Communications à grande distance avec un lecteur ISO 14443

Pierre-Michel Ricordel[1] et Yoan Burny[2]
pierre-michel.ricordel@ssi.gouv.fr
wouyam@proton.me

[1] Agence Nationale de la Sécurité des Systèmes d'Information
[2] Centre de Formation à la Sécurité des Systèmes d'Information

Résumé. Ce papier présente un type d'attaque peu étudié dans la littérature : la communication à grande distance avec un lecteur de cartes sans contact ISO 14443. Il présente le contexte, l'état de l'art dans le domaine, les enjeux sécuritaires et les contraintes techniques. Un démonstrateur a été réalisé, qui a permis de multiplier par dix la distance normale d'accès au lecteur.

1 Contexte

Ce papier se situe dans le contexte des cartes sans contact suivant la norme ISO 14443 [1]. Cette norme, par ses caractéristiques techniques, permet au lecteur de transmettre beaucoup d'énergie à la carte, et offre un débit de communication élevé (106 kbit/s ou plus). Ces caractéristiques sont très importantes dès lors qu'il est nécessaire de mettre en œuvre un composant sécurisé intégrant des primitives cryptographiques. En conséquence, cette norme domine aujourd'hui le marché des cartes sans contact sécurisées, dans des domaines comme le contrôle d'accès, la billettique ou le paiement sans contact. Elle sert aussi de fondation à la norme NFC utilisée par les téléphones mobiles.

2 Principes de fonctionnement

Le lecteur génère un champ magnétique à la fréquence de 13,56 MHz, localement très intense (supérieur à 1,5 Ampère/mètre). Ce champ va jouer deux rôles : fournir de l'énergie à la carte et, par sa modulation d'amplitude, envoyer des commandes à la carte. Une carte plongée dans ce champ va en tirer son alimentation électrique. Pour communiquer, elle renvoie ses réponses par modulation de charge, c'est-à-dire qu'elle module artificiellement sa consommation d'énergie. Cette variation de

consommation est détectée et interprétée par le lecteur, qui mesure le courant passant dans son antenne.

Les premiers échanges entre un lecteur et une carte se font à l'aide d'un protocole dit d'anticollision. Le but de ce protocole est de permettre au lecteur de déterminer si plusieurs cartes sont présentes simultanément dans son champ, puis le cas échéant de les énumérer, afin de ne sélectionner qu'une seule carte. Les autres cartes se mettent alors en pause. A la suite de ce protocole, des commandes applicatives de plus haut niveau (par exemple des commandes de carte à contact ISO 7816) peuvent être échangées avec la carte sélectionnée.

3 Distance de lecture

Dans son fonctionnement normal, la distance de lecture d'une carte ISO 14443 est limitée à environ 10 cm. Cette distance est liée aux contraintes physiques et techniques du système, notamment la taille des antennes du lecteur et de la carte, l'intensité du champ émis par le lecteur, le niveau de puissance minimal nécessaire au démarrage du composant de la carte, et la capacité à établir des communications intelligibles.

Comme dans tous système radio, il existe un certain nombre de menaces liées à l'augmentation de la distance d'accès au système, au-delà de la distance de fonctionnement usuelle. Avant d'étudier ces menaces, il est important de rappeler quelques notions importantes sur la propagation électromagnétique, et de les appliquer au contexte du standard ISO 14443.

4 Notions de propagation électromagnétique

Dans cette section nous présentons de manière intuitive comment un champ électromagnétique se propage. Une description plus formelle peut être trouvée dans des livres de référence, par exemple le chapitre 18.7 de [8]. Un champ électromagnétique est formé par deux composantes : un champ électrique (E en V/m) et un champ magnétique (B en A/m). A l'équilibre (hypothèse de l'onde plane), le rapport du champ électrique sur le champ magnétique (E/B) vaut environ 377 Ohm (impédance du vide). Une antenne boucle, telle que celle utilisée par le lecteur, va engendrer un champ très majoritairement magnétique. Ce champ au niveau de l'antenne est déséquilibré, mais il va, au fur et à mesure que l'on s'éloigne de l'antenne, converger vers l'onde plane. Cela se traduit schématiquement par deux zones où le champ va varier de manière différente : une zone dite de champ proche, où le champ magnétique de l'antenne va décroitre

très vite (au cube de la distance) car il engendre du champ électrique pour tendre vers l'équilibre, et une seconde zone dite de champ lointain, où E/B vaut 377 Ohm, et le champ magnétique décroit linéairement par rapport à la distance.

