Travail de diplôme

présenté pour obtenir le titre d'ingénieur

de la Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

Filière : Télécommunications

Léonard Gross

Sécurité RFID et préservation de la sphère privée

soutenu en janvier 2007

Professeur responsable : Stephan Robert

Institute for Information and Communication Technologies

À mes parents

Remerciements

Avec ce travail de diplôme s'achève un cursus de trois ans à la HEIG-VD d'Yverdon-les-Bains. Je profite de ce moment pour exprimer ma gratitude, ma reconnaissance et mes remerciements à toutes les personnes que j'ai côtoyées non seulement pendant le diplôme, mais aussi tout au long des quelques années passées ici. Le risque d'oublier des noms est important et je prie d'ores et déjà les personnes omises de m'excuser.

Tout d'abord mes pensées vont aux étudiants de la TR2006 aux côtés desquels j'ai eu le plaisir de passer des bons moments dans une ambiance de travail en tous points positive. Merci donc à Joao Alves pour les interminables discussions sur des sujets aussi passionants que variés, à Grégoire Galland pour les palabres et digressions sur ce formidable outil qu'est LaTeX, à Yoann Dind pour sa bonne humeur et le bon temps passé en B03 cet automne, à Sébastien Weber sans qui les vendredi après-midi auraient paru bien mornes, à Rachid Abdoun maître incontesté de la concentration qui ferait pâlir d'envie le plus aguerri des moines Shaolin, à Tiburce Gandji pour les apéritifs prolongés et ses conseils médicinaux, à Raphaël Dussere pour sa clairvoyance et sa vivacité d'esprit, à François Deppierraz pour les dépannages et coups de mains sur Linux, à Kerim Teboulbi pour son flegme bien souvent rassurant, à Nicola Gaudiosi pour son aptitude à régler les litiges, à Renato Martins pour son sens inné de l'investigation et à Laurent Dormont grand spécialiste des transat.

Mes remerciements s'adressent aussi aux professeurs de l'IICT : M. Stephan Robert qui a dirigé ce travail de diplôme et MM. Ventura, Dedieu, Jaton, Hufschmid, Ehrensberger, Lefrançois et Rubinstein pour la qualité de leurs cours, leur érudition et l'enthousiasme avec lequel ils transmettent leur savoir.

La période consacrée au diplôme m'a permis d'établir des contacts avec des personnes du monde RFID auxquelles je tiens à exprimer ici ma gratitude. Tout d'abord Gildas Avoine du MIT qui m'a apporté ses précieux conseils tout au long de ces douze semaines au travers de son expérience et sa grande maîtrise du sujet, Jorge Munilla de l'Université de Malaga pour son aide et ses informations sur son protocole, Beat Clerc de NagraID et Stephan Wullscheger de PBV Kaufmann Systeme GmbH pour m'avoir grâcieusement envoyé des smartcards, Jérôme Vernez pour ses tuyaux sur UWB et Jérémy Briod pour l'aide précieuse et les conseils qu'il m'a prodigués pour la partie hardware.

Enfin, last but not least, mes pensées vont à mes amis Lorenzo, Patrick, Eric, à toute l'équipe du LOFT Mirko, Dom, Olivier, Antonio, Jean, Chris et les autres, à ma famille et mes proches qui m'ont toujours soutenu.

Résumé

Georges Orwell l'avait prédit il y a un peu plus de cinquante ans, sa fameuse mise en garde « *Big Brother is watching you* » s'avère être de plus en plus vérifiée dans les faits. L'avènement du tout numérique, l'expansion du réseau Internet et le développement des systèmes de localisation ont favorisé l'utilisation croissante du système d'identification par radiofréquences **RFID**, qui connaît aujourd'hui un véritable essor et constitue un exemple typique de technologie pervasive. En effet, bien au delà des seuls ordinateurs, de nombreux objets de notre quotidien contiennent des processeurs. Ceux-ci peuvent être nécéssaires à leur fonctionnement ou leur fournir de l'information propre de manière à faciliter leur gestion et leur manipulation. C'est le cas des tags RFID auxquels il est difficile d'échapper tant ils équipent des entités diverses (automobiles, appareils électroniques, vêtements, livres, ameublement, jouets, emballages alimentaires, animaux ...). Ils constituent une sorte de carte d'identité de l'objet correspondant en lui attribuant de manière intrinsèque de l'information qu'il est possible de consulter et de modifier à l'aide d'un lecteur.

Malgré la simplicité du concept – l'identification d'objets sans contact physique ou visuel – et de l'indéniable confort qu'il apporte au niveau logistique, son déploiement rapide suscite de nombreuses inquiétudes tout à fait justifiées. Le grand boom d'une généralisation annoncée pour 2010 sera marqué par une prolifération à grande échelle, au grand dam d'associations de consommateurs ou de défense des libertés publiques qui les redoutent comme un avenir cauchemardesque où chaque objet pourra nous dénoncer. Un argument fédère les craintes : dans une société de consommation où chaque individu est entouré de milliers d'objets, l'analyse à distance de ces produits peut être assimilée à un profilage qui porte atteinte à la vie privée. Cette technologie a donc besoin d'être encadrée en gardant à l'esprit que nous changeons d'époque et que les objets ne resteront pas inertes par rapport aux hommes.

Dans ce travail de diplôme, nous nous proposons d'aborder les aspects de confidentialité des données d'une personne portant des objets munis de tags RFID. Les vulnérabilités du systèmes seront passées en revue, en particulier l'attaque relai contre laquelle des protocoles de *distance bounding* ont été développés. Le travail est axé sur l'étude de ces protocoles et leur éventuelle possibilité de déploiement dans la pratique.

Dans le **Chapitre 1** nous décrivons brièvement les bases de la technologie RFID et son utilisation actuelle. Les aspects physiques nécéssaires à la compréhension des chapitres ultérieurs seront abordés. L'accent sera mis sur les aspects de vulnérabilité et les dangers

inhérents à la traçabilité des informations et des personnes qui en découlent.

Le **Chapitre 2** est consacré aux attaques relais et à leur impact. Ces attaques nécessitent une redéfinition de la notion d'authentification dans lesquelles la notion de proximité revêt une importance particulière. Nous montrons que ce type d'attaque est à prendre au sérieux au travers de cas concrets et nous passons en revue les moyens existant à l'heure actuelle pour s'en protéger.

Une famille de protocoles permettant de se prémunir contre les attaques relais est présentée au **Chapitre 3**. Trois *distance bounding protocols* sont étudiés en détail. Pour visualiser et comprendre leur fonctionnement, des simulations informatiques sont effectuées.

Enfin le **Chapitre 4** constitue une synthèse du travail et ouvre la voie à des éventuels approfondissements ultérieurs.

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

Pour des raisons de lisibilité, la signification d'une abréviation ou d'un acronyme n'est souvent rappelée qu'à sa première apparition dans le texte d'un chapitre. Par ailleurs, puisque nous utilisons toujours l'abréviation la plus usuelle, il est fréquent que ce soit le terme anglais qui soit employé, auquel cas nous présentons une traduction si nécéssaire.

