En effet, la RFID est aujourd'hui très employée dans des domaines aussi variés que le contrôle d'accès, les transports en commun, la santé, les entreprises et les universités. Elle commence maintenant à apparaître dans les cartes de paiement et les passeports. Par ailleurs, les téléphones intelligents sont de plus en plus nombreux à intégrer la technologie NFC.

Dans ce contexte, il est essentiel de s'assurer que les informations échangées lors d'une communication soient correctement protégées pour prévenir d'éventuelles fraudes, usurpations d'identité ou vols d'informations confidentielles. Or, un des arguments souvent avancé, pour justifier la sécurité de la RFID en bande HF et de NFC dans les applications grand public, est leur faible distance de lecture de quelques centimètres.

Dans un premier temps, nous avons ainsi cherché à établir théoriquement la distance maximale de lecture de différents transpondeurs HF en proposant un nouveau modèle d'attaque : nous supposons que le lecteur de l'attaquant peut fonctionner à une fréquence différente de 13.56 MHz, contrairement à un lecteur ordinaire. En effet, la fréquence de résonance de certains transpondeurs HF est supérieure à cette porteuse. Nous avons trouvé que la distance de lecture varie significativement d'un transpondeur à l'autre et qu'accorder le lecteur sur la fréquence de résonance du transpondeur permet parfois d'augmenter considérablement la portée de l'attaque.

Dans un second temps, nous avons cherché à adresser une des difficultés techniques posées par la fabrication d'un lecteur ayant une portée importante : le filtrage de la porteuse dans son circuit de réception. Nous avons ainsi proposé un filtre passif d'ordre 5 capable de filtrer 65 dB de porteuse. Cette atténuation n'est cependant pas suffisante pour atteindre des distances de lecture intéressantes sans ajouter un second étage de filtrage. Nous avons également proposé une expérience pour vérifier le bon fonctionnnement du filtre.

ABSTRACT

RFID (Radio Frequency IDentification) allows remote identification of wireless devices that often do not contain a power supply. NFC (Near Field Communication) extends the protocol stack of HF RFID to wireless communication. In recent years, those two technologies have rapidly spread. RFID based access control is used by many transit systems, universities and entreprises. Passports and credit cards now feature NFC chips, along with modern smartphones.

In this context, enforcing the security of communication protocols used in those applications is of utmost importance if frauds, confidential information theft and identity theft are to be avoided. Yet, a recurring argument to prove the intrinsic security of HF RFID and NFC is that their range is limited to a few centimeters at best.

To challenge that argument, we first established a theorical model to estimate the maximal read distance of HF RFID tags. We considered a new threat model where the attacker can tune his reader to a different frequency than 13.56 MHz. Indeed, the resonant frequency of HF RFID tags is often higher than the carrier frequency of readers. We found out that this hack could significantly increase the read range of certain tags. We also observed that the read out distance strongly depends on characteristics that vary from one tag to another.

Secondly, we addressed one of the difficulties posed by the implementation of a reader with an extended read range: the cancellation of the carrier in the receiver circuit. Thus, we designed a 5 order passive filter attenuating 65 dB of carrier. We also proposed an experience to test how well it could fit in a real RFID system, but unfortunately its response is not sufficient to achieve interesting read out distances.

TABLE DES MATIÈRES

LISTE DES TABLEAUX

LISTE DES FIGURES

LISTE DES ANNEXES

LISTE DES SIGLES ET ABRÉVIATIONS

ADC	Convertisseur analogique-numérique (Analog to Digital Converter)
ADS	Advanced Design System
AWG	American Wire Gauge
ARQS	Approximation des Régimes Quasi Stationnaires
ASK	Modulation par déplacement d'amplitude (Amplitude Shift Keying)
BPSK	Déplacement Binaire de Phase (Binary Phase-Shift Keying)
CVV	Cryptogramme visuel (Card Verification Value)
DAC	Convertisseur numérique-analogique (Digital to Analog Converter)
DSP	Densité Spectrale de Puissance
ECMA	Ecma International
EM	Électromagnétique
ERC	European Radiocommunications Committee
ESR	Résistance équivalente série (Equivalent Series Resistor)
FET	Transistor à effet de champ (Field Effect Transistor)
FFT	Transformation de Fourier Rapide (Fast Fourier Transform)
FSK	Déplacement de Fréquence (Frequency-Shift Keying)
HF	Haute Fréquence (High Frequency)
IEC	Commission électrotechnique internationale (International Electrotechnical Commission)
IEEE	Institute of Electrical and Electronics Engineers
ITU	L'Union Internationale des Télécommunications
ISO	Organisation internationale de normalisation (International Standard Organization)
LF	Basse fréquence (Low Frequency)
LNA	Amplificateur faible bruit (Low Noise Amplifier)
NFC	Communication en champ proche (Near Field Communication)
NRZ	Non Retour à Zéro (Non-Return-to-Zero)
NRZ-L	Non Retour à Zéro Niveau (Non-Return-to-Zero Level)
OOK	Modulation par déplacement d'amplitude avec index de modulation maximal (On-Off Keying)
PCB	Circuit imprimé (Printed Circuit Board)
RFID	Identification radio-fréquence (Radio-Frequency IDentification)
RMS	Valeur efficace (Root Mean Square)

SCR	Rapport signal sur porteuse (Signal to Carrier Ratio)
SHF	Super Haute Fréquence (Signal High Frequency)
SNR	Rapport signal sur bruit (Signal to Noise Ratio)
UHF	Ultra Haute Fréquence (Ultra High Frequency)

CHAPITRE 1

INTRODUCTION

La RFID (Radio Frequency IDentification) est une technologie sans fil permettant l'identification à distance d'entités. Apparue il y a une vingtaine d'années [28], elle s'est rapidement développée grâce à ses très nombreux champs d'applications. Elle est aujourd'hui omniprésente dans de nombreuses industries ainsi que dans nos quotidiens : elle représente en effet en 2014 un marché de plus de 20 milliards de dollars. S'il est possible de se réjouir des progrès apportés par ces deux technologies, il faut aussi s'inquiéter des problèmes de sécurité qu'elles posent. Il y a notamment un risque d'atteinte à la vie privée, car souvent les cartes contiennent des informations propres à leur utilisateur, et un risque d'usurpation d'identité lorsqu'une carte peut être dupliquée. Bien que des vulnérabilités existent dans les systèmes de RFID, leur faible distance de lecture est souvent utilisée comme argument de sécurité. Dans ce contexte, nous nous sommes intéressés à l'attaque sangsue, qui consiste à augmenter cette distance de lecture pour interroger une carte à l'insu de son propriétaire.

Dans ce chapitre, nous verrons dans un premier temps comment fonctionnent ces technologies ainsi que leurs applications. Dans un second temps, justifierons l'importance de l'attaque sangsue et d'une autre attaque similaire, l'attaque d'espionnage. Nous donnerons alors nos objectifs de recherche avant de présenter le plan de ce mémoire.

1.1 La technologie RFID

Derrière le terme RFID se cache un large éventail de normes utilisant des techniques de modulation et de codage des symboles variés. Deux principes physiques différents sont également utilisés, on distingue ainsi la RFID en champ proche de la RFID en champ lointain. Ces implémentations répondent en fait à des cas d'usage différents où certains paramètres comme le coût de fabrication, la portée ou encore la puissance de calcul du transpondeur doivent être privilégiés. Une première partie de cette section sera consacrée à la présentation des éléments constituants un système de RFID. Le fonctionnement de la RFID en champ lointain et de la RFID en champ proche feront ensuite l'objet d'une section. Nous présenterons enfin leurs applications actuelles.

1.1.1 Composants d'un système de RFID

La RFID fait intervenir deux éléments au minimum ; un lecteur et un transpondeur. Le transpondeur est constitué d'un circuit électrique, d'une antenne et optionnellement d'une source d'énergie. On distingue alors trois types de transpondeurs : passif, semi-passif et actif. Les transpondeurs passifs sont les plus fréquents en raison de leur coût plus faible. Ils ne contiennent pas de source d'énergie propre et sont donc alimentés à distance par le lecteur. Les transpondeurs semi-passifs et actifs sont dotés d'une source d'alimentation propre qui leur permet d'avoir une électronique plus complexe. Cependant, les transpondeurs semi-passifs n'utilisent pas cette énergie pour communiquer avec le lecteur contrairement aux actifs qui disposent par conséquent d'une portée plus importante.

Pour communiquer et/ou pour alimenter le transpondeur, le lecteur émet un champ électromagnétique, qui permet d'une part d'alimenter le transpondeur dans le cas passif et d'autre part de lui transmettre de l'information en utilisant une technique de modulation définie par la norme utilisée. La fréquence de la porteuse varie selon les normes de la RFID, il existe des transpondeurs fonctionnant dans les bandes LF (30-300 kHz) à 120-150 kHz et HF (3-30 MHz) à 13.56 MHz. Ils fonctionnent en champ proche, leur portée est donc assez limitée et varie entre quelques centimètres et un mètre. D'autres fonctionnent dans les bandes UHF (300-3000 MHz) à 433 MHz, 865-868 MHz, 902-928 MHz et fonctionnent en champ lointain. Leur portée varie alors entre un et cent mètres. Plus récemment (en 2010), la norme Bluetooth a été étendue pour supporter l'identification de périphériques se comportant comme des transpondeurs actifs fonctionnant dans la bande SHF (3-30 GHz).

1.1.2 Deux principes de fonctionnement

Les systèmes de RFID fonctionnant dans les bandes UHF et SHF n'utilisent pas le même principe physique pour échanger de l'information que ceux fonctionnant dans les bandes LF et HF. En effet, pour ces systèmes, le lecteur émet une onde électromagnétique progressive vers le transpondeur. Pour communiquer avec le lecteur, celui-ci fait alors varier son coefficient de réflexion de sorte à renvoyer l'onde électromagnétique avec une amplitude plus ou moins importante. La figure 1.1 illustre ce principe de fonctionnement.

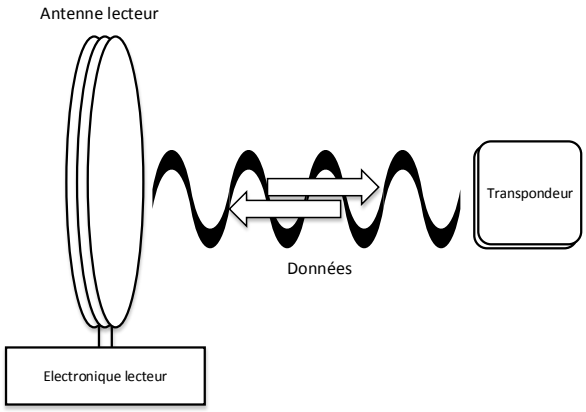

Figure 1.1 Principe de fonctionnement de la RFID en champ lointain.

Contrairement au champ proche ou (sauf dans les cas simples, comme les antennes cadre magnétique) il est difficile de déterminer la topologie des champs électrique **E** et magnétique **H**, le champ lointain d'une antenne est occupé par une onde électromagnétique progressive telle que **E** et **H** sont orthogonaux entre eux, et orthogonaux à la direction de propagation de l'onde. La présence d'un obstacle sur le trajet de l'onde ne provoque pas de rétroaction immédiate sur l'antenne comme c'est le cas dans le champ proche. L'onde est par contre partiellement réfléchie sur l'obstacle et revient vers l'antenne. Outre la RFID en bande UHF et SHF, d'autres systèmes de RF passifs fonctionnent avec ce principe-là comme les transpondeurs aéronautiques ou les radars.

En revanche, pour les systèmes LF et HF, le lecteur et le transpondeur ne communiquent pas par le biais d'une onde électromagnétique, mais à l'aide d'un couplage magnétique qui permet à chacun des deux circuits de s'influencer mutuellement : une variation de courant dans l'une des deux antennes se traduit par une variation du courant dans la seconde. Ainsi, pour communiquer avec le transpondeur le lecteur module en amplitude ou en fréquence le courant qu'il injecte dans son antenne. Dans le cas d'un transpondeur passif ou semi-passif, celui-ci répond en faisant commuter une résistance, ou une capacité dite "de modulation" afin de moduler à son tour le courant traversant son antenne. La figure 1.2 illustre ce principe de fonctionnement.

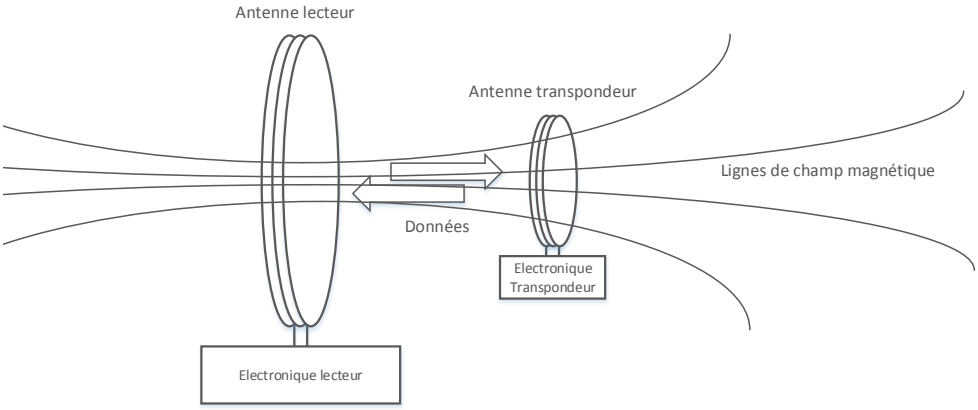

Figure 1.2 Principe de fonctionnement de la RFID en champ proche.

Le phénomène de couplage magnétique ne peut cependant se produire qu'à condition que le transpondeur se trouve dans la zone de champ proche réactif de l'antenne du lecteur, car dans cette région l'énergie magnétique générée par l'antenne n'est pas radiée, mais reste au voisinage de l'antenne. Le champ proche réactif se situe à moins de $\frac{\lambda}{2\pi}$ de l'antenne, où λ la longueur d'onde de la porteuse. Ainsi, à 13.56 MHz, il s'arrête à 3.5 m de l'antenne environ et il n'est pas possible d'observer le phénomène de couplage mutuel à une distance plus grande [12] [19].

1.1.3 Applications de la RFID

Les applications de ces technologies sont très variées. Dans tous les cas, le transpondeur contient une banque de données concernant une entité qui peut être un objet, un animal ou une personne. Au minimum, ces données se résument à un identifiant unique permettant d'identifier l'entité. Souvent, des informations additionnelles sont également incluses. La RFID est ainsi utilisée, par exemple, pour simplifier la logistique de chaînes de montage ou d'inventaires en marquant les objets avec un transpondeur, ou encore pour marquer les animaux domestiques dans certains pays. Les cas d'usages qui nous intéressent en priorité sont les applications grand public où un transpondeur est utilisé pour identifier une personne. La liste suivante récapitule les plus connues :

— **Cartes de transport :** dans de nombreuses villes, les réseaux de transport utilisent maintenant des cartes RFID pour contrôler leurs utilisateurs. Plus particulièrement, beaucoup utilisent des cartes MIFARE Classic, par exemple Boston, Londres, la Corée du Sud, Hong Kong, Beijing [40].

— **Contrôle d'accès :** de nombreuses entreprises utilisent la RFID pour contrôler l'accès des employés. Souvent les technologies utilisées sont MIFARE Classic et HID iCLASS®. La RFID est également utilisée pour l'ouverture des portes d'immeubles. En France, un million d'immeubles sont par exemple protégés par un système Vigik [32] qui utilise MIFARE Classic. Certains immeubles utilisent des cartes ISO 15693 et l'identifiant de l'utilisateur est alors transmis en clair.

— **Documents d'identité :** les passeports biométriques, aussi appelés "e-passport", maintenant utilisés dans de nombreux pays – en 2006, les États-Unis ont demandé à 26 pays d'utiliser un passeport électronique [19] – intègrent un transpondeur ISO 14443 contenant des informations sur l'identité de son possesseur. Les permis de conduire et les "Passport Card" délivrés aux États-Unis intègrent des transpondeurs EPC de deuxième génération [27].

— **Cartes bancaires :** c'est une des innovations les plus récentes permises par la RFID. Nombreuses sont les banques à proposer aujourd'hui des cartes intégrant une interface sans fil pour accélérer les petits paiements. Les noms commerciaux les plus connus de cette technologie sont PayPass et PayWave respectivement proposée par MasterCard et Visa.

1.2 Problématique

Les applications de la RFID précédemment citées, où un transpondeur est utilisé pour identifier une personne, posent deux problèmes de sécurité : un risque d'atteinte à la vie privée, et un risque d'usurpation d'identité. La vie privée de l'utilisateur est menacée lorsque le transpondeur contient des informations permettant de l'identifier – par exemple un identifiant unique – accessible en interrogeant le transpondeur ou en interceptant une communication entre lecteur et transpondeur. Il est alors potentiellement possible de localiser ou suivre l'utilisateur à son insu. L'usurpation d'identité est possible lorsqu'il est possible de cloner – c'est-à-dire de créer une réplique exacte – du transpondeur d'un individu pour un service donné. Un attaquant peut alors, par exemple, entrer sans autorisation dans les locaux d'une entreprise, d'une université, d'un service de transport, à la place de l'utilisateur légitime. Nous allons voir maintenant que de nombreuses vulnérabilités existent dans les systèmes de RFID utilisés aujourd'hui, nous verrons ensuite que les attaques d'espionnage et sangsue permettent d'utiliser ses vulnérabilités à distance.

1.2.1 Faiblesse des solutions existantes

Idéalement, les transpondeurs doivent utiliser un protocole de communication sécurisé : la communication entre lecteur et transpondeur doit commencer par une authentification mutuelle et les données échangées doivent être chiffrées. Enfin, les détails du fonctionnement et de l'implémentation du protocole employé doivent être publics afin de pouvoir être revus et étudiés par tous. Cette condition, appelée principe de Kerckhoffs, est essentielle pour que les éventuelles vulnérabilités d'un cryptosystème puissent être identifiées et corrigées. L'objectif est ainsi de rendre les informations des transpondeurs difficilement accessibles par un attaquant. Cependant, dans le monde de la RFID, ces exigences ne sont souvent pas encore respectées.

Pour commencer, certains transpondeurs fonctionnant dans les bandes LF et HF ne supportent aucune cryptographie et communiquent en clair. Dans certains systèmes de contrôle d'accès, le transpondeur contient seulement en mémoire un identifiant unique qui est transmis en clair au lecteur. C'est le cas, par exemple, des transpondeurs MIFARE Ultralight et MIFARE Ultralight EV1 [44]. Ils peuvent ainsi être interrogés et clonés sans difficulté. Il existe ensuite plusieurs technologies dont la sécurité a été brisée par des équipes de chercheurs en sécurité, leurs vulnérabilités sont alors publiques. C'est le cas par exemple des cartes MIFARE Classic de la société NXP et des cartes iCLASS® de l'entreprise HID, qui comme nous l'avons vu dans la section précédente sont extrêmement répandues. Deux articles en 2007 [6] et 2008 [13] ont ainsi exhibé des vulnérabilités dans la sécurité des cartes MIFARE Classic permettant, à partir d'une trace de la communication entre un lecteur et une carte, de retrouver les 48 bits de la clé secrète la protégeant. Retrouver cette clé est également possible en ayant seulement accès à la carte selon un article de 2009 [7]. 300 requêtes à la carte environ sont alors nécessaires. Les faiblesses de sécurité des cartes iCLASS® ont, elles, été mises en évidence en 2010 par Meriac Milosch [35]. Les cartes iCLASS Standard utilisent ainsi toutes la même clé de cryptographie. Un attaquant la connaissant peut modifier et cloner n'importe quelle carte de ce type. Toutes les cartes vendues par ces entreprises n'ont cependant pas encore été publiquement brisées. Les cartes MIFARE DESFire EV1, DESFire EV2 et MIFARE Plus n'ont par exemple pas de vulnérabilité connue.

Les technologies Paypass et Paywave présentent également des lacunes de sécurité inquiétantes. La communication avec le lecteur se fait sans authentification et en clair. Parmi les informations accessibles par l'interface sans fil on trouve : le numéro à seize chiffres, la date d'expiration et l'identité du possesseur (nom, prénom, sexe) [3]. Le CVV est par contre dans ce cas-ci généré à chaque transaction à partir d'une clé privée contenue sur la puce de la

carte ainsi que d'un challenge envoyé par le lecteur. Rappelons cependant que ces informations suffisent pour commander sur certains sites internet qui ne demandent pas le CVV. Cette implémentation a été privilégiée parce qu'elle permet une mise à jour des points de vente sans avoir à remplacer les anciennes caisses enregistreuses.

Enfin, la sécurité des passeports biométriques a aussi été critiquée. Pour le moment, la lecture des données contenues sur le passeport est protégée par la norme BAC ("Basic Access Control") : pour communiquer avec celui-ci, le lecteur doit dériver une clé à partir du numéro du passeport, de sa date d'expiration ainsi que la date de naissance du possesseur. Cependant, l'article [2] a montré, d'une part que certains passeports en Belgique (les 2/3 en 2011) ne supportent pas le BAC et peuvent être lus sans restriction, et d'autre part que l'entropie de la clé du BAC est en réalité suffisamment faible pour permettre une attaque par force brute dans certains pays, notamment en Belgique.

1.2.2 Attaque sangsue et attaque d'espionnage

Le manque d'intérêt des entreprises à utiliser ou développer des solutions de RFID mieux sécurisées vient souvent du présupposé que les signaux échangés ne sont pas – ou très difficilement – interceptables au-delà de la distance prévue par les normes existantes. En effet, pour la RFID à 13.56 MHz, la plupart des normes prévoient des communications à une dizaine de centimètres au maximum ; exception faite de la norme ISO 15693 dans son mode "vicinity", prévu pour fonctionner à 1.5 m, mais qui est peu courant dans les applications grand public. Ce présupposé a déjà été nuancé par des équipes de recherche, notamment en proposant deux attaques visant à intercepter ou voler les informations d'un transpondeur RFID. La première est l'attaque d'espionnage qui consiste à intercepter de loin les informations échangées entre un lecteur légitime et un transpondeur. La seconde est l'attaque sangsue ou "skimming attack", qui consiste à activer un transpondeur de loin pour lui voler les informations qu'il contient sans le consentement de son propriétaire et à son insu. L'objectif de ces deux attaques est donc d'exploiter les vulnérabilités des systèmes de RFID, sans entrer en contact avec la victime.

Attaque d'espionnage

L'attaque d'espionnage ("eavesdropping attack") consiste à écouter à distance une communication légitime entre un lecteur et un transpondeur. Deux topologies sont envisageables :

— **le cas monostatique :** une seule antenne est utilisée pour recevoir le signal émis par

le lecteur et par le transpondeur. Cette configuration est illustrée sur la figure 1.3.

— **le cas bistatique :** deux antennes sont utilisées, une pour recevoir le signal du lecteur, et une autre pour recevoir le signal du transpondeur. Le signal du transpondeur n'est pas exactement centré sur 13.56 MHz (voir le chapitre sur les différentes normes), la seconde antenne et le circuit de réception pourront donc être ajustés en conséquence.

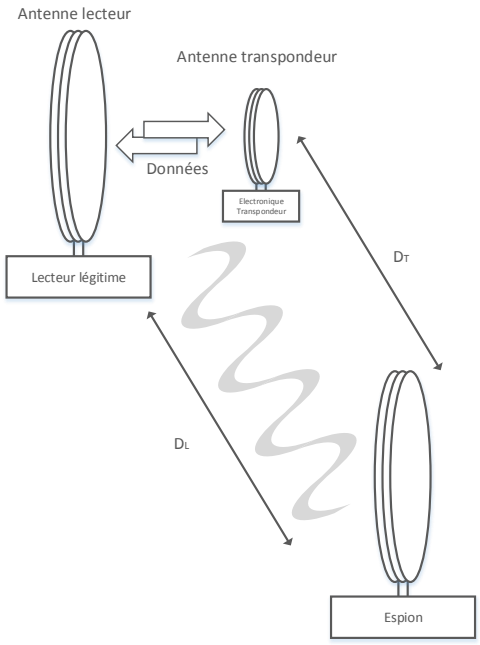

Figure 1.3 Attaque d'espionnage dans le cas monostatique.

Attaque sangsue ("skimming attack")

Pour interroger un transpondeur, le lecteur de l'attaquant doit être capable de l'activer et de lui envoyer ses requêtes. Il doit ensuite être également capable de démoduler les signaux transmis par le transpondeur. On note D_{TX} et D_{RX} respectivement ces deux sens de la communication. Deux topologies sont alors envisageables pour le lecteur malicieux :

— **le cas monostatique :** l'émission et la réception se font sur la même antenne, ce scénario est représenté sur la figure 1.4.

— **le cas bistatique :** deux antennes, une pour la réception et une pour l'émission. Ce scénario est représenté sur la figure 1.5.

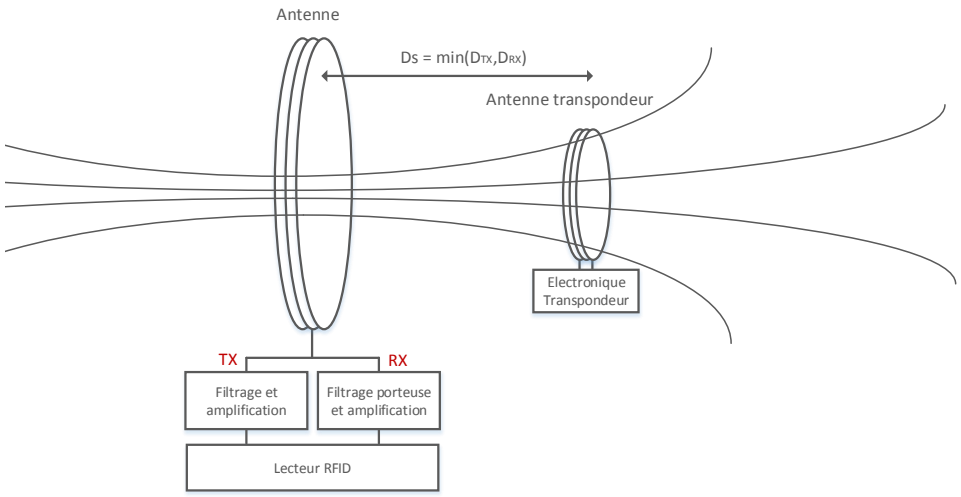

Figure 1.4 Attaque sangsue dans le cas monostatique.

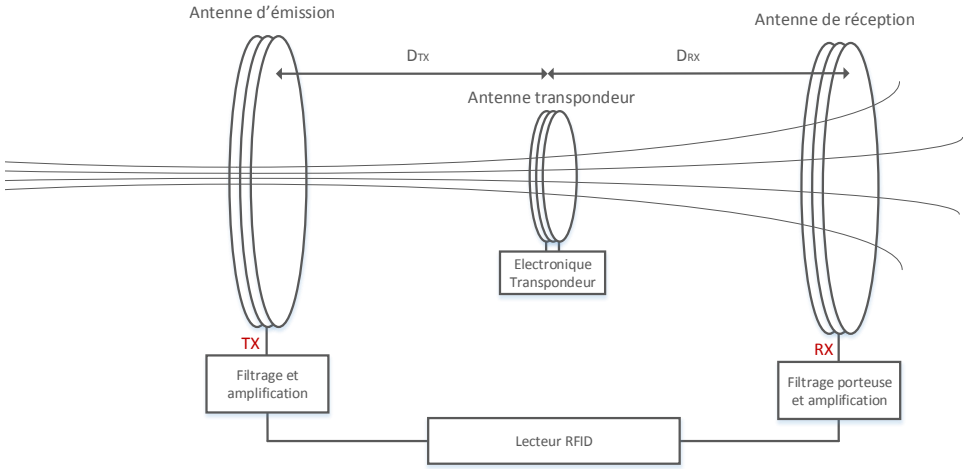

Figure 1.5 Attaque sangsue dans le cas bistatique.

Le cas bistatique présente le désavantage d'être plus encombrant est plus compliqué à mettre en place pour l'attaquant, mais en contrepartie il permet théoriquement d'augmenter la distance entre les deux antennes et le transpondeur. En effet, seule une partie du champ émis par l'antenne d'émission traversera l'antenne de réception : l'antenne de réception est donc plus fortement couplée au transpondeur qu'à l'antenne d'émission, le signal du transpondeur doit donc dans ce cas être plus facile à distinguer de la porteuse qui alimente le transpondeur.

C'est par le biais de ces deux attaques que les informations d'un transpondeur peuvent être récupérées sans avoir directement accès à celui-ci. Ces informations peuvent ensuite être utilisées pour localiser et suivre à son insu un usager, récupérer des numéros de carte bancaire, ou usurper une identité. Il est donc important d'évaluer la faisabilité de ces attaques. Nous avons cependant concentré nos efforts sur l'attaque sangsue pour trois raisons. Premièrement, celle-ci a pour l'instant été moins étudiée dans la littérature. Deuxièmement, pour un attaquant, les opportunités de réaliser l'attaque sont plus nombreuses puisqu'il est seulement nécessaire de se trouver à proximité du transpondeur visé. L'attaque d'espionnage nécessite par contre d'être au bon endroit et au bon moment pour intercepter une communication légitime entre lecteur et transpondeur. Enfin, l'attaque sangsue est également indispensable pour l'implémentation d'une attaque de "l'homme du milieu". Dans ce scénario, le transpondeur de la victime est interrogé via une attaque sangsue et ses réponses sont envoyées à un lecteur légitime, ce qui permet d'usurper son identité sans même avoir à briser la sécurité du transpondeur. Nous nous sommes par ailleurs concentrés sur le cas monostatique de l'attaque. Bien que le cas bistatique permette théoriquement d'atteindre une portée plus importante, il est plus difficile à mettre en place pour l'attaquant puisque deux antennes doivent être dissimulées au lieu d'une. Par ailleurs, nous verrons dans la revue de littérature que les seuls essais expérimentaux qui ont été menés dans le cas bistatique n'ont pas permis d'obtenir d'amélioration significative de la portée de l'attaque.

Atteindre des distances de lecture importantes pose également un problème pratique : plus la portée du lecteur augmente, plus la puissance de la porteuse à émettre augmente et plus la puissance du signal reçu du transpondeur diminue. Filtrer cette porteuse est ainsi un problème délicat qui n'a pas été abordé dans la littérature sur l'attaque sangsue.

1.3 Objectifs de recherche

Notre objectif est de contribuer à l'évaluation des risques liés à l'utilisation de la RFID en sécurité en estimant la portée maximale de l'attaque sangsue dans le cas monostatique. Cet objectif nous a amenés à nous poser plusieurs questions de recherche auxquelles nous essayerons de répondre :

1. Comment déterminer théoriquement la distance maximale de l'attaque ?
2. Comment les caractéristiques d'un transpondeur (géométrie de l'antenne, facteur de qualité...) influencent-elles cette distance ?
3. La fréquence de la porteuse d'un lecteur est normalement fixée à 13.56 MHz. Peut-on

augmenter la portée de l'attaque en la modifiant ?

4. Une des difficultés techniques de l'attaque sangsue est le filtrage de la porteuse dans le circuit de réception du lecteur malicieux. Nous proposons ainsi de fabriquer un filtre remplissant cette fonction et de mettre en place une expérience pour le tester afin d'évaluer la viabilité pratique de l'attaque.

1.4 Plan du mémoire

Ce mémoire est divisé en six chapitres. Dans le chapitre 2, nous avons étudié les contributions existantes dans la littérature sur les attaques sangsue et d'espionnage en bande HF. Dans le chapitre 3, nous avons regroupé et détaillé l'ensemble des outils tirés de la littérature sur lesquels nous nous sommes basés pour construire un modèle théorique de l'attaque sangsue. Ce modèle et les résultats que nous avons obtenus sont développés dans le chapitre 4. Dans le chapitre 5, nous présentons nos efforts visant à fabriquer un filtre passif permettant d'éliminer la porteuse dans le circuit de réception d'un lecteur RFID. Nous présentons par ailleurs l'expérience que nous avons envisagé pour évaluer ses performances. Nous concluons enfin notre recherche dans le chapitre 6.