La frontière entre la zone de champ proche et la zone de champ lointain dépend de la fréquence du champ. A 13,56 MHz cette frontière se situe à 3,5 m du lecteur. Cela a pour conséquence que, à moins de 3,5 m du lecteur, le champ magnétique décroit extrêmement vite, et l'effort qu'il faut fournir pour augmenter la distance croit au cube de cette dernière. Cela est à comparer, par exemple, avec le WiFi à 2,4 GHz, où la limite de champ proche est de 2 cm, et où donc l'augmentation de distance se fait dans la zone de champ lointain, où l'effort est linéairement proportionnel à la distance.

5 Attaques à distance des RFID : de l'importance de la norme attaquée

Dans le domaine des attaques cherchant à allonger la distance d'accès à des systèmes RFID, il est primordial de bien préciser quelle norme ou standard est concerné. En effet, il existe une très grande variété dans les standards de RFID, notamment :

- La fréquence de fonctionnement, qui peut être par exemple 125 kHz, 13,56 MHz, 866 MHz ou 5,8 GHz selon les technologies, avec pour conséquence une propagation qui se fait majoritairement en champ proche ou en champ lointain ;
- L'intensité et le type de champ minimal de fonctionnement du tag RFID. Par exemple la norme ISO 14443 demande un champ supérieur à 1,5 A/m alors que la norme ISO 15693 demande un champ de 0,15 A/m à la même fréquence ;
- La vitesse de communication, qui impose des contraintes de bande passante et de rapport signal à bruit.

Comme énoncé précédemment, cette étude concerne spécifiquement la norme ISO 14443.

6 Attaques connues se basant sur l'augmentation des distances d'accès en ISO 14443

Au fil des années, un certain nombre de publications ont décrit des attaques se basant sur des scénarios d'élongation de la distance d'accès. Les scénarios envisagés sont les suivants :

6.1 Lecture d'une carte à distance

Dans ce scénario, l'attaquant essaye de lire une carte à distance, le plus souvent à l'insu de son porteur. Le dispositif d'attaque doit donc à la fois alimenter et communiquer avec la carte. A moins de 3.5 m de la carte, dans la zone de champ proche, l'effort de l'attaquant croît au cube de la distance. Les travaux de Kfir et. al. [10] montrent l'évolution du courant dans l'antenne en fonction de la distance dans la figure 1.

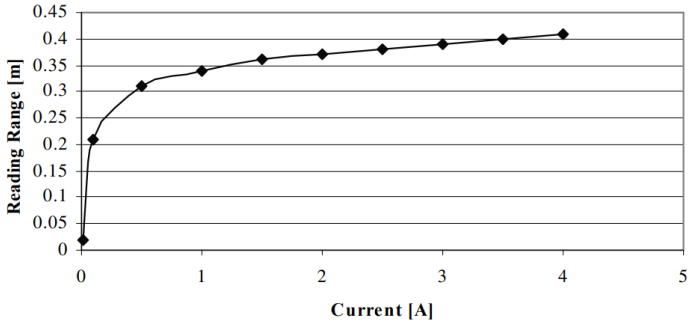

Fig. 1. Courant dans l'antenne en fonction de la distance de lecture, d'après Kfir et al. [10].

On constate que, au-delà de quelques dizaines de centimètres, le courant devient extrêmement important, au point qu'il n'est plus possible pour le lecteur d'y discerner le signal de modulation de charge. La distance maximale obtenue dans [5] est de 27 cm avec une puissance de 4 Watts dans une antenne au format A3. Une distance de 60 cm a été obtenue dans une configuration plus complexe utilisant deux antennes configurées comme un portique antivol [4] : une antenne d'alimentation utilisant un amplificateur de 60 Watts, et une antenne de réception qui capte un signal harmonique de la réponse. La carte est placée entre les deux antennes.

6.2 Interception des communications à distance

Cette attaque consiste à intercepter les communications entre un lecteur légitime et une carte légitime. Les messages issus du lecteur sont relativement faciles à intercepter : le champ émis par le lecteur est intense, donc malgré les pertes dues à la zone de champ proche, il reste un signal qui peut être détectable à grande distance par un récepteur de grande sensibilité. Les phénomènes de couplage dans des conducteurs fortuits

peuvent également aider à augmenter cette distance. Les travaux de G. Hancke [6] ont montré que cette distance peut dépasser 10 mètres.

En revanche, les messages issus de la carte sont beaucoup plus faibles, ce qui limite la portée d'interception à environ 1 mètre, selon les mêmes travaux de Hancke.