AES	Advanced Encryption Standard	Standard de chiffrement avancé
ALU	Arithmetic Logic Unit	Unité arithmétique et logique
CDMA	Code Division Multiple Access	Accès multiple par répartition en code
CIA	Central Intelligence Agency	Agence centrale du renseignement
CSMA	Carrier Sense Multiple Access	
DNS	Domain Name System	Système de noms de domaine
EPC	Electronic Product Code	
ETSI	European Telecommunications Standards Institute	Institut européen des normes de télécommunications
HF	High Frequencies	Hautes fréquences (3 à 30 MHz)
ICMP	Internet Control Message Protocol	
IEEE	Institute of Electrical and Electronics Engineers	
ISM	Industrial Scientific and Medical	bandes de fréquences réservées aux domaines industriel scientifique et médical
ISO	International Organization for Standardization	Organisation internationale de normalisation
LF	Low Frequencies	Basses fréquences (30 à 300 kHz)
MAC	Medium Access Control	
PAN	Personal Area Network	
RFID	Radio Frequency IDentification	Identification par radiofréquence
RTT	Round Trip Time	Temps d'aller retour
TDMA	Time Division Multiple Access	Accès multiple à répartition dans le temps
UHF	Ultra High Frequencies	Ultra hautes fréquences (300 Mhz à 3 GHz)

URL	Uniform Ressource Locator	
UWB	Ultra Wide Band	Ultra large bande
WAN	Wide Area Network	
WSN	Wireless Sensor network	Réseau de senseurs
XML	Extensible Markup Language	

Chapitre 1

La technologie RFID

« Il faut distinguer la liberté naturelle qui n'a pour bornes que les forces de l'individu, de la liberté civile qui est limitée par la volonté générale. »

J.-J. Rousseau (1712-1778)

Bien que considérée comme une technologie nouvelle, la RFID existe déjà depuis plus d'un demi-siècle. Les systèmes la mettant en œuvre sont donc relativement nombreux et les domaines d'application sont variés. Les normalisations émergent peu à peu dans une jungle de variantes propres à chaque fabricant et à chaque utilisation. Dans ce premier chapitre nous présentons les aspects fondamentaux de la technologie, son fonctionnement général et les points importants qui sont utiles pour la compréhension de la suite. Il ne constitue pas une étude approfondie, mais plutôt un passage en revue des bases essentielles de la technologie pour aborder sereinement les chapitres ultérieurs qui constituent le coeur du travail. Pour de plus amples détails, nous conseillons la lecture de [18], un bon ouvrage de référence ainsi que [50], une présentation très complète.

1.1 Présentation générale

Cette première section présente la RFID dans ses grandes lignes. Après un bref historique, le principe de fonctionnement et la différenciation des tags sont évoqués. La dernière partie, plus abstraite, modélise la technologie et définit quelques termes qui seront utilisé dans la suite lorsque nous parlerons de protocoles.

1.1.1 Historique

La notion d'identification par radiofréquence date de la 2^{e}guerre mondiale. En ces temps belliqueux, l'armée de l'air a vu s'accélérer le développement du radar et de la radio. Du côté des Alliés, la Royal Air Force utilisait des *transpondeurs* pour répondre aux sollicitations de ses radars et ainsi détecter si les avions étaient amis ou ennemis (*Identify : Friend or Foe*). On trouve d'ailleurs toujours des transpondeurs – contraction de *trans*mitter res*ponder* – dans les équipements aéronautiques actuels.

Peu après la guerre, un ingénieur du nom de Harry Stockman montra qu'il était possible d'alimenter un transpondeur uniquement par un signal radio. Dès lors et au fil des années, les progrès technologiques et les recherches dans le domaine entraînèrent une utilisation croissante du système. Dans les années 1970, la RFID est utilisée pour les contrôles d'accès à des sites sensibles, nucléaires ou militaires.

La miniaturisation conduit dans les années 1980 à la démocratisation du système, qui atteint les marchés privés. Les premières applications commerciales font leur apparition dans les péages d'autoroute, les remontées mécaniques des stations des ski ou l'identification du bétail et des animaux domestiques. Parallèlement, les besoins en identification automatique ont crû de la même manière dans l'industrie, les manufactures et les chaînes d'approvisionnement. Le code barre, basé sur une analyse optique en constitue l'exemple le plus connu mais on peut aussi citer les procédures biométriques ou l'identification vocale.

La RFID, de par sa simplicité est peu à peu amenée à remplacer le code barre en formant en quelque sorte son prolongement. En effet l'innovation marquante par rapport à celui-ci est la possibilité de lire plus d'une centaine de tags par seconde sans le moindre contact.

1.1.2 Principe de fonctionnement

Comme nous l'avons dit précédemment, il existe un large éventail de systèmes dits RFID du fait de l'immense variété des constructeurs et du vaste domaine d'utilisation de la technologie et il n'est pas aisé d'en donner une définition précise. Le principe de fonctionnement est cependant toujours le même. Il s'agit d'une interaction entre une base appelée *lecteur* et un transpondeur ou *tag* au moyen d'une onde électromagnétique.

Le système est asymétrique dans le sens où le lecteur est complexe, consomme du courant et est par conséquent plus onéreux que les tags, qui pour les plus simples ne coûtent que quelques centimes. La figure 1.1 schématise le fonctionnement du système.

Notons que la dénomination *lecteur* constitue un abus de langage car, selon le système, celui-ci peut fonctionner en lecture ou en lecture/écriture. Par souci de simplicité, nous parlerons de *lecteur* dans la suite. Il est essentiellement constitué d'un module radio

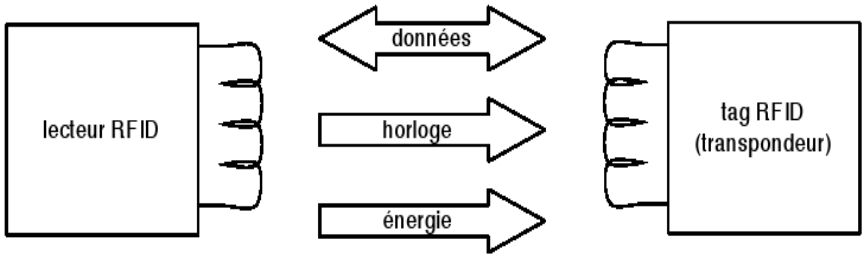

Fig. 1.1 – Fonctionnement RFID

fréquence, d'une unité de contrôle et d'éléments nécessaires au couplage (bobines, condensateurs, antenne). Leurs formes peuvent être variées et ils peuvent être fixes ou mobiles selon l'utilisation. En outre, les lecteurs disposent en général d'une interface (e.g. RS 232, USB) permettant de transmettre les données plus loin vers des systèmes applicatifs permettant leur traitement.

Les tags, quant à eux disposent d'éléments de couplage, d'un microchip et éventuellement d'une mémoire (EEPROM, SRAM) leur permettant de stocker plus qu'un simple identifiant. De par leur petite taille, ils peuvent être placés à peu près partout. Ils sont très répandus dans les smartcards sans contact, étiquettes adhésives, clés de voiture ou encore téléphones mobiles. Quelques tags sont visibles à la figure 1.2. Les aspects phy-

Fig. 1.2 – Tags RFID

siques de l'interaction entre tag et lecteur seront abordés dans la section 1.2. On constate que les tags peuvent prendre les formes les plus diverses de manière à s'adapter au mieux à l'environnement auquel ils sont destinés.