CHAPITRE 2

LES ATTAQUES SANGSUE ET D'ESPIONNAGE DANS LA LITTÉRATURE

Depuis 2005, l'attaque sangsue a été évoquée dans de nombreuses publications et rapports, mais peu lui sont effectivement consacrés. De plus, seuls les articles concernant les transpondeurs fonctionnant en bande HF nous intéressent dans le cadre de ce mémoire. Les principes physiques utilisés par les transpondeurs UHF sont en effet différents et les résultats publiés pour ceux-ci ne sont pas exploitables. Ainsi, quatre articles et rapports nous intéressent directement et feront l'objet de la première partie de cette revue. Nous nous pencherons ensuite sur la littérature concernant l'attaque d'espionnage sur les transpondeurs HF. Nous insisterons alors sur les outils et résultats qui peuvent être réutilisés dans le cadre de l'attaque sangsue.

2.1 Attaque sangsue

Nous allons revenir ici sur les méthodologies employées par différentes équipes de chercheurs en sécurité informatique pour estimer la distance maximale à laquelle l'attaque sangsue serait réalisable. Deux articles ont été écrits par des chercheurs de l'université de Tel-Aviv, un en 2005 [24] et l'autre en 2006 [26]. Le premier s'appuie sur une simulation pour montrer que la portée d'un lecteur RFID peut être augmentée jusqu'à 55 cm. Dans le second, l'équipe est allée plus loin et a modifié un lecteur, ils ont ainsi pu lire des transpondeurs ISO 14443 à 25 cm. Nous examinerons également l'article de 2011 de Gerhard P. Hancke [20] de l'université de Londres. Il a cherché à réaliser expérimentalement l'attaque sangsue dans le cas bistatique (deux antennes) et est parvenu à lire un transpondeur HF à 27 cm. Enfin, nous reviendrons sur le mémoire de 2012 de Pierre Brun-Murol qui a notamment essayé de voir jusqu'à quelle distance il est possible d'activer un transpondeur HF. Il existe en outre un rapport de NXP daté de 2008 annonçant un résultat théorique de 30 cm, nous n'avons cependant pas pu y avoir accès.

2.1.1 Limite théorique

L'article de Kfir et Wool [24] publié en 2005 est encore aujourd'hui le seul à proposer un résultat académique théorique pour l'attaque sangsue en bande HF. Les auteurs sont arrivés à la conclusion qu'une distance de lecture comprise entre 40 et 55 cm est atteignable pour un transpondeur ISO 14443 type B. Pour arriver à ce résultat, ils ont utilisé un simulateur

proposé en 2000 par T. W. H. Fockens pour simuler la couche physique d'un système inductif de RFID, ils l'ont ensuite modifié pour respecter la norme ISO 14443 type B. Le modèle permet alors de prendre en compte deux sources de bruit :

— Le bruit externe ou ambiant qui doit être indiqué au simulateur. Pour l'estimer, les auteurs ont supposé la présence d'un lecteur RFID émettant à la puissance maximale autorisée par les réglementations et situé à 100 m du transpondeur à activer.
— Le bruit interne, introduit par l'électronique du système simulé. Ce bruit est calculé par le simulateur, mais aucun détail sur son fonctionnement ni aucun ordre de grandeur ne sont donnés dans l'article pour étayer les résultats obtenus.

L'article donne donc finalement peu de détails sur le modèle utilisé. Cependant, les auteurs fournissent certaines considérations intéressantes sur les facteurs limitant la portée de l'attaque sangsue. En effet, obtenir une distance de lecture élevée implique à la fois d'augmenter la puissance émise par le lecteur – afin d'activer le transpondeur – et de maximiser sa sensibilité. Or ces deux conditions sont difficiles à réunir en même temps, car le bruit interne augmente avec la puissance et limite le SNR de la communication. En d'autres termes, augmenter la distance d'activation limite la distance de réception du signal du transpondeur.

Pour mitiger cette difficulté, les auteurs proposent deux solutions astucieuses pour abaisser le SNR minimal requis pour communiquer avec le transpondeur. La première optimisation repose sur l'idée que le SNR minimal requis pour que le récepteur du lecteur soit capable de se verrouiller sur le signal du transpondeur est inférieur au SNR requis pour obtenir une communication sans erreur. En se contentant de ce premier SNR, il est alors possible de reconstituer l'information envoyée par le transpondeur en l'interrogeant plusieurs fois. Avec 5 retransmissions, la distance de lecture peut d'après les auteurs être augmentée de 40 à 55 cm environ. La seconde méthode est plus compliquée à implémenter, mais permet de ne pas avoir à se soucier du SNR minimal permettant de verrouiller le signal du transpondeur. Cette solution consiste à entrelacer les réponses du transpondeur à une même requête dans une même trame qu'on cherche alors à démoduler. La trame obtenue ayant une bande passante plus étroite, le SNR se trouve augmenté. Avec cette méthode les auteurs pensent également pouvoir augmenter la distance de lecture jusqu'à 55 cm.

2.1.2 Performances atteintes en pratique

Le premier article décrivant un système de RFID capable d'augmenter la distance de lecture d'un transpondeur HF est celui de Kirschenbaum et Wool [26] (2006). Ils ont utilisé un

lecteur RFID programmable du commerce, le TI S4100 sur lequel ils ont remplacé l'antenne par un amplificateur de puissance connecté à une antenne de 40 cm de diamètre. Pour récupérer le signal du transpondeur sans endommager le lecteur avec une porteuse d'amplitude trop grande, l'équipe a rajouté un atténuateur connecté d'une part à la sortie de l'amplificateur et d'autre part à l'entrée du TI S4100. La distance de lecture atteinte avec ce montage est de 25 cm pour un transpondeur ISO 14443 type A dont la référence n'est pas précisée. La figure 2.1 montre les différents étages du montage.

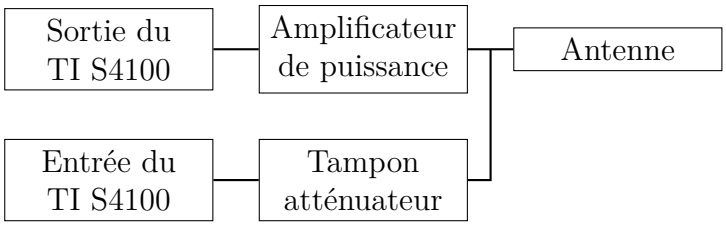

Figure 2.1 Architecture du lecteur RFID de Kirschenbaum et Wool

Les auteurs ont essayé de minimiser au mieux le bruit de l'électronique en utilisant une source de tension – qu'ils ont eux-mêmes fabriquée – alimentée soit par une source stabilisée de laboratoire, soit par une batterie 12 V. Cependant, les facteurs de bruit de celle-ci ainsi que de l'amplificateur de puissance n'ont pas été mesurés ni comparés faute d'équipements adéquats. Il n'est donc pas possible de quantifier à quel point le bruit a été un facteur limitant les performances de l'attaque.

Une des limitations du montage est sans doute l'étage atténuateur. Celui-ci atténue en effet la porteuse à 13.56 MHz, mais aussi le signal du transpondeur. Un filtre bien choisi permettrait de ne pas atténuer la partie du spectre occupée par ce signal.

Le montage utilisé par Hancke [20] en 2011 est très différent. Il a en effet essayé l'attaque sangsue sur un transpondeur Mifare ISO 14443 type A dans le cas bistatique, c'est-à-dire avec deux antennes : une pour activer le transpondeur, et l'autre pour mesurer son signal. Il a par ailleurs utilisé des équipements beaucoup plus dispendieux : la réception du signal du transpondeur est faite avec un récepteur R-1250 de Dynamic Sciences ainsi qu'avec l'antenne active R-1150-10A de la même entreprise. En théorie, il semble que le montage de Hancke présente des avantages certains :

— Le récepteur est muni d'un filtre configurable qui pour l'expérience a été réglé sur 500 kHz. Le montage de Kirschenbaum et Wool comprend seulement le filtre du lecteur RFID alors que la puissance du signal du transpondeur est atténuée par le tampon.
— Le cas bistatique doit permettre d'atteindre des distances de lecture plus élevées puisque le couplage mutuel entre l'antenne réceptrice et l'antenne émettrice est inférieur au couplage mutuel entre l'antenne réceptrice et le transpondeur ce qui permet d'avoir un meilleur index de modulation que dans le cas monostatique.
— Le matériel utilisé est de qualité professionnelle et non fabriqué à la main avec peu de moyens. On peut donc s'attendre à des niveaux de bruit plus faibles.

Les deux attaques ont été réalisées sur des transpondeurs respectant la même norme et pourtant les résultats de Hancke sont inférieurs. La distance d'activation maximale atteinte – c'est-à-dire, la distance maximale à laquelle il est parvenu à activer un transpondeur – est de 27 cm en utilisant une antenne de 30 par 40 cm et une puissance de 4 W. Il n'a par contre pas été capable de retrouver le signal du transpondeur dans ce cas. Il propose par contre deux scénarios où la communication peut se faire dans les deux sens. Le premier consiste à placer une antenne de 14.8x21 cm à 15 cm du transpondeur pour l'activer et une seconde de 14.8x21 cm à 2 m pour recevoir les réponses. Dans le second scénario, les deux antennes sont placées à 20 cm du transpondeur. Comment alors expliquer cet écart de performance ? Nous voyons deux raisons possibles, mais plus de détails sur les expériences de ces deux articles seraient nécessaires pour conclure.

— Les transpondeurs utilisés ne sont pas les mêmes : il est possible que leurs caractéristiques (facteur de qualité, fréquence de résonance, tension seuil d'activation du circuit intégré) soient très différentes et que le transpondeur utilisé par Kirschenbaum et Wool soit plus vulnérable.
— Le facteur de qualité de l'antenne utilisée par Kirschenbaum et Wool n'est pas indiqué, mais il est possible que celui-ci soit plus élevé que celui de l'antenne d'émission utilisée par Hancke. Il a en effet fixé le facteur de qualité à 5, sans élaborer ce choix, ce qui semble peu élevé. Plus le facteur de qualité de l'antenne d'émission est faible, plus la puissance nécessaire pour activer le transpondeur est élevée, ce qui entraîne un niveau de bruit plus élevé. Le facteur de qualité ne doit pas non plus être trop élevé comme nous le verrons dans le chapitre 4.

Finalement, Pierre Brun-Murol [3] a, dans son mémoire, cherché la distance maximale d'activation d'une carte HID iCLASS®. Après avoir programmé le protocole de HID sur la Proxmark3, il a implémenté l'attaque sangsue dans le cas bistatique. Il a utilisé une antenne

de 40 cm de diamètre alimentée par un amplificateur de 40 dB pour émettre le signal du lecteur. Pour contrôler la puissance émise, il a utilisé un atténuateur variable en sortie de la Proxmark3. Pour écouter les réponses du transpondeur, il a utilisé une petite antenne de 8x5 cm directement reliée à la Proxmark3 et toujours maintenu à proximité (quelques centimètres) du transpondeur. Pendant son expérience il a, pour plusieurs puissances d'émission différentes, cherché la distance maximale à laquelle il pouvait placer la grande antenne par rapport au transpondeur de sorte que la communication se déroule correctement. Les résultats qu'il a obtenus sont indiqués dans le tableau 2.1.

Puissance	Distance (en cm)
3.8 W	56 cm
4.2 W	64 cm
4.8 W	66 cm
5.4 W	66 cm
5.9 W	69 cm
7.2 W	75 cm
18 W	81 cm

Tableau 2.1 Distance d'activation d'une carte HID iCLASS® en fonction de la puissance fournie à l'antenne.

2.2 Attaque d'espionnage

L'attaque d'espionnage est moins complexe techniquement à réaliser que l'attaque sangsue, il n'est en effet pas nécessaire d'activer le transpondeur puisque celui-ci communique avec un lecteur légitime pendant l'attaque. Ils sont également proches l'un de l'autre, typiquement à quelques centimètres, ce qui garantit un index de modulation bien supérieur à celui de l'attaque sangsue. La question est alors de savoir jusqu'à quelle distance leurs signaux respectifs peuvent être démodulés avant que le bruit externe, et le bruit interne rajouté par l'espion ne dégradent trop le SNR. Nous verrons dans un premier temps la méthode théorique de Pfeiffer et collègues [38] pour estimer la distance maximale de l'attaque. Puis nous verrons dans un second temps quelles performances ont été atteintes en pratique.

2.2.1 Limite théorique

L'article de Pfeiffer et collègues [38] pour approximer la distance maximale à laquelle il est possible d'espionner une communication ISO 14443A à 106 kb/s est très bien détaillé et

nous allons revenir ici sur la méthodologie qu'il présente. Premièrement, les auteurs calculent le BER minimum nécessaire pour espérer démoduler correctement une trame d'un certain nombre d'octets. Il en déduisent alors le SNR minimal requis pour démoduler les signaux espionnés en utilisant les équaitons suivantes :

— Pour un signal modulé en amplitude, en présence d'un bruit blanc gaussien, et avec une démodulation cohérente :

$$BER = \frac{1}{2} erfc(\frac{1}{2}\sqrt{2SNR_{HF}}) \tag{2.1}$$

— Si la démodulation est non cohérente :

$$BER = \frac{1}{2} erfc(\frac{1}{2}\sqrt{SNR_{HF}}) \tag{2.2}$$

Ainsi, pour avoir un BER de 0.01% et en supposant une démodulation cohérente, il faut un SNR de 11.4 dB minimum.

Deuxièmement, ils cherchent à estimer le bruit externe (ou bruit ambiant) en utilisant [11] comme Kfir et Wool [24] en 2005. Contrairement à ce que nous avons vu précédemment et à ce qui est dit dans l'article de Hancke [20], les auteurs ne considèrent par contre qu'une bande passante de 106 kHz pour le signal du transpondeur et non de 424 kHz, ce qui semble être une erreur. Pour déterminer à quelle distance on peut espionner le signal du lecteur il ne reste ensuite plus qu'à résoudre l'équation suivante :

$$H(r = r_{max}) = H_{min}$$

Où $H(r)$ est l'équation du champ magnétique crée par une antenne cadre magnétique à une distance r et où H_{min} désigne l'amplitude minimale du champ permettant d'avoir le SNR calculé précédemment. Dans un environnement urbain, les auteurs estiment, qu'il est possible d'espionner un lecteur à 9 m avec un BER de 0.01% si celui-ci génère un champ de 1.5 $\mathrm{A\,m^{-1}}$ à $r = 0$ avec une antenne de 3 cm de diamètre. Un lecteur avec une antenne de 7.5 cm de rayon émettant un champ de 7.5 $\mathrm{A\,m^{-1}}$ peut par contre être espionné à une distance de 700 m dans les mêmes conditions. D'autres résultats sont donnés pour différents niveaux de bruit. Il n'est pas évident de savoir à quel point les niveaux de bruit fournis par l'ITU sont valables, mais il est clair d'après ces résultats qu'il est essentiel de préciser quel est le rayon de l'antenne du lecteur et l'amplitude du champ magnétique qu'il génère lors d'une expérience d'espionnage.

Approximer la distance à laquelle le signal du transpondeur peut-être espionné est par contre plus compliqué. Il faut en effet déterminer la puissance du signal émis par celui-ci, ce qui implique une étape de modélisation et la mesure de certains paramètres physiques du transpondeur pour évaluer les paramètres du modèle. Les auteurs ont ainsi été amenés à ouvrir un transpondeur et à faire des mesures de tension pendant son fonctionnement. Nous reviendrons plus tard sur la modélisation du transpondeur, le modèle utilisé dans l'article est tiré de [12], c'est aussi celui que nous utiliserons. Ils ont alors pu déterminer pour deux valeurs différentes de champ magnétique au niveau du transpondeur, le courant parcouru dans l'antenne du transpondeur. De là, il est possible de calculer l'index de modulation du signal et donc de déduire la puissance contenue dans une bande latérale du spectre à partir de la puissance de la porteuse (émise par le lecteur). Il ne reste alors plus qu'à résoudre l'équation précédente avec $H(r) = H_{USB}(r)$ l'amplitude du champ magnétique créé par la modulation d'amplitude. La distance maximale obtenue dépend fortement de l'amplitude du champ du lecteur au niveau du transpondeur et du bruit externe. Dans un environnement urbain, pour un BER de 0.01% et en supposant un démodulateur cohérent ils obtiennent ainsi des distances de 2.1 m et 3 m pour des amplitudes de 4.5 $\mathrm{A\,m^{-1}}$ et 1.5 $\mathrm{A\,m^{-1}}$ respectivement.

Les mesures effectuées par l'équipe sur le transpondeur ainsi que leurs résultats montrent que le rayon de l'antenne du lecteur et l'amplitude du champ au niveau du transpondeur a un impact important sur l'index de la modulation d'amplitude et donc sur la distance de l'attaque d'espionnage. Cette variation de l'index de modulation dépend des caractéristiques du transpondeur (fréquence de résonance, facteur de qualité, géométrie de l'antenne...). Une expérience rigoureuse doit donc tenir compte de tous ces paramètres.

2.2.2 Performances atteintes en pratique

Les distances mesurées en pratique pour l'attaque d'espionnage varient significativement selon le matériel utilisé et les conditions de l'expérience. L'une des premières expériences d'espionnage a été conduite par le NIST en 2006 [16] [36] [37]. Un lecteur NXP Pegoda ISO 14443A ainsi que 7 transpondeurs ont été testés. Les résultats obtenus varient de 8 m à 15 m selon le modèle de transpondeur ce qui montre bien l'influence que peuvent avoir leurs caractéristiques physiques sur les performances de l'attaque. Le protocole expérimental n'est cependant pas bien précisé et le seul critère utilisé pour considérer l'attaque comme réussite est un SNR de 6 dB qui serait insuffisant pour correctement démoduler l'intégralité d'une conversation.

En 2008, Hancke [18] [20] a proposé une implémentation complète de l'attaque utilisant

un démodulateur cohérent, le matériel utilisé est le même que dans l'attaque sangsue évoquée précédemment. Il propose des mesures pour les trois normes les plus courantes de la RFID en bande HF dans deux environnements différents à l'intérieur d'un bâtiment. Pour les normes ISO 14443A et B, il obtient 1 m et 3 m, et pour ISO 15693 seulement 1 m. C'est toujours le signal du transpondeur qui limite la portée de l'attaque sauf dans le cas de la norme ISO 14443B où celui-ci a pu être démodulé à 4 m. Hancke montre donc que la norme influence bien la portée de l'attaque.

En 2011 Thevenon *et al.* [41] ont également implémenté l'attaque et rapporte une distance de 3.5 m pour un transpondeur ISO 14443. Peu d'information est donnée sur le matériel utilisé. Les auteurs font cependant remarquer qu'à l'intérieur d'un bâtiment, le signal peut potentiellement porter plus loin, car les câbles et l'armature peuvent se comporter comme des relais.

Enfin, en 2013, Diakos *et al.* [10] ont proposé une nouvelle approche pour mesurer la portée de l'attaque sur un transpondeur ISO 14443A. Plutôt que d'utiliser un lecteur et un transpondeur du commerce, ils ont fabriqué un outil émettant le signal qu'enverrait un transpondeur lors d'une communication. L'avantage de cette solution est de pouvoir contrôler la puissance de la porteuse, qui, comme nous l'avons vu, a une influence importante sur la distance maximale de l'attaque. L'antenne de réception est accordée sur 13.56 MHz, ce choix n'est pas justifié, pourtant accorder l'antenne sur une bande latérale de la modulation d'amplitude du signal semble plus approprié. L'index de la modulation est de plus choisi égal à 100%. Or lors d'une réelle communication, celui-ci est beaucoup plus faible et peu varier significativement en fonction de la distance entre le lecteur et le transpondeur. Les tests ont seulement été réalisés dans une chambre anéchoïque et les distances obtenues varient entre 20 cm et 90 cm.

2.3 Récapitulatif

Les résultats des articles revus concernant l'attaque sangsue et l'attaque d'espionnage sont résumés respectivement dans les tableaux 2.2 et 2.3. Les performances de l'attaque sangsue sont limitées par certaines difficultés techniques :

— L'index de la modulation d'amplitude est beaucoup plus faible que lors d'une communication classique entre un lecteur et un transpondeur. Le filtre de la chaîne de réception du lecteur est une importante difficulté technique.

— L'activation du transpondeur demande une puissance qui augmente rapidement avec la distance.
— Le rapport signal sur bruit de la communication est limité par le bruit émis par l'amplificateur de puissance de la porteuse du lecteur.

Le montage de Kirschenbaum et Wool [26] obtient les meilleurs résultats sans adresser le problème du filtrage de la porteuse et sans chercher à maximiser le facteur de qualité de l'antenne du lecteur, il est donc possible que de meilleures performances puissent effectivement être atteintes. Cependant, comme nous l'avons vu, il est probable que les caractéristiques d'un transpondeur influent fortement la portée de l'attaque.

Date	Norme, débit	Équipe	T/E	Distance	Scénario
2005	14443B à 106 kb/s	Kfir et Wool [24]	T	55 cm	M
2006	14443A à 106 kb/s	Kirschenbaum et Wool [26]	E	25 cm	M
2008	14443 à 106 kb/s	NXP [42]	T	30 cm	M
2011	14443B à 106 kb/s	Hancke [20]	E	20 cm/20 cm	B
2013	15693 à 46.48 kb/s	Hancke [3]	E	80 cm/5 cm	B

Tableau 2.2 Résumé des performances obtenues pour l'attaque de "skimming" à 13.56 MHz. T : Théorique, E : Expérimental. M : Monostatique, B : Bistatique. Dans le cas bistatique, la première longueur indique la distance entre l'antenne émettrice et le transpondeur, la seconde indique celle séparant l'antenne réceptrice du transpondeur.

Date	Norme, débit	Équipe	T/E	Distance
2006	14443A, 106 kb/s	NIST [16] [36] [37]	E	8-15 m
2007	14443, 106 kb/s	NXP [42]	T	3.5 m
2008	14443A, 106 kb/s 14443B 106 kb/s 15693, 26 kb/s	Hancke [18] [20]	E	3 m 3 m 1 m
2011	14443, 106 kb/s	Thevenon *et al.* [41]	E	3.5 m
2012	14443A, 106 kb/s	Pfeiffer *et al.* [38]	T	1.8-3.9 m
2013	14443A, 106 kb/s	Diakos *et al.* [10]	E	20-90 cm

Tableau 2.3 Résumé des performances de l'attaque d'espionnage à 13.56 MHz. T : Théorique, E : Expérimental.

CHAPITRE 3

OUTILS POUR LA MODÉLISATION D'UN SYSTÈME DE RFID EN BANDE HF

Pour construire un modèle théorique de l'attaque sangsue nous avons dans un premier temps cherché dans la littérature les outils pertinents pour modéliser les différents composants d'un système lecteur-transpondeur. Dans un premier temps, nous rappellerons les principes physiques qui interviennent dans la RFID en bande HF. Nous rappellerons, dans un second temps, quelles sont les normes les plus courantes de la RFID, quelles techniques de modulation et de codage des symboles elles utilisent, et quelle est l'occupation du spectre des signaux du lecteur et du transpondeur. Dans un troisième temps, nous expliquerons comment sont modélisés les transpondeurs HF dans la littérature. Nous verrons alors comment fonctionne un lecteur RFID. Enfin, nous verrons quels ordres de grandeur sont disponibles pour le bruit magnétique ambiant dans la bande HF.

3.1 Principes physiques de la RFID en bande HF

Dans cette section, nous allons rappeler les principes de la physique qui interviennent en RFID et nous énoncerons les équations dont nous aurons besoin dans notre modèle. Nous rappellerons d'abord comment s'écrit la loi de Faraday. Nous verrons ensuite comment est calculée l'inductance propre d'une spire de courant. Enfin, nous donnerons les méthodes de calcul disponibles pour calculer l'induction mutuelle entre deux spires de courant.

3.1.1 Loi de Faraday

Quand un circuit électrique C est soumis à un champ magnétique variable $\mathbf{H}$, il apparaît en son sein une force électromotrice e susceptible d'engendrer un courant électrique. La loi permettant de quantifier cette force en fonction du flux ϕ du champ magnétique traversant le circuit s'appelle la loi de Faraday. Elle s'écrit comme suit :

$$e = -\frac{\mathrm{d}\phi}{\mathrm{d}t} \tag{3.1}$$

Où le flux ϕ s'exprime en fonction du champ magnétique $\mathbf{H}$ comme suit :

$$\phi = -\oiint_C \mathbf{H} \cdot \mathrm{d}\mathbf{s} \tag{3.2}$$

3.1.2 Auto-induction

Une boucle parcourue par un courant I provoque en son sein une force électromotrice $e = -L\frac{\mathrm{d}I}{\mathrm{d}t}$ qui est auto induite. La formule suivante permet de calculer approximativement l'auto-inductance d'une boucle de N tours, de rayon R et ayant une section de rayon r [12].

$$L = N^2 \mu_0 R(\ln(\frac{8R}{r}) - 2) \tag{3.3}$$

Plus le nombre de tours est important, plus cette relation est approximative.

3.1.3 Induction mutuelle

Considérons maintenant deux spires B_1 et B_2 ayant respectivement les rayons r_1 et r_2, les surfaces S_1 et S_2 et enfin les nombres de tours N_1 et N_2. Appelons également d la distance les séparant. On suppose par ailleurs que B_1 est parcourue par un courant I_1. La situation est représentée sur la figure 3.1.

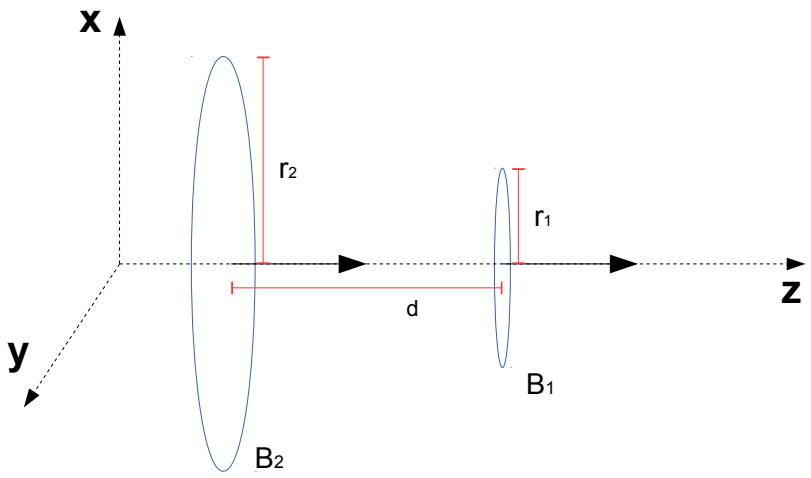

Figure 3.1 Positions des boucles B_1 et B_2.

La boucle B_2 génère un champ proche magnétique dont l'amplitude sur son axe peut être dérivée en appliquant la formule de Biot et Savart :

$$|H_z(d)| = \frac{I_1 N_2 r_2^2}{2\sqrt{(r_2^2 + d^2)^3}} \tag{3.4}$$

Cependant, pour une longueur $2\pi N_1 R$ de même ordre de grandeur que la longueur d'onde du courant qui la parcourt, on ne peut plus le considérer comme constant dans toute la boucle.

Autrement dit, l'approximation des régimes quasi stationnaires (ARQS) n'est plus valable. Un article de Wim Aerts *et al.* [1] donne une expression du module de H_z tenant compte de ce phénomène :

$$|H_z(d)| = \frac{I_1 r_2 \lambda \sqrt{2(1-\cos(\beta r_2))}}{8\pi^2 \sqrt{(r_2^2+d^2)^3}} \left| \sum_{n=0}^{N_2-1} e^{j\beta n r_2} \right| \tag{3.5}$$

Où $\lambda = \frac{c}{f_0}$, $\beta = \frac{4\pi^2}{\lambda}$, avec f_0 la fréquence du courant parcourant l'antenne, c'est-à-dire, la fréquence de la porteuse dans le cas de la RFID. En faisant le développement limité de l'expression précédente à l'ordre 2 quand βr_2 tend vers 0, on retrouve bien l'expression 3.4.

En supposant le champ émis par B_2 uniforme au niveau de B_1 et le courant constant dans B_2, on peut approximer la force électromotrice induite dans B_1 en appliquant la loi de Faraday :

$$e = -\frac{d\phi_{21}}{dt} = -\mu_0 N_1 \pi r_1^2 \frac{\mathrm{d}H_z}{\mathrm{d}t} = -\frac{\mu_0 \pi N_1 N_2 (r_1 r_2)^2}{2\sqrt{(r_2^2+d^2)^3}} \frac{\mathrm{d}I_1}{\mathrm{d}t} \tag{3.6}$$

La force électromotrice dans B_2 est ainsi proportionnelle à la dérivée du courant circulant dans B_1. Le coefficient de proportionnalité s'appelle le coefficient d'inductance mutuelle M_{12}. Le théorème de Neumann permet de démontrer qu'en réalité $M_{12} = M_{21} = M$, on utilisera donc M pour désigner dans la suite l'inductance mutuelle entre les deux boucles.

Ainsi, pour deux boucles de rayon r_2 et r_1 sur un même axe en supposant $r_2 \gg r_1$ et dans l'ARQS on a donc :

$$M = \frac{\mu_0 \pi N_1 N_2 (r_1 r_2)^2}{2\sqrt{(r_2^2+d^2)^3}} \tag{3.7}$$

Dans le cas où on ne peut plus supposer le courant constant dans B_2, l'expression de e devient :

$$e = \frac{\mu_0 \pi r_1^2 N_2 r_2 \lambda \sqrt{2(1-\cos(\beta r_2))}}{8\pi^2 \sqrt{(r_2^2+d^2)^3}} \left| \sum_{n=0}^{N_2-1} e^{j\beta n r_2} \right| \frac{dI_1}{dt} \tag{3.8}$$

Ainsi, pour deux boucles de rayon r_1 et r_2 sur un même axe en supposant $r_2 \gg r_1$ et quand l'ARQS n'est plus valable dans la grande boucle :

$$M = \frac{\mu_0 N_2 r_1^2 r_2 \lambda \sqrt{2(1-\cos(\beta r_2))}}{8\pi \sqrt{(r_2^2+d^2)^3}} \left| \sum_{n=0}^{N_2-1} e^{j\beta n r_2} \right| \tag{3.9}$$

Dans le cas général, quand l'ARQS est valable, le coefficient d'inductance mutuelle entre deux circuits C_1 et C_2 est calculé avec la formule de Neumann [9] :

$$M = \frac{\mu_0}{4\pi} \iint \frac{\mathbf{ds} \cdot \mathbf{ds}'}{r} \tag{3.10}$$

ds et **ds**′ étant des vecteurs élémentaires séparés par la distance r qu'on déplace le long de C_1 et C_2.

On définit également le coefficient k de couplage mutuel entre deux circuits d'inductances L_1 et L_2 par :

$$0 \leq k \leq 1\,; \quad k = \frac{M}{\sqrt{L_1 L_2}} \tag{3.11}$$

3.2 Normes de RFID en bande HF

Pour les transpondeurs fonctionnant dans la bande HF, les normes les plus courantes sont ISO/IEC 14443 type A, ISO/IEC 14443 type B, ISO/IEC 15693. Certaines entreprises n'implémentent pas complètement ces normes et/ou les modifient pour leurs solutions propriétaires. C'est le cas de certaines cartes MIFARE de NXP – qui sont les plus répandues au monde avec environ 3.5 milliards de transpondeurs en circulation – ou des cartes iCLASS® de HID.