6.3 Attaque par relais

Cette attaque consiste à allonger la distance d'interaction entre un lecteur légitime et une carte légitime. Pour ce faire, l'attaquant utilise deux dispositifs : un émulateur de carte placé très proche du lecteur légitime, et un lecteur de carte placé très proche de la carte légitime. Ces équipements communiquent par un moyen de communication longue portée quelconque (liaison radio, internet, etc.) et font transiter les messages échangés entre le lecteur légitime et la carte légitime. Cette attaque ne fait pas appel à des moyens radio complexes car hypothèse est faite que l'attaquant a un accès proche (<10cm) aussi bien du lecteur que de la carte légitime.

6.4 Communication à distance avec un lecteur

Cette attaque consiste à établir une communication à distance avec un lecteur, en l'absence de carte légitime. Etrangement ce type d'attaque est rarement abordé la littérature sur le sujet que nous avons pu consulter.[3] Même dans des publications rétrospectives sur la sécurité des RFID (par exemple [12]) nous ne trouvons pas de référence à ce type d'attaque. Nous allons donc dans la suite de ce papier étudier cette question.

7 Pourquoi étudier les communications à distance avec un lecteur ?

7.1 Raisons physiques

Comme nous l'avons vu, la couche physique de l'ISO 14443 n'est pas propice aux communications à grande distance, du fait de son fonctionnement en champ proche. Cependant, dans le scénario d'une communication à distance avec un lecteur, plusieurs facteurs sont propices à une élongation de distance de grande ampleur :

[3] Après la rédaction de cet article, il a été porté à notre connaissance deux publications portant sur ce même type d'attaque, respectivement [3] et [11]. Nous incitons le lecteur intéressé par ce sujet à les consulter, car elles proposent des méthodes et des techniques légèrement différentes des notres. Les conclusions des trois études restent cependant globalement comparables.

— L'écoute des messages en provenance du lecteur peut se faire à grande distance (>10 m d'après Hancke) du fait de la grande intensité du champ du lecteur ;
— L'envoi de messages vers le lecteur peut également se faire potentiellement à grande distance si l'attaquant arrive à émettre un signal de grande intensité qui peut être interprété par le lecteur comme un signal de consommation de carte. En effet, contrairement à une carte légitime qui dépend de l'énergie envoyée par le lecteur, l'attaquant peut disposer de sa propre source d'énergie. De plus, les lecteurs sont optimisés pour détecter de très faibles variations du courant passant dans leur antenne pour détecter la modulation de charge de la carte. Il suffit que l'attaquant transmette un signal mimant ce signal de modulation de charge pour que le lecteur l'interprète comme une réponse de carte.

7.2 Raisons logiques

La communication à grande distance avec un lecteur permet d'envisager plusieurs scénarios d'attaques crédibles :

— Le déclenchement à distance d'une action nécessitant la présentation d'une carte à proximité immédiate ;
— L'exploitation de vulnérabilités dans le firmware du lecteur ;
— La reconfiguration ou la modification du firmware du lecteur (certains produits sur le marché offrent cette fonctionnalité) , sans avoir un accès physique à celui-ci ;
— L'injection de données corrompues dans les systèmes qui interprètent les données de la carte, comme suggéré par [13], sans avoir accès physique au lecteur.

Parmi les systèmes qui peuvent faire l'objet de ces attaques, on peut citer :

— Les systèmes de contrôle d'accès physiques (par exemple l'activation d'un lecteur inaccessible à travers un mur ou un plancher) ;
— Les lecteurs RFID installés sur les systèmes d'impression sécurisée pour déclencher l'impression en présence de l'utilisateur ;
— Les lecteurs RFID d'ouverture de session sur des systèmes d'information.

Enfin, dans le cadre d'une attaque par relais, cette attaque permettrait de rendre furtive la partie de l'attaque qui est proche du lecteur.

8 Développement d'un démonstrateur

En l'absence de publications sur ce sujet, nous avons développé un démonstrateur afin de déterminer la faisabilité de ce scénario.

8.1 Contraintes techniques

Afin d'atteindre notre objectif, nous avons besoin d'équipements radioélectriques classiques (antennes, câbles, préamplificateur, amplificateur de puissance) et d'un dispositif spécifique capable d'émuler fonctionnellement une carte sans contact. De tels dispositifs existent déjà (par exemple la Proxmark3 [7]) cependant ils sont conçus pour interagir avec le lecteur par modulation de charge, à l'instar des cartes qu'ils émulent. Pour remplir notre objectif nous avons besoin d'une plateforme plus générique, capable de synthétiser des signaux de notre choix, qui seront amplifiés et transmis par une antenne, dans le but d'induire dans l'antenne du lecteur cible des signaux analogues à ceux d'une modulation de charge. De plus, les signaux que nous allons capter à distance risquent d'avoir un rapport signal à bruit bien moins bon que ceux traités par les émulateurs de carte existants, qui sont conçus pour fonctionner très près du lecteur. Notre dispositif doit donc être robuste vis-à-vis du rapport signal à bruit reçu.