1.1.3 Classification des tags

La kyrielle de tags existants et leurs caractéristiques diverses rendent leur classification délicate. Cependant, on distingue trois grandes familles :

- Les tags passifs, les plus simples et les plus répandus, n'utilisent pas de source d'énergie propre. Ils ne sont activés qu'au travers de l'influence d'un lecteur via l'onde électromagnétique générée. Le fait de ne pas être alimentés leur garantit une durée de vie certaine et un coût de production très bas.
- Les tags semi-passifs dans lesquels une pile fournit l'énergie pour les calculs internes, mais qui nécessitent l'énergie du lecteur pour la transmission.
- Les tags actifs qui disposent d'une pile qui leur fournit de l'énergie pour les calculs et la transmission. Ils sont plus performants, plus fiables mais aussi plus chers et moins répandus.

L'avantage flagrant est la totale autonomie du point de vue énergétique des tags passifs. Par contre la distance au lecteur pour le transfert d'informations est relativement limitée comme nous le verrons. Nous nous focaliserons sur ces tags dans la suite car ils représentent le challenge au niveau de la sécurité et de la sphère privée au vu de leur relative faiblesse en matière de calculs et de ressources. De plus, c'est sur des tags passifs que seront effectuées les manipulations pratiques décrites dans le prochain chapitre.

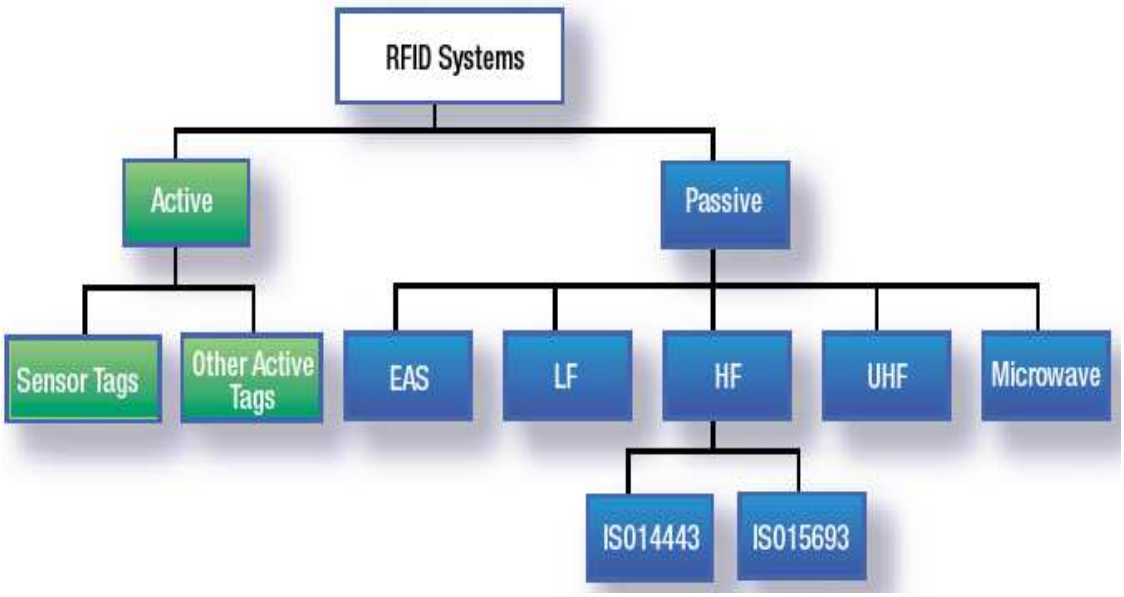

Fig. 1.3 – Classification des tags selon leur fréquence

Les tags se distinguent aussi par la fréquence de l'onde émise par le lecteur, qui influence *de facto* la distance maximum à laquelle le tag est lisible (portée). En tant que système radio, les fréquences sont attribuées par des organismes nationaux qui fixent des

règles précises d'utilisation pour chacune d'elles. La figure 1.3 classifie que les tags selon leurs fréquences de fonctionnement. Les tags passifs comportent quatre familles principales :

- les *basses fréquences* qui utilisent le 125 kHz et le 134 kHz ;
- les *hautes fréquences* qui utilisent le 13.56 MHz ;
- les *ultra hautes fréquences* qui utilisent la bande de 860 à 930 MHz ;
- les *micro-ondes* qui utilisent le 2.45 GHz, le 5.8 GHz ayant été abandonné faute de demande.

Afin d'éviter les interférences et les problèmes potentiels avec d'autres entités utilisant des ondes radio, les trois dernières familles appartiennent aux bandes dites ISM réservées pour usage industriel, scientifique et médical. La famille de tags EAS (*Electronic Article Surveillance*) est un peu à part. Ils équipent les dispositifs d'antivol et ne comportent qu'un seul bit qui correspond à un état actif ou inactif, et ne permettent pas l'identification à proprement parler. La figure 1.4 permet de se faire une idée de cette répartition dans le