Nous verrons ici en particulier quelle est l'occupation du spectre pour ces différentes normes. Or il est surprenant de voir des réponses différentes dans la littérature à ce sujet. Par exemple pour la communication du transpondeur vers le lecteur pour la norme ISO 14443 type A à 106 kb/s, l'article de Hancke [20] nous dit que la bande passante consommée est de 424 kHz, mais l'article de Pfeiffer [38] indique seulement 106 kHz, tout comme le livre "RFID and the Internet of Things" [4]. Il convient donc de clarifier deux points pour comprendre ces écarts. Premièrement, il faut distinguer bande passante pour un signal en bande de base et bande passante pour un signal modulé. Un signal ayant une bande passante B en bande de base verra celle-ci doubler après modulation. En effet, en bande de base la définition courante de bande passante ne tient compte que des fréquences positives, or après modulation le spectre du signal est translaté autour de la porteuse avec à gauche de celle-ci le spectre auparavant situé à des fréquences négatives. Deuxièmement, pour une modulation ASK avec un temps symbole T_s et une porteuse de fréquence F_0, la bande passante minimale requise est de $\frac{1}{T_s}$ mais si on regarde le lobe principal de la DSP du signal modulé, celui-ci s'étend de $F_0 - \frac{1}{T_s}$ à $F_0 + \frac{1}{T_s}$, d'où une bande passante de $\frac{2}{T_s}$.

Les choses se compliquent quand on cherche à savoir si la bande passante minimale est suffisante pour communiquer avec un transpondeur. En effet, plus la bande passante de l'antenne du lecteur est étroite, plus le régime transitoire présent au moment d'un changement d'état du signal émis sera long. Or les normes de la RFID précisent la durée maximale de ces régimes transitoires. On peut donc réduire la bande passante requise aussi longtemps que ceux-ci respectent la norme. Il est également possible que les transpondeurs soient plus laxistes que les normes qu'ils supportent.

Dans la suite, on ne parlera que de bande passante de signaux modulés (et non en bande de base), et les largeurs de bande indiquées correspondront au premier lobe autour de la porteuse ou de la sous-porteuse. On notera de plus f_0 la fréquence de la porteuse (13.56 MHz dans le cas d'un lecteur "normal").

3.2.1 ISO/IEC 14443 type B

Quatre débits différents sont supportés par la norme, 106 kb/s ($f_0/128$), 212 kb/s ($f_0/64$), 424 kb/s ($f_0/32$), 848 kb/s ($f_0/16$) [22]. La norme prévoit qu'un transpondeur peut fonctionner correctement en étant soumis à champ magnétique compris entre 1.5 A/m et 7.5 A/m (rms) [22].

Le lecteur communique avec la carte en utilisant une modulation ASK avec un index de 10%, les bits sont codés avec un code NRZ. La largeur du premier lobe autour de la porteuse est alors égale à deux fois le débit utilisé, soit par exemple 212 kHz à 106 kb/s. Un pic important est présent à 0 Hz, il correspond à la composante continue du signal qui est élevée puisque l'index de modulation n'est que de 10%.

Pour communiquer, le transpondeur génère une sous-porteuse de fréquence 848 kHz ($f_0/16$). Deux pics sont alors présents autour de la porteuse à $f_0 - f_0/16 = 12.71$ MHz et $f_0 + f_0/16 = 14.40$ MHz. La sous-porteuse est modulée par les bits à transmettre en utilisant une modulation BPSK et un code NRZ-L. Par conséquent, la largeur du premier lobe autour de la sous-porteuse est égale au double du débit symbole, soit par exemple 212 kHz à 106 kb/s.

3.2.2 ISO/IEC 14443 type A

Comme pour la norme 14443 type B, quatre débits différents sont supportés : 106 kb/s ($f_0/128$), 212 kb/s ($f_0/64$), 424 kb/s ($f_0/32$), 848 kb/s ($f_0/16$) [22].

Le lecteur communique avec la carte en utilisant une modulation de la porteuse ASK 100% à 106 kb/s et inférieure à 100% pour les débits supérieurs. Les bits sont codés avec un code de Miller modifié détaillé dans la norme [22] : le principe est de coder les bits avec des impulsions d'une durée d'environ 5/16 de la durée d'un symbole. C'est la position du pulse durant le symbole qui code le bit, un pulse en deuxième moitié de symbole code un 1 et un pulse en début de symbole ou pas de pulse du tout code un 0. Par exemple, à 106 kb/s, le pulse dur environ 3 µs. Le premier lobe autour de la porteuse est donc large de $2\frac{16}{5}D$, avec D le débit utilisé. À 106 kb/s, le premier lobe occupe donc 660 kHz.

Les transpondeurs de type A génèrent également une sous-porteuse de fréquence $f_0/16 =$ 848 kHz. Celle-ci est alors modulée par les bits à transmettre. À 106 kb/s, une modulation ASK et un code Manchester sont utilisés. Le premier lobe autour de la sous-porteuse est donc large de $f_0/32 = 424$ kHz, le code Manchester ayant pour effet de doubler la bande passante consommée. Par contre, pour les débits supérieurs le même principe de modulation et de codage des bits que pour les transpondeurs de type B est utilisé.

3.2.3 ISO/IEC 15693

Deux débits sont supportés : 26.48 kb/s ($f_0/512$) et 6.62 kb/s ($f_0/2048$). La norme prévoit qu'un transpondeur doit pouvoir fonctionner correctement en étant soumis à un champ magnétique compris entre 150 mA/m et 5 A/m (rms) [21]. Nous ne nous intéresserons qu'au débit de 26.48 kb/s.

À 26.48 kb/s, le lecteur communique avec la carte en utilisant un code PPM ("Pulse Position Modulation") avec un alphabet de 2^2 transitions. Les bits sont donc transmis deux par deux. Un pulse a une durée de 9.44 µs ($128/f_0$). Une modulation ASK de la porteuse avec un index de 10% ou 100% est utilisée, le choix de l'index est laissé au lecteur. Le premier lobe autour de la porteuse a donc une largeur de 106 kHz.

Le transpondeur communique avec le lecteur en utilisant soit une modulation FSK, soit une modulation ASK. Nous ne parlerons que de cette deuxième option. Dans ce cas, une sous porteuse de 424 kHz est utilisée et les bits sont codés avec un code Manchester. Le premier

lobe autour de la sous-porteuse est alors large de 106 kHz. Celui-ci est répété deux fois autour de 13.4 MHz et 14.0 MHz.

	Lecteur		Transpondeur	
	Modulation	Codage	Modulation	Codage
ISO 14443 A	ASK	Miller modifié	ASK ou BPSK	Manchester ou NRZ-L
ISO 14443 B	ASK	NRZ	BPSK	NRZ-L
ISO 15693	ASK	PPM	ASK ou FSK	Manchester

Tableau 3.1 Recapitulatif du fonctionnement des normes de la RFID en bande HF.

3.3 Modélisation d'un transpondeur HF

Comme nous l'avons précédemment expliqué, la plupart des transpondeurs HF passifs fonctionnent en utilisant le principe de la modulation de charge. Pour communiquer avec le lecteur, ils utilisent l'énergie fournie par la porteuse du lecteur pour faire commuter une résistance dite "de modulation" en fonction des bits à transmettre. Cependant, il existe également des transpondeurs fonctionnant en faisant commuter un condensateur, nous ne considérerons ici que ce premier type de transpondeurs.

3.3.1 Justification du modèle

En regardant à l'intérieur d'un transpondeur, on peut observer deux éléments principaux directement connectés l'un sur l'autre : une antenne cadre de plusieurs tours reliées à un circuit intégré. Le circuit intégré contient l'électronique du transpondeur. En entrée de celui-ci, on trouve un pont redresseur suivi d'un régulateur chargé de fournir une tension continue constante qui alimente les circuits logiques du transpondeur. La résistance de modulation peut se trouver en amont ou bien en aval du régulateur. Dans le premier cas, l'antenne est court-circuitée et le transpondeur ne peut pas utiliser la porteuse du lecteur comme horloge pour fonctionner, cette solution est donc réservée aux transpondeurs contenant une horloge interne. Dans, les deux cas, on peut modéliser le circuit intégré par une impédance comprenant une charge R_L en parallèle avec un condensateur C_{IC}.

L'antenne cadre du transpondeur se comporte comme un circuit RLC résonant. Les boucles de l'antenne forment une inductance L_1 avec des pertes R_1 avec en parallèle une capacité [1] parasite C_c créée par effet de proximité entre les tours. Le plastique qui enveloppe

1. Le terme "capacité" est utilisé au sens de capacitance.

l'antenne introduit également une capacité parasite C_{pack} [34]. On notera N_1 le nombre de tours de l'antenne et r_1 son rayon moyen.

Enfin, la connexion entre l'antenne et le circuit intégré introduit une capacité C_{con} et une résistance R_{con} parasites faibles. Le modèle ainsi obtenu pour le transpondeur est montré sur la figure 3.2. Les ordres de grandeur des différents composants sont tirés d'un document de référence de NXP [34].

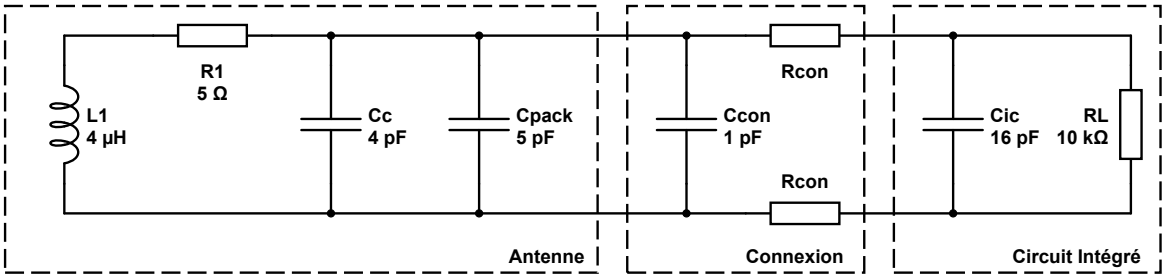

Figure 3.2 Modèle utilisé pour un transpondeur utilisant la modulation de charge.

En négligeant R_{con} qui est en général inférieure à 1 Ohm, on peut regrouper toutes les capacités parasites ainsi que la capacité d'entrée du circuit intégré en une seule et unique capacité C_1, le modèle ainsi simplifié est montré sur la figure 3.3. Ce modèle est par ailleurs utilisé partout dans la littérature sur la RFID [12] [46] [33] [38] [14].

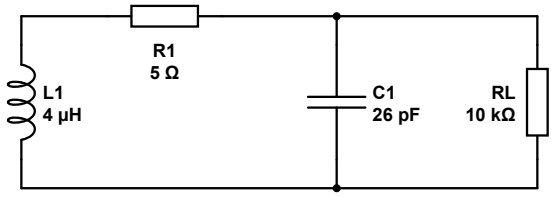

Figure 3.3 Modèle utilisé pour un transpondeur HF. Un ordre de grandeur des composants est indiqué à titre d'exemple.

Le transpondeur se comporte donc comme un circuit résonant, on notera ω_t sa fréquence de résonance qui est approximée par la relation suivante :

$$\omega_t \approx \frac{1}{\sqrt{L_1 C_1}} \tag{3.12}$$

On définit également les notations suivantes :

— Le facteur de qualité série : $Q_s = \frac{\omega_t L_1}{R_1}$
— Le facteur de qualité parallèle : $Q_p = \frac{R_L}{\omega_t L_1}$
— Et le facteur de qualité du transpondeur : $Q_t = \frac{1}{\frac{1}{Q_s}+\frac{1}{Q_p}} = \frac{1}{\frac{R_1}{\omega_t L_1}+\frac{\omega_t L_1}{R_L}}$

Les deux paramètres R_L et C_{IC} varient avec l'amplitude du champ magnétique H qui traverse l'antenne. Les variations de C_{IC}, mesurées par exemple dans [15] et [17] sont relativement faibles, on le supposera donc constant. Les variations de R_L ne sont par contre absolument pas négligeables. En effet, plus le champ magnétique qui alimente le transpondeur est fort, plus le régulateur du transpondeur fait baisser sa résistance d'entrée afin de maintenir constante la tension d'alimentation de l'électronique du transpondeur. R_L et Q_t diminuent donc quand H augmente.

On notera Q_{max} (resp. Q_{min}) le facteur de qualité du transpondeur quand la résistance de commutation est connectée (resp. déconnectée). Par défaut – quand le transpondeur ne communique pas – cette résistance est déconnectée [14] et Q_t est donc égale à Q_{max}. Au moment où celle-ci commute, Q_t décroit rapidement pour atteindre Q_{min}. Pour les transpondeurs ayant une résistance de modulation directement connectée à l'antenne, $Q_{min} = 0$, pour les autres, le ratio $\frac{Q_{min}}{Q_{max}}$ peut varier de 0.1 à 0.7 en fonction du transpondeur et de l'amplitude du champ H [46] [38] : plus H augmente, plus ce ratio se rapproche de 1.

Pour fonctionner, le transpondeur a besoin qu'une tension minimale V_{min} (en Volt efficace) soit atteinte aux bornes de son circuit intégré (c'est-à-dire aux bornes de R_L), on notera H_{min} l'amplitude du champ magnétique qui permet d'atteindre cette tension et Q_{max_0} le facteur de qualité correspondant. Avec nos notations, quand $H = H_{min}$, alors $Q_{max} = Q_{max_0}$ et $Q_{min} = Q_{min_0}$ et quand $H > H_{min}$, alors $Q_{max} < Q_{max_0}$ et $Q_{min} < Q_{min_0}$.

3.3.2 Impédance transformée

Quand un lecteur est à proximité du transpondeur, celui-ci induit une source de tension e_1 en série avec L_1 qui dépend du coefficient de couplage mutuel entre les deux antennes et du courant qui parcourt l'antenne du lecteur. Cette situation est représentée sur la figure 3.4.

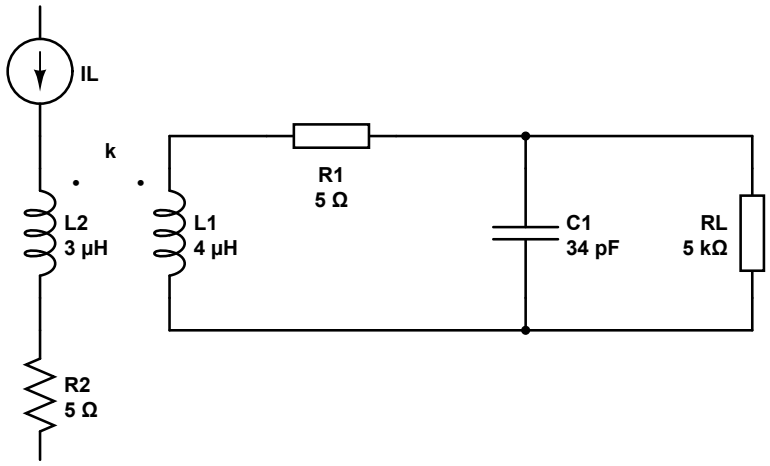

Figure 3.4 Couplage du transpondeur avec une boucle parcourue par un courant I_L.

On peut calculer le courant I_t dans l'antenne du transpondeur en fonction de e_1 :

$$e_1 = (jL_1\omega + R_1 + \frac{1}{\frac{1}{R_L} + jC_1\omega})I_t$$

En utilisant 3.7, on peut exprimer le courant I_t en fonction du courant dans l'antenne du lecteur I_l.

$$e_1 = jM\omega I_l = (jL_1\omega + R_1 + \frac{1}{\frac{1}{R_L} + jC_1\omega})I_t$$

$$I_t = \frac{jM\omega}{jL_1\omega + R_1 + \frac{1}{\frac{1}{R_L}+jC_1\omega}} I_l$$

Côté lecteur, le courant I_t entraîne également l'apparition d'une source de tension dépendante de M.

$$e_2 = jM\omega I_t = \frac{M^2\omega^2}{jL_1\omega + R_1 + \frac{1}{\frac{1}{R_L}+jC_1\omega}} I_l$$

e_2 est finalement proportionnel à I_l, l'influence du transpondeur peut être vu comme l'apparition d'une impédance Z_t en série avec l'inductance de l'antenne du lecteur.

$$Z_t = \frac{M^2\omega^2}{jL_1\omega + R_1 + \frac{1}{\frac{1}{R_L}+jC_1\omega}} \tag{3.13}$$

3.3.3 Simplification de l'impédance transformée

Dans le cas où $R_1 \ll R_L$ et $Q_p \ll Q_s$, on peut approximer Z_t de la manière suivante [46] :

$$Z_t \approx \widehat{Z}_t = \frac{1 + jQ_t\frac{\omega}{\omega_t}}{Q_t(\frac{\omega_t}{\omega} - \frac{\omega}{\omega_t}) + j} k^2 \omega L_2 \tag{3.14}$$

3.3.4 Relation entre le champ magnétique et la tension aux bornes du circuit intégré

Nous allons ici exprimer la relation entre l'amplitude du champ magnétique traversant l'antenne du transpondeur et la tension aux bornes de son circuit intégré. En appliquant la loi de Faraday, on peut exprimer l'amplitude de la source de tension e induite dans l'antenne en fonction de H :

$$e = \mu_0 \omega N_1 \pi r^2 H \tag{3.15}$$

On passe de la tension e, à la tension V aux bornes du circuit intégré du transpondeur avec un pont diviseur de tension faisant intervenir d'une part l'impédance de la l'antenne Z_A , modélisée – comme précédemment expliqué – par une inductance L_1 en série avec une résistance R_1 et d'autre part, l'impédance Z_{IC} du circuit intégré qui correspond à la capacité C_1 en parallèle avec la charge R_L.

$$\begin{aligned}
e &= |1 + \frac{Z_A}{Z_{IC}}|V \\
&= |1 + \frac{R_1}{R_L} - L_1 C_1 \omega^2 + j(\frac{L_1 \omega}{R_L} + R_1 C_1 \omega)|V \\
&= |1 + \frac{R_1}{R_L} - \frac{\omega^2}{\omega_t^2} + j(\frac{\omega}{Q_p \omega_t} + \frac{\omega}{Q_s \omega_t})|V \\
&= |1 + \frac{R_1}{R_L} - \frac{\omega^2}{\omega_t^2} + j\frac{1}{Q_t}\frac{\omega}{\omega_t}|V
\end{aligned}$$

En négligeant $\frac{R_1}{R_L}$, on trouve alors :

$$e = \sqrt{(1 - \frac{\omega^2}{\omega_t^2})^2 + \frac{1}{Q_t^2}\frac{\omega^2}{\omega_t^2}}V \tag{3.16}$$

Finalement :

$$H = \frac{\sqrt{(1 - \frac{\omega^2}{\omega_t^2})^2 + \frac{1}{Q_t^2}\frac{\omega^2}{\omega_t^2}}}{\mu_0 \omega N_1 \pi r^2} V \tag{3.17}$$

À partir de la tension V_{min} d'activation d'un transpondeur, on peut donc déterminer le champ H_{min} :

$$H_{min} = \frac{\sqrt{(1 - \frac{\omega^2}{\omega_t^2})^2 + \frac{1}{Q_{max_0}^2}\frac{\omega^2}{\omega_t^2}}}{\mu_0 \omega N_1 \pi r^2} V_{min} \tag{3.18}$$

3.3.5 Extrapolation de Q_t pour $H > H_{min}$

Pour estimer la distance maximale à laquelle il est possible de communiquer avec un transpondeur, nous verrons que la connaissance de Q_{max_0} ne suffit pas, il faut donc un moyen d'estimer comment Q_{max} décroît quand H augmente. L'article [46] de Wobak *et al.* donne une solution qui consiste à supposer V constant et égale à V_{min} dès que le transpondeur est activé. On peut alors exprimer Q_{max} en fonction de H à partir de l'expression 3.17 :

$$Q_{max} = \frac{1}{\frac{\omega_t}{\omega}\sqrt{(\mu_0 \omega N_1 \pi r^2)^2 \frac{H^2}{V_{min}^2} - (1 - \frac{\omega^2}{\omega_t^2})^2}} \tag{3.19}$$

3.3.6 Valeurs typiques des paramètres du modèle du transpondeur

Le modèle présenté précédemment n'a d'utilité qu'à condition de connaître les ordres de grandeur de ses différents paramètres. Récapitulons dans un premier temps ces paramètres :

- Fréquence de résonnance $f_t = 2\pi\omega_t$
- Les facteurs de qualité Q_{max_0} et Q_{min_0}
- Tension seuil V_{min} requise aux bornes du circuit intégré du transpondeur pour l'activer
- Inductance L_1 de l'antenne
- Géométrie de l'antenne : nombre de tours N_1 et rayon moyen r_1

Nous verrons que les différents paramètres du modèle peuvent varier significativement d'un transpondeur à l'autre, nous ne garderons donc que quelques jeux de valeurs afin de limiter les cas de figure. Un corollaire de cette information est qu'il n'est pas possible de concevoir un lecteur malicieux qui aura les mêmes performances avec tous les transpondeurs. Ainsi, en nous appuyant sur un document fourni par NXP [34] nous établirons deux jeux de paramètres pour les transpondeurs MIFARE. Un article de Gebhart *et al.* [15] nous permettra d'étaler un jeu de paramètres pour un transpondeur basé sur une smartcard. Un troisième jeu de paramètres pour un transpondeur ISO 14443 sera enfin présenté à partir d'un article de Zangl *et al.* [47]. Finalement, nous nous intéresserons à l'écart-type entre les paramètres du modèle en utilisant, en plus des références citées précédemment, un article de Henry P

Romero *et al.* [39].

Tous les ordres de grandeur de paramètres trouvés ici concernent des transpondeurs ISO 14443 type A. La norme ISO 14443 type B étant très similaire, nous supposerons que ceux-ci sont aussi applicables à cette deuxième norme. Nous n'avons par contre pas pu trouver de valeurs typiques pour les paramètres d'un transpondeur ISO 15693.

Le document [34] fourni par NXP est destiné aux fabricants de transpondeurs HF qui désirent produire des cartes MIFARE. Il a vocation à indiquer comment choisir les paramètres de l'antenne afin que le transpondeur puisse passer la spécification MIFARE. Un des critères qui nous intéresse est que la fréquence de résonance d'un transpondeur doit être comprise entre 14.5 MHz et 18.5 MHz. Même pour un transpondeur MIFARE, f_t peut donc varier significativement d'un fabricant à l'autre.

Deux exemples d'antennes respectant les spécifications sont donnés en exemple ainsi que les caractéristiques des circuits intégrés vendus par NXP. À partir de ces deux exemples, on peut établir deux jeux de paramètres pour le modèle du transpondeur ainsi que l'incertitude sur la fréquence de résonance f_t.

Pour chaque exemple, le document récapitule toutes les capacités qui interviennent dans le calcul de C_1. Celles-ci sont récapitulées ci-après pour le premier exemple :

— Capacité introduite par le plastique autour de l'antenne $C_{pack} = 5.3\ pF \pm 5\%$
— Capacité d'entrée du circuit intégré de la carte MIFARE, il s'agit d'une valeur typique, mais en pratique C_{IC} varie avec la tension appliquée à la puce. Valeur typique : $C_{IC} = 16.1\ pF$
— L'antenne ne se comporte pas comme une inductance pure. $C_c = 3.6\ pF \pm 3\%$.
— Capacité parasite introduite pas la connexion de l'antenne au circuit intégré. $C_{Con} = 0.5 - 2\ pF$.

C_1 est calculé en sommant ces quatre capacités :

$$C_1 = C_{pack} + C_{IC} + C_c + C_{Con} \tag{3.20}$$

Le tableau 3.2 récapitule les deux jeux de paramètres obtenus.

	Modèle 1		Modèle 2	
Paramètre	Valeur	Incertitude	Valeur	Incertitude
N_1	4	-	4	-
r_1 (mm)	33	-	33	-
L_1 (µH)	3.6	3%	3.65	1%
C_1 (pF)	26	4%	27	8%
R_1 (Ω)	6	4%	6.3	4%
R_L (kΩ)	15	-	15	-
V_{min} (V_{RMS})	2	-	2	-
f_t (MHz)	16.4	15.6 - 17.3	16.1	15.4 - 16.9
Q_{max_0}	25	-	24	-

Tableau 3.2 Paramètres des deux transpondeurs MIFARE.

L'article de Gebhart *et al.* [15] présente une méthode permettant de caractériser l'impédance d'entrée du circuit intégré d'un transpondeur. Il fournit un tableau récapitulatif de leurs mesures pour un transpondeur contenant un smartcard. La fréquence de résonance naturelle – c'est-à-dire la fréquence de résonance du transpondeur quand le couplage est faible – n'y est pas précisée, mais les courbes de H en fonction de f_0 indiquent que celle-ci est voisine de 13.56 MHz. L'article indique que le facteur de qualité est proche de zéro quand la résistance de modulation est connectée, ce qui semble indiquer que celle-ci se trouve en amont du régulateur. On prendra donc $Q_{min} \approx 0$. Le tableau 3.3 récapitule les paramètres obtenus.

Paramètre	Valeur
N_1	3.8
r_1 (mm)	21
L_1 (µH)	1.86
C_1 (pF)	75
R_1 (Ω)	1.7
R_L (kΩ)	1.5
V_{min} (V_{RMS})	2.7
f_t (MHz)	13.7
Q_{max_0}	8.5
Q_{min}	0

Tableau 3.3 Paramètres de la smartcard.

L'article de Zangl *et al.* [47] fournit l'ensemble des paramètres du modèle pour un transpondeur ISO 14443 pour deux amplitudes du champ magnétique H. Notons que ces ampli-

tudes sont probablement supérieures au champ H_{min}. Les facteurs de qualités mesurés (Q_{max} et Q_{min} à 1.5 et 4.5 $\mathrm{A\,m^{-1}}$) sont donc sans doute inférieurs à Q_{max_0} et Q_{min_0}. Les mesures de l'équipe sont récapitulées dans le tableau 3.4.

Paramètres	1.5 A/m	4.5 A/m
N_1	7	7
r_1 (mm)	29	29
C_1 (pF)	28	28
L_1 (µH)	4	4
R_1 (Ω)	3	3
R_L (Ω)	426 - 175	169 - 117
U (V_{RMS})	3.50 - 1.48	4.29 - 2.98
f_t (MHz)	15	15
Q_{max}	1.12	0.45
Q_{min}	0.46	0.31

Tableau 3.4 Paramètres mesurés par Pfeiffer *et al.* pour un transpondeur ISO 14443 type A.

3.4 Fonctionnement d'un lecteur RFID

Comme tout système de télécommunication, un lecteur RFID comprend une chaîne d'émission et une chaîne de réception. La chaîne d'émission permet d'injecter du courant dans l'antenne du lecteur et de le moduler afin d'activer et de communiquer avec le transpondeur. La chaîne de réception se charge de filtrer la porteuse émise en permanence par le lecteur afin d'extraire le signal du transpondeur quand celui-ci transmet.

La plupart des lecteurs RFID fonctionnent alors comme représenté sur le schéma 3.5 [12] :

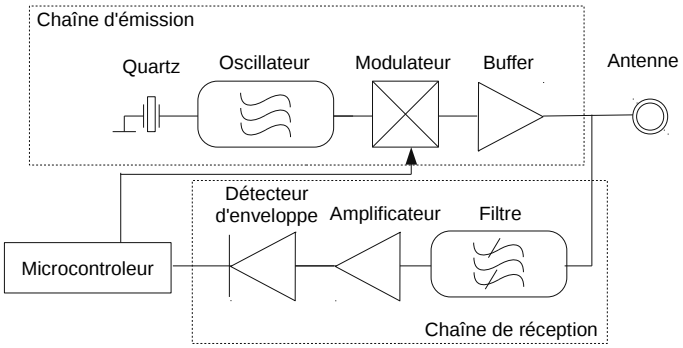

Figure 3.5 Architecture d'un lecteur RFID [12].

Le schéma 3.5 est tiré de [12] mais on peut le retrouver sous des formes similaires dans d'autres articles comme [5] ou [25]. Essentiellement, la chaîne de réception contient toujours un filtre pour sélectionner la réponse du transpondeur dans le spectre du signal présent aux bornes de l'antenne. Ce signal et ensuite amplifié et ramener en bande de base à l'aide d'un détecteur d'enveloppe. La chaîne d'émission permet d'émettre la porteuse qui alimente le transpondeur et de la moduler quand le lecteur transmet.

L'antenne du lecteur est toujours une antenne cadre magnétique. La façon d'injecter du courant dans celle-ci peut par contre varier. L'article de [1] donne deux façons de procéder : soit en utilisant un réseau RLC passif, soit de manière active avec un amplificateur. L'article se concentre sur la première méthode dont le but est d'obtenir dans la boucle une résonance en courant : pour former un circuit d'accord passif, plusieurs topologies sont possibles, mais dans tous les cas, l'antenne et son circuit doivent former un réseau RLC résonant. On peut par exemple :

- ajouter une capacité en série avec l'inductance formée par l'antenne et obtenir un réseau RLC série
- ajouter une capacité en parallèle, on forme alors un réseau RLC parallèle
- ajouter une capacité en parallèle puis une en série, l'ensemble forme un réseau en L
- ajouter une capacité en série, puis une en parallèle

La topologie choisie ne change rien aux performances du lecteur, mais conditionne le choix de l'amplificateur qui alimente l'ensemble ainsi que la fabrication de l'antenne. Le réseau en L peut par exemple être accordé à 50 Ω, et l'antenne peut ainsi être alimentée avec un amplificateur standard adapté à cette impédance. Il permet également d'ajouter une ligne de transmission entre la sortie de l'amplificateur et l'antenne. C'est le choix qui semble le plus courant dans l'industrie : on peut par exemple citer les lecteurs fabriqués par SCEMTEC, le MIFARE Pegoda MF RD 700 utilisé par [1], le TRF7960 de TI, ou encore les chipsets vendus par NXP comme le PN532.

Les figures 3.6 et 3.7 illustrent les cas du circuit RLC série et du réseau en L. L'antenne est représentée par l'inductance L_2 en série avec une résistance R_2. R_2 permet de tenir compte de la résistance équivalente série de l'inductance, de la résistance de radiation (de l'ordre de 0.1 Ω pour une antenne cadre magnétique), et d'une éventuelle résistance ajoutée pour abaisser le facteur de qualité de l'antenne. Les capacités C_2, C_s et C_p représentent les capacités d'accord des deux réseaux. Sur les deux figures, la tension U indique la tension en entrée de la chaîne de réception du lecteur, elle doit être filtrée et amplifiée afin d'extraire le signal du transpondeur. La tension E représente la tension de sortie de l'amplificateur qui

alimente l'antenne.

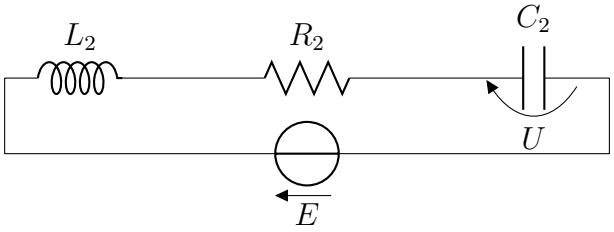

Figure 3.6 Antenne accordée avec une capacité série.

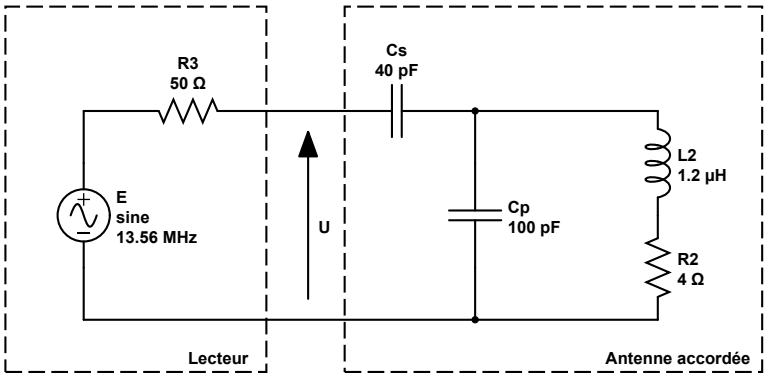

Figure 3.7 Antenne accordée avec un réseau en L.