Le choix est donc fait de développer un émulateur de carte nous-même, en tenant compte des contraintes d'interface énoncées ci-dessus. Cette décision entraine une contrainte supplémentaire : pour émuler une carte, il faut implémenter le protocole dit d'anticollision, décrit dans la norme ISO 14443-3 et présenté au début de ce papier. Pour fonctionner, ce protocole s'appuie sur le fait que les cartes vont répondre aux commandes d'anticollisions dans un délai de temps court et précis, permettant au lecteur de détecter les collisions des messages qui seraient émis par plusieurs cartes dans son champ. Le temps de réponse requis est d'environ 90 microsecondes, ce qui est très court, et incompatible avec les architectures de radio logicielles courantes, qui ont une latence de traitement beaucoup plus grande.

8.2 Solution choisie

Afin de répondre aux contraintes énoncées précédemment, à savoir un dispositif matériel capable d'émuler une carte ISO 14443 à 13,56 MHz avec des entrées/sorties 50 Ohm standard, et un temps de réponse infé-

rieur à 90 microsecondes, nous avons choisi la plateforme Adalm2000 [2] développée par Analog Devices.[4]

Fig. 2. Photographie d'un Adalm 2000 avec un adaptateur BNC.

Il s'agit d'un système à faible coût (environ 220€) intégrant deux convertisseurs analogiques numériques (CAN) à 100 Méga-échantillons par seconde, deux convertisseurs numériques analogiques (CNA) à 150 Méga-échantillons par seconde et un SOC [5] Xilinx Zynq7000 intégrant un FPGA et deux processeurs ARM Cortex A9. Ces derniers exécutent un système Linux embarqué (basé sur la distribution Buildroot). Une interface USB 2.0 permet de contrôler l'ensemble depuis un PC.

L'Adalm2000 a été développée dans un but éducatif, et l'ensemble de son implémentation est OpenSource (y compris le code du FPGA). Pour la partie FPGA, l'environnement de build utilise des makefile, des scripts TCL développés par Analog Devices, et le logiciel Xilinx Vivado dans sa version gratuite. Le firmware de l'Adalm2000 peut donc être modifié et recompilé à volonté.

Cette plateforme, avec ses CAN et CNA rapides directement accessibles par le FPGA est capable de faire les traitements d'entrée/sortie avec une

[4] Une autre variante de cette plateforme est connue sous le nom d'Adalm Pluto. Cette dernière, qui est une radio logicielle, n'a pas été retenue car elle ne permet pas d'accéder à la bande 13,56 MHz.

[5] SOC : *System on a Chip*

latence extrêmement faible. Nous avons donc développé une IP [6] écrite avec le langage de description matériel VHDL, réalisant la fonction d'émulation de carte dans le FPGA.

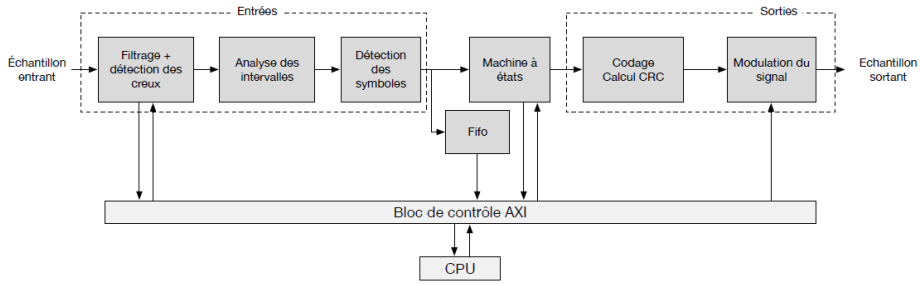

Fig. 3. Description schématique de l'implémentation VHDL réalisée.