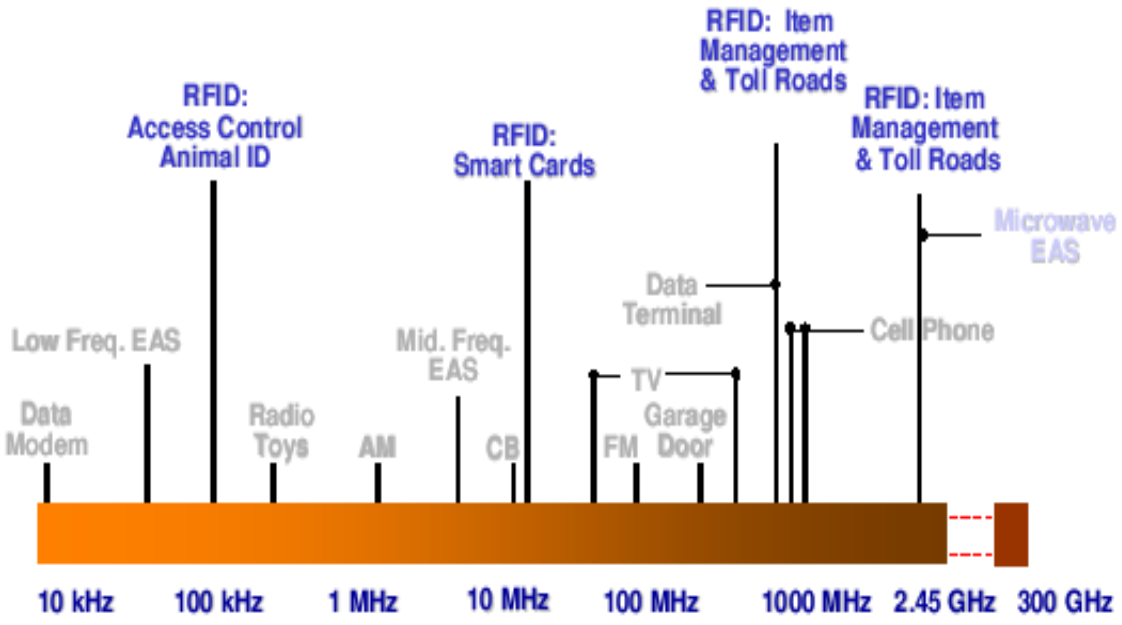

Fig. 1.4 – RFID dans le spectre radiofréquence

spectre radiofréquence usuel. Chaque fréquence possède des caractéristiques différentes tant du point de vue des paramètres de communication que vis à vis de l'environnement dans lequel elle fonctionne. Il est donc utopique d'imaginer une fréquence unique pour toutes les applications. Chacune aura son domaine d'application particulier. Le tableau 1.1 en donne quelques exemples. La portée de lecture, la taille de l'antenne et la méthode de couplage (voir section 1.2) sont autant de paramètres qui fluctuent selon la gamme de fréquences considérée. Pour finir cet aperçu de classification, nous dressons les principales caractéristiques dans le tableau 1.2.

Bande de fréquence	Utilisation
LF	identification d'animaux, clés de voiture
HF	smartcards, livres en bibliothèque, vêtements
UHF	tracking dans chaîne d'approvisionnement
Micro-ondes	identification d'objets à grande vitesse

Tab. 1.1 – Exemples d'utilisation

On constate que la portée et le taux de transfert augmentent avec la fréquence. En revanche les ondes basses fréquences sont moins sensibles à l'environnement et donc plus pénétrantes dans les liquides ou certains métaux, ce qui peut être utile suivant l'application. Notons encore que la portée dépend aussi de la puissance d'émission normalisée par l'ETSI.

Bande	LF	HF	UHF	Micro-ondes
Fréquence	125-134 kHz	13.553-13.567 MHz	860-960 MHz	2.4000-2.4835 GHz
Transfert	< 1 kbit/s	25 kbit/s	30 kbit/s	jusqu'à 100 kbit/s
Portée	< 50 cm	< 1 m	0.5 à 5 m	jusqu'à 10 m

Tab. 1.2 – Caractéristiques

Avant le déploiement d'un système RFID il convient donc de considérer les paramètres suivants pour faire son choix :

- La distance de lecture
- La place disponible pour l'encombrement des tags
- L'environnement (température, pression, humidité etc.)
- Le positionnement des lecteurs et des antennes.

Pour les applications pratiques dans la suite du document, nous utiliserons toujours des tags HF (13.56 MHz) de type étiquette adhésive (smart label figure 1.5) ou smartcard sans contact (figure 1.6).

1.1.4 Standards et normalisations

La question de l'interopérabilité se pose immédiatement tant la multitude d'objets taggés sont appelés à se côtoyer. Des standards sont donc nécessaires voire indispensables à tous les niveaux (interface tag/lecteur, structure des données, applications). Les enjeux de la normalisation sont considérables, en effet la garantie du fonctionnement de l'ensemble à notre époque de mondialisation est primordiale, la circulation des biens se faisant au

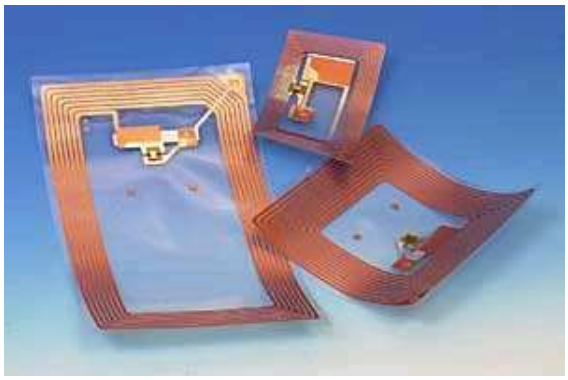

Fig. 1.5 – Etiquettes adhésives

Fig. 1.6 – Smartcard sans contact

niveau planétaire et de manière dense et perpétuelle. Deux standards se démarquent et nous n'en citerons que quelques cas nous concernant. Il s'agit de ISO[1] et de EPC[2].

ISO La fameuse organisation de normalisation a attribué une liste parmi lesquelles se trouve la série ISO 18000-x définissant la fréquence de fonctionnement et le mode de communication entre les tags et les lecteurs, cette norme garantit l'interopérabilité des matériels. La norme ISO 15963 garantit la compatibilité des identifiants attribués par les différents fabricants de tags. Celui-ci est unique et formé par trois éléments :

- La *Registration Category*,
- Le numéro d'identité du fabricant,
- Un numéro de série

Citons encore la norme ISO 14443 définie pour les smartcards sans contact utilisées pour la traçabilité des personnes (contrôle d'accès). D'autres normes ont été développées concernant des tests de conformité, de performances ou de gestion des données. Elles ne nous concernent pas directement, c'est pourquoi nous ne les citerons pas ici.

EPC La norme EPC, moins connue du grand public, est née au sein du MIT de Boston avec le soutien d'importantes sociétés commerciales. L'objectif était d'identifier de manière univoque au niveau mondial tout objet produit et commercialisé. Ce système définit aussi plus haut les architectures réseau nécessaires pour garantir la traçabilité du produit. La notion d'*Internet des objets* en a découlé. Elle a suscité l'intérêt entre autres de Wal-Mart, Procter & Gambel et Gillette qui l'utilisent dans leurs chaînes d'approvisionnement. Les tags sont distingués dans différentes classes selon leurs fonctionnalités – classe 1 pour les tags passifs les plus simples à classe 4 pour les tags actifs. La philosophie d'EPC réside dans la promotion l'utilisation d'un système global qui va au delà de l'interaction tag/lecteur. Des solutions logicielles de middleware pour la gestion des données récoltées sont proposées ainsi que des possibilités de communication avec des systèmes de gestion de bases de données comme Oracle. Cette uniformisation constitue le point fort d'EPC qui

[1] `http://www.iso.org`
[2] `http://www.epcglobalinc.org`

ont imaginé un service ONS – *Object Naming Service* – semblable au DNS bien connu du monde Internet qui associe le numéro d'identification EPC de 96 bits à un URL contenant des informations sur le produit correspondant. Parallèlement, pour faciliter l'échange des données entre systèmes d'information, un langage PML de balisage a été introduit sur le modèle de XML.

1.1.5 Protocoles de communication

Pour conclure cette vue d'ensemble de la technologie, nous présentons sa modélisation en termes de protocoles de communication dans une approche téléinformatique. Par analogie aux modèles OSI et TCP/IP bien connus et en accord avec la norme ISO 18000-1, nous pouvons établir un modèle de communication en couches distinctes (figure 1.7).