Dans le cas de la RFID, on définit la bande passante de l'antenne comme l'ensemble des fréquences pour lesquelles le courant $I(\omega)$ dans L_2 est supérieur à -3 dB de sa valeur maximale. Autrement dit, en notant $\omega_0 = 2\pi f_0$ la pulsation de résonance de l'antenne accordée, $\Delta\omega = |\omega_1 - \omega_2|$ où ω_1 et ω_2 sont solutions de $I(\omega) = \frac{I(\omega_0)}{\sqrt{2}}$. On peut alors définir le facteur de qualité Q_a comme suit :

$$Q_a = \frac{\omega_0}{|\omega_1 - \omega_2|} \tag{3.21}$$

On définit par ailleurs le facteur de qualité Q_b comme suit :

$$Q_b = \frac{\omega_0 L_2}{R_2} \tag{3.22}$$

On peut alors montrer que dans le cas du circuit RLC série, $Q_a = Q_b$ et dans le cas du réseau en L, $Q_b = 2Q_a$. Avec ce second réseau d'accord, la résistance R_2 est donc deux fois plus faible à bande passante égale, les pertes par effet joule sont cependant les mêmes dans les deux circuits, car pour un réseau en L, il faut tenir compte de la puissance dissipée dans

la résistance de sortie R_3 de l'amplificateur de puissance.

3.5 Bruit électromagnétique ambiant dans la bande HF

Comme nous l'avons vu précédemment, une des sources de bruit limitant le rapport signal sur bruit de la communication entre un lecteur et un transpondeur – et donc la distance de l'attaque sangsue – est le bruit électromagnétique ambiant (appelé bruit EM dans la suite). Il est donc nécessaire de déterminer un ordre de grandeur du bruit électromagnétique ambiant dans les environnements où cette attaque peut se produire. Nous verrons que des ordres de grandeur du bruit EM sont disponibles dans la littérature pour un environnement urbain, comme une rue en ville, mais peu de données utilisables existent pour des environnements semi-fermés, comme l'intérieur d'un bâtiment ou d'un bus. Nous utiliserons ensuite ces mesures pour estimer la densité spectrale de bruit magnétique dans une bande de fréquence B centrée sur une fréquence f.

Dans la revue de littérature, nous avons vu qu'une référence datée de 1999, "Propagation Model and Interference Range Calculation for Inductive Systems 10 kHz – 30 MHz" [11], est récurrente [47] [38] [24] pour estimer le bruit EM en milieu urbain, il s'agit d'un document d'un comité de la *Conférence européenne des administrations des postes et télécommunications* (CEPT) nommé *Comité européen des radiocommunications* (ERC). En lisant celui-ci, on peut s'apercevoir que la partie qui nous intéresse se trouve dans l'annexe B qui n'est autre qu'un résumé du document "Recommendation ITU-R P.372-11 "Radio noise"" [43] de *L'Union internationale des télécommunications* (ITU). Ce document se trouve être une référence compilant des données sur les niveaux de bruit EM sur terre sur une large plage de fréquence. Il distingue trois sources de bruits EM distinctes : le bruit galactique, le bruit atmosphérique et le bruit provenant des activités humaines. Le document de l'ERC fait plus précisément référence à une version de 1994 (P.372-6) du document de l'ITU. Or celui-ci a depuis été mis à jour cinq fois, la version la plus récente étant datée de 2013 (P.372-11). Il est donc plus intéressant de s'intéresser directement à ce document.

Le document de l'ITU n'est cependant pas le seul disponible pour obtenir des ordres de grandeur du bruit EM ambiant. Il existe une revue de littérature [31] datée de septembre 2010 qui recense un certain nombre d'articles fournissant des mesures de bruit EM d'origine humaine dans différentes bandes de fréquence. On y apprend que les mesures fournies par l'ITU datent des années 70 et que depuis des données plus récentes sont disponibles. Un

article de 1994 [29] montre par exemple que dans la bande HF à cette époque, le niveau de bruit EM n'avait pas beaucoup changé. L'auteur explique ce phénomène par la disparition d'anciennes sources de bruits EM, comme les lignes haute-tension qui sont maintenant plus souvent enterrées. Les mesures de l'article avaient été effectuées dans les centres-ville d'Ottawa et de Montréal. Il semble que les mesures les plus récentes dans la bande HF datent de 2007 et ont été effectuées par Miki Iwama [23] dans un quartier résidentiel au Japon. L'endroit exact n'est pas précisé. Ses résultats indiquent des niveaux de bruit un peu plus élevés que ceux de l'ITU. D'après la revue de littérature [31], peu de mesures sont en revanche disponibles pour les environnements semi-fermés.

Dans ces articles, le bruit est toujours indiqué en terme de figure de bruit F_{aM} d'une antenne idéale, aussi appelé facteur de bruit externe. F_{aM} est ainsi la différence (en dB) entre la puissance de bruit disponible aux bornes d'une antenne sans perte adaptée et la puissance de bruit disponible aux bornes d'une charge adaptée à température ambiante (290 K) :

$$F_{aM} = 10 \log(\frac{p_n}{kT_0B}) \tag{3.23}$$

Dans la définition 3.23, p_n indique la puissance du bruit EM, k la constante de Boltzmann, T_0 la température ambiante moyenne sur terre (290 K), et B la bande passante de bruit considérée.

La figure 3.8 montre les valeurs obtenues par l'ITU [43] et par Miki Iwama [23] pour F_{aM}. Nous utiliserons les mesures fournies par ces deux documents pour calculer l'ordre de grandeur du bruit reçu par le lecteur de l'attaquant.

La valeur efficace du champ électrique $|E|$ peut ensuite être calculée en fonction de F_{am} [43] :

$$|E|(dB\mu V/m) = F_{am} - 95.5 + 20 \times \log(\frac{f}{1 \text{ MHz}}) + 10 \times \log(\frac{B}{1 \text{ Hz}}) \tag{3.24}$$

Où f est la fréquence centrale de la bande B considérée. En supposant que l'impédance liant les champs électrique et magnétique est celle du vide, on peut écrire :

$$|H_b|(dB\mu A/m) = |E|(dB\mu V/m) - 20 \times \log(377\ \Omega) \tag{3.25}$$

On a ainsi :

$$|H_b|(dB\mu A/m) = F_{am} - 147 + 20 \times \log(\frac{f}{1 \text{ MHz}}) + 10 \times \log(\frac{B}{1 \text{ Hz}}) \tag{3.26}$$

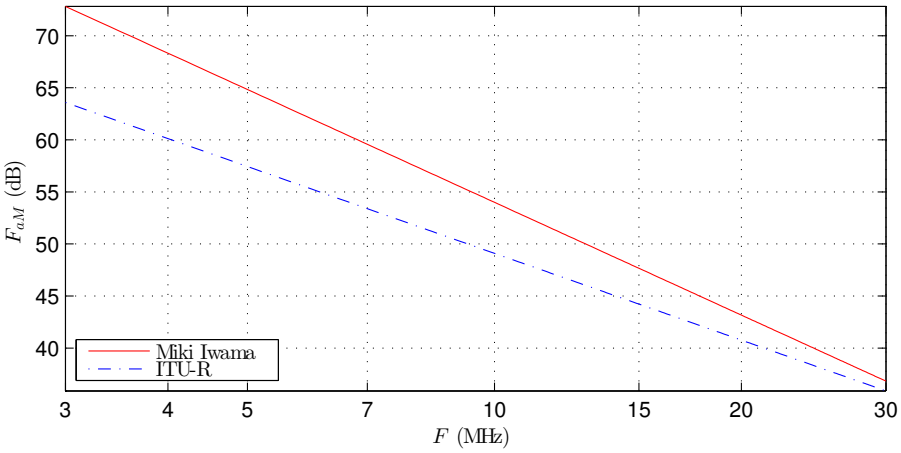

Figure 3.8 Niveaux de bruit EM en milieu urbain dû aux activités humaines.

CHAPITRE 4

ÉTUDE THÉORIQUE DE L'ATTAQUE SANGSUE

L'objectif de ce chapitre est de calculer une approximation par excès de la distance maximale de l'attaque sangsue, dans le cas monostatique, ainsi que les ordres de grandeur de la puissance nécessaire pour l'atteindre et du rapport signal sur porteuse (SCR), en fonction des paramètres du transpondeur (géométrie de l'antenne, fréquence de résonnance, facteur de qualité) et de la fréquence f_0 de la porteuse du lecteur. Pour cela, nous avons été amenés à faire plusieurs hypothèses et approximations sur l'attaque qui sont détaillées dans la section 4.1. Les calculs de la puissance nécessaire à l'activation du transpondeur ainsi que celui de l'index de la modulation d'amplitude font intervenir le facteur de qualité Q_a de l'antenne du lecteur et le coefficient de couplage mutuel k entre les deux antennes. Nous avons donc besoin de connaître k en fonction de la distance d séparant les deux antennes. Cette relation est établie dans la section 4.2. Il nous faut également calculer un ordre de grandeur du facteur de qualité Q_a, en fonction de la norme de RFID utilisée. C'est ce que nous verrons dans la section 4.3. Le SNR de la communication est limité dans notre modèle par le bruit magnétique ambiant. Nous calculerons la valeur efficace de cette source de bruit aux bornes de l'antenne du lecteur dans la section 4.4. Nous calculerons alors la puissance nécessaire à l'activation du transpondeur dans la section 4.5 et l'index de la modulation d'amplitude dans la section 4.6. Ces deux dernières sections nous permettront d'établir nos résultats dans la section 4.7.

4.1 Hypothèses et approximations du modèle

Notre modèle fait quatre hypothèses concernant l'attaque sangsue détaillées ci-après :

1. Nous avons supposé que l'architecture du lecteur de l'attaquant correspond à celle décrite dans la section 3.4, et utilise une antenne cadre magnétique accordée avec un réseau en L. Comme nous l'avons vu dans la section 3.4, ce type de lecteur est très répandu. La figure 4.1 montre ainsi le schéma électrique du montage considéré.
2. Nous n'avons considéré que le cas d'une antenne d'un seul tour. L'augmentation du nombre de tours N_2 de l'antenne du lecteur peut permettre d'augmenter k à condition que l'inductance de l'antenne L_2 croisse plus lentement que N_2^2, ce qui est le cas par exemple pour une antenne en forme de spirale. Si chaque tour a le même rayon, augmenter N_2 n'apporte aucun avantage puisque L_2 est dans ce cas à peu près pro-

portionnel à N_2^2 et se simplifie par conséquent dans le calcul de k. Il existe cependant une distance à partir de laquelle le cas $N_2 = 1$ permettra un meilleur couplage. En effet, plus N_2 est grand, plus la longueur totale de l'antenne est importante et plus le déphasage du courant le long de l'antenne sera important [1], réduisant ainsi le couplage k. De surcroît, augmenter N_2 entraîne l'apparition de capacités parasites entre les tours de l'antenne qui font baisser sa fréquence de résonance propre [1]. Or celle-ci ne doit pas être inférieure à la fréquence de la porteuse f_0. Pour les raisons brièvement évoquées ici, nous avons choisi de ne considérer que le cas $N_2 = 1$. Il est cependant possible que $N_2 > 1$ est préférable pour certaines distances de lecture d.

3. Dans nos calculs, nous n'avons pas tenu compte de l'influence du champ lointain émis par l'antenne du lecteur. Nous ne tenons compte que du couplage mutuel entre les antennes du lecteur et du transpondeur.
4. Nous supposons que l'attaquant se trouve en plein air dans une grande ville. En effet, les ordres de grandeur que nous utilisons pour le bruit magnétique ambiant viennent de mesures effectuées dans ces conditions, comme nous l'avons vu dans la section 3.5.

Nous avons par ailleurs fait plusieurs approximations permettant de simplifier la modélisation de l'attaque :

1. La seule source de bruit que nous avons considérée est le bruit magnétique ambiant. Nous négligeons le bruit introduit par l'électronique du lecteur.
2. Les filtres du lecteur idéaux : sans perte et atténuant complètement en dehors de leur bande passante.
3. Les axes – définis comme passant par le centre de l'antenne et orthogonaux aux boucles – de l'antenne du lecteur et du transpondeur sont confondus. En réalité, la présence d'un angle entre ces deux axes conduit à abaisser le coefficient de couplage mutuel entre les antennes.
4. Pour calculer l'amplitude du signal du transpondeur reçu par le lecteur, nous négligeons l'influence des régimes transitoires dus à la commutation de la résistance de modulation. Cela revient à approximer par excès l'index de la modulation.

Toutes ces approximations entraînent une exagération de la portée de l'attaque. En réalité, celle-ci sera donc plus faible que les résultats que nous avons obtenus.

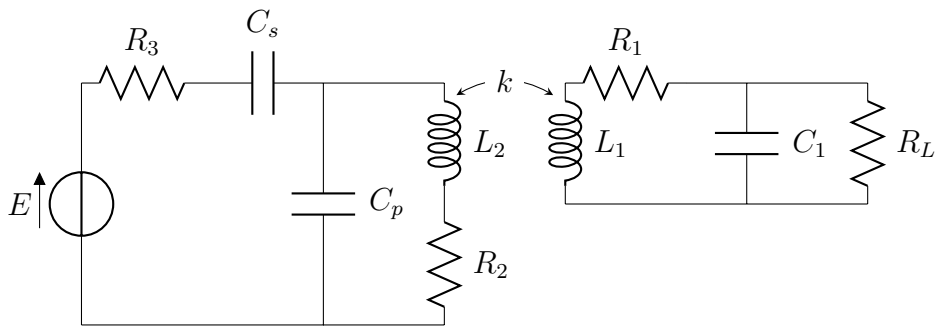

Figure 4.1 Schéma électrique montrant les modèles du lecteur et du transpondeur couplés.

4.2 Coefficient de couplage mutuel maximal

Dans cette section, nous allons calculer le coefficient de couplage mutuel k maximal que l'attaquant peut espérer atteindre à une distance d d'un transpondeur, en fonction des caractéristiques géométriques de celui-ci et avec une antenne d'un seul tour ($N_2 = 1$).

Pour cela, il faut calculer le rayon r_2 de l'antenne du lecteur qui convient le mieux à une distance d. L'article de Wim Aerts *et al.* [1] montre qu'en tenant compte de la phase du courant, la relation liant d et r_2 peut être obtenue en résolvant l'équation suivante dans le cas $N_2 = 1$:

$$\frac{(2\rho^2 - 1)\lambda}{\rho} - \frac{\sin(\beta\rho d)}{1 - \cos(\beta\rho d)} 2\pi^2 d(1 + \rho^2) = 0 \tag{4.1}$$

Avec $\rho = \frac{r_2}{d}$, $\lambda = \frac{c}{f_0}$, $\beta = \frac{4\pi^2}{\lambda}$ et f_0 la fréquence du courant parcourant l'antenne, c'est-à-dire, la fréquence de la porteuse.

L'équation 4.1 permet de choisir le rayon r_2 permettant de maximiser $\frac{\mathrm{d}H_z}{\mathrm{d}\rho}$ (en reprenant les notations de l'équation 3.4) à la distance d, ce qui revient à maximiser le couplage mutuel M entre les deux antennes. Cependant, quand l'antenne du lecteur est accordée, c'est le coefficient de couplage mutuel $k = \frac{1}{\sqrt{L_1 L_2}}$ qui doit être maximisé. Or plus le rayon r_2 de l'antenne est grand, plus son inductance L_2 augmente ce qui a pour effet de diminuer k. Chercher à maximiser k donne donc un avantage aux antennes de rayon faible.

Pour déterminer le ratio ρ permettant de maximiser k, nous allons supposer que L_2 augmente proportionnellement à r_2, ce qui revient à supposer le rapport $\frac{r}{r_2} = a$ constant. On a alors en utilisant l'équation 3.3 :

$$L_2 = \mu_0 r_2 (\ln(\frac{8}{a}) - 2) = \mu_0 \alpha^2 r_2 \tag{4.2}$$

Avec ces notations, en utilisant les équations 3.9 et 4.2 :

$$k = \frac{N_2 r_1^2 \lambda}{8\pi\alpha\sqrt{L_1}} \frac{\sqrt{2r_2(1-\cos(\beta r_2))}}{\sqrt{(r_2^2+d^2)^3}} \tag{4.3}$$

Résoudre $\frac{\mathrm{d}k}{\mathrm{d}\rho} = 0$ revient alors à résoudre :

$$\frac{\mathrm{d}}{\mathrm{d}\rho}\left(\sqrt{\frac{2\rho(1-\cos(\beta\rho d))}{d^5(\rho+1)^3}}\right) = 0 \tag{4.4}$$

En calculant cette dérivée, on trouve :

$$\rho d\beta \sin(\beta\rho d)(\rho^2+1) + (5\rho^2-1)(\cos(\beta\rho d)-1) = 0 \tag{4.5}$$

Le rayon optimal ne dépend donc ni de a ni de la géométrie de l'antenne du transpondeur (L_1, r_1, N_1). Les résultats obtenus en résolvant numériquement 4.1 et 4.5 sont donnés sur la figure 4.2. On observe que pour maximiser k, il est préférable d'utiliser un rayon r_2 entre 15% et 30% plut petit que dans le cas où M est maximisé pour $0.1 < d < 2$ m.

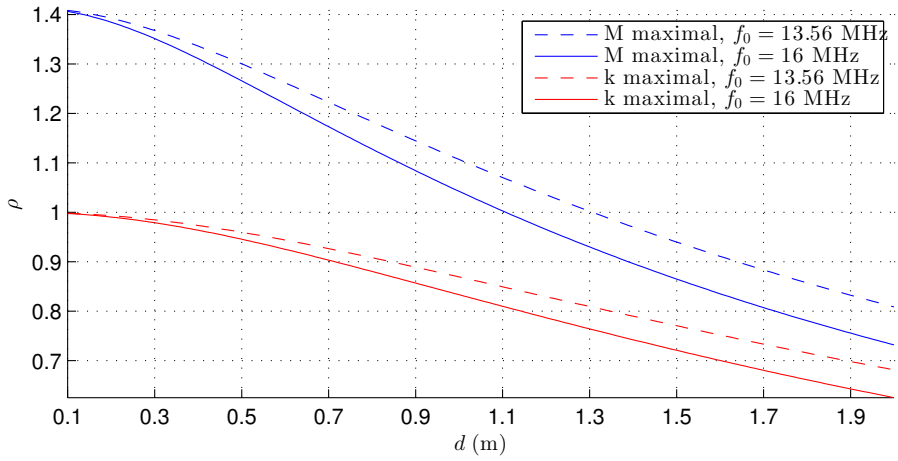

Figure 4.2 Rapport ρ entre le rayon r_2 et la distance de lecture d permettant de maximiser M ou k à 13.56 MHz et 16 MHz.

La figure 4.3 montre le coefficient de couplage mutuel obtenu en prenant pour chaque distance d le rayon r_2 optimal d'une antenne à un tour et en prenant les paramètres typiques suivant pour l'antenne du transpondeur :

$$L_1 = 3.6\ \mu\text{H}$$
$$r = 30\ mm$$
$$N_1 = 4$$

On suppose de plus que les deux antennes sont parallèles (voir figure 3.1). Dans le cas où les antennes ne sont pas parallèles, k décroît comme le cosinus de l'angle formé par les deux axes des boucles.

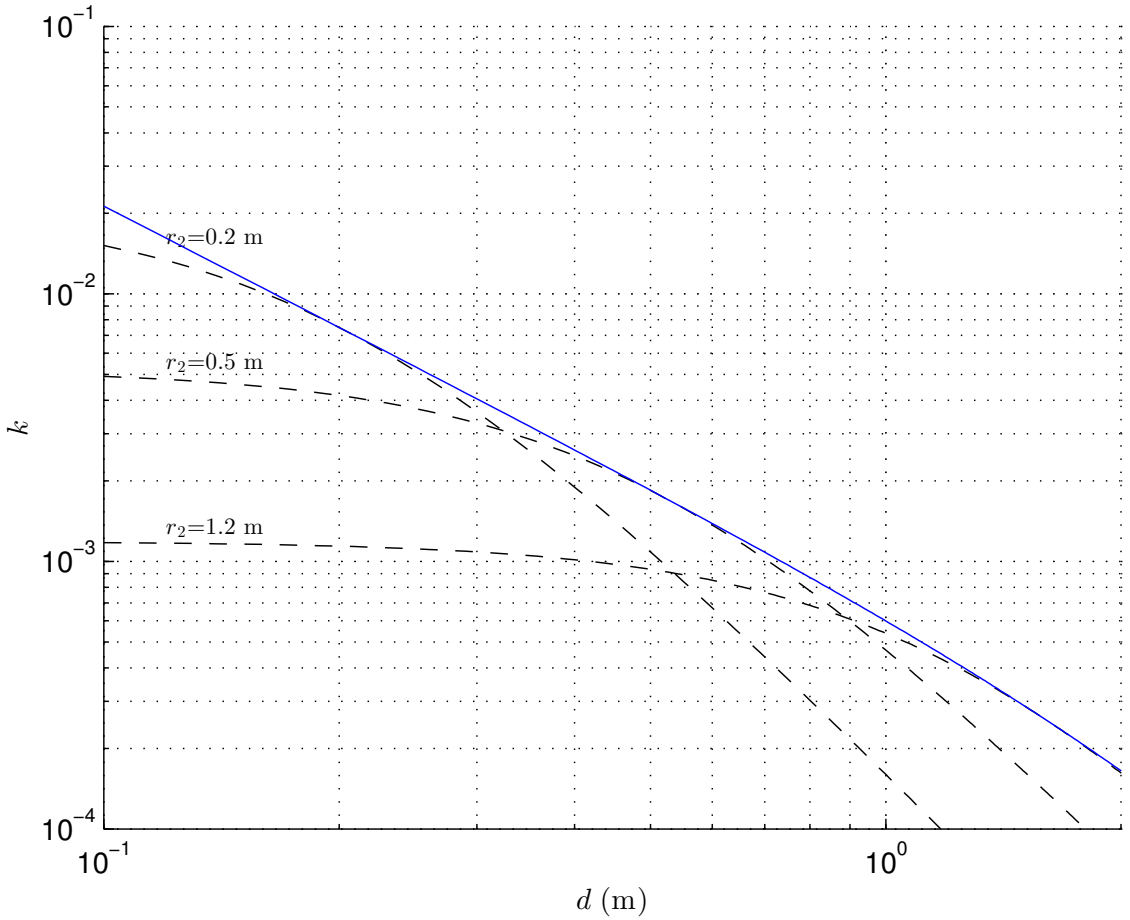

Figure 4.3 Tracé du coefficient de couplage mutuel maximal à une distance d pour $N_2 = 1$ en bleu. Les autres courbes correspondent à k en fonction de d pour r_2 fixé.

Sur la figure 4.3 les courbes en noirs montrent les tracés de k pour différentes valeurs de r_2 fixées. On observe bien que le tracé de k optimal est toujours au-dessus des autres courbes, tout en étant tangent à chacune d'elle en un unique point.

4.3 Facteur de qualité maximal pour l'antenne du lecteur

Le second paramètre que nous allons chercher à optimiser est le facteur de qualité Q_a de l'antenne du lecteur. Un facteur de qualité élevé permet de diminuer la puissance nécessaire pour activer le transpondeur, mais dégrade le rapport signal sur bruit (SNR) ainsi que le rapport signal sur porteuse (SCR) de la communication. Plus précisément, chacun des sens de la communication entre lecteur et transpondeur impose une contrainte sur Q_a et la valeur maximale possible pour celui-ci correspond à la contrainte la plus forte. Nous estimerons dans un premier temps quelle limite sur Q_a est imposée par la communication du lecteur vers le transpondeur. Dans un second temps, nous estimerons la contrainte imposée par l'autre sens de la communication.

4.3.1 Limite imposée par la communication du lecteur vers le transpondeur

Le lecteur doit pouvoir émettre sans qu'il y ait d'interférence inter symbole. La bande passante de son antenne doit donc être suffisamment large pour couvrir le spectre du protocole considéré quand le lecteur communique avec le transpondeur. On a ainsi une condition incontournable sur le facteur de qualité :

$$Q_a < \frac{f_0}{\Delta f} \tag{4.6}$$

Avec f_0 la fréquence centrale de l'antenne, qui est aussi la fréquence à laquelle on alimentera le transpondeur, et Δf la bande passante requise par le protocole utilisé par le lecteur. Nous avons vu précédemment cette bande passante est plus compliquée à estimer qu'il n'y paraît, à cause des régimes transitoires qui apparaissent dès lors qu'on essaye de la réduire et qui peuvent alors se trouver plus longs que ce qui est toléré par les normes. Nous nous contenterons donc ici de donner un intervalle encadrant le facteur de qualité maximal possible.

Pour la norme ISO 14443 type A, les symboles sont envoyés en interrompant la transmission de la porteuse pendant une durée T_p et c'est la position de ce pulse dans le temps qui code un bit. La durée d'un pulse est donnée par la relation suivante :

$$T_p = \frac{5}{16}\frac{128}{nf_0}$$

Avec n est égal à, respectivement, 1, 2 ou 3 pour un débit de 106 kb/s, 212 kb/s ou 424 kb/s.

Il faut donc que la bande passante de l'antenne soit suffisamment large pour ne pas filtrer

ces pulses. La bande passante minimale requise se trouve donc quelque part entre $\frac{1}{T_p}$ et $\frac{2}{T_p}$. Avec $\Delta f = \frac{2}{T_p}$, on est sûr que les constantes de temps des régimes transitoires au moment d'un changement d'état du signal du lecteur sont assez courtes pour respecter la norme. Avec $\Delta f = \frac{1}{T_p}$ par contre, il faudrait faire une analyse plus poussée. On a donc l'encadrement suivant pour $Q_{a,max}$:

$$\frac{1}{2}\frac{5}{16}\frac{128}{n} < Q_{a,max} < \frac{5}{16}\frac{128}{n} \tag{4.7}$$

Pour la norme ISO 14443 type B, les symboles sont envoyés en utilisant une modulation ASK avec un débit de $\frac{nf_0}{128}$ où n égal à, respectivement, 1, 2 ou 3 pour un débit de 106 kb/s, 212 kb/s ou 424 kb/s. La bande passante nécessaire est donc comprise entre $\frac{nf_0}{128}$ et $2\frac{nf_0}{128}$. D'où la condition :

$$\frac{128}{2n} < Q_{a,max} < \frac{128}{n} \tag{4.8}$$

Pour la norme ISO 15693, avec un débit symbole de 26.48 kb/s, le lecteur envoie des pulses de $\frac{128}{f_0}$, on a donc :

$$64 < Q_{a,max} < 128 \tag{4.9}$$

Le tableau 4.1 récapitule pour les différents protocoles de la RFID la contrainte imposée par la communication du lecteur vers le transpondeur. Il est important de noter que ces résultats sont indépendants de la fréquence de la porteuse utilisée par le lecteur de l'attaquant. La bande passante occupée par les protocoles dépend toujours de la porteuse f_0 qui se simplifie par conséquent dans le calcul de Q_a.

Débit	ISO 14443 A	ISO 14443 B	ISO 15693
26.48 kb/s	-	-	64 - 128
106 kb/s	20 - 40	64 - 128	-
212 kb/s	10 - 20	32 - 64	-
424 kb/s	5 - 10	16 - 32	-

Tableau 4.1 Facteur de qualité maximal pour l'antenne du lecteur

4.3.2 Limite imposée par la communication du transpondeur vers le lecteur

Le transpondeur communique avec le lecteur en commutant sa résistance de modulation en fonction des bits à transmettre. Sa commutation entraîne l'apparition de régimes transitoires dans l'amplitude de la tension mesurée par le lecteur pour démoduler les symboles reçus. Il

faut donc s'assurer que ces régimes transitoires ne soient pas trop longs ce qui pourrait entraîner des interférences inter symbole. Nous allons ainsi ici dériver les constantes de temps de ces régimes transitoires et en déduire des conditions sur les facteurs de qualité des antennes du lecteur et du transpondeur. Nous reprendrons pour cela de manière détaillée la méthodologie exposée dans l'article de Vuza [45] en l'appliquant à la RFID à 13.56 MHz – alors que l'article parle de RFID à 125 kHz. L'article suppose également que les fréquences de résonnance du lecteur et du transpondeur sont identiques, nous nous affranchirons ici de cette hypothèse puisque la fréquence de résonance des transpondeurs HF est souvent supérieure à 13.56 MHz.

Considérons dans un premier temps le cas d'une antenne accordée avec un circuit RLC série (figure 3.6). La lecture du signal du transpondeur se fait en mesurant la tension U aux bornes de la capacité d'accord du lecteur. Cette tension s'exprime comme suit en fonction des paramètres du système et de la tension d'alimentation E.

$$U = \frac{\frac{1}{jC_2w}}{\frac{1}{jwC_2} + jL_2w + R_2 + Z_t}E \tag{4.10}$$

On peut alors exprimer la fonction de transfert canonique – en notant p la variable de Laplace – entre les tensions U et E. Le calcul détaillé de cette fonction est donné en annexe.

$$\frac{U}{E} = \frac{1+\frac{1}{Q_t\omega_t}p+\frac{1}{\omega_a^2}p^2}{1+(\frac{1}{Q_t\omega_t}+\frac{1}{Q_a\omega_a})p+(\frac{1}{\omega_t^2}+\frac{1}{\omega_a^2}+\frac{1}{Q_aQ_t\omega_a\omega_t})p^2+\frac{1}{\omega_t}(\frac{1}{Q_a\omega_a\omega_t}+\frac{1}{Q_t}(\frac{1}{\omega_a^2}-\frac{k^2}{\omega_t^2}))p^3+\frac{1}{\omega_t^2}(\frac{1}{\omega_a^2}-\frac{k^2}{\omega_a^2})p^4} \tag{4.11}$$

Appelons alors $D(p)$ le dénominateur de l'équation 4.11 obtenue précédemment :

$$\begin{aligned} D(p) &= 1 + (\frac{1}{Q_t\omega_t} + \frac{1}{Q_a\omega_a})p + (\frac{1}{\omega_t^2} + \frac{1}{\omega_a^2} + \frac{1}{Q_aQ_t\omega_a\omega_t})p^2 \\ &+\frac{1}{\omega_t}(\frac{1}{Q_a\omega_a\omega_t} + \frac{1}{Q_t}(\frac{1}{\omega_a^2} - \frac{k^2}{\omega_t^2}))p^3 + \frac{1}{\omega_t^2}(\frac{1}{\omega_a^2} - \frac{k^2}{\omega_a^2})p^4 \end{aligned} \tag{4.12}$$

Pour déterminer une expression des racines du polynôme $D(p)$ – et donc les constantes de temps des régimes transitoires du système – nous allons faire l'approximation $k \approx 0$, ce qui permet de le factoriser facilement. Sans cette approximation, il n'est pas possible de trouver une expression simple des quatre racines complexes de $D(x)$.

$$D|_{k=0}(p) = (1 + \frac{1}{\omega_t Q_t}p + \frac{1}{\omega_t^2}p^2)(1 + \frac{1}{\omega_0 Q_a}p + \frac{1}{\omega_0^2}p^2) \tag{4.13}$$

$D|_{k=0}(p)$ a ainsi quatre racines complexes conjuguées deux à deux :

$$\widehat{p}_{1,2} = -\frac{\omega_0}{2Q_a} \pm j\omega_0\sqrt{1-\frac{1}{4Q_a}}$$

$$\widehat{p}_{3,4} = -\frac{\omega_t}{2Q_t} \pm j\omega_t\sqrt{1-\frac{1}{4Q_t}}$$

On en déduit ainsi une approximation des deux constantes de temps du système $\widehat{T}_t$ et $\widehat{T}_a$:

$$\widehat{T}_a = -\frac{1}{Re(\widehat{p}_{1,2})} = \frac{2Q_a}{\omega_0} = \frac{Q_a}{\pi f_a} \tag{4.14}$$

$$\widehat{T}_t = -\frac{1}{Re(\widehat{p}_{3,4})} = \frac{2Q_t}{\omega_t} = \frac{Q_t}{\pi f_t} \tag{4.15}$$

Il est intéressant de constater que les rôles des facteurs de qualité de l'antenne Q_a et du transpondeur Q_t sont complètement interchangeables. Le régime transitoire le plus long vient donc simplement du facteur de qualité le plus élevé.