Les caractéristiques de cette implémentation sont les suivantes :

— L'implémentation est cadencée à 33,3 MHz (CAN, CNA et logique). C'est une horloge interne qui n'est pas synchronisée avec celle du lecteur. Ce détail est important car il a des conséquences sur plusieurs aspects de l'implémentation. Ce choix a été fait pour des raisons de simplicité d'implémentation et de robustesse du décodage en situation de faible rapport signal à bruit (il est difficile de se synchroniser sur un mauvais signal) ;

— Les signaux d'entrée sont préalablement filtrés analogiquement puis numérisés en bande de base par un CAN et font l'objet d'un décodage par détection d'enveloppe, afin d'en extraire les requêtes du lecteur ;

— Une machine à états détermine quelle réponse doit être donnée aux requêtes, en fonction du contexte et du paramétrage. Un délai est ajouté pour respecter les contraintes imposées par le protocole anticollision ;

— Les réponses sont modulées selon le mode de modulation paramétré. Nous présenterons plus loin la méthode de modulation que nous avons jugé la plus efficace. Les signaux modulés en bande de base sont transmis à un des CNA ;

— Une interface de contrôle permet de paramétrer l'implémentation, et de consulter les messages décodés (via une FIFO), à travers un

[6] IP : *Intellectual Property*. Bloc fonctionnel matériel (Jargon spécifique au développement FPGA).

bus AXI. Ce bus permet d'exposer les registres de paramétrage de notre implémentation dans l'espace d'adressage des processeurs ARM, accessibles par le périphérique /dev/mem du système Linux embarqué sur l'Adalm2000.

Notre but étant de réaliser une preuve de concept, et cette étude étant réalisée en temps contraint, notre implémentation se limite à n'implémenter que le protocole anticollision d'une carte ISO 14443 Type A. Ce protocole nécessite trois échanges successifs entre le lecteur et la carte : REQA/ATQA, SEL*/UID puis SEL UID/SAK. A l'issue de cet échange, la carte est sélectionnée par le lecteur, et ce dernier fournit l'UID à l'applicatif qui le contrôle. Comme expliqué précédemment, ces échanges sont ceux qui nécessitent le temps de réponse le plus strict. Les échanges suivants, de nature applicatifs, n'ont pas ces contraintes. Nous considérons donc que l'exécution réussie du protocole anticollision suffit à prouver que les échanges applicatifs suivants pourraient se faire de la même manière.

8.3 Signal de modulation active

Nous avons réalisé plusieurs essais afin de déterminer quel signal de modulation actif est le plus propice à être interprété comme un signal de modulation de charge venant d'une carte.

Dans le cas normal (modulation de charge), le signal présent dans l'antenne du lecteur est composé du signal d'alimentation principal à 13,56 MHz (provenant du lecteur), faiblement modulé en amplitude par une sous-porteuse à 847 kHz (provenant de la carte). Dans le cas de l'ISO 14443 Type A cette sous-porteuse est modulée à 100

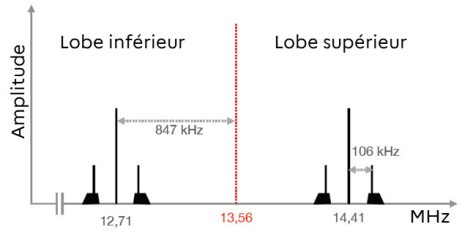

Fig. 4. Vue spectrale du signal dans l'antenne du lecteur, en présence du signal d'une carte.

Du point de vue spectral, ce signal est donc composé de deux lobes autour de la porteuse à 13,56 MHz : un lobe inférieur à 12,71 MHz et

un lobe supérieur à 14,41 MHz. Pour simuler ce signal nous pourrions transmettre ces deux lobes vers l'antenne du lecteur. Cependant cette approche présente deux problèmes :

1. L'écartement en fréquence entre les deux lobes (1,697 MHz) est grand relativement à la fréquence porteuse (autour de 13,56 MHz). En conséquence il ne sera pas possible de réaliser une antenne d'émission ayant un bon facteur de qualité, c'est-à-dire qu'elle ne pourra pas être résonnante car elle doit avoir une grande bande passante relativement à sa fréquence d'accord. En conséquence l'antenne ne pourra pas être efficace ;
2. Notre implémentation utilise une référence de temps qui n'est pas synchronisée avec celle du lecteur. En conséquence la porteuse à 13,56 MHz en provenance du lecteur ne sera pas exactement au centre des lobes générés par notre dispositif, à cause de l'imprécision des sources de temps des deux appareils. Lors de la démodulation en amplitude par le lecteur, cela va occasionner un phénomène de battement qui va faire varier périodiquement l'amplitude du signal démodulé, et qui va donc très fortement perturber le décodage.