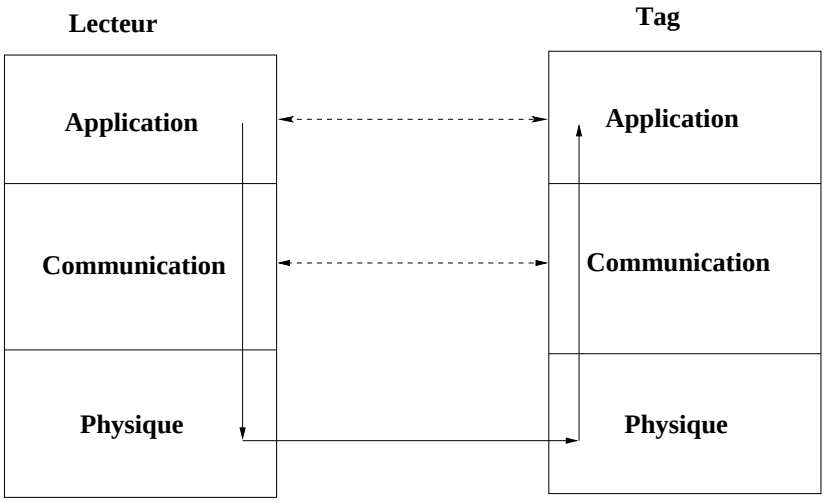

Fig. 1.7 – Modèle en couches

Le modèle est cependant plus simple que les modèles OSI et TCP/IP classiques, le nombre de couches s'en trouve par conséquent réduit. Par contre les couches conservent leur hétérogénéité et les communications entre couches du même niveau se font via des protocoles. On distingue trois couches distinctes :

- La *couche applicative* qui gère les données et les messages relatifs au processus de l'utilisateur comme l'identifiant du tag. C'est là qu'interviennent les opérations cryptographiques.
- La *couche communication* définit la manière de communiquer entre tag et lecteur et gère la reconnaissance et l'identification d'un ou de plusieurs tags entrant dans le champ du lecteur.
- La *couche physique* qui gère l'interface air et la propagation des ondes *i.e.* la modulation, le codage, la vitesse de transmission etc.

Les protocoles de communication, symbolisés par les flèches en traitillé, constituent un des points clé pour aborder et comprendre les aspects sécuritaires qui seront traités dans ce travail. La communication horizontale est en quelque sorte virtuelle puisqu'elle transite en fait par les couches inférieures en utilisant leurs services jusqu'au niveau physique, avant d'être transmise physiquement à bon port et de remonter jusqu'à la couche de laquelle elle provenait. Les protocoles constituent une sorte de langage pour que les couches de même niveau se comprennent. Ils sont représentés en traitillé. Dans la RFID, on en distingue trois familles :

- Les protocoles d'identification et d'authentification pour le niveau applicatif. Ils dépendent des ressources des tags car ils peuvent devoir mettre en œuvre de la génération d'information et des mécanisme de cryptographie symétrique.
- Les protocoles de contrôle d'accès au médium (MAC) au niveau 2 qui gèrent les collisions entre plusieurs tags entrant dans le champ d'un lecteur. Ils sont de type déterministes ou probabilistes.
- Les protocoles de transmission au niveau physique définissent la modulation (ASK, FSK) et le codage des informations.

1.2 Considérations physiques

Cette section a pour but de présenter brièvement le phénomène physique de *couplage inductif* et la notion de *facteur de qualité* d'une antenne tels qu'ils interviennent en RFID. Ces notions font appel à des éléments d'électromagnétisme et d'électronique.

1.2.1 Le couplage inductif

Les diverses fréquences utilisées par RFID impliquent une utilisation différente du champ électromagnétique pour l'échange d'information entre tag et lecteur. On distingue le fonctionnement en champ proche et en champ lointain — *near field* et *far field*. Pour le premier (LF et HF) la longueur d'onde λ est grande par rapport à la distance de lecture, la composante magnétique du champ domine et la bobine joue le rôle d'antenne. On parle alors de *couplage inductif*. Dans le second cas (UHF) la longueur d'onde est petite par rapport à la distance de lecture et c'est la composante électrique du champ qui domine. Le tag se comporte comme un composant radio. Les systèmes fonctionnent alors en mode propagation d'onde et l'antenne est un conducteur filaire.

Les tags passifs bon marché, ceux qui nous concernent dans cet exposé, utilisent le couplage inductif et nous ne présenterons essentiellement que ce cas. Le calcul de la longueur d'onde donne :

$$\lambda = \frac{c}{f} = 22.12 \text{ m}$$

où $c = 3 \cdot 10^8$ m/s est la vitesse de la lumière et $f = 13.56$ MHz la fréquence de fonctionnement du système. Une borne supérieure de la portée est donnée par :

$$r \leq \frac{\lambda}{2\pi} = 3.58 \text{ m}$$

Cette limite reste théorique car comme nous le verrons dans nos expériences, elle se situe bien en deçà.

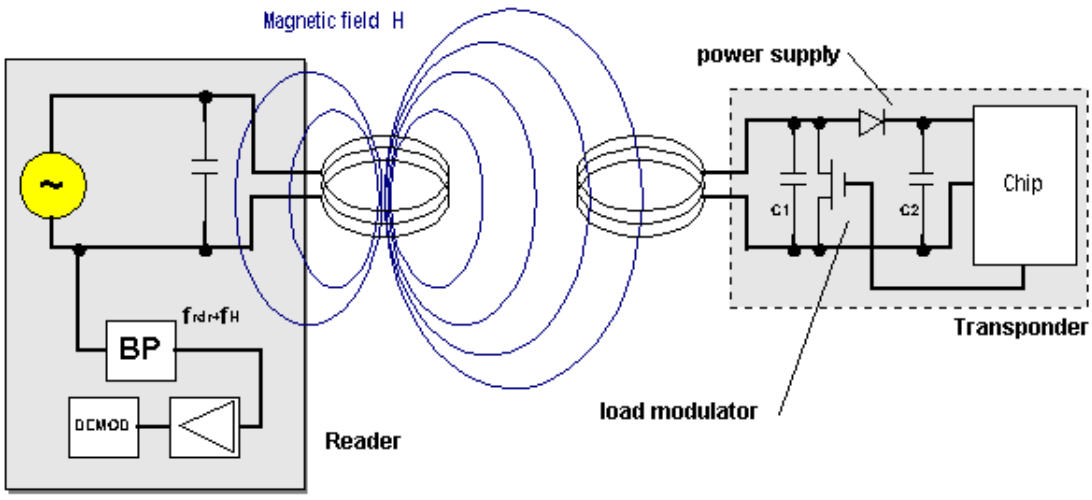

Fig. 1.8 – Couplage inductif, source : RFID-Handbook

La figure 1.8 illustre le fonctionnement général du couplage inductif. Un oscillateur du lecteur génère un courant alternatif dans la bobine qui génère à son tour un champ électromagnétique variant dans le temps. La loi de Faraday[3] assure que les variations de flux ainsi créées entraînent une tension induite dans la bobine (antenne) du tag. Cette tension, redressée au travers d'une diode, charge le condensateur C_2 qui active le chip dès qu'il est chargé. Le chip émet un signal qui contient ses informations. Ce signal, formé de niveaux hauts et bas correspondant aux 1 et au 0 des informations agissent sur un transistor à effet de champ comme un interrupteur. Le tag génère ainsi son propre champ magnétique qui interagit avec celui du lecteur en modifiant l'impédance de celui-ci. Cette technique dite de la *modulation de charge* permet au lecteur de recevoir le signal et donc l'identifiant du tag après conversion analogique/numérique.