Supposons que les régimes transitoires atteignent 95% de leur valeur finale en un temps τ correspondant à la durée séparant deux commutations de la résistance de modulation. On en déduit la relation suivante entre τ et le temps propre du régime transitoire $\widehat{T}$.

$$exp(-\frac{\tau}{\widehat{T}}) = 0.05 \implies \tau \approx 3\widehat{T}$$

Pour les normes ISO 14443 type A et type B, la résistance commute à une fréquence de $\frac{1}{\tau} = \frac{f_a}{16}$, ce qui correspond à la fréquence de la sous-porteuse utilisée par le transpondeur. Pour la norme ISO 15693, la sous-porteuse a une fréquence de $\frac{1}{\tau} = \frac{f_a}{32}$.

On a ainsi la condition suivante sur le facteur de qualité de l'antenne d'un lecteur ISO 14443 (type A ou B) :

$$Q_a < \frac{\pi\tau f_a}{3} \implies Q_a < \frac{16}{3}\pi \approx 17 \tag{4.16}$$

Pour un lecteur ISO 15693, le facteur de qualité peut être deux fois plus élevé :

$$Q_a < \frac{32}{3}\pi \approx 34 \tag{4.17}$$

Il est également intéressant de regarder la condition obtenue pour un transpondeur. Pour un transpondeur ISO 14443, celle-ci s'écrit :

$$Q_t < \frac{\pi\tau f_t}{3} \implies Q_t < \frac{16\pi}{3}\frac{f_t}{f_a} \tag{4.18}$$

Pour un transpondeur accordé sur 16 MHz fonctionnant avec un lecteur accordé sur 13.56 MHz, on trouve $Q_t < 20$. On s'aperçoit par ailleurs qu'augmenter la fréquence de fonctionnement d'un lecteur va faire baisser le SNR.

Intéressons-nous maintenant au cas d'une antenne accordée avec un réseau en L. Nous allons appliquer ici le même raisonnement que dans le cas du premier modèle de lecteur, c'est-à-dire chercher les pôles du dénominateur de la fonction de transfert liant la tension aux bornes de l'antenne et la tension d'alimentation du lecteur. On part donc de l'expression 4.31 :

$$U = \frac{\frac{1}{jC_p\omega + \frac{1}{R_2 + jL_2\omega + Z_t}} + \frac{1}{jC_s\omega}}{\frac{1}{jC_p\omega + \frac{1}{R_2 + jL_2\omega + Z_t}} + \frac{1}{jC_s\omega} + R_3} E$$

On note p la variable de Laplace et $D(p)$ le dénominateur de la fonction de transfert $\frac{U}{E}$. En faisant l'approximation $k \approx 0$, on s'aperçoit qu'il est possible de factoriser $D(p)$ en deux facteurs. Le premier ne fait intervenir que le facteur de qualité du transpondeur Q_t comme dans l'expression 4.13, et le second ne fait intervenir que les paramètres du lecteur.

$$\begin{aligned} D(p) &= (\tfrac{1}{\omega_t^2}p^2 + \tfrac{1}{\omega_t}\tfrac{1}{Q_t}p + 1)(R_3C_sC_pL_2p^3 \\ &\quad +((C_s + C_p)L_2 + C_sC_pR_3R_2)p^2 + ((C_s + C_p)R_2 + C_sR_3)p + 1) \end{aligned} \tag{4.19}$$

$D(p)$ a deux racines conjuguées et une racine simple, le lecteur introduit donc deux constantes de temps qu'on peut calculer numériquement pour différentes valeurs du facteur de qualité. On s'aperçoit alors que la constante de temps due à la racine simple est négligeable (de l'ordre de la ns). La figure 4.4 montre la valeur calculée numériquement de la seconde constante pour $Qa < 40$ pour un lecteur accordé sur 13.56 MHz.

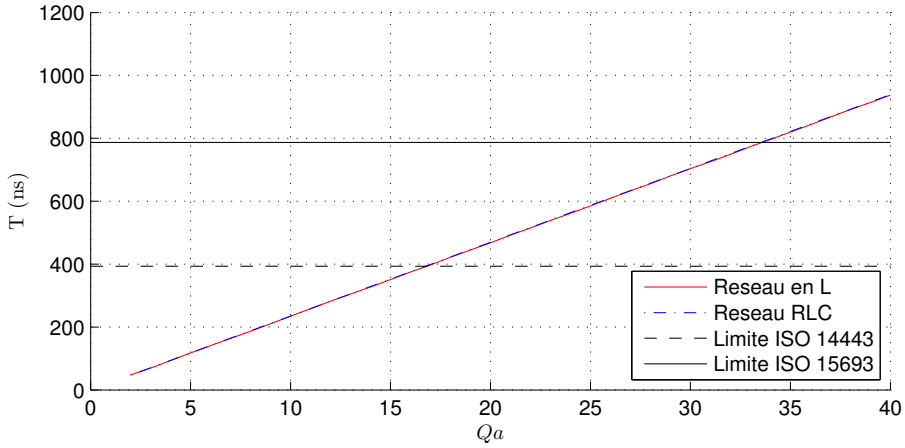

Figure 4.4 Constante de temps due au lecteur en fonction du facteur de qualité de l'antenne à 13.56 MHz. Les limites indiquent la valeur maximale que peut prendre $\widehat{T_a}$.

Les constantes de temps sont exactement les mêmes pour les deux circuits d'accord envisagés. Il est donc certainement possible de factoriser $D(p)$ de manière à faire apparaître ω_0 et Q_a comme dans le cas du circuit RLC.

Le tableau 4.2 suivant récapitule la contrainte sur le facteur de qualité de l'antenne du lecteur imposée par le transpondeur. La contrainte est indépendante de la fréquence centrale f_0 de l'antenne.

ISO 14443 A	ISO 14443 B	ISO 15693
17	17	34

Tableau 4.2 Contrainte sur le facteur de qualité imposée par le transpondeur

L'antenne SCEMTEC utilisée par Pierre Brun-Murol [3] a été conçue pour la norme ISO 15693. En mesurant sa bande passante (au sens du paramètre S_{11}) avec un analyseur de réseaux, on trouve environ 180 kHz, soit un facteur de qualité de 25 (en supposant que le BalUn de l'antenne est un 4 :1), ce qui est proche des résultats obtenus.

4.3.3 Résultats

Le tableau 4.3 donne finalement un ordre de grandeur du facteur de qualité maximal possible pour une antenne accordée par protocole et par débit.

Débit	ISO 14443 A	ISO 14443 B	ISO 15693
26.48 kb/s	-	-	34
106 kb/s	17	17	-
212 kb/s	10 - 17	17	-
424 kb/s	5 - 10	17	-

Tableau 4.3 Facteur de qualité maximal possible par norme et par débit

Pour la norme ISO 14443 type A, un attaquant aurait intérêt à se limiter au débit de 106 kb/s afin de maximiser Q_a. Pour le type B par contre le débit n'influence pas le facteur de qualité maximal, car le protocole est moins demandeur en bande passante.

4.4 Bruit EM aux bornes de l'antenne du lecteur

Le bruit EM dont nous avons vu des ordres de grandeur dans la section 3.5 entraîne l'apparition d'une tension parasite U_b (en Volt efficace) qui se superpose à la tension U mesurée par le lecteur. Notre objectif est ici de calculer la valeur efficace de U_b dans la bande passante occupée par la bande latérale supérieure du signal du transpondeur pour les trois normes de la RIFD qui nous intéresse.

La figure 4.5 montre l'antenne du lecteur connectée à l'amplificateur de puissance. En série avec L_2 est représentée la source de tension E_b induite par le bruit magnétique H_b au voisinage de l'antenne.

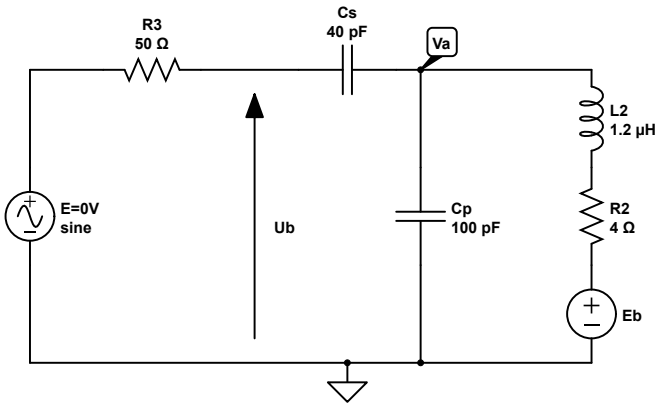

Figure 4.5 Circuit de l'antenne avec la source E_b induite par le bruit EM ambiant. Les valeurs des composants sont indiquées à titre d'exemple.

Premièrement, en partant de l'équation 3.26, calculons la densité spectrale N_{EM} du bruit

magnétique sur une bande B centrée en f. En supposant ce bruit blanc, on peut exprimer N_{EM} en calculant $\frac{H_b^2}{B}$:

$$N_{EM,dB} = F_{am} - 147 + 20 \times \log(\frac{f}{1\ \text{MHz}}) \tag{4.20}$$

Avec $N_{EM,dB} = 10\log(N_0)$. N_0 est ici en $\mu\text{A}^2\,\text{m}^{-1}\,\text{s}^{-1}$.

Deuxièmement, trouvons l'expression de la fonction de transfert qui lie la tension U_b au champ magnétique H_b traversant la boucle de l'antenne. En supposant H_b uniforme sur la surface de la boucle, la loi de Faraday nous permet d'écrire :

$$E_b = -j\omega\mu_0 S_a H_b \tag{4.21}$$

Où S_a la surface de la boucle de l'antenne.

Troisièmement, on cherche la relation liant U_b à E_b. Pour mener ce calcul, on applique le principe de superposition, la source E qui alimente normalement l'antenne est donc ici éteinte. On calcule alors l'expression du potentiel V_a en appliquant le théorème de Millman :

$$V_a(\frac{1}{jL_2\omega + R_2} + jC_p\omega + \frac{jC_s\omega}{1 + jR_3C_s\omega}) = \frac{E_b}{jL_2\omega + R_2} \tag{4.22}$$

On exprime ensuite U_b en fonction de V_a avec un pont diviseur de tension :

$$U_b = \frac{jC_sR_3\omega}{1 + jC_sR_3\omega}V_a \tag{4.23}$$

Les équations 4.22 et 4.23 permettent alors d'exprimer U_b en fonction de E_b :

$$U_b\frac{(1 + jC_sR_3\omega)(1 + jC_p\omega(jL_2\omega + R_2)) + jC_s\omega(jL_2\omega + R_2)}{jC_sR_3\omega} = E_b \tag{4.24}$$

Appelons $H_a(\omega)$ la fonction de transfert liant U_b à E_b :

$$H_a(\omega) = \frac{U_b}{E_b} = \frac{jC_sR_3\omega}{(1 + jC_sR_3\omega)(1 + jC_p\omega(jL_2\omega + R_2)) + jC_s\omega(jL_2\omega + R_2)} \tag{4.25}$$

En utilisant 4.21 et 4.25, on obtient enfin la fonction de transfert recherchée $H(\omega)$:

$$H(\omega) = \frac{U_b}{H_b} = \frac{\omega^2 \mu_0 S_a C_s R_3}{(1 + jC_s R_3 \omega)(1 + jC_p \omega(jL_2\omega + R_2)) + jC_s\omega(jL_2\omega + R_2)} \tag{4.26}$$

Notons f la fréquence centrale de la bande latérale supérieure du signal du transpondeur et B sa largeur. On peut alors calculer la variance de U_b dans cette bande de fréquence en filtrant le bruit blanc de densité spectrale N_{EM} calculé avec l'équation 4.20 à travers le filtre $H(\omega)$:

$$U_b^2 = \int_{f-\frac{B}{2}}^{f+\frac{B}{2}} N_{EM} |H(2\pi f)|^2 df \tag{4.27}$$

Les résultats obtenus sont regroupés sur la figure 4.6. Plutôt que de tracer la tension efficace du bruit U_b en fonction du rayon de l'antenne r_2, on a préféré mettre en abscisse la distance de lecture d en prenant une antenne de rayon optimal selon les résultats de la section 4.2. Les courbes présentées peuvent ainsi être directement utilisées pour calculer le rapport signal sur bruit de la communication entre lecteur et transpondeur en fonction de d lorsque les autres sources de bruit sont négligées. L'inductance de l'antenne est calculée pour chaque rayon avec l'équation 4.2 en prenant un ratio $a = \frac{r}{r_2} = 0.05$. Pour chaque norme, on a également supposé un facteur de qualité Q_a correspondant aux résultats de la section 4.3.

4.5 Puissance d'activation

Comme nous l'avons vu dans la section 3.3, un transpondeur HF s'active dès lors que la tension V aux bornes de son circuit intégré dépasse V_{min}. Il n'existe ainsi pas de limite maximale pour l'activation d'un transpondeur : celui-ci peut être activé à une distance arbitraire aussi longtemps qu'on dispose de la puissance nécessaire pour créer un champ magnétique d'amplitude supérieure à H_{min} au niveau de son antenne. Nous allons donc maintenant chercher la relation liant la puissance consommée dans l'antenne du lecteur au coefficient de couplage mutuel k entre les deux antennes du système.

Pour établir cette relation, on part de l'expression 3.16 qui lie la tension (efficace) engendrée par induction dans l'antenne du transpondeur e à la tension V (efficace) aux bornes de son circuit intégré :

$$e = \sqrt{(1 - \frac{\omega^2}{\omega_t^2})^2 + \frac{1}{Q_t^2}\frac{\omega^2}{\omega_t^2}} V$$

En utilisant la loi de Faraday (3.1), la tension induite e peut s'exprimer en fonction de

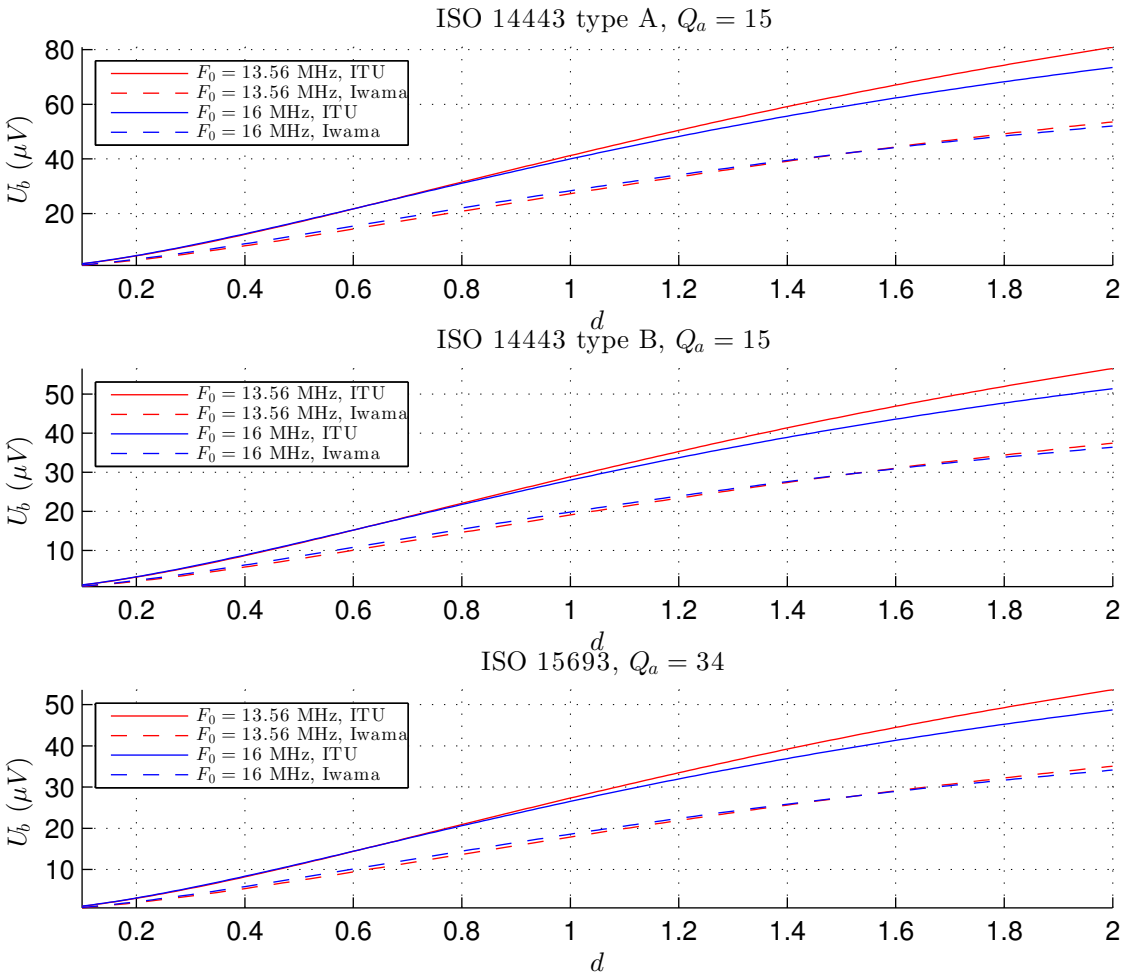

Figure 4.6 Tension efficace U_b en fonction de d pour les trois normes étudiées, pour un lecteur accordé sur 13.56 MHz et pour un lecteur accordé sur 16 MHz. Dans chaque cas, les mesures de l'ITU et de Miki Iwama ont été utilisées.

l'inductance mutuelle entre les deux antennes et du courant I_2 circulant dans l'antenne du lecteur : $e = \omega M I_2$.

$$I_2 = \sqrt{(1 - \frac{\omega^2}{\omega_t^2})^2 + \frac{1}{Q_t^2}\frac{\omega^2}{\omega_t^2}}\frac{1}{\omega M}V$$

La puissance consommée par l'antenne du lecteur, sans compter celle due au transpondeur, est $P_2 = R_2 {I_2}^2$:

$$\begin{aligned} P_2 &= R_2 {I_2}^2 \\ &= \Big((1-\frac{\omega^2}{\omega_t^2})^2 + \frac{1}{Q_t^2}\frac{\omega^2}{\omega_t^2}\Big)^2 \frac{R_2}{\omega^2 M^2} V^2 \\ &= \Big((1-\frac{\omega^2}{\omega_t^2})^2 + \frac{1}{Q_t^2}\frac{\omega^2}{\omega_t^2}\Big)^2 \frac{R_2}{\omega^2 k^2 L_1 L_2} V^2 \end{aligned}$$

On suppose que le lecteur fonctionne à sa fréquence de résonance, on peut donc écrire $\omega = \omega_0$ et $\frac{\omega_0 L_2}{R_2} = Q_b$:

$$P_2 = \Big((1-\frac{\omega_0^2}{\omega_t^2})^2 + \frac{1}{Q_t^2}\frac{\omega_0^2}{\omega_t^2}\Big) \frac{1}{Q_b \omega_0 k^2 L_1} V^2 \tag{4.28}$$

On ajoute ensuite la puissance P_1 consommée par le transpondeur. En négligeant R_1 – ce qui revient à faire l'approximation $Q_t \approx Q_p$ – on peut écrire :

$$P_1 \approx \frac{V^2}{R_L} \approx \frac{V^2}{Q_t \omega_t L_1} \tag{4.29}$$

Finalement, la puissance totale consommée dans l'antenne du lecteur est $P = P_1 + P_2$:

$$P = \Big(\Big((1-\frac{\omega_0^2}{\omega_t^2})^2 + \frac{1}{Q_t^2}\frac{\omega_0^2}{\omega_t^2}\Big)\frac{1}{Q_b \omega_0 k^2} + \frac{1}{Q_t \omega_t}\Big)\frac{V^2}{L_1} \tag{4.30}$$

La puissance nécessaire pour activer le transpondeur est minimisée quand le champ magnétique au niveau de celui-ci est égal à H_{min}. Dans ce cas, $Q_t = Q_{max_0}$ et $V = V_{min}$. La puissance nécessaire pour avoir $H > H_{min}$ au niveau du transpondeur pour k fixé peut être calculée en remplaçant d'une part Q_t par $Q_{max}(H)$ et d'autre part V par $V(H)$. Il est cependant difficile de trouver des mesures de $V(H)$ et $Q_{max}(H)$, en première approximation on peut donc supposer V égale à V_{min} et utiliser l'expression 3.19 pour extrapoler $Q_{max}(H)$.

La relation 4.30 montre que P varie comme $\frac{1}{k^2}$. On sait par ailleurs que k varie comme $\frac{1}{d^3}$. La puissance P requise pour activer le transpondeur varie donc comme d^6, autrement dit, pour doubler la distance d'activation il faut multiplier par 64 la puissance nécessaire.

4.6 Index de modulation et signal du transpondeur

Nous allons maintenant chercher à calculer l'index de modulation d'amplitude m créé par le transpondeur lors de sa communication avec le lecteur. Nous verrons alors comment la fré-

quence de la porteuse f_0 et l'amplitude du champ magnétique H_0 traversant le transpondeur influencent m. Nous en déduirons deux facteurs limitant la distance de l'attaque sangsue : le rapport signal sur porteuse ("SCR") et l'amplitude efficace du signal du transpondeur.

4.6.1 Index de modulation

Lorsque la résistance de modulation commute, le facteur de qualité Q_t du transpondeur varie entre Q_{max} et Q_{min}, et la tension U (voir figure 3.7 de la section 3.4) est alors modulée en amplitude. En négligeant les régimes transitoires dus à la commutation de la résistance de modulation, on a pour un lecteur avec un réseau en L :

$$U(Q_t) = \frac{\frac{1}{jC_p\omega_0 + \frac{1}{R_2 + jL_2\omega_0 + Z_t(Q_t)}} + \frac{1}{jC_s\omega_0}}{\frac{1}{jC_p\omega_0 + \frac{1}{R_2 + jL_2\omega_0 + Z_t(Q_t)}} + \frac{1}{jC_s\omega_0} + R_3} E \tag{4.31}$$

L'index de modulation m s'écrit alors :

$$m = \frac{||U(Q_{max})| - |U(Q_{min})||}{|U(Q_{max})| + |U(Q_{min})|} \tag{4.32}$$

La figure 4.7 montre ainsi les tracés pour plusieurs valeurs de f_0 de $|\frac{U(Q_t)}{U(0)}|$. La division par $|U(0)|$ permet de simplifier E qui disparaît de toute façon du calcule de m. Les courbes ont été tracées pour $Q_a = 15$, $k = 5 \times 10^{-3}$, $f_t = 16$ MHz et $L_1 = 3.6$ µH.

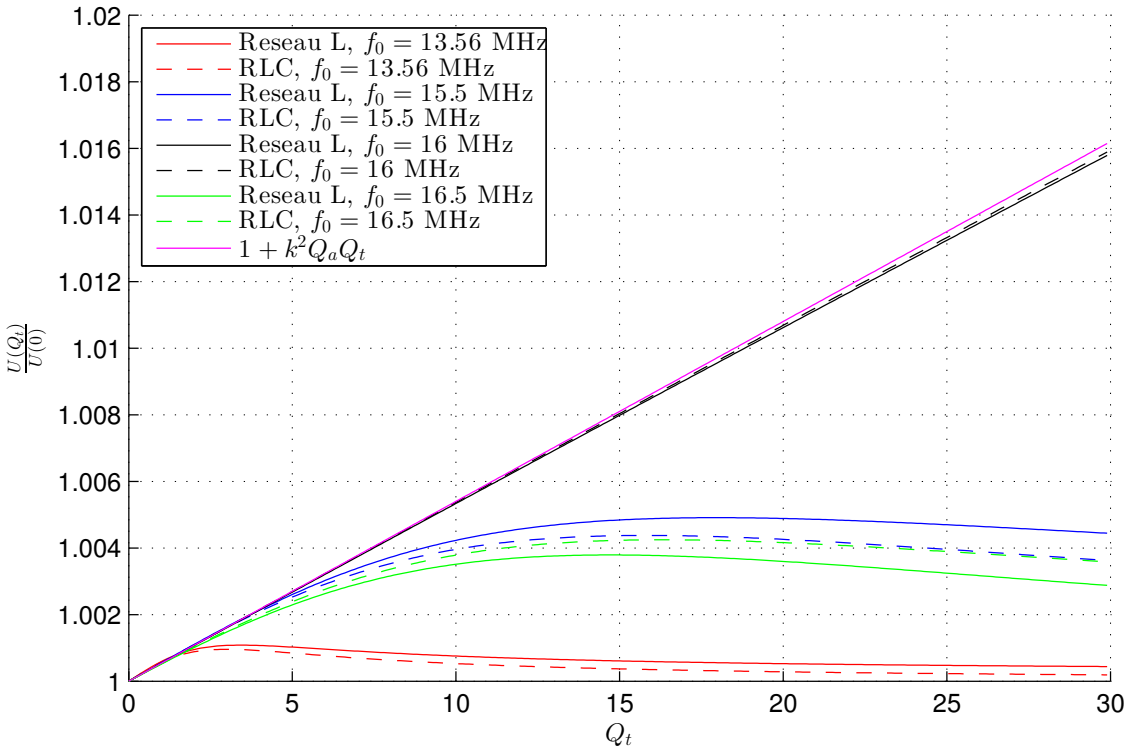

Figure 4.7 $\frac{U(Q_t)}{U(0)}$ pour différentes fréquences de porteuse. $Q_a = 15$, $k = 5 \times 10^{-3}$, $f_t = 16$ MHz et $L_1 = 3.6$ µH.

On observe que pour un lecteur non accordé sur la fréquence de résonance du transpondeur, $|\frac{U(Q_t)}{U(0)}|$ passe par un maximum avant de décroître. Avoir un facteur de qualité Q_{max} le plus élevé possible n'implique donc pas forcément un index de modulation maximal. Par exemple, sur la figure, pour $f_0 = 13.56$ MHz, l'index de modulation est plus élevé pour $Q_{min} = 1.6$ et $Q_{max} = 4$ ($m = 1 \times 10^{-4}$) que pour $Q_{min} = 1.6$ et $Q_{max} = 8$ ($m = 2 \times 10^{-6}$). Par conséquent, il peut-être intéressant de dépasser le champ magnétique H_{min} seuil pour activer un transpondeur afin de faire baisser ("dumper") son facteur de qualité Q_{max} (et Q_{min} si $Q_{min} > 0$).

On observe également que l'index de modulation est maximisé dans le cas où le lecteur est accordé sur la fréquence de résonance du transpondeur. Dans cette situation, on peut approximer $\frac{|U(Q_t)|}{|U(0)|}$ par $1+k^2 Q_a Q_t$ comme montre la figure 4.7 (ce résultat peut se retrouver par le calcul dans le cas de l'antenne RLC). Par ailleurs, pour $k \ll 1$, on peut faire l'approximation $m \approx \frac{||U(Q_{max})|-|U(Q_{min})||}{2|U(0)|}$ dans la mesure où $|U(Q_{max})| + |U(Q_{min})| \approx 2$. Dans ce cas, on peut finalement approximer m par :

$$m \approx \frac{1}{2} k^2 Q_a (Q_{max} - Q_{min}) \tag{4.33}$$

Cette approximation reste par ailleurs valable pour $f_0 \neq f_t$ si Q_{max} est suffisamment faible, car les fonctions $|\frac{U(Q_t)}{U(0)}|$ sont équivalentes au voisinage de 0 peu importe f_0.

4.6.2 Signal du transpondeur

Le signal qui nous intéresse se trouve dans les bandes latérales de la modulation d'amplitude de la tension U. Nous allons calculer la valeur efficace de ce signal en fonction de celui de la porteuse et de l'index de modulation.

On notera respectivement, U_s et U_p les valeurs efficaces des amplitudes du signal dans une bande latérale et de la porteuse. Pour modulation d'amplitude, le rapport $\frac{U_s}{U_p}$ dépend du codage des symboles [38]. Si les états hauts et bas de la sous-porteuse sont équiprobables, pour un index de modulation m, on a $\frac{U_s}{U_p} = \frac{m}{\sqrt{2}}$. Par contre, pour une norme utilisant un code Manchester, $\frac{U_s}{U_p} = \frac{m}{2}$.

Pour $m \ll 1$, la tension efficace U_p se calcule par ailleurs facilement à partir de la puissance active P déterminée dans la partie précédente. Il s'agit en effet de la puissance injectée dans l'antenne, qui correspond à une charge de 50 Ω à la fréquence de résonance de celle-ci. Par conséquent :

$$U_p = \sqrt{50P} \tag{4.34}$$

Finalement, on peut dresser le tableau 4.5, qui montre l'expression de U_s en fonction de P pour les trois normes les plus courantes.

Norme	U_s
ISO 14443 A	$\frac{m}{2}\sqrt{50P}$
ISO 14443 B	$\frac{m}{\sqrt{2}}\sqrt{50P}$
ISO 15693	$\frac{m}{2}\sqrt{50P}$

Tableau 4.4 Signal U_s en fonction de la puissance P par une norme.

4.6.3 Rapport signal sur porteuse

Le rapport signal sur porteuse est donné par l'expression suivante :

$$\mathrm{SCR}_{\mathrm{dB}} = 20 \log \frac{U_s}{U_p} \tag{4.35}$$

Encore une fois, l'expression du SCR en fonction de l'index de modulation va dépendre du codage des symboles. On peut donc dresser le tableau qui récapitule l'expression du SCR pour chaque norme.

Norme	$\mathrm{SCR}_{\mathrm{dB}}$
ISO 14443 A	$20 \log \frac{m}{2}$
ISO 14443 B	$20 \log \frac{m}{\sqrt{2}}$
ISO 15693	$20 \log \frac{m}{2}$

Tableau 4.5 SCR en fonction de m par norme.

4.7 Résultats

4.7.1 Méthodologie

Dans cette section, nous allons détailler comment nous avons utilisé les équations des chapitres 3 et 4 pour déterminer la distance maximale de lecture des trois modèles de transpondeur ISO 14443 type A dont nous connaissons les caractéristiques (section 3.3.6) : le modèle de transpondeur MIFARE ("transpondeur 1"), le modèle tiré de l'article de Pfeiffer *et al.* ("transpondeur 2"), et celui tiré de l'article de Gebhart *et al.* [15] ("transpondeur 3").

Nous avons implémenté avec MATLAB un algorithme qui, pour chaque distance d (séparant les antennes du lecteur et du transpondeur) et pour chaque modèle de transpondeur, effectue les calculs suivants :

1. Le rayon de l'antenne du lecteur est calculé en utilisant l'équation 4.5 de la section 4.2. L'attaquant dispose ainsi toujours du rayon d'antenne le plus adapté pour une lecture à une distance d : c'est-à-dire le rayon permettant d'avoir k maximal à une distance d.
2. La puissance P qui doit être consommée par l'antenne du lecteur pour activer le transpondeur est calculée avec l'équation 4.30 de la section 4.5. Le facteur de qualité de l'antenne est fixé à 15, comme établi dans la section 4.3.
3. L'index de la modulation d'amplitude m est calculé en utilisant l'équation 4.32 de la section 4.6. La valeur efficace du signal U_s du transpondeur aux bornes de l'antenne est alors calculée avec l'équation donnée dans le tableau 4.5 à partir des calculs de P et m.