Une solution à ces problèmes consiste à n'envoyer que l'un des deux lobes. Le choix entre le lobe inférieur et le lobe supérieur est fait en étudiant l'antenne du lecteur de carte sans contact : cette antenne est réalisée par une boucle de plusieurs spires qui forme une inductance. Cette inductance est accordée à une fréquence de résonnance par un condensateur. Lorsque l'on approche une carte du lecteur, il se produit un phénomène physique dit d'inductance mutuelle : la valeur d'inductance de l'antenne du lecteur va augmenter lorsque l'antenne de la carte s'approche, par influence mutuelle. Pour tenir compte de ce phénomène, qui est de nature à dérégler la fréquence de résonnance des antennes, on règle l'antenne des lecteurs afin que la résonnance soit à 13,56 MHz en présence d'une carte. En absence de carte, l'inductance diminue, ce qui se traduit par une fréquence de résonnance plus élevée. En conséquence, en l'absence de carte (ce qui est le cas de notre scénario d'attaque), l'antenne d'un lecteur sera toujours plus performante à une fréquence supérieure à 13,56 MHz qu'à une fréquence inférieure. Nous choisissons donc le lobe supérieur. L'utilisation d'un seul lobe résout élégamment les deux problèmes précédemment présentés :

1. La bande passante nécessaire à notre antenne d'émission est beaucoup plus petite (212 kHz) que précédemment, ce qui permet d'envisager une antenne d'émission plus résonnante, et donc plus performante ;

2. La démodulation par le lecteur d'un signal composé d'une porteuse et d'un lobe unique légèrement décalé par rapport à sa fréquence optimale produit le signal attendu, sans battement, mais légèrement décalé en fréquence. Ce décalage est faible et nos expérimentations montrent qu'il n'est pas de nature à perturber le décodeur d'un lecteur de carte. Conception des antennes

Pour atteindre notre objectif, nous avons besoin de deux antennes longue portée ayant les caractéristiques suivantes :

— Antenne de réception : Fréquence centrale : 13,56 MHz, bande passante d'environ 212 kHz, 50 Ohm
— Antenne d'émission : Fréquence centrale : 14,41 MHz (bande latérale supérieure), bande passante d'environ 212 kHz, 50 Ohm, capable de supporter une puissance d'émission de plusieurs dizaines de Watts.

Les antennes les plus compactes et les plus simples à construire à ces fréquences sont des boucles résonnantes. Pour atteindre de grandes distances, il est préférable d'utiliser une boucle dont la dimension est la plus grande possible. Nous nous sommes inspirés de la référence [9] pour concevoir notre antenne.

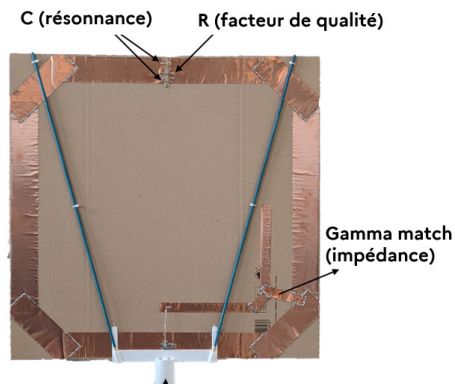

Fig. 5. Une des deux antennes construitre.

Il s'agit d'antennes carrées, mesurant 58 cm de côté, composées d'une boucle en bande de cuivre faisant office d'inductance, en parallèle avec un condensateur variable, permettant de régler la fréquence de résonnance, et une résistance, permettant de régler le facteur de qualité Q, c'est-à-dire la bande passante de l'antenne. Enfin, l'alimentation des antennes se fait par une bande dont la position est déterminée afin que l'antenne aie une

impédance mesurée de 50 Ohm à la fréquence de résonnance (méthode dite du « gamma » match).

8.4 Assemblage du démonstrateur

Les éléments présentés précédemment sont assemblés afin de créer notre démonstrateur. L'antenne de réception est branchée sur un filtre passe-bande centré à 13,56 MHz, puis à un préamplificateur à faible bruit avant d'arriver dans l'Adalm2000. Le signal généré par cette dernière est tout d'abord filtré afin de réduire les harmoniques générées par l'aliasing du convertisseur numérique analogique, puis il est amplifié à l'aide d'un amplificateur de 10 Watts, avant d'être transmis par l'antenne d'émission. Le démonstrateur est complété par un lecteur cible, configuré pour donner l'UID des cartes qu'il détecte.