1.2.2 Résonance et facteur de qualité

Pour optimiser le couplage et maximiser le transfert d'énergie, des circuits LC résonnants sont utilisés de manière a générer des gros courants dans les bobines. Les circuits LC sont

[3] sous sa forme locale : $\vec{\nabla} \wedge \vec{E} = -\frac{\partial \vec{B}}{\partial t}$

en série dans le lecteur (pour maximiser le champ généré, impédance nulle à la fréquence de résonance) et en parallèle dans le tag (pour maximiser la tension, impédance infinie à la résonance) comme le montre la figure 1.9. En modulant le champ généré, le lecteur peut écrire sur le tag.

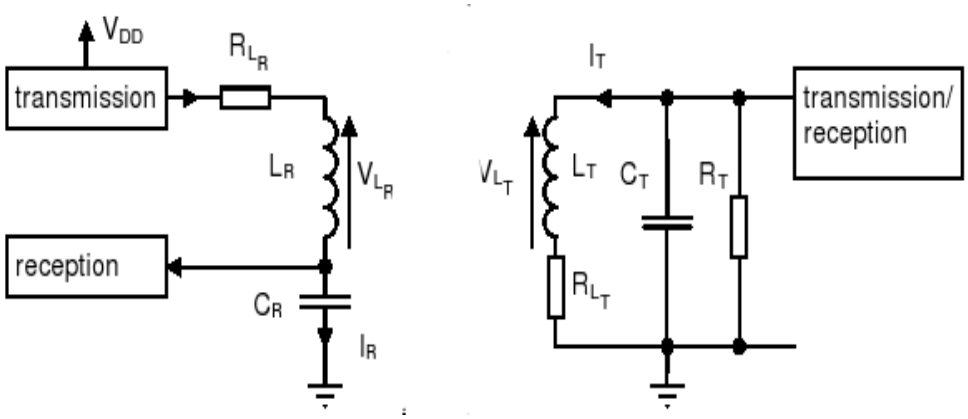

Fig. 1.9 – Circuits équivalents du tag et du lecteur

Les valeurs des inductances L sont liées aux bobines et les capacités doivent être choisies de manière à ce que la relation suivante soit satisfaite :

$$f = f_{\text{res}} = \frac{1}{2\pi\sqrt{LC}}$$

La fréquence de résonance doit être égale à la fréquence de transmission pour que la tension induite dans le tag atteigne un maximum. Le système peut être comparé à un transformateur avec bobines primaire et secondaire. Le facteur de qualité d'un circuit résonant est un paramètre important du système. Il se calcule comme suit :

$$Q = 2\pi f \frac{L}{R}$$

Il mesure en quelque sorte l'étalement de la courbe de réponse en fréquence, défini comme le ratio énergie transmise sur énergie dissipée.

1.3 Applications

Pour conclure ce chapitre, les avantages et inconvénients flagrants de la technologie sont évoqués. La section constitue une transition et une motivation au chapitre suivant. Nous exposons quelques exemples d'applications et la problématique liée à la préservation de la sphère privée qui est au yeux du grand public le talon d'achille de la technologie. En effet, les communications sont invisibles à l'homme et peuvent donc se faire à son insu.

Une immense brèche est ainsi ouverte qui alimente le débat sur la protection des consommateurs. L'unicité des identifiants permet une traçabilité de chaque objet et *a fortiori* l'association d'un objet à une personne dans une base de données. La multiplication des lecteurs soulève ce problème majeur de confidentialité des données et fait courir un risque aux libertés individuelles.

1.3.1 Avantages

La RFID présente des avantages par rapport aux systèmes d'identification classiques. Comme bien souvent, il existe un revers de la médaille et ce qui est gagné se perd sous un autre aspect.

1. *Automatisation :* les code-barres ou les systèmes plus anciens nécessitent une visibilité directe entre lecteur et objet pour la lecture des données et donc une intervention humaine. Les tags RFID au contraire ne requièrent pas d'orientation spéciale par rapport au lecteur et augmentent ainsi l'automatisation du processus de lecture.
2. *Identification améliorée :* les tags RFID, de par leur nature, peuvent disposer de plus d'information que les code-barres. Ceci permet aux fabriquants de ne pas stocker uniquement un identifiant générique au produit (« ceci est une boite de haricots »), mais un numéro unique (« c'est la boite numéro 987654 ») qui peut pointer vers une base de données pour accéder à des données détaillées (« produit en septembre 2006 à l'usine de Lausanne » etc.).
3. *Intégration :* Le système de fonctionnement confère encore à la logistique un autre avantage pratique. En effet la RFID évite les problèmes d'endommagement sur une surface fragile et fonctionne même en présence de poussière ou de saleté éventuelle. La robustesse est donc à souligner.

Ces trois avantages mènent au concept d'identification automatisée. Parallèlement à l'identification, les possibilités d'authentification constituent un autre point attrayant de la RFID. La possibilité est donnée au lecteur de reconnaître un tag légitime d'une contrefaçon et inversement. Cet aspect est essentiel pour les nombreuses applications actuelles. Une différenciation formelle entre authentification et identification sera explicitée au début du prochain chapitre.

1.3.2 Inconvénients

Les avantages cités dans la section précédente constituent en même temps des inconvénients qui vont nous intéresser dans le reste de ce travail.

1. *Automatisation :* le fait de ne pas nécessiter d'intervention humaine facilite l'accès aux données. Cela ouvre la voie à une possibilité de lire des tags de manière continue et discrète.

2. *Identification :* elle n'est plus générique, mais porte sur chaque tag individuellement. L'obtention d'information s'en trouve raffinée et la possibilité de profiler des personnes se présente.
3. *Intégration :* les tags peuvent être lus à l'insu de leur détenteur, qui peut ne même pas savoir que son produit en possède.

L'authentification devient alors indispensable surtout si les données sont sensibles ou confidentielles ce qui est de plus en plus le cas dans la pratique.

1.3.3 Quelques exemples d'applications

Nous donnons ici une liste non exhaustive des domaines dans lesquels la technologie est utilisée.

Chaînes d'approvisionnement Le premier exemple type concerne le tracé des objets dans l'industrie et le commerce. L'industrie aéronautique et d'autres entreprises de l'industrie lourde utilisent la RFID pour le suivi et l'identification des pièces détachées. Dans le domaine commercial, l'avantage est indéniable, le produit pouvant être surveillé de sa fabrication à son achat par le consommateur en passant par le transport le stockage et le point de vente. De plus la gestion des inventaires est facilitée car la marge d'erreur liée aux interventions manuelles est limitée. Aux Etats-Unis l'enseigne de distribution Wal-Mart utilise les tags EPC. Le Gouvernement fédéral lui a emboîté le pas. En effet, le département de la défense demande à ses fournisseurs de marquer leurs palettes depuis 2005.