4. La valeur efficace de la tension U_b aux bornes de l'antenne due au bruit magnétique ambiant est calculée à partir de l'équation 4.27 de la section 4.4.
5. Le rapport signal sur bruit $SNR_{dB} = 20\log(\frac{U_s}{U_b})$ est enfin calculé à partir de U_s et U_b. Le rapport signal sur porteuse SCR_{db} est également calculé à partir de l'équation donnée dans le tableau 4.5.

Dans le cas du transpondeur 1, nous avons également, pour chaque distance de lecture d, fait varier le champ magnétique auquel il est exposé entre H_{min} et 1.5 A/m. En effet, comme nous l'avons vu dans la section 4.6, si $f_t \neq f_0$, un facteur de qualité élevé pour le transpondeur ne permet pas forcément d'avoir l'index de modulation le plus important et donc la distance de lecture la plus élevée. Cependant, plus l'amplitude du champ magnétique au niveau de transpondeur est élevée, plus ce facteur de qualité décroît à cause du régulateur du transpondeur. À l'inverse, un facteur de qualité trop faible n'est pas non plus souhaitable. D'une part parce que la puissance émise par le lecteur est plus importante, et d'autre part parce que cela diminue l'index de modulation. Pour les transpondeurs MIFARE, le facteur de qualité Q_{max_0} est élevé, car l'impédance d'entrée du circuit intégré de NXP est élevée (15 kΩ), il faut donc chercher l'amplitude du champ magnétique H qui convient le mieux. Nous utilisons ainsi la méthode d'interpolation du facteur de qualité expliquée dans la section 3.3, qui permet d'estimer Q_{max} en fonction de H.

La figure 4.8 montre par exemple l'amplitude du signal U_s du transpondeur en fonction de H. Les paramètres de la simulation sont les suivants : $d = 30$ cm, $Q_a = 15$, les paramètres du transpondeur sont ceux que nous avons tirés du document de NXP : $f_t = 16.4$ MHz, $Q_{max_0} = 25$, $L_1 = 3.6$ µH, $V_{min} = 2$ V, $r_1 = 3.3$ mm, $N_1 = 4$. On observe bien qu'augmenter H conduit à un signal U_s plus fort. Par ailleurs, plus la fréquence de résonance du lecteur est proche de celle du transpondeur, plus U_s augmente rapidement avec H.

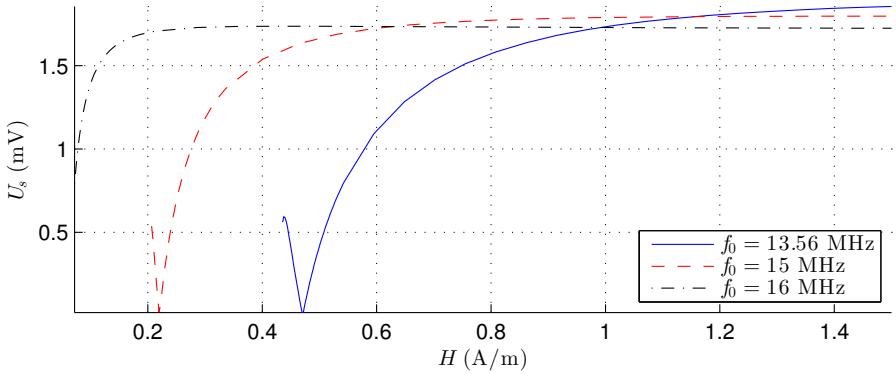

Figure 4.8 Amplitude du signal U_s du transpondeur MIFARE à une distance $d = 30$ cm en fonction de l'amplitude du champ magnétique H auquel il est exposé.

Nous avons alors exécuté cette simulation avec deux conditions d'arrêt différentes, correspondant à deux scénarios pratiques :

— **Scénario 1 :** On suppose que l'attaquant dispose d'une puissance illimitée. Seul le bruit magnétique ambiant limite la distance de lecture du transpondeur. La seule condition d'arrêt est $\mathrm{SNR}_{\mathrm{dB}} < 11.4$ dB.

— **Scénario 2 :** En plus de la condition précédente sur le SNR, on suppose la puissance P transmise dans l'antenne du lecteur inférieure à 10 W. L'objectif de cette condition est de simuler un lecteur dont l'ordre de grandeur de la puissance est plus réaliste que ceux obtenus dans le scénario 1.

4.7.2 Scénario 1 : lecteur idéal

On suppose ici le lecteur idéal ; aucune borne n'est imposée ni sur le SCR, ni sur la puissance P du lecteur. Seul le bruit magnétique ambiant limite la distance de lecture du transpondeur. Les résultats de la simulation sont présentés sur la figure 4.9 :

— **Transpondeur 1 :** la distance de lecture est de 1.2 m peu importe la fréquence f_0. À 13.56 MHz, une puissance de quelques kilowatts et un SCR de -125 dB sont nécessaires pour lire le transpondeur. À la résonance, la puissance et le SCR chutent respectivement à 12 W et -105 dB.

— **Transpondeur 2 :** la limite imposée par le bruit magnétique ambiant est comprise entre 1.3 et 1.4 m environ, peu importe f_0. Pour l'atteindre, une puissance de plus de 1 kW et un filtre de 124 dB sont nécessaires.

— **Transpondeur 3 :** pour $f_0 = 13.56$ MHz, quasiment à la fréquence de résonance du

transpondeur, la distance de lecture maximale est de 1.4 m. Une puissance de 470 W et un SCR -117 dB sont nécessaires.

Hormis le cas du transpondeur MIFARE (transpondeur 1) avec f_0 proche de la fréquence de résonance du lecteur, ces conditions sont certainement irréalisables en pratique. Pour l'attaquant, les distances de lecture atteintes ne sont de toute façon pas assez intéressantes pour justifier l'achat d'un amplificateur de plusieurs kilowatts. Ces résultats permettent surtout d'établir une limite maximale théorique pour la lecture des transpondeurs ISO 14443 type A : entre 1.2 et 1.4 m. Ainsi, dans un milieu urbain en plein air, nous ne pensons pas que ce type de transpondeur puisse être lu à une distance supérieure à 1.5 m environ, peu importe les sommes d'argent investies dans la fabrication du lecteur malicieux. Autrement dit, le possésseur d'une carte ISO 14443 type A peut se considérer en sécurité si personne se trouve à l'intérieur d'un rayon de 1.5 m autour de lui.

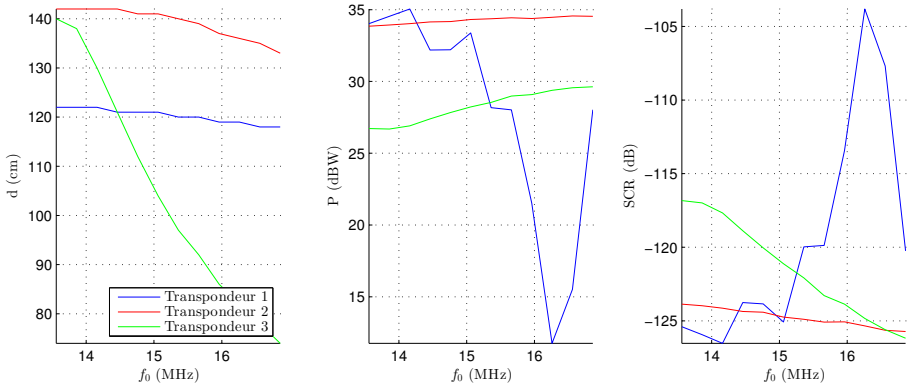

Figure 4.9 Distances de lecture des transpondeurs, puissances de la porteuse et SCR simulés pour le scénario 1 (lecteur idéal).

4.7.3 Scénario 2 : lecteur de 10 W

La puissance maximale injectée dans l'antenne du lecteur est ici limitée à 10 W. La condition sur le SNR s'applique toujours. Ce scénario nous donne une borne supérieure pour la distance de lecture des transpondeurs ISO 14443 type A dans le cas d'un lecteur dont la puissance est facilement atteignable avec un amplificateur du commerce, ou fabriqué par l'attaquant. Les résultats obtenus sont montrés sur la figure 4.10. Le transpondeur 1 peut être lu à 40 cm à 13.56 MHz et à 1 m – soit 2.5x plus loin – à sa fréquence de résonance. Le transpondeur 2, dont le facteur de qualité est beaucoup plus faible ne peut être lu qu'à 26 cm peu importe la fréquence de la porteuse. Enfin, le transpondeur 3 peut être lu à 43 cm à sa fréquence de résonance.

Ces résultats nous permettent de faire deux remarques encore absentes de la littérature sur l'attaque sangsue. Premièrement, à puissance fixée, la portée de l'attaque dépend des caractéristiques du transpondeur (fréquence de résonance, facteur de qualité...). On observe ainsi que le transpondeur 3 – fonctionnant avec une smartcard – peut être lu à une distance inférieure à celle du transpondeur 1 – qui lui contient une électronique plus simple. Par conséquent, lorsque l'attaque sangsue est réalisée expérimentalement, il est nécessaire de préciser les caractéristiques des transpondeurs testés. Deuxièmement, choisir une fréquence de porteuse f_0 proche de celle du transpondeur attaqué permet bien d'atteindre une distance de lecture plus élevée : 2.5x plus élevée dans le cas du transpondeur 1. Connaître la fréquence de résonance d'un transpondeur n'est cependant pas facile : elle varie d'un fabriquant à l'autre et dépend des incertitudes sur les composants choisis.

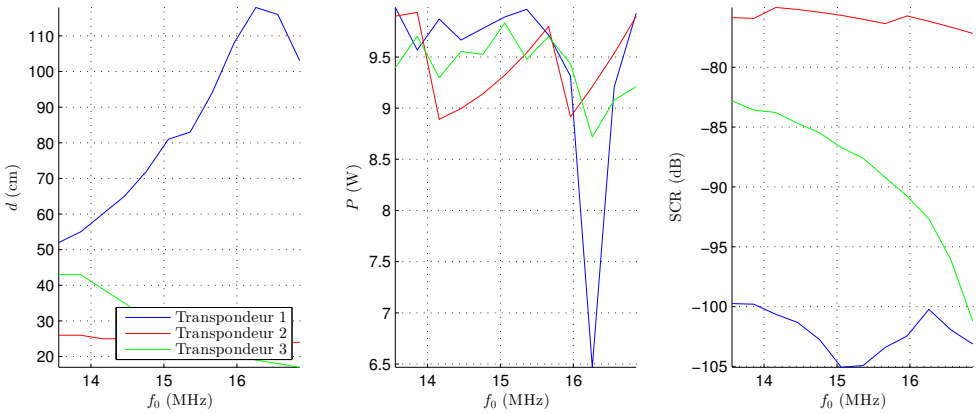

Figure 4.10 Distances de lecture des transpondeurs et puissances de la porteuse pour le scénario 2 (lecteur de 10 W).

De plus, nos calculs optimistes du SCR montrent que pour atteindre la distance maximale de lecture des transpondeurs étudiés, il est au moins nécessaire de filtrer entre 105 dB et 125 dB de porteuse. Dans le cas du scénario 2, atteindre la distance maximale de lecture du transpondeur 1 requière un filtre de 100 dB. Cependant, selon [12], un lecteur ordinaire de RFID en bande HF filtre seulement 80 dB de porteuse. Une solution de filtrage plus performante est donc nécessaire dans le cas de l'attaque sangsue. Le chapitre suivant de ce mémoire porte sur nos efforts pour fabriquer et tester un tel filtre.

CHAPITRE 5

ASPECTS EXPÉRIMENTAUX DE L'ATTAQUE SANGSUE

Une des difficultés techniques de l'attaque sangsue, qui n'a pas encore été résolue dans la littérature, est le filtrage de la porteuse dans le circuit de réception du lecteur. Elle est en effet plus puissante que dans le cas d'un lecteur ordinaire et le SCR est plus faible. Dans ce chapitre, nous détaillons nos efforts pour la fabrication d'un filtre adapté aux transpondeurs ISO 14443 pour l'atténuation de la porteuse ainsi que l'expérience que nous avons envisagé pour le tester. Nous verrons d'abord comment nous avons conçu ce filtre et quelle atténuation nous avons pu atteindre. Nous verrons ensuite l'expérience que nous proposons pour tester ce filtre dans un système de RFID simplifié et faire un premier pas dans la direction d'une implémentation de l'attaque sangsue.

5.1 Filtrage de la porteuse

Le filtre de la chaîne de réception est essentiel pour éliminer la porteuse émise par le lecteur et permettre l'extraction du signal du transpondeur. Nous avons fabriqué trois prototypes de filtres passifs pour essayer d'atteindre une atténuation suffisante de la porteuse, ils seront présentés dans cette section.

5.1.1 Filtre elliptique d'ordre 3

Les filtres elliptiques sont connus pour avoir une raideur optimale, ils sont donc adaptés aux situations où il est nécessaire d'avoir une transition très brutale entre la bande passante et la bande rejetée. En contrepartie, ils présentent d'importantes variations de gain et de phase. Dans la bande rejetée, ces variations sont dues aux zéros de la fonction de transfert du filtre. La figure 5.1 montre le schéma d'un tel filtre avec une topologie série. Le zéro est dû au circuit RLC résonant formé par C_p, L_p et la résistance équivalente série de l'inductance R_p.

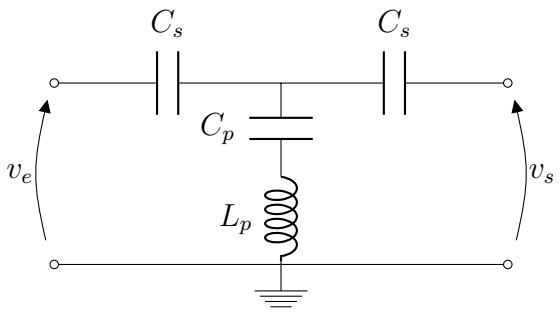

Figure 5.1 Schéma d'un filtre elliptique d'ordre 3 avec une topologie série.

L'idée que nous avons eue est de faire correspondre ce zéro du filtre avec la fréquence f_0 de la porteuse émise par le lecteur afin de l'atténuer fortement. La figure 5.3 montre le gain d'un filtre elliptique passe-haut passif d'ordre 3 dont le zéro est égal à 13.56 MHz. On peut observer que même un filtre d'ordre 3 est suffisamment raide pour que la bande latérale supérieure de la norme ISO 14443A type A (et *a fortiori* pour le type B) soit peu atténuée. On a par ailleurs fait varier l'ESR R_p entre 0.1 à 4.1 Ω.

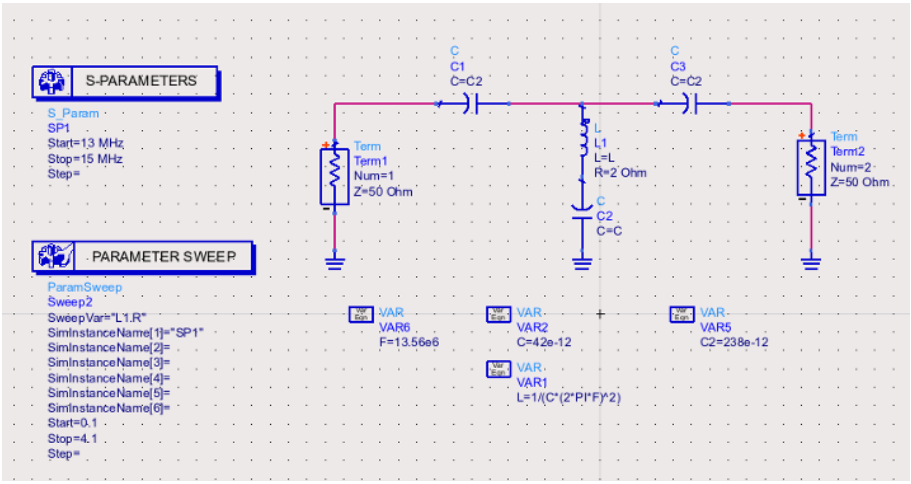

Figure 5.2 Simulation du filtre elliptique avec ADS.

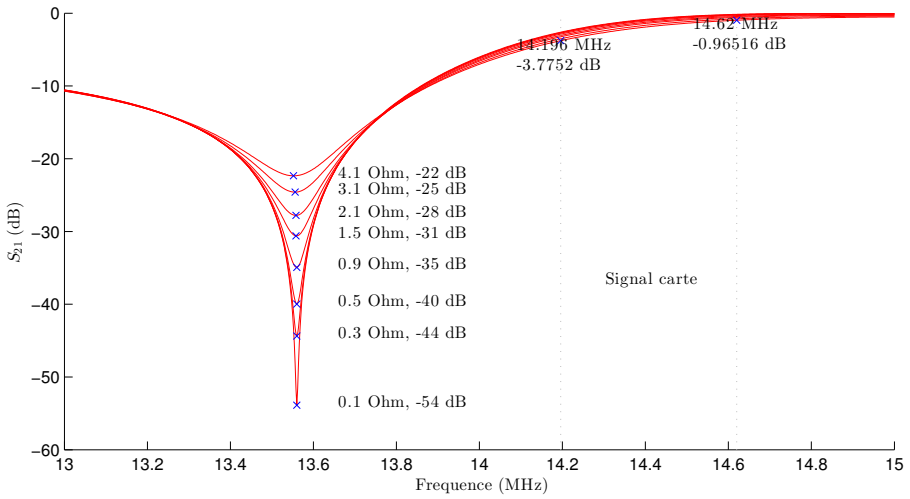

Figure 5.3 Résultat de la simulation : gain du filtre pour différentes valeurs de R_p.

En pratique, nous nous sommes aperçus en mesurant les ESRs de plusieurs bobines commandées sur digikey que celles-ci sont trop élevées pour atteindre une atténuation de plus de 25 dB. La meilleure bobine que nous avons achetée a en effet une ESR de 3 Ω à 13 MHz. De plus, l'ESR augmente très rapidement avec la fréquence à cause de l'effet de peau : la même bobine a une ESR de 2.2 Ω à 10 MHz.

Nous avons donc essayé d'utiliser du fil de Litz pour fabriquer nous même une bobine avec un meilleur facteur de qualité. Un fil de Litz contient un grand nombre de brins de cuivre isolés, il permet ainsi de limiter l'effet de peau en augmentant la surface efficace du conducteur. Nous avons utilisé un fil comprenant 175 brins de 46 AWG. La photo 5.4 montre la bobine obtenue ainsi que l'analyseur d'impédance utilisé pour toutes nos mesures.

L'ESR obtenue à 13 MHz est de 4 Ω pour une inductance de 4.4 µH. Cette solution ne permet donc pas d'améliorer significativement la qualité du filtre. L'explication vient sans doute d'un phénomène difficile à modéliser appelé "effet de proximité" : la proximité entre les brins du fil provoque une baisse de la surface efficace du conducteur quand la fréquence augmente. À partir d'un certain nombre de brins, l'avantage apporté par la diminution de l'effet de peau est en fait annulé par ce phénomène.

Nous avons ensuite décidé d'augmenter l'ordre du filtre pour essayer d'obtenir une meilleure atténuation de la porteuse avec des bobines ayant des ESR de l'ordre du Ohm.

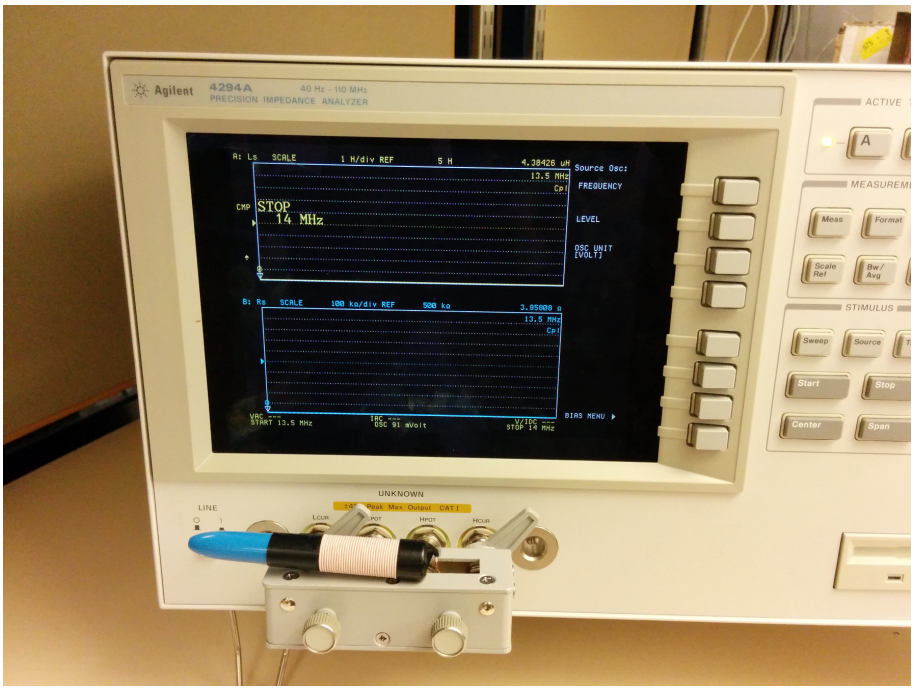

Figure 5.4 Mesure de l'impédance de la bobine maison.

5.1.2 Premier filtre d'ordre 5

Pluôt que de réaliser un filtre elliptique d'ordre 5, dont l'un des deux zéros seulement serait ajusté sur f_0, nous proposons de superposer les deux zéros sur cette fréquence pour atténuer au maximum la porteuse. Le filtre présenté ici n'est donc pas un filtre elliptique d'ordre 5, il en a seulement la topologie. La figure 5.5 montre le schéma électrique du filtre.

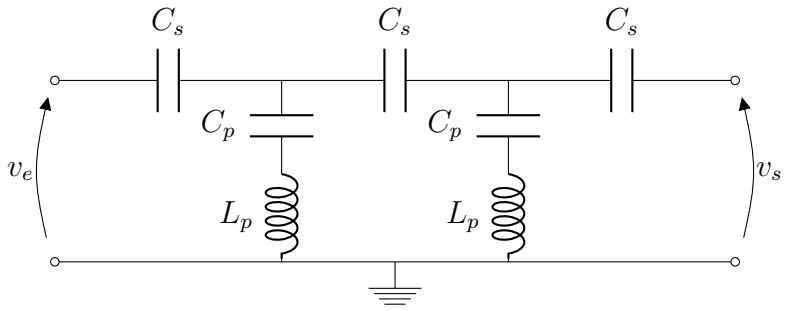

Figure 5.5 Schéma électrique du filtre d'ordre 5.

Nous avons simulé ce filtre avec le logiciel ltspice de Linear Technology. Les valeurs des capacités C_p et L_p ne posent pas de problème, l'essentiel est de former un circuit RCL résonant à 13.56 MHz. Plus L_p est grand, plus la transition entre la bande rejetée et la bande passante

est rapide. Cependant, plus L_p augmente, plus l'ESR limite le taux de rejet de fréquence éliminée. Nous avons ainsi choisi L_p de l'ordre de 4 µH. La valeur de C_s a été choisi à partir de celle du filtre d'ordre 3. Nous avons ensuite fait varier sa valeur dans ltspice en cherchant à maximiser le taux de rejet de la porteuse. L'image 5.6 montre un résultat de simulation dans ltspice.

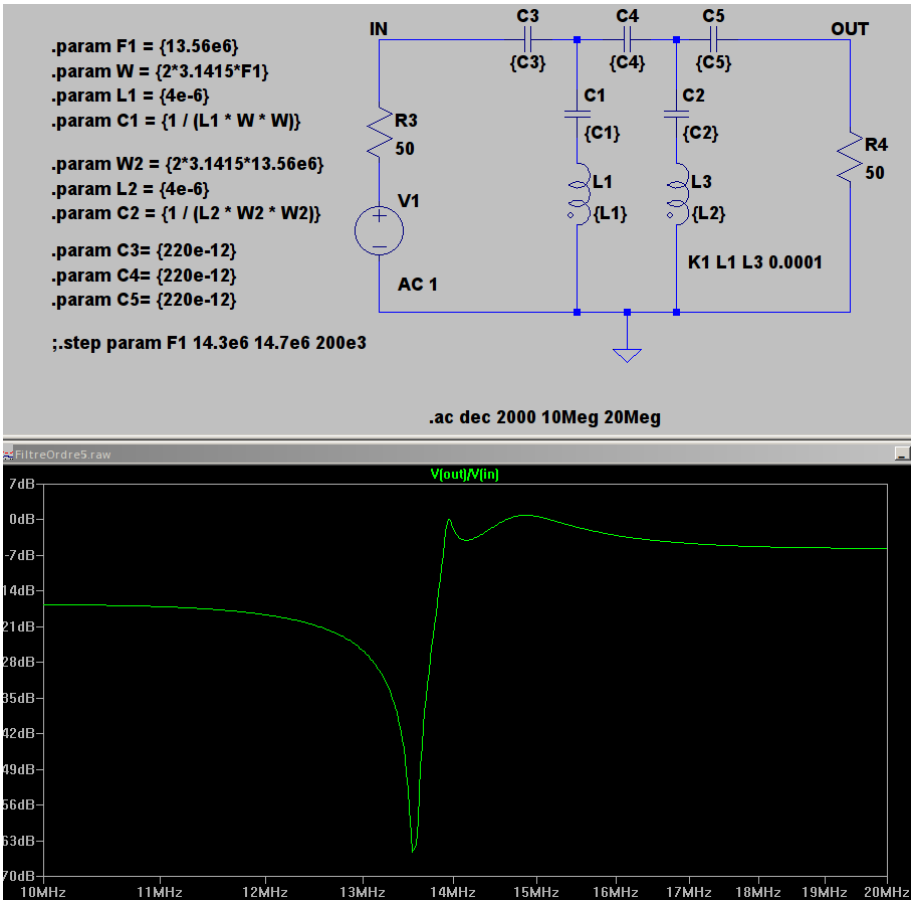

Figure 5.6 Simulation du filtre d'ordre 5 avec ltspice.

Nous avons ensuite fabriqué le filtre en utilisant des capacités en mica et argent. Ce type de capacité présente d'excellents facteurs de qualité. Par exemple, nous avons mesuré qu'une une capacité en mica de 220 pF présente une ESR de seulement 60 mΩ à 13 MHz et une fréquence de résonance de l'ordre de 100 MHz. Pour les bobines, nous avons premièrement utilisé deux bobines commandées chez digikey du modèle ayant l'ESR la plus faible que nous avons pu trouver (3 Ω à 13 MHz). Nous avons ensuite essayé de remplacer l'une d'elles par la bobine en fil de Litz. La photo 5.7 montre le PCB du circuit. Par ailleurs, nous avons placé deux capacités variables en série avec les deux bobines. Nous les avons ajustées à la main

pour rejeter la fréquence 13.56 MHz.

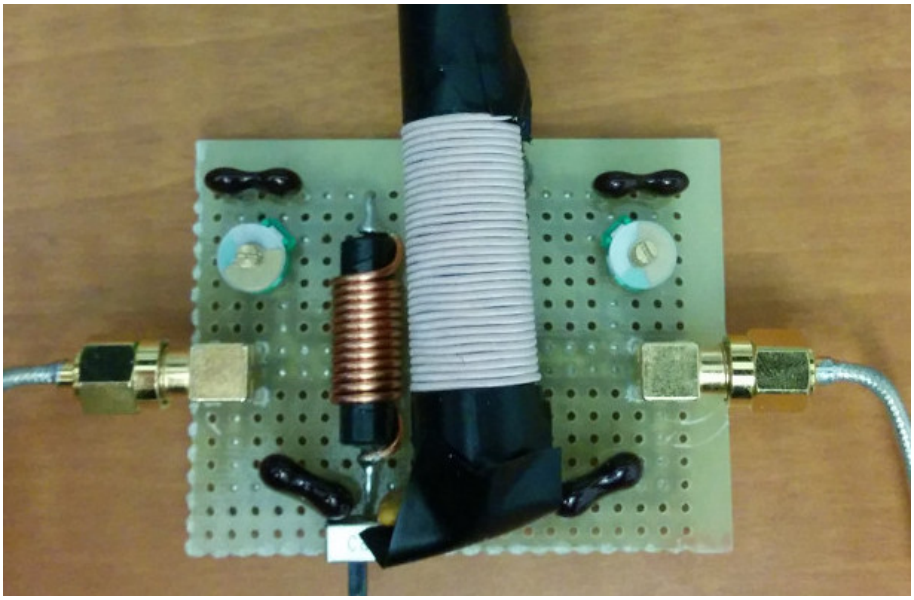

Figure 5.7 Filtre d'ordre 5 avec une bobine 20% ferrite et la bobine en fil de Litz.

Les figures 5.8 et 5.9 montrent les performances obtenues en pratique, les courbes ont étés obtenus avec un analyseur de réseaux Agilent E5071C.

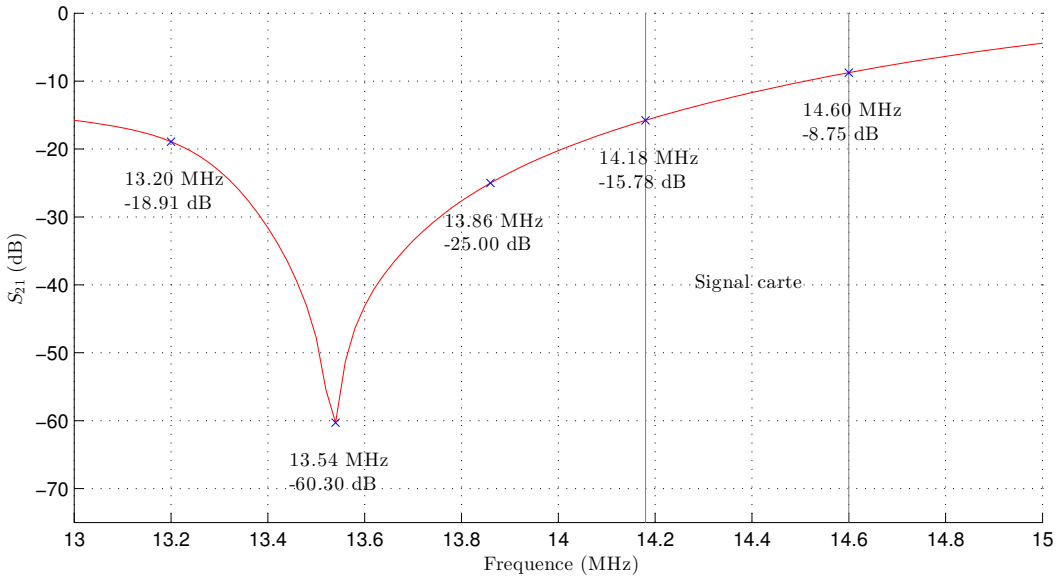

Figure 5.8 Gain du filtre d'ordre 5 avec deux bobines 20% ferrite.