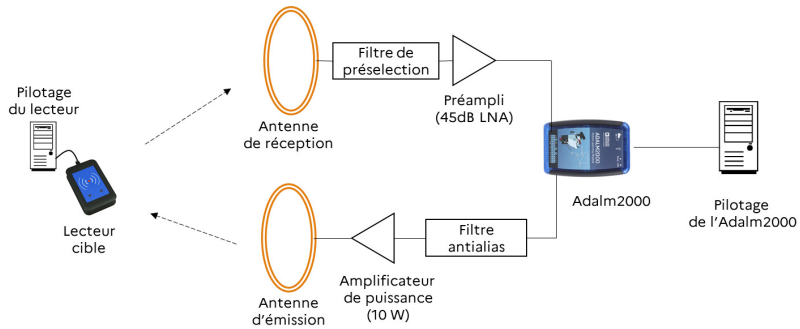

Fig. 6. Vue d'ensemble du démonstrateur.

D'une manière générale, afin d'éviter la destruction du préamplificateur par l'énergie émise par la chaîne d'émission, nous avons cherché à écarter le plus possible les deux antennes, en les plaçant de part et d'autre du lecteur cible par exemple. Pour éviter ce désagrément, il faudrait que le filtre de présélection, centré à 13,56 MHz, rejette fortement la fréquence d'émission, à 14,41 MHz, mais nous n'avons pas pu mettre au point un filtre suffisamment performant.

Enfin, dans certaines expérimentations, nous avons remplacé une antenne par une pince de couplage, qui permet de mesurer ou d'injecter les signaux couplés dans des câbles en mode commun.

9 Expérimentations

Les expérimentations se sont faites dans deux lieux : dans un laboratoire, puis dans un jardin.

9.1 Le laboratoire

Le laboratoire est une pièce dans une tour de bureaux, dont les murs et planchers sont fait de panneaux métalliques, en présence de câbles de toutes sortes et de plusieurs têtes de lecture de contrôle d'accès à proximité.

Test en rayonnement La présence de nombreux lecteurs à proximité et la présence de masses métalliques et de câbles ne facilitent pas la reproductibilité des résultats. De plus l'exiguïté des locaux n'a pas permis de mettre en œuvre l'ensemble de la chaine avec des résultats satisfaisants. Nous avons pu cependant mesurer la distance en émission ou en réception, alternativement (l'une des antennes est maintenue à proximité du lecteur, l'autre est reculée). Les distances obtenues sont les suivantes :

— Emission uniquement : 3,5 mètres
— Réception uniquement : 1,5 mètres

Test en conduction Des essais avec une pince de couplage on permit de mettre en évidence l'existence de phénomènes de couplage dans les câbles d'alimentation secteur, mais il n'a pas été possible en pratique de déterminer jusqu'à quelle distance.

9.2 Le jardin

Le jardin est une zone isolée sans habitations à moins d'une dizaine de mètres environ. C'est un environnement de mesure idéal car il n'y a pas de sources de parasites dans l'environnement, et l'absence de masses métalliques ou de câbles permet d'assurer une meilleure reproductibilité des mesures.

Test en rayonnement En plaçant les antennes d'émission et de réception de part et d'autre du lecteur cible nous avons pu éloigner les deux antennes jusqu'aux distances suivantes :

— Emission : 1,5 mètres
— Réception : 2,5 mètres

Test en conduction Ne disposant que d'une seule pince de couplage, nous n'avons testé soit l'émission, soit la réception avec la pince (une antenne servant dans l'autre direction). La pince est placée sur le câble secteur alimentant le lecteur. Les signaux se sont donc propagés et/ou couplés depuis le lecteur vers le câble USB du lecteur, l'ordinateur portable qui le pilote, le câble d'alimentation de l'ordinateur portable, son alimentation et enfin le câble secteur. Les distances sont les suivantes :

— Emission uniquement : 6 mètres
— Réception uniquement : 17 mètres

A l'occasion des tests, nous avons également constaté l'importance des phénomènes de couplage dans les câbles, et à quel point il est difficile d'anticiper ces phénomènes, très dépendant de la proximité et des cheminements des câbles : nous avons ainsi constaté que notre système était capable de décoder en réception les signaux du lecteur même lorsque l'antenne de réception était débranchée de son câble coaxial, dès lors que ce câble passe à moins de deux mètres du lecteur.