Contrôle d'accès Un autre domaine dans lequel la RFID connaît un véritable essor est celui du contrôle d'accès. De nombreux bâtiments comprenant des salles à accès restreint utilisent des cartes d'accès sans fil. La RATP[4] (*Régie Autonome des Transports Parisiens*) équipe ses pass Navigo de tags depuis cette année. Il en va de même pour de nombreux domaines skiables qui ont remplacé le bon vieux forfait par des cartes d'accès sans fil. L'avantage est double car au gain de temps s'ajoute le fait d'avoir un suivi des informations utilisables ultérieurement pour des statistiques par exemple. Nous pouvons encore citer les péages d'autoroute dans lesquels le payement peut se faire sans arrêt du véhicule, par simple lecture de son identifiant.

Secteur du transport et marché de la mobilité Le suivi et le tri des bagages dans les aéroports, le tri postal dans les centres de tri sont d'autres exemples. La collecte des déchets, domaine relatif aux enjeux écologiques actuels, se préoccupe d'améliorer la répartition de la charge du ramassage et tendent à utiliser la RFID.

[4] `http://www.ratp.fr/`

Implants sous-cutanés En Espagne et en Hollande, quelques téméraires se sont fait implanter un tag sous la peau. Ils l'utilisent comme moyen de paiement et pour accéder à des discothèques. Cette technique peut paraître effrayante car elle ouvre la voie à toutes les dérives (marquage des prisonniers en milieu carcéral par exemple). Toutefois, dans le domaine animalier, le marquage est utilisé depuis longtemps et a fait ses preuves.

1.3.4 RFID : tags ou mouchards ?

Les inconvénients que nous avons vus posent donc problème au niveau de la sphère privée – les anglo-saxons parlent de *privacy*. Le lieu où se trouve une personne ainsi que des données la concernant peuvent être déterminés à son insu.

Observons l'article 13 de la constitution fédérale.

> ☞ *Toute personne a droit au respect de sa vie privée et familiale, de son domicile, de sa correspondance et des relations qu'elle établit par la poste et les télécommunications.*
>
> ☞ *Toute personne a le droit d'être protégée contre l'emploi abusif des données qui la concernent.*

De nos jours, de nombreuses technologies très répandues permettent la localisation et la traçabilité des personnes (e.g. GSM, GPS, Bluetooth). Cependant la RFID a un côté plus gênant. La traçabilité est accessible à tout un chacun de par le coût relativement faible de l'équipement nécessaire, la passivité des tags, leur diffusion discrète vu leur petite taille et la relative facilité de mettre en place des processus automatiques. Les défenseurs réfuteront ces arguments en mettant en avant la faible distance de lecture qui nécessite un grand nombre de lecteurs ou la possibilité de désactiver les tags. Néanmoins, comme nous le verrons, il est possible d'augmenter sensiblement la portée en agissant sur des paramètres physiques, ou d'effectuer des attaques complètement transparentes au porteur du tag. En adoptant un point de vue pessimiste et un soupçon paranoïaque, cette transparence est inquiétante puisque chaque curieux pourrait faire l'inventaire de ce que nous portons sur nous. De même le caddie de chaque acheteur potentiel dans un magasin ou une grande surface pourrait être scanné pour connaître son identité et ce qu'il a dépensé. La technologie va encore faire couler beaucoup d'encre, les Parlements sont de plus en plus appelés à légiférer et les consommateurs enclins aux réticences. Les recherches actuelles se concentrent sur ces aspects, pour que ces craintes s'amoindrissent et que le système puisse susciter l'enthousiasme de tout le monde.

La Commission Européenne a lancé en 2006 une consultation sur l'usage des technologies RFID dans la société[5] à l'initiative de Viviane Reding la commissaire en charge de la Société de l'information et des médias. Le questionnaire comportait une quarantaine

[5] `http://www.rfidconsultation.eu/`

de questions sensées permettre de « *connaître le ressenti de cette technologie vis-à-vis du public et ses implications sur la vie privée et la santé* » . Il en est ressorti que les risques associés doivent être clairement décrits et que le citoyen estime que la technologie doit être améliorée en fonction du niveau de risque. Une indication claire de la présence de telles puces et les moyens de leur destruction sont également demandés. Viviane Reding compte maintenant se centrer sur trois axes : création d'un cadre réglementaire adapté, sensibilisation aux bénéfices et aux risques de la technologie RFID, moyens de garantir la vie privée.

Les craintes sont fédérées autour de quatre facteurs principaux :

- Le *scanning clandestin i.e.* le fait d'obtenir des données sans le consentement du porteur du tag. Ces « données » sont à prendre au sens large du terme. Cette méthode peut amener à un traçage clandestin, si le tag est scanné à plusieurs reprises dans une zone géographique restreinte.
- L'*écoute clandestine* – ou *eavesdropping* – qui consiste à intercepter la communication entre tag et lecteur de manière non autorisée.
- La *fuite d'information i.e.* le fait que plus d'informations que nécessaire soit transmis par le tag et rendu visible malgré leur nature confidentielle. Cela ouvre potentiellement la voie à de l'espionnage industriel ou de la contrefaçon, menaçant ainsi non seulement les particuliers mais aussi les entreprises.
- L'*usurpation d'identité* qui peut conduire à des fraudes dans des systèmes contrôles d'accès en déjouant l'authentification du porteur du tag.

Il convient de garder en mémoire le modèle en couche de la section 1.1.5. En effet, la problématique de la traçabilité y est liée de manière intrinsèque, puisqu'elle dépend de chacune des couches ce qui souligne son aspect délicat. Pour être vraiment efficaces, les moyens de parade contre la traçabilité doivent être assurés à tous les niveaux. Avoine et Oechslin dans [3] montrent qu'il faut considérer le modèle dans son intégralité, car toutes les couches peuvent révéler des informations pouvant servir à tracer les tags.

Chapitre 2

Menaces et attaque relai

« Usez, n'abusez pas, le sage ainsi l'ordonne. »

Voltaire (1694-1778)

Comme toute technologie en évolution, la RFID soulève des problèmes relevant de la sécurité. Les faibles ressources des tags impliquent une certaine vulnérabilité ouvrant la porte à toutes sortes d'abus. Nous avons brièvement introduit les menaces inhérentes aux aspects de protection de la vie privée au chapitre précédent. Ce chapitre aborde le problème de manière plus détaillée. Il est consacré aux menaces qui pèsent sur les systèmes RFID et les attaques potentielles envisageables par des utilisateurs malveillants. Aux problèmes de traçabilité s'ajoutent les problèmes plus classiques comme les dénis de service. La section 2.3 concerne l'attaque relai, sur laquelle nous nous attarderons plus longuement puisqu'elle a donné lieu à l'élaboration des protocoles de *distance bounding* qui feront l'objet du chapitre 3.

2.1 Familles de protocoles

Nous commençons par définir de manière formelle et aussi précise que possible des concepts importants. La RFID tout comme la biométrie implique la définition et la distinction précise de deux notions fondamentales. Il s'agit de *l'identification* et de *l'authentification* qui diffèrent dans leur concept mais qui sont indissociables. L'amalgame est souvent fait entre *l'identité* et *la preuve d'identité*, c'est pourquoi il n'est pas superflu de s'attarder sur ces notions. Les protocoles mettant en oeuvre ces deux notions sont des protocoles de niveau 3 (application) dans le modèle en couches défini au chapitre précédent. Il est aussi utile d'aborder l'anti-collision relative au niveau 2 (communication) pour avoir une vue

d'ensemble des protocoles utilisés en RFID avant d'aborder les attaques. Nous adoptons l'approche de G. Avoine dans [2].