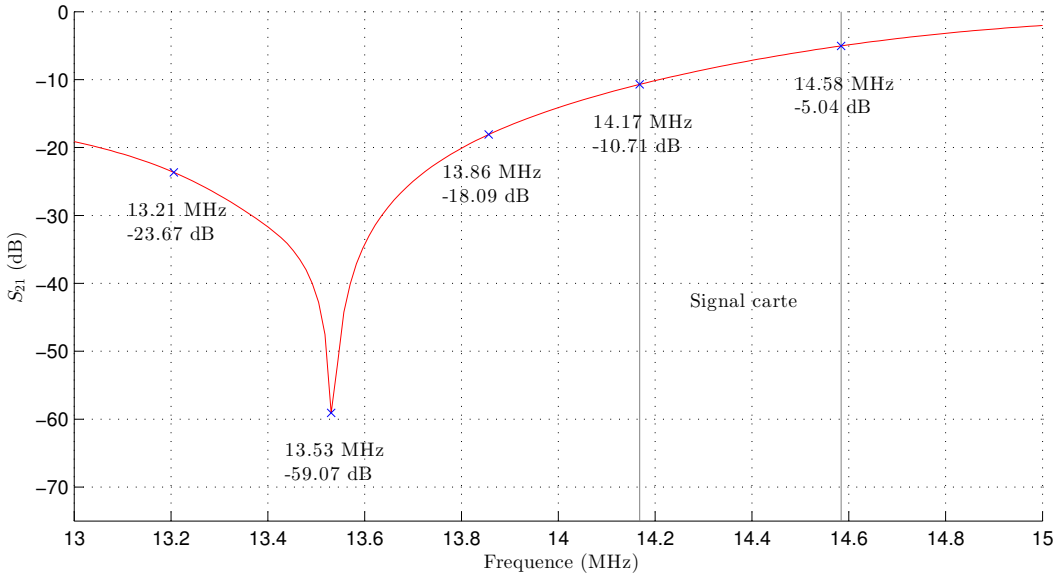

Figure 5.9 Gain du filtre d'ordre 5 avec une bobine 20% ferrite et la bobine en fil de Litz.

La seconde configuration donne de meilleurs résultats, car la bande passante est moins fortement atténuée (11 dB au lieu de 16 dB à 14.2 MHz). Sur la bande de fréquence occupée par le signal du transpondeur, l'atténuation varie entre 11 et 5 dB, le taux de rejection de la porteuse est donc d'environ 50 dB.

5.1.3 Second filtre d'ordre 5

La transition entre la bande rejetée et la bande passante du filtre précédent est plus lente que prévu par les simulations. Nous avons donc cherché à vérifier si le problème est dû à l'augmentation trop rapide des ESR des bobines utilisées. Pour cela nous avons fabriqué une dernière bobine utilisant un fil de diamètre beaucoup plus large afin de limiter au maximum son ESR.

Nous avons ainsi bobiné environ 13 tours d'un fil de cuivre composé de 5 brins et de diamètre 3 mm autour d'un tube en carton de diamètre 7 cm. Des simulations avaient été préalablement effectuées afin de s'assurer que l'inductance obtenue soit de l'ordre de 4 µH. Ce premier essai a donné une inductance de 9 µH. Après avoir retiré environ 6 tours, nous avons mesuré une inductance de 4.4 µH, une ESR inférieure à 1 Ω à 13 MHz et une fréquence de résonance d'environ 35 MHz. La photo 5.10 montre la bobine connectée à l'analyseur de réseaux Agilent E5071C que nous avons utilisé pour les mesures.

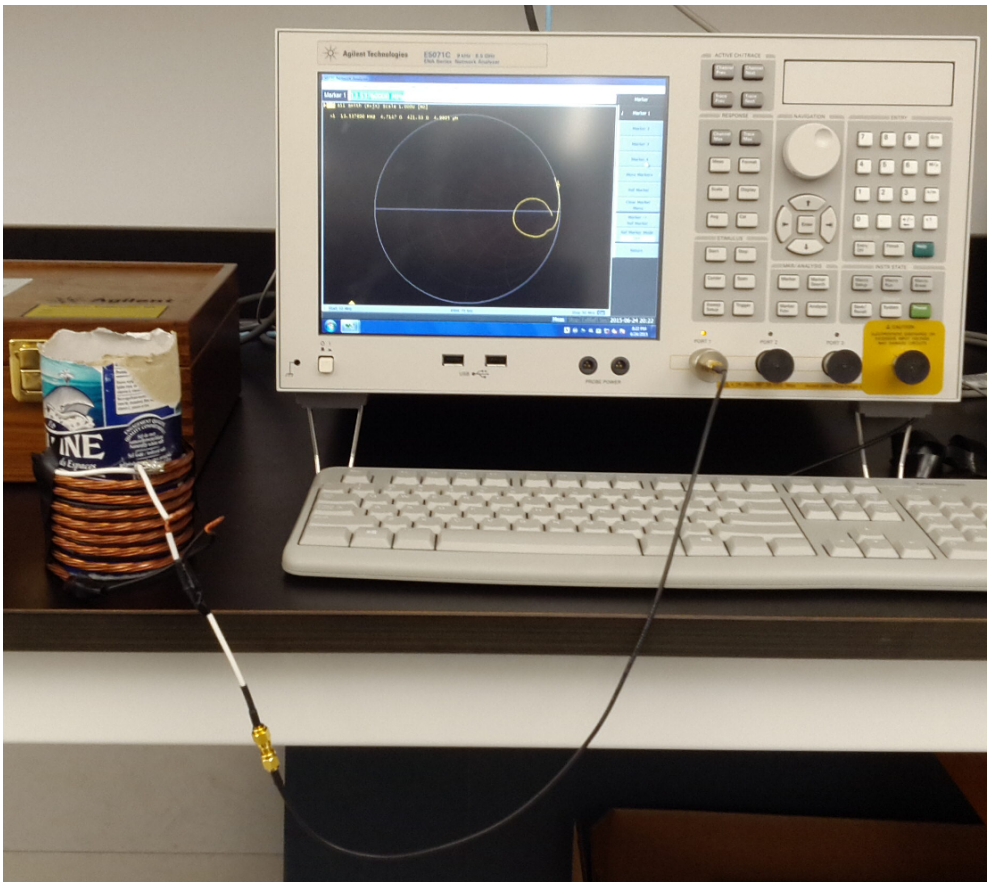

Figure 5.10 Mesure de l'impédance de la bobine de 7 cm de diamètre.

L'ESR finalement obtenu est significativement plus faible. Nous avons alors remplacé, sur le filtre de la section précédente, la bobine en fil de Litz par cette nouvelle bobine. La photo 5.11 montre la mesure du gain du filtre obtenu avec l'analyseur de réseaux Agilent E5071C. Enfin, la courbe 5.12 montre le tracé du gain du filtre.

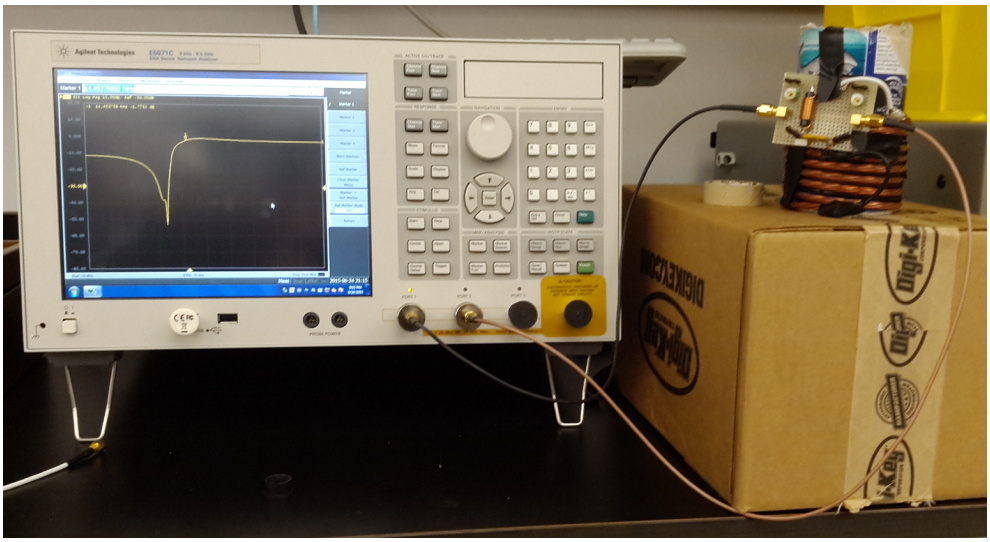

Figure 5.11 Mesure du gain du second filte d'ordre 5.

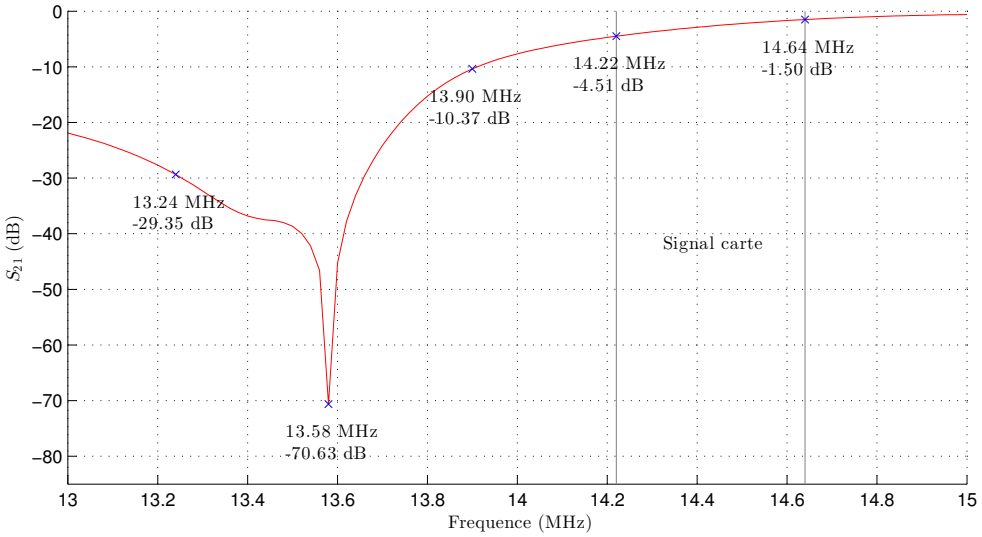

Figure 5.12 Gain du second filte d'ordre 5.

5.1.4 Résumé

Le filtre que nous proposons a l'avantage d'avoir un ordre faible qui simplifie sa fabrication. Il est sans doute possible de l'améliorer encore en remplaçant la deuxième bobine du filtre par une bobine de taille plus importante. La réponse du filtre est cependant pour l'instant très sensible à l'environnement, la fabrication d'un boîtier blindé autour du filtre permettrait de régler ce problème.

Nous avons utilisé notre modèle théorique pour estimer la distance de lecture atteignable avec un filtre atténuant seulement 65 dB de porteuse comme celui que nous avons fabriqué ici. Même pour le transpondeur MIFARE, qui a le facteur de qualité le plus élevé des trois modèles de transpondeur dont nous disposons, la distance de lecture n'atteint que 32 cm à la résonance. Seul, ce filtre ne peut donc être utilisé pour améliorer l'état de l'art sur l'attaque sangsue. Il serait donc nécessaire de fabriquer un second étage de filtrage, qui lui pourrait être actif, pour atteindre une atténuation intéressante de la porteuse.

5.2 Système de RFID simplifié

Plutôt que d'implémenter directement un système de RFID complet utilisant notre filtre pour l'atténuation de la porteuse, nous proposons le montage représenté sur la figure 5.13.

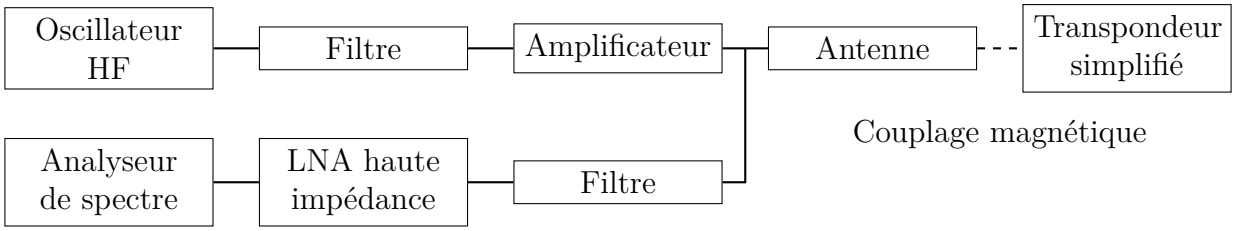

Figure 5.13 Architecture du lecteur RFID simplifié.

Au lieu d'émettre un signal respectant une norme de la RFID, seule la porteuse est générée en continue par un oscillateur HF. Le transpondeur utilisé, que nous appellerons "transpondeur simplifié", n'est pas un véritable transpondeur et se contente lorsqu'il est correctement alimenté par le champ magnétique de l'antenne de réaliser une modulation de charge. Il n'y a ainsi pas de paquets d'octets envoyés entre un lecteur et un transpondeur, mais juste une modulation de charge présente en permanence aussi longtemps que le transpondeur simplifié est suffisamment alimenté.

L'objectif de cette expérience est de s'assurer que la partie puissance du système fonctionnne bien, et que le filtre proposé permet de correctement filtrer la porteuse sans se préoccuper du respect d'une norme de RFID (ISO 14443 type A ou B). Il s'agit d'une étape intermédiaire avant l'implémentation d'une attaque sangsue complète. Lorsque le transpondeur simplifié est placé à une distance d de l'antenne, en mesurant sur l'analyseur de spectre l'amplitude de la bande latérale supérieure de la modulation d'amplitude ainsi que le niveau de bruit, on peut déterminer approximativement si l'attaque est possible.

Chacune des parties de cette section porte sur un des étages du montage sur lesquels nous avons travaillé.

5.2.1 Oscillateur HF

Plusieurs raisons nous ont poussées à fabriquer nous même l'oscillateur plutôt que de directement filtrer la sortie d'un générateur de fonction, cette solution permet en effet :

— d'utiliser facilement une batterie pour alimenter l'oscillateur de façon à limiter le bruit provenant du secteur
— d'utiliser un quartz pour limiter au maximum le bruit sur la phase de la porteuse
— de limiter le nombre de composants de l'électronique et de pouvoir les choisir les plus silencieux possible

Nous avons alors choisi de fabriquer un oscillateur de Pierce. La chaîne d'amplification de ce type d'oscillateur est formée par une porte logique NOT. La chaîne de réaction est formée par un quartz et deux capacités. La figure 5.14 montre le schéma électrique de l'oscillateur, la source d'alimentation de la porte NOT n'est pas représentée.

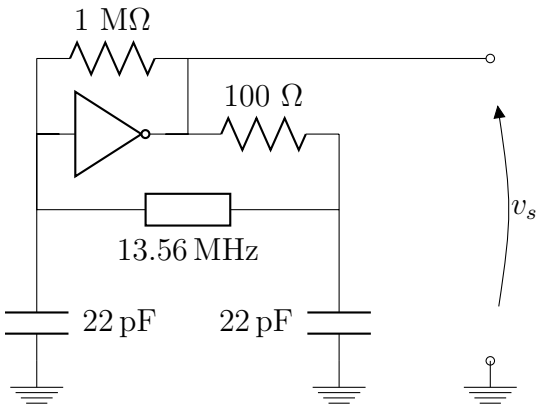

Figure 5.14 Schéma électrique de l'oscillateur de Pierce fabriqué.

Pour la porte NOT, nous avons utilisé un circuit intégré MC74VHC1GT04 de chez ON Semiconducteur que nous avons alimentée avec un régulateur linéaire LT1962 de Linear Technologies. L'oscillateur est isolé du reste de l'électronique avec un tampon 74LVC1G126 de chez NXP.

5.2.2 Filtrage de la sortie de l'oscillateur

L'oscillateur HF est suivi d'un filtre qui permet d'atténuer, d'une part le bruit de l'électronique de l'oscillateur, et d'autre part les harmoniques de la porteuse. Nous l'avons conçu en utilisant le logiciel ADS ("Advanced Design System") qui est une référence pour la conception de filtres et qui fournit de nombreux outils pour en faciliter le développement. Nos critères de qualité ont été les suivants :

- la seconde harmonique à 27.12 MHz doit être fortement atténuée : nous avons décidé d'avoir une atténuation d'au moins 50 dB de celle-ci.
- le filtre ne doit pas contenir d'inductance trop élevée, aux fréquences qui nous intéressent, il faut limiter celles-ci à quelques µH ($3-4\mu H$). Nous reviendrons sur ce critère dans la section concernant le filtre de la porteuse de la chaîne de réception qui est en fait le premier filtre sur lequel nous avons travaillé. Le choix des inductances est un des problèmes les plus délicats que nous avons rencontrés pour la conception de filtre dans la bande HF à cause de leur résistance équivalente série ("ESR") qui augmente très rapidement avec la fréquence et l'inductance.
- l'ordre du filtre ne doit pas être trop élevé pour faciliter sa fabrication.

Après avoir essayé plusieurs types de réseaux passifs (elliptique, Butterworth...), nous avons décidé d'utiliser un filtre de Tchebychev d'ordre 3 avec une topologie parallèle. Ce choix permet de respecter les spécifications précédentes. En particulier, il ne contient qu'une seule inductance de l'ordre dû µH ce qui simplifie grandement sa fabrication. La figure 5.15 montre une des dernières étapes de sa conception dans ADS qui a concerné le choix de la capacité C_2. Une des étapes de la conception a en effet été d'itérer la génération du filtre de sorte que les valeurs idéales des composants puissent être remplacées par celles de la série normalisée E12, car elles sont les plus faciles à trouver dans le commerce.

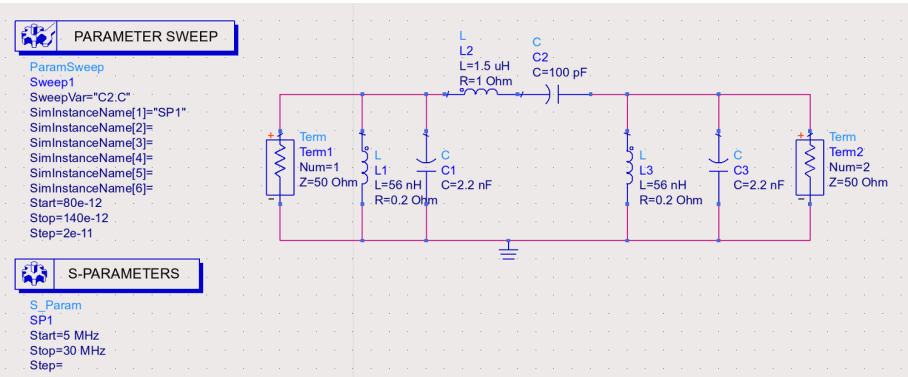

Figure 5.15 Simulation du filtre avec ADS.

Finalement le filtre obtenu et sa réponse fréquentielle sont montrés respectivement sur les figures 5.16 et 5.17 .

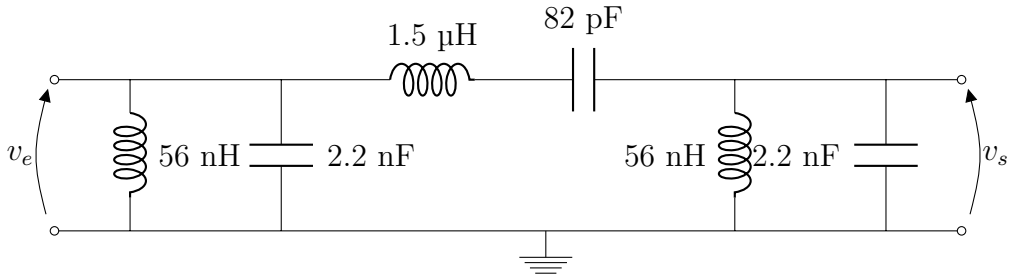

Figure 5.16 Schéma électrique du filtre retenu.

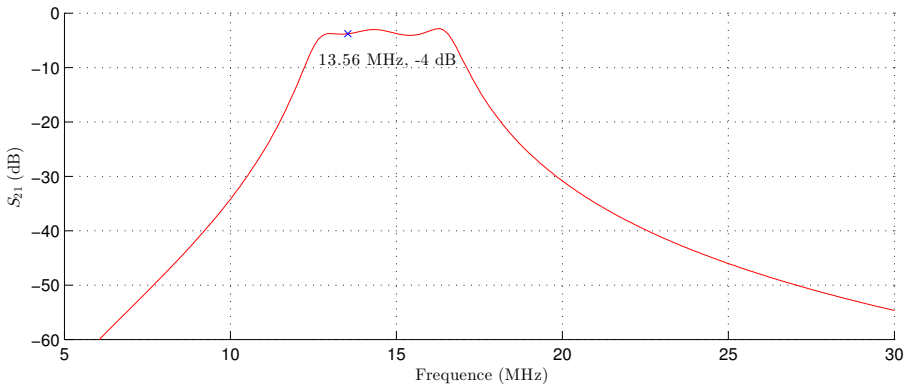

Figure 5.17 Résultat de la simulation du gain avec ADS.

La photo 5.18 montre le circuit comprenant l'oscillateur HF et son filtre que nous avons fabriqué. La photo 5.19 montre la transformée de Fourier du signal de sortie du montage. Il contient bien un pic important à 13.6 MHz environ. Le premier harmonique $2f_0$ du signal n'est pas visible à l'oscilloscope. Le signal indésirable le plus visible se trouve à 32.4 MHz, et a une amplitude 45 dB plus faible que la porteuse.

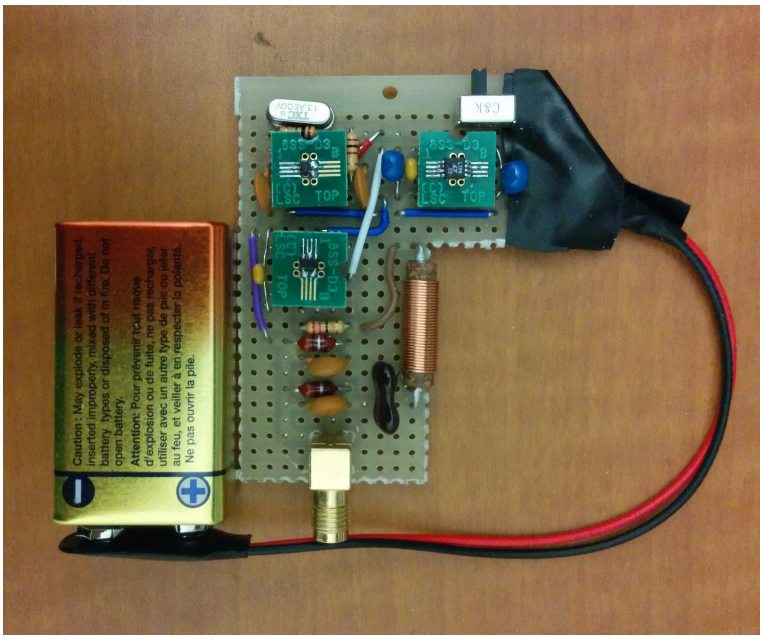

Figure 5.18 Photo de l'oscillateur suivi de son filtre.

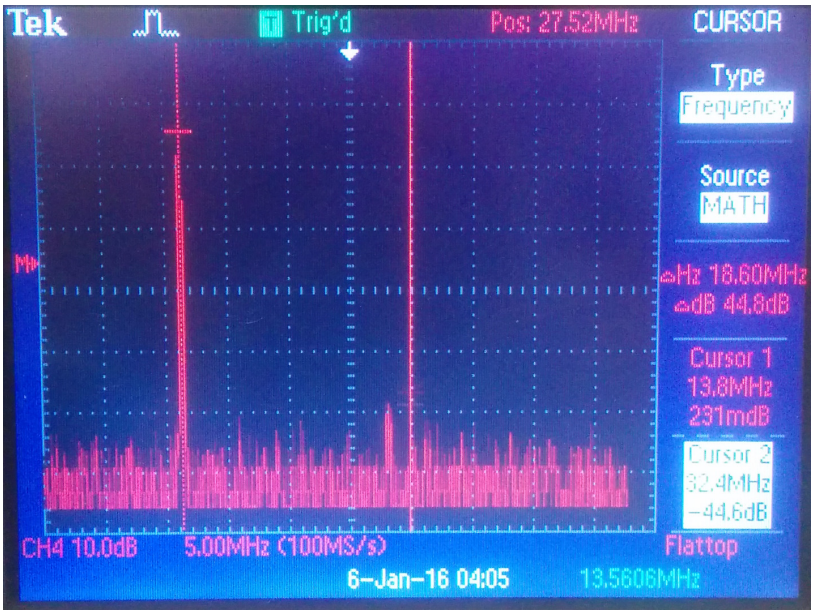

Figure 5.19 FFT du signal de sortie de l'oscillateur capturé à l'oscilloscope.

5.2.3 Antenne cadre

L'antenne dont nous disposons une antenne cadre magnétique de 40 cm de diamètre, elle est fabriquée par la société SCEMTEC spécialement pour des applications de RFID à

13.56 MHz. C'est cette même antenne que Pierre Brun-Murol [3] a utilisé pour l'expérience où il a cherché la distance maximale à laquelle il pouvait alimenter une carte HID iCLASS®.

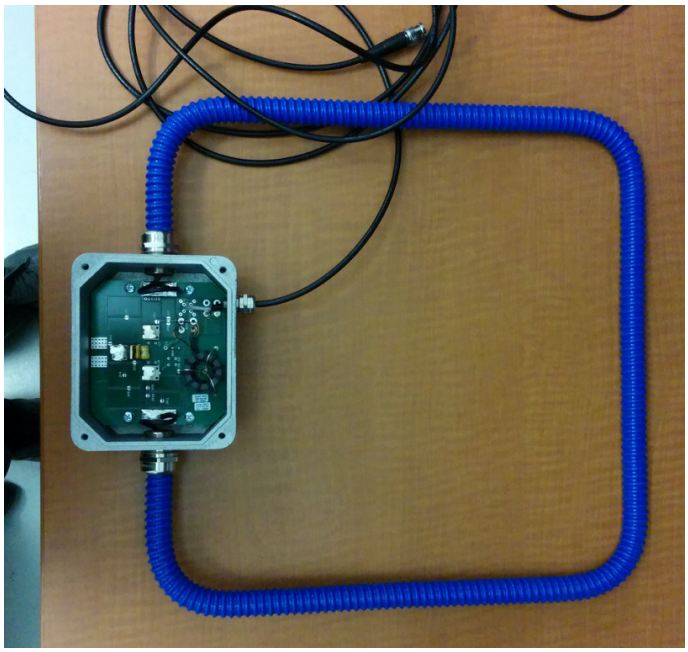

Figure 5.20 Antenne SCEMTEC utilisée pour l'expérience.

Pour une attaque sangsue sur un transpondeur ISO 14443, nous avons vu que le facteur de qualité ne doit pas dépasser 15. Nous avons donc commencé par mesurer le facteur de qualité de l'antenne pour s'assurer que cette condition est bien vérifiée. Pour cela, nous avons besoin de connaître l'inductance et la résistance de la boucle de l'antenne à environ 13 MHz.

Il n'est pas possible de déconnecter le câble coaxial de l'antenne, nous avons donc commencé par le court-circuiter au niveau du boîtier de l'antenne pour tenir compte du déphasage induit par celui-ci pour les mesures suivantes. Nous avons ensuite court-circuité les composants du circuit d'accord de façon à ne laisser que la boucle de l'antenne connectée au câble coaxial. Il est alors possible de mesurer à l'aide d'un analyseur de réseaux l'impédance de la boucle.

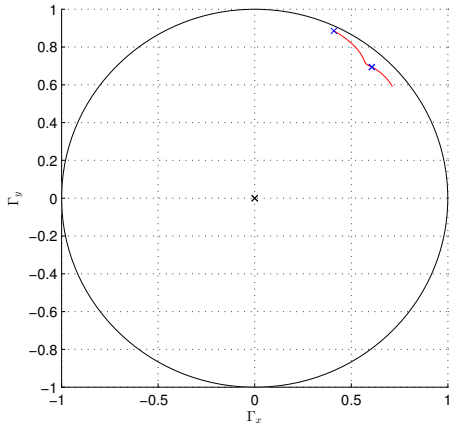

Figure 5.21 Impédance de la boucle de l'antenne entre 12 et 15 MHz représentée sur un abaque de Smith.

Sur la figure 5.21, on observe bien un comportement inductif et résistif, on peut d'ailleurs voir que la résistance augmente avec la fréquence. À 13.56 MHz, on trouve une inductance de 1.2 µH et une résistance de 12 Ω. Vu la section de la boucle sa résistance ne doit pas dépasser 1 ou 2 Ω, notre mesure est donc beaucoup trop imprécise.

Nous avons alors essayé une autre méthode pour mesurer le facteur de qualité de l'antenne. Nous avons mesuré sa bande passante à -10 dB pour le paramètre S_{11} (figure 5.22) ainsi que sa fréquence de résonance. Nous avons ensuite modélisé son circuit d'accord sur matlab – qui comprend un balun 4 :1, deux capacités et une résistance de "damping" – et cherché pour quel facteur de qualité la même bande passante est obtenue. Avec cette méthode, nous avons trouvé $Q_a = 25$.

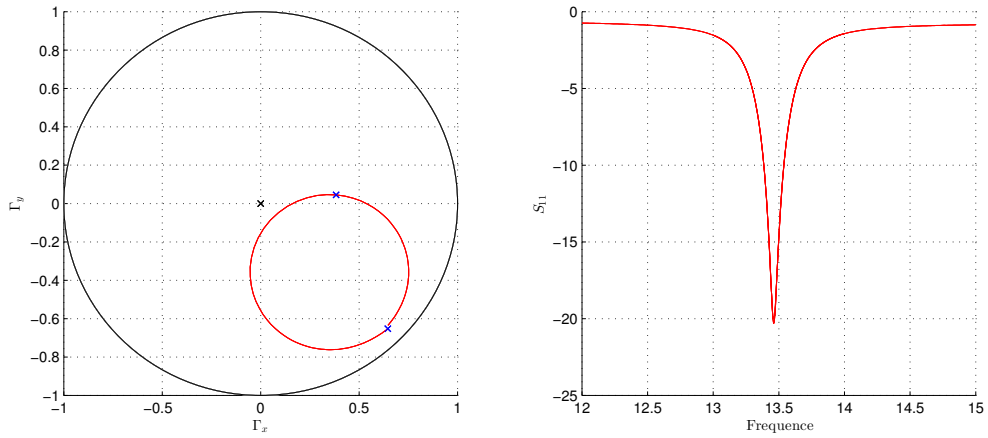

Figure 5.22 Impédance de l'antenne entre 12 et 15 MHz représentée sur un abaque de Smith à gauche et paramètre S_{11} à droite.

Le facteur de qualité de cette antenne est donc trop élevé, pour réaliser l'expérience que nous proposons, il est nécessaire de remplacer les composants de son circuit d'accord de manière à abaisser son facteur de qualité.

5.2.4 Transpondeur simplifié

Le schéma électrique du transpondeur simplifié est inspiré du circuit donné par Finkenzeller dans [12]. Ce schéma est montré sur la figure 5.23. Il est constitué d'une antenne modélisée par une inductance en série avec une ESR. En parallèle de l'antenne, une capacité variable permet d'accorder le transpondeur. L'ensemble est relié à un pont redresseur permettant de fournir la tension continue qui alimente un compteur. La porteuse sert d'horloge au compteur qui la divise par un facteur 16. Une charge R_3 est ainsi connectée et déconnectée au circuit à une fréquence de $f_0/16$ ce qui provoque la modulation de charge. Une diode zener permet de limiter la tension fournie au compteur à 3 V. Enfin, nous avons rajouté une LED qui s'allume lorsque le circuit est alimenté et qui permet de vérifier rapidement son fonctionnement.