9.3 Analyse des résultats

Notre interprétation des résultats est la suivante :

— La réception est moins performante en laboratoire en raison du fort niveau de bruit, notamment la présence d'autres lecteurs ISO 14443 dans l'environnement qui perturbent notre décodeur. Dans le jardin, le bruit dans la bande est quasi nul, ce qui a permis d'amplifier très fortement les signaux d'entrée ;
— L'émission est plus performante en laboratoire car l'environnement métallique a tendance à contenir le champ et à favoriser les couplages par des conducteurs fortuits. En revanche dans le jardin le champ s'évanouit plus vite, et moins d'éléments conducteurs vont participer à une propagation par conduction ;
— Les signaux à 13,56 MHz sont dans une bande de fréquence qui est extrêmement propice à la propagation par conduction.

Le champ du lecteur étant localement très fort, il va se coupler sur des conducteurs proches et va se propager ensuite bien plus facilement par conduction que par rayonnement. Ils peuvent franchir des obstacles comme les alimentations d'ordinateurs ou se coupler d'un câble à l'autre. Ces phénomènes sont cependant difficiles à maitriser du fait qu'ils dépendent de nombreux facteurs et sont donc complexes à modéliser.

10 Conclusion

Dans cet article nous avons présenté un scénario d'attaque particulier et peu étudié : la communication à distance avec un lecteur RFID à la norme ISO 14443. Nous avons présenté la réalisation d'un démonstrateur capable de réaliser un échange d'anticollision conforme au Type A de la norme, en proposant notamment une forme d'onde optimisée pour ce scénario : la modulation par bande latérale unique haute. Avec ce démonstrateur, la distance d'interaction en rayonnement a été multipliée par 10 par rapport au standard, passant d'une distance décimétrique à une distance métrique. Des échelles de distances encore plus grandes sont possibles en conduction, par la même méthode mais en utilisant des pinces de couplage.

En conséquence, lors de déploiement de systèmes sensibles employant des lecteurs ISO 14443, il est important que les hypothèses de distance d'accès faites lors de l'analyse de risque tiennent compte de ces résultats. L'attaquant peut agir sur le système à une distance bien supérieure qu'à la distance usuelle de lecture d'une carte. Il peut se trouver derrière un mur, à un autre étage, voir beaucoup plus loin dans le bâtiment s'il arrive à obtenir un bon couplage en conduction.

Cette étude a dû être réalisée dans un temps limité : les choix techniques ont été orientés vers les solutions les plus simples, et la phase d'expérimentation a été très brève. Cette étude ne présente donc qu'une ébauche de ce qu'il est possible de faire dans le cadre de ce scénario. Parmi les axes d'amélioration possibles nous suggérons les suivants :

- Optimiser le démodulateur (en mode synchrone ou asynchrone) pour améliorer ses performances lorsque le rapport signal à bruit est faible ;
- Améliorer le filtrage analogique des signaux pour faciliter la cohabitation des antennes de réception et d'émission ;
- Implémenter le Type B et des couches applicative ISO 14443 (par exemple la partie 4 de la norme, ou bien des cartes comme la Mifare Classic et les attaques cryptographiques connues sur ces produits, à l'instar de ce que fait la Proxmark3) ;
- Poursuivre les travaux sur les antennes, les effets de l'environnement et les phénomènes de couplage par conduction.

Références

1. Iso/iec 14443, cards and security devices for personal identification, contactless proximity objects. Technical report, International Organization for Standardization.

2. Analog Devices. Adalm2000 (m2k) active learning module. https://wiki.analog.com/university/tools/m2k.
3. K. Finkenzeller, F. Pfeiffer, and E. Biebl. Range extension of an iso/iec 14443 type a rfid system with actively emulating load modulation. 2011.
4. R. Habraken, P. Dolron, E. Poll, and J. de Ruiter. An rfid skimming gate using higher harmonics. 2015.
5. G. Hanke. Practical attacks on proximity identification systems (short paper). 2006.
6. G. Hanke. Eavesdropping attacks on high-frequency rfid tokens. 2008.
7. C. Herrmann, P. Teuwen, O. Moiseenko, M. Walker, et al. Proxmark3 – Iceman repo. https://github.com/RfidResearchGroup/proxmark3.
8. N. Ida. *Engineering Electromagnetics*. Springer Science, 2000.
9. Texas Instrument. Hf antenna cookbook, technical application report. 2004.
10. Z. Kfir and A. Wool. Picking virtual pockets using relay attacks on contactless smartcard systems. 2005.
11. Y. Oren, D. Schirman, and A. Wool. Range extension attacks on contactless smart cards. 2013.
12. P-H. Thevenon, O. Savry, S. Tedjini, and R. Malherbi-Martins. Attacks on the hf physical layer of contactless and rfid systems. 2011.
13. Q. Zhang and X. Wang. Sql injections through back-end of rfid system. 2009.