2.1.1 Identification

En langage courant, l'identification est la réponse à la question « Qui suis-je ? » . Les applications RFID les moins sensibles telles que l'amélioration des chaînes d'approvisionnement ou de fabrication, de tri de déchets par exemple nécessitent un degré de sécurité moindre, le but étant d'obtenir uniquement l'identité du tag. Elles utilisent donc des protocoles d'identification.

Définition 1 (Identification) *L'identification d'un tag est l'obtention de son identité par le lecteur sans qu'une preuve ne soit donnée.*

Schématiquement les échanges effectués lors d'une procédure d'identification sont visibles à la figure 2.1. Le lecteur envoie une requête au tag à laquelle celui-ci renvoie une réponse contenant son identifiant ID. Le lecteur traite ensuite cet identifiant en amont dans une base de données. L'identification ne nécessite pas de grandes ressources et peut être réalisable avec les tags les plus légers.

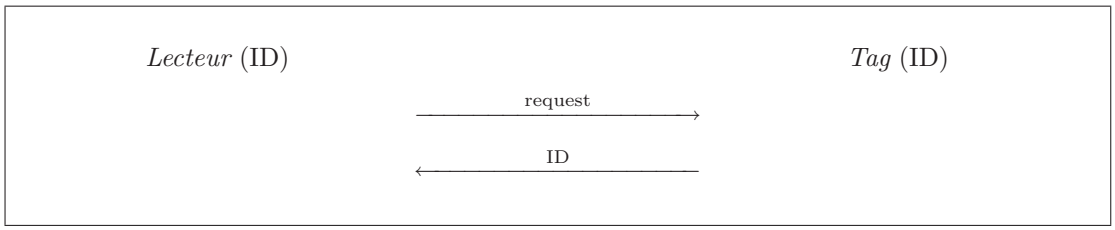

Fig. 2.1 – Procédure d'identification

Par souci de simplicité, les échanges seront toujours symbolisés par une interaction entre le lecteur et le tag. En réalité le lecteur n'est que rarement seul et interagit avec un système. L'entité « lecteur » est donc à considérer au sens large.

2.1.2 Authentification

L'authentification est le fait de prouver que je suis celui que je prétends être. Les applications plus sensibles comme le contrôle d'accès qui doivent fournir un niveau de sécurité supérieur mènent souvent *in fine* à l'utilisation de protocoles d'authentification.

Définition 2 (Authentification) *L'authentification d'un tag est l'obtention de l'identité du tag par le lecteur et d'une preuve que cette identité est correcte.*

De manière symétrique l'authentification d'un lecteur permet au tag d'obtenir l'identité du lecteur ainsi qu'une preuve de celle-ci. Si les deux conditions sont remplies, on parle d'*authentification mutuelle*. La procédure d'authentification (figure 2.2) consiste en l'envoi d'un *nonce – number used once*, un nombre aléatoire ou pseudo-aléatoire généré par le lecteur – au tag qui répond avec son identifiant ID et une preuve de celui-ci calculée au moyen d'une fonction cryptographique F. Les tags ne disposant que de capacités de calcul limitées, la cryptographie asymétrique (*i.e.* à clé publique) se trouve être difficilement réalisable, des mécanismes symétriques lui sont donc préférés. Tag et lecteur partagent une clé secrète K qui est utilisée pour le chiffrement par F du nonce. Ce besoin de ressources supplémentaires se ressent sur la complexité donc le prix des tags. La fonction F peut prendre différentes formes : fonction de chiffrement $\mathcal{E}$, fonction de hachage h etc.

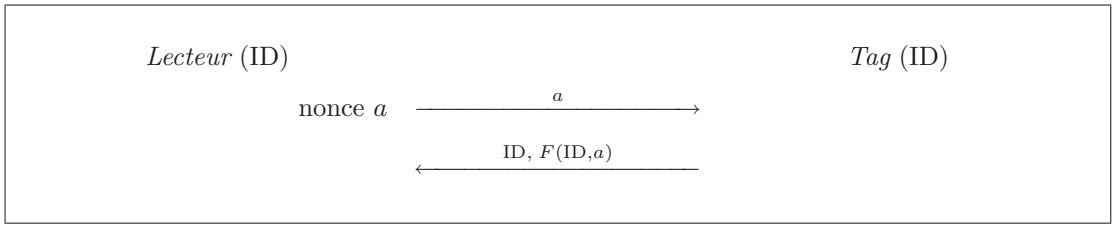

Fig. 2.2 – Procédure d'authentification

La procédure contient l'identification, mais y ajoute une preuve. Elle se base sur la connaissance commune d'un secret partagé par les deux parties et d'une fonction F. Il s'agit d'une procédure *two way handshake* dans le jargon utilisé en télécom. L'authentification en RFID a fait l'objet de nombreuses recherches [4, 5, 11, 12, 15, 16, 26, 27, 35, 38, 42, 53, 51] et continue a être une source de publications régulières.

2.1.3 Anti-collision

Les protocoles d'anti-collision représentent les protocoles MAC d'accès au medium. Leur besoin se justifie par le fait que plusieurs tags peuvent être interrogés simultanément par un même lecteur, ceci en mode *broadcast* (figure 2.3), et que leurs réponses respectives tentent d'atteindre le lecteur en même temps en mode multi-accès (figure 2.4), ce qui cause des collisions.

Les tags sont incapables de communiquer entre eux et c'est donc le lecteur qui doit gérer l'évitement de collision. Les procédures à cet effet peuvent être considérées comme synchrones puisque tous les tags sont interrogés par le lecteur simultanément. Un tag particulier est ensuite choisi parmi l'ensemble se trouvant dans le champ d'interrogation du lecteur grâce à un algorithme d'anti-collision puis la communication de niveau 3 peut être effectuée. Une fois celle-ci terminée, un autre tag est considéré. Le processus porte le nom anglais de *singulation*. Ces protocoles sont souvent propriétaires mais les standards ISO et EPC en définissent deux grandes familles. L'utilisation de l'un ou de l'autre est

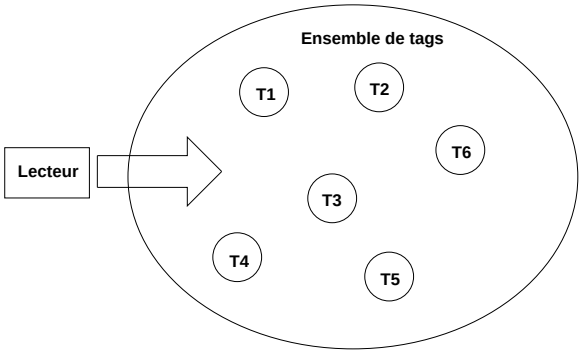

Fig. 2.3 – Interrogation des tags