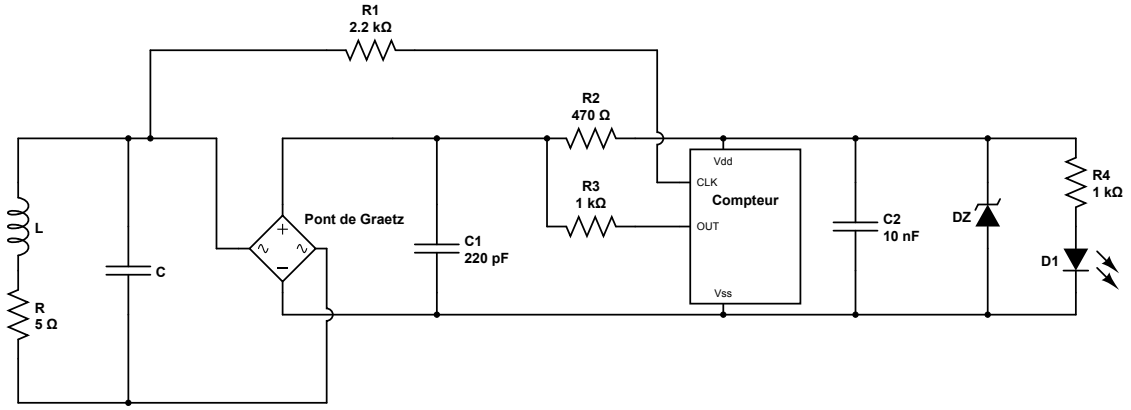

Figure 5.23 Schéma électrique du transpondeur simplifié.

La photo 5.24 montre le prototype fabriqué. Nous avons utilisé une antenne prévue pour la Proxmark3.

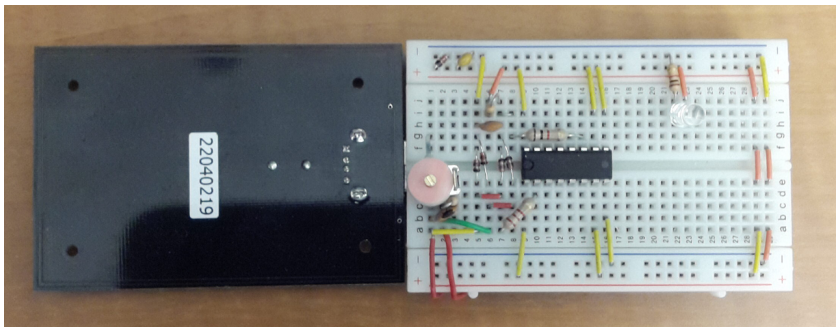

Figure 5.24 Transpondeur simplifié.

Pour vérifier le fonctionnement du transpondeur simplifié, nous avons utilisé une Proxmark3 configurée pour émettre une porteuse à 13.56 MHz. La photo 5.25 montre le placement du transpondeur et de l'antenne de la Proxmark3 pendant l'expérience.

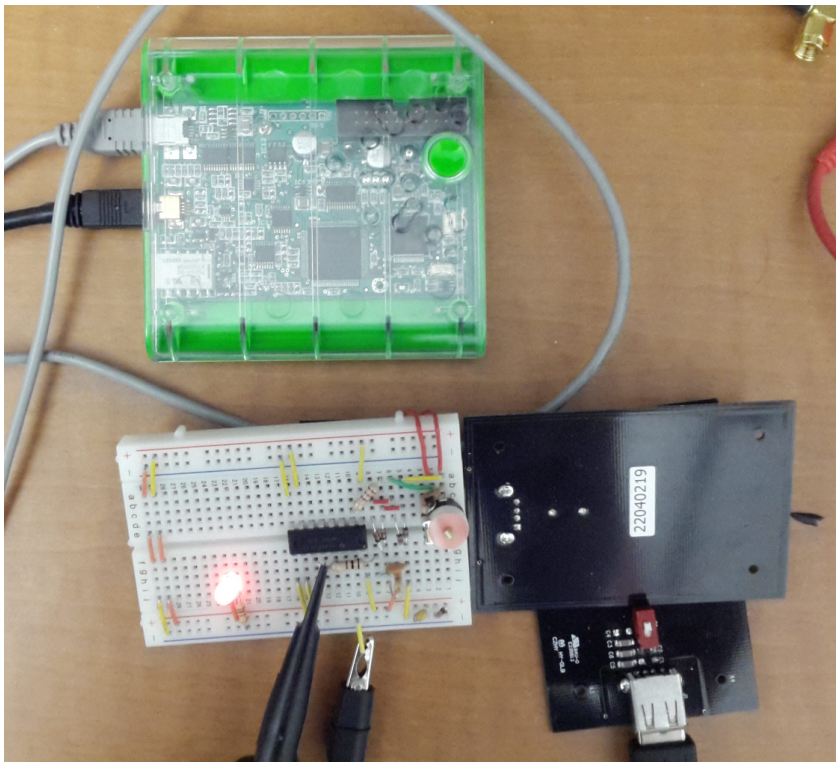

Figure 5.25 Transpondeur simplifié alimenté par la Proxmark3.

Nous avons alors capturé les tensions présentes en sortie du compteur (photo 5.26) et aux bornes de l'antenne du transpondeur (photo 5.27).

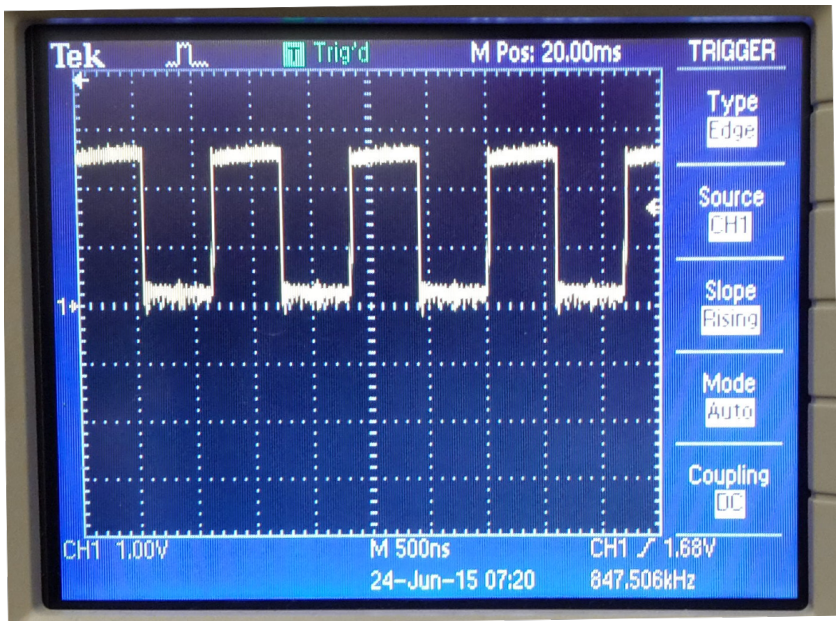

Figure 5.26 Tension de sortie du compteur du transpondeur simplifié.

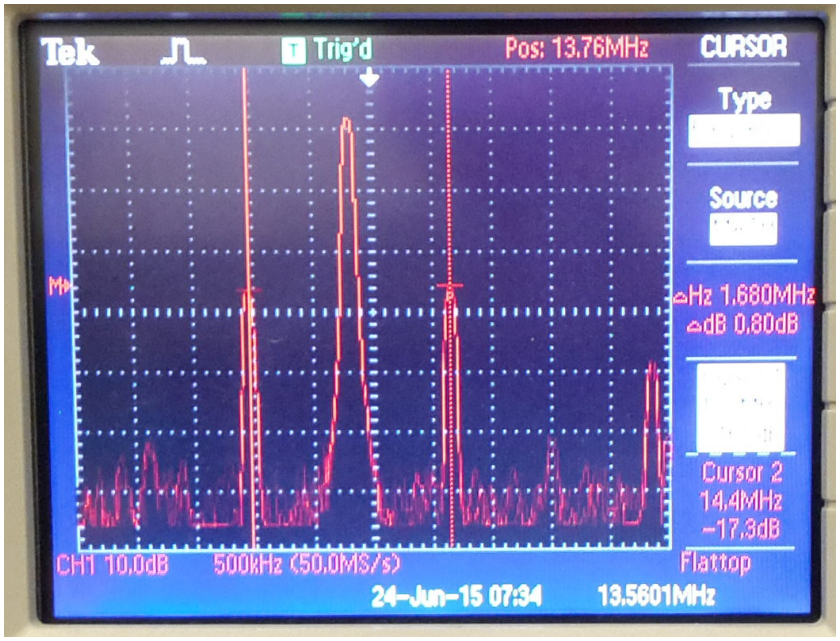

Figure 5.27 Transformée de Fourier du signal aux bornes de l'antenne du transpondeur simplifié.

La photo 5.27 montre bien les deux bandes latérales de la modulation d'amplitude créée par le transpondeur et valide son bon fonctionnement. Cependant, en l'état sont intérêt reste limité, car son facteur de qualité n'est pas bien connu. Un moyen de mesurer le facteur de

qualité Q_{max_0} quand la résistance de modulation R_3 est déconnectée et le facteur de qualité Q_{min_0} quand celle-ci est connectée est nécessaire.

5.3 Résultats

Nous avons présenté les trois essais de filtres passifs que nous avons fabriqués dans le but d'atténuer la porteuse dans le circuit de réception d'un lecteur RFID. Notre dernier essai permet d'atténuer celle-ci de 65 dB. L'atténuation est alors au maximum de 4.5 dB dans la bande passante du signal du transpondeur. Un autre étage de filtrage, qui pourrait par exemple être actif, serait nécessaire pour atteindre une distance de lecture qui dépasse significativement les résultats déjà obtenus dans la littérature pour l'attaque sangsue sur les transpondeurs ISO 14443.

Nous avons ensuite présenté une expérience que nous avons envisagée pour tester ce filtre et faire un premier pas dans la direction d'une implémentation complète de l'attaque sangsue sur les transpondeurs ISO 14443. Nous avons alors montré les différents étages du montage sur lesquels nous avons travaillés. Pour finir cette expérience, il faut dans un permier temps améliorer le filtre de la porteuse.

CHAPITRE 6

CONCLUSION

6.1 Synthèse des travaux

La première partie de nos recherches a consisté à chercher une borne supérieure pour la portée de l'attaque sangsue sur les transpondeurs HF dans le cas monostatique (une seule antenne pour le lecteur). Nous avons également évalué les ordres de grandeur de la puissance et du rapport signal sur porteuse (SCR) nécessaires pour l'atteindre. Le modèle d'attaque que nous avons envisagé est nouveau, car nous avons supposé variable la fréquence de la porteuse f_0 du lecteur. Ce travail de modélisation peut être résumé en trois étapes :

1. Modélisation d'un transpondeur HF. Ce travail est couvert par la littérature, nous l'avons résumé dans la section 3.3. Nous avons également tiré de la littérature trois jeux de paramètres pour des transpondeurs ISO 14443 type A (section 3.3.6).
2. Modélisation d'un lecteur RFID en bande HF et de son antenne. Nous considérons le cas d'un lecteur dont la sortie est une source de tension accordée par un réseau capacitif en L à une boucle d'un tour. Les hypothèses de notre modèle sont détaillées dans la section 4.1. Nous n'entrons pas dans le détail du fonctionnement du lecteur, car nous sommes seulement intéressés par l'index de modulation m engendré par le transpondeur aux bornes de l'antenne du lecteur dans le meilleur des cas pour l'attaquant. Nous cherchons pour cela le coefficient de couplage mutuel maximal possible à une distance d du transpondeur dans la section 4.2 et le facteur de qualité Q_a maximal dans la section 4.3.
3. Modélisation des sources de bruits. La seule source de bruit dont nous avons tenu compte est le bruit magnétique ambiant. Les ordres de grandeur pour ce bruit sont tirés de la littérature dans la section 3.5. Nous déduisons alors du calcule de m et du niveau de bruit, la portée maximale de l'attaque.

Nous avons envisagé deux scénarios différents. Le premier ne tient compte que du bruit magnétique ambiant et permet de fixer une borne supérieure à l'attaque sangsue. Nous avons alors trouvé entre 1.2 et 1.4 m selon le transpondeur. Dans le second, la puissance de la porteuse est limitée à 10 W. Les distances de lecture varient alors de 26 cm à 50 cm à 13.56 MHz et, à sa fréquence de résonance, le transpondeur MIFARE peut être lu à 1.2 m.

Ce travail nous permet de faire deux remarques encore absentes de la littérature. Premièrement, la distance de l'attaque varie d'un transpondeur à l'autre. Par exemple, un transpondeur utilisant une smartcard contient plus d'électronique et a donc un facteur de qualité plus faible qu'un transpondeur MIFARE Classic. Sa distance de lecture est donc inférieure. Ainsi, tout travail expérimental sur l'attaque sangsue doit bien préciser les caractéristiques du transpondeur utilisé. Mentionner le standard supporté par le transpondeur ne suffit pas. Deuxièmement, approcher la fréquence de la porteuse de la fréquence de résonance du transpondeur peut permettre d'augmenter la distance de lecture d'un facteur deux environ, dépendamment du transpondeur.

Cela étant dit, malgré nos approximations par excès et la possibilité de faire varier la fréquence f_0 de la porteuse, la portée de l'attaque sangsue sur un transpondeur ISO 14443 type A reste limitée à des distances de l'ordre du mètre au mieux. Ainsi, sous réserve de nos hypothèses (section 4.1), nous ne pensons pas qu'il soit possible de construire un système – financé par exemple par un gouvernement ou le crime organisé, d'une puissance très élevée et comprenant une antenne très grande – permettant de dépasser cet ordre de grandeur dans un environnement où le bruit magnétique ambiant n'est pas contrôlé. Lire un transpondeur HF posé dans un local depuis l'extérieur n'est ainsi pas envisageable. De manière générale, le possesseur d'une carte RFID HF peut se considérer en sécurité si personne n'est à moins d'un mètre de lui. Nos résultats ne contredisent pas les travaux expérimentaux présents dans la littérature [20] [26] qui montrent qu'une attaque à 30 cm est possible.

Nos calculs optimistes du SCR montrent que pour atteindre la distance maximale de lecture des transpondeurs étudiés, il est au moins nécessaire de filtrer entre 105 dB et 125 dB de porteuse. Un lecteur "normal" filtre seulement 80 dB [12] à l'aide, en général, d'un détecteur de crête. Une solution de filtrage plus performante est donc essentielle dans le cas de l'attaque sangsue. La seconde partie de nos recherches concerne cette difficulté. Nous avons conçu un filtre pour atténuer la porteuse f_0 et proposé une expérience pour le tester dans un système de RFID simplifié. Cette expérience est un premier pas avant la fabrication d'un système de RFID complet utilisant le filtre proposé. À la troisième itération du cycle de conception et fabrication, nous avons obtenu un filtre d'ordre 5 capable d'atténuer 66 dB de porteuse et ayant entre -4.5 dB et -1.5 dB d'atténuation dans sa bande passante. Nous avons également été amenés à implémenter un filtre pour la chaîne d'émission du lecteur ainsi qu'un transpondeur simplifié dont la fréquence de résonance et le facteur de qualité peuvent être modifié afin de mesurer en pratique l'influence de ces paramètres. Nous n'avons cependant pas pu finir l'expérience à cause d'un certain nombre de limitations de notre travail : seul, ce filtre

est insuffisant et le matériel que nous avons utilisé était limité. Nous reviendrons sur nos difficultés dans la prochaine section. Notre travail montre cependant que la conception d'un filtre pour l'attaque sangsue n'est pas triviale. L'attaquant doit avoir de bonnes connaissances en électronique pour le fabriquer. Il doit également avoir accès à du matériel coûteux, tel qu'un analyseur de réseaux.

6.2 Limitations

Notre modèle théorique fait quatre hypothèses – détaillées dans la section 4.1 – qui limite sa validité :

1. Nous considérons le cas d'un lecteur dont la sortie est une source de tension accordée par un réseau capacitif en L.
2. Nous supposons une antenne à un seul tour.
3. Nous négligeons le champ lointain émis par l'antenne du lecteur. Nous ne pensons cependant pas que celui-ci change significativement la portée de l'attaque pour deux raisons. Premièrement, les antennes cadre magnétique ont une résistance de radiation très faible, la puissance radiée est donc très faible. Deuxièmement, nous nous attendons à trouver une distance maximale de lecture faible par rapport à la longueur d'onde des signaux échangés. En effet, la longueur d'onde de la porteuse pour la RFID en bande HF est de l'ordre de 20 m. Or, pour l'instant, la portée de l'attaque est de l'ordre de plusieurs dizaines de centimètres. Ainsi, pendant l'attaque, le transpondeur se trouve dans une région où le champ lointain de l'antenne de l'attaquant est négligeable devant celui du champ proche.
4. Les ordres de grandeur pour le bruit ambiant disponibles ont été effectués en plein air, en milieu urbain. Nous ne savons donc pas dans quelle limite celles-ci sont pertinentes dans un couloir d'entreprise ou dans un métro. Cependant, il est probable qu'en pratique le bruit généré par l'électronique du lecteur soit plus important que le bruit ambiant.

Deux autres éléments limitent nos résultats. Premièrement, peu de mesures de caractéristiques de transpondeur sont disponibles, notamment pour les normes ISO 14443 type B et ISO 15693. Deuxièmement, les deux idées proposées par Kfir et Wool [24] pour abaisser le SNR minimal permettant d'interroger le transpondeur ne sont pas envisagées (répétitions des trames et "jumbo frame").

En ce qui concerne la partie expérimentale de notre travail, plusieurs limitations nous ont empêchées de terminer l'expérience, c'est-à-dire de mesurer en pratique jusqu'à quelle distance la bande latérale supérieure de la modulation d'amplitude créée par le transpondeur simplifié peut être observée avant d'être masquée par une source de bruit. Le filtre d'ordre 5 que nous avons conçu ne permet pas d'atténuer suffisamment la porteuse ; une atténuation d'au moins 90 dB est nécessaire pour obtenir des résultats intéressants. L'antenne SCEMTEC dont nous disposons a un facteur de qualité d'environ 25 ce qui est trop élevé. En effet, le transpondeur simplifié et le filtre sont prévus pour une sous porteuse de 848 kHz, et dans ce cas un facteur de qualité de 15 maximum est souhaitable. Son rayon est par ailleurs de seulement 20 cm, ce qui est optimal pour une distance de lecture de 20 cm. Cela ne veut pas dire qu'il n'est pas possible de lire un transpondeur à une distance supérieure, mais dans ce cas, le coefficient de couplage mutuel est plus faible qu'avec une antenne plus grande. Une antenne plus grande serait donc également souhaitable.

6.3 Travaux futurs

Concernant notre modèle théorique, plusieurs pistes de recherche permettraient d'améliorer le modèle théorique proposé. Premièrement, la validité des hypothèses de la section 4.1 pourrait être approfondie. La contribution du champ lointain à l'amplitude du champ magnétique au niveau du transpondeur pourrait être estimée théoriquement. Des mesures du bruit magnétique ambiant dans d'autres environnements que ceux fournis par l'ITU [43] et où l'attaque sangsue est susceptible de se produire pourraient être envisagées, par exemple dans un souterrain comme le métro d'une grande ville. Deuxièmement, plus de caractéristiques de transpondeurs pourraient être mesurées, notamment pour les transpondeurs ISO 14443 type B et ISO 15693, afin d'être utilisée avec notre modèle. Enfin, les idées proposées par Kfir et Wool [24] pour abaisser le SNR minimal permettant d'interroger le transpondeur pourraient être implémentées pour étudier leur influence sur la distance de lecture des transpondeurs.

Par ailleurs, le filtre proposé dans la partie expérimentale pour le filtrage de la porteuse pourrait être utilisé avec une seconde solution de filtrage comme un détecteur de crête pour terminer l'expérience que nous avons proposée dans le chapitre 5.

RÉFÉRENCES

[1] Wim Aerts, Elke De Mulder, Bart Preneel, Guy AE Vandenbosch, and Ingrid Verbauwhede. Dependence of rfid reader antenna design on read out distance. *Antennas and Propagation, IEEE Transactions on*, 56(12) :3829–3837, 2008.

[2] Gildas Avoine, Kassem Kalach, and Jean-Jacques Quisquater. epassport : Securing international contacts with contactless chips. In *Financial Cryptography and Data Security*, pages 141–155. Springer, 2008.

[3] Pierre Brun-Murol. *Vers une méthodologie normalisée d'évaluation dse solutions RFID en application de sécurité*. Université de Montréal, 2012.

[4] Harvé Chabanne, Pascal Urien, and Jean-Ferdinand Susini. *RFID and the Internet of Things*. John Wiley & Sons, 2013.

[5] Steve CQ Chen and Valerie Thomas. Optimization of inductive rfid technology. In *Electronics and the Environment, 2001. Proceedings of the 2001 IEEE International Symposium on*, pages 82–87. IEEE, 2001.

[6] Nicolas Courtois, Karsten Nohl, and Sean O'Neil. Algebraic attacks on the crypto-1 stream cipher in mifare classic and oyster cards. *IACR Cryptology ePrint Archive*, 2008 :166, 2008.

[7] Nicolas T Courtois. The dark side of security by obscurity and cloning mifare classic rail and building passes, anywhere, anytime. 2009.

[8] Kevin Curran, Amanda Millar, and Conor Mc Garvey. Near field communication. *International Journal of Electrical and Computer Engineering (IJECE)*, 2(3) :371–382, 2012.

[9] Antonio Carlos M de Queiroz. Mutual inductance and inductance calculations by maxwell's method. *Home page of Dr. Antonio Carlos M. de Queiroz*, 2005.

[10] Thomas P Diakos, Johann A Briffa, Tim WC Brown, and Stephan Wesemeyer. Eavesdropping near-field contactless payments : a quantitative analysis. *The Journal of Engineering*, 1(1), 2013.

[11] European Radiocommunications Committee (ERC). Propagation model and interference range calculation for inductive systems 10 khz – 30 mhz. *ERC report 69*, 1999.

[12] Klaus Finkenzeller. *RFID Handbook : Radio-frequency identification fundamentals and applications*. Wiley, 1999.

[13] Flavio D Garcia, Gerhard de Koning Gans, Ruben Muijrers, Peter Van Rossum, Roel Verdult, Ronny Wichers Schreur, and Bart Jacobs. Dismantling mifare classic. In *Computer Security-ESORICS 2008*, pages 97–114. Springer, 2008.

[14] M Gebhart. Analytical considerations for an iso/iec14443 compliant smartcard transponder. In *Telecommunications (ConTEL), Proceedings of the 2011 11th International Conference on*, pages 9–16. IEEE, 2011.

[15] Michael Gebhart, Johannes Bruckbauer, and Martin Gossar. Chip impedance characterization for contactless proximity personal cards. In *Communication Systems Networks and Digital Signal Processing (CSNDSP), 2010 7th International Symposium on*, pages 826–830. IEEE, 2010.

[16] J Guerrieri and D Novotny. Hf rfid eavesdropping and jamming tests. electromagnetics division, electronics and electrical engineering laboratory, national institute of standards and technology. Technical report, Report, 2006.

[17] Nikola Gvozdenovic, Lukas W Mayer, and Christoph F Mecklenbrauker. Measurement of harmonic distortions and impedance of hf rfid chips. In *Antennas and Propagation (EuCAP), 2014 8th European Conference on*, pages 2940–2944. IEEE, 2014.

[18] Gerhard Hancke et al. Eavesdropping attacks on high-frequency rfid tokens. In *4th Workshop on RFID Security (RFIDSec)*, pages 100–113, 2008.

[19] Gerhard P Hancke. Practical attacks on proximity identification systems. In *Security and Privacy, 2006 IEEE Symposium on*, pages 6–pp. IEEE, 2006.

[20] Gerhard P Hancke. Practical eavesdropping and skimming attacks on high-frequency rfid tokens. *Journal of Computer Security*, 19(2) :259–288, 2011.

[21] ISO. *Identification cards — Contactless integrated circuit(s) cards — Vicinity cards — Part 2 : Air interface and initialization*. 2006.

[22] ISO. *ISO/IEC 14443-2.3 Identification Cards – Contactless integrated circuit(s) cards – Proximity cards – Part 2 : Radio frequency power and signal interface*. 2010.

[23] Miki Iwama. Estimation of background noise in hf-band. In *Electromagnetic Compatibility and 19th International Zurich Symposium on Electromagnetic Compatibility, 2008. APEMC 2008. Asia-Pacific Symposium on*, pages 470–473. IEEE, 2008.

[24] Ziv Kfir and Avishai Wool. Picking virtual pockets using relay attacks on contactless smartcard. In *Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on*, pages 47–58. IEEE, 2005.

[25] Young-Han Kim, Yong-Chang Choi, Min-Woo Seo, Sang-Sun Yoo, and Hyung-Joun Yoo. A cmos transceiver for a multistandard 13.56-mhz rfid reader soc. *Industrial Electronics, IEEE Transactions on*, 57(5) :1563–1572, 2010.

[26] Ilan Kirschenbaum and Avishai Wool. How to build a low-cost, extended-range rfid skimmer. *IACR Cryptology ePrint Archive*, page 54, 2006.

[27] Karl Koscher, Ari Juels, Vjekoslav Brajkovic, and Tadayoshi Kohno. Epc rfid tag security weaknesses and defenses : passport cards, enhanced drivers licenses, and beyond. In *Proceedings of the 16th ACM conference on Computer and communications security*, pages 33–42. ACM, 2009.

[28] Jeremy Landt. The history of rfid. *Potentials, IEEE*, 24(4) :8–11, 2005.

[29] WR Lauber, JM Bertrand, and PR Bouliane. An update of ccir business and residential noise levels. In *Electromagnetic Compatibility, 1994. Symposium Record. Compatibility in the Loop., IEEE International Symposium on*, pages 348–353. IEEE, 1994.

[30] Youbok Lee. Antenna circuit design for rfid applications. 20033.

[31] Frank Leferink, Ferran Silva, Johan Catrysse, Sven Batterman, Véronique Beauvois, and Anne Roc'h. Man-made noise in our living environments. *Radio Science Bulletin*, (334) :49–57, 2010.

[32] Renaud Lifchitz. A common weakness in rsa signatures : extracting public keys from communications and embedded devices. `http://2014.hackitoergosum.org/slides/day3_A_common_weakness_in_RSA_signatures:extracting_public_keys_from_communications_and_embedded_devices_Renaud_Lifchitz_hes2014.pdf`, 2014.

[33] Wei Lin, Bernd Geck, Hermann Eul, Christian Lanschuetzer, and Peter Raggam. A novel method for determining the resonance frequency of piccs. In *Communication Systems, Networks and Digital Signal Processing, 2008. CNSDSP 2008. 6th International Symposium on*, pages 311–315. IEEE, 2008.

[34] Ingo Lütkebohle. Mifare (card) coil design guide. `http://www.nxp.com/documents/application_note/M011732.pdf`, 2006.

[35] Milosch Meriac. Heart of darkness-exploring the uncharted backwaters of hid iclasstm security. In *27th Chaos Communication Congress*, 2010.

[36] NIST. Guidance for securing radio frequency identification (rfid) systems. *Special Publication 800-98*, April 2007.

[37] David R Novotny, Jeffrey R Guerrieri, Michael Francis, and Kate Remley. Hf rfid electromagnetic emissions and performance. In *Electromagnetic Compatibility, 2008. EMC 2008. IEEE International Symposium on*, pages 1–7. IEEE, 2008.

[38] Florian Pfeiffer, Klaus Finkenzeller, and Erwin Biebl. Theoretical limits of iso/iec 14443 type a rfid eavesdropping attacks. *ITG-Fachbericht-Smart SysTech 2012*, 2012.

[39] Henry P Romero, Kate A Remley, Dylan F Williams, Chih-Ming Wang, and Timothy X Brown. Identifying rf identification cards from measurements of resonance and carrier harmonics. *Microwave Theory and Techniques, IEEE Transactions on*, 58(7) :1758–1765, 2010.

[40] Alessandro Chiesa Russell Ryan, Zack Anderson. Anatomy of a subway hack. `http://tech.mit.edu/V128/N30/subway/Defcon_Presentation.pdf`, 2008.

[41] Pierre-Henri Thevenon, Olivier Savry, Ricardo Malherbi-Martins, and Smail Tedjini. *Attacks on the HF physical layer of contactless and RFID systems*. INTECH Open Access Publisher, 2011.

[42] W Tobergte and R Bienert. Eavesdropping and activation distance for iso/iec 14443 devices. *NXP White Paper*, 2007.

[43] International Telecommunication Union. Recommendation itu-r p.372-11 "radio noise". 2013.

[44] Roel Verdult. Proof of concept, cloning the ov-chip card. Technical report, Technical report, Radboud University Nijmegen, 2008.

[45] Dan Tudor Vuza and Reinhold Frosch. Rfid readers for the hdx protocol-a designer's perspective. *Current Trends and Challenges in RFID, C. Turcu, Ed. InTech Open Access Publisher, Rijeka*, pages 229–254, 2011.

[46] Markus Wobak, Michael Gebhart, and Ulrich Muehlmann. Physical limits of batteryless hf rfid transponders defined by system properties. In *RFID-Technologies and Applications (RFID-TA), 2012 IEEE International Conference on*, pages 142–147. IEEE, 2012.

[47] Hubert Zangl and Thomas Bretterklieber. Limitations of range of operation and data rate for 13.56 mhz load-modulation systems. *Signal*, 60 :80, 2007.

ANNEXE A

Détail du calcul de l'expression (4.11)

Cette annexe donne le calcul détaillé de l'expression (4.11).
En remplaçant Z_t dans 4.10 par l'approximation 3.14, on obtient :

$$\begin{aligned}\frac{U}{E} &= \frac{\frac{1}{jC_2\omega}}{\frac{1}{j\omega C_2} + jL_2\omega + R_2 + \frac{1+jQ_t\frac{\omega}{\omega_t}}{Q_t(\frac{\omega_t}{\omega}-\frac{\omega}{\omega_t})+j}k^2\omega L_2} \\ &= \frac{1}{1 - C_2L_2\omega^2 + jC_2R_2\omega + j\frac{1+jQ_t\frac{\omega}{\omega_t}}{Q_t(\frac{\omega_t}{\omega}-\frac{\omega}{\omega_t})+j}k^2\omega^2C_2L_2} \\ &= \frac{1}{1 - \frac{\omega^2}{\omega_a^2} + j\frac{1}{Q_a}\frac{\omega}{\omega_a} + j\frac{1+jQ_t\frac{\omega}{\omega_t}}{Q_t(\frac{\omega_t}{\omega}-\frac{\omega}{\omega_t})+j}k^2\frac{\omega^2}{\omega_t^2}}\end{aligned}$$

On appelle p la variable de Laplace : $p = j\omega$. En exprimant U en fonction de p on trouve :

$$\begin{aligned}\frac{U}{E} &= \frac{1}{1 + \frac{1}{\omega_a^2}p^2 + \frac{1}{\omega_aQ_a}p - j\frac{1+\frac{Q_t}{\omega_t}p}{Q_t(\frac{j\omega_t}{p}-\frac{p}{j\omega_t})+j}\frac{k^2p^2}{\omega_t^2}} \\ &= \frac{1}{1 + \frac{1}{\omega_a^2}p^2 + \frac{1}{\omega_aQ_a}p - \frac{1+\frac{Q_t}{\omega_t}p}{Q_t(\frac{\omega_t}{p}+\frac{p}{\omega_t})+1}\frac{k^2p^2}{\omega_t^2}}\end{aligned}$$

Reste à mettre sous forme canonique la fonction de transfert obtenue :

$$\frac{U}{E} = \frac{1+\frac{1}{Q_t\omega_t}p+\frac{1}{\omega_a^2}p^2}{1+(\frac{1}{Q_t\omega_t}+\frac{1}{Q_a\omega_a})p+(\frac{1}{\omega_t^2}+\frac{1}{\omega_a^2}+\frac{1}{Q_aQ_t\omega_a\omega_t})p^2+\frac{1}{\omega_t}(\frac{1}{Q_a\omega_a\omega_t}+\frac{1}{Q_t}(\frac{1}{\omega_a^2}-\frac{k^2}{\omega_t^2}))p^3+\frac{1}{\omega_t^2}(\frac{1}{\omega_a^2}-\frac{k^2}{\omega_a^2})p^4} \quad \text{(A.1)}$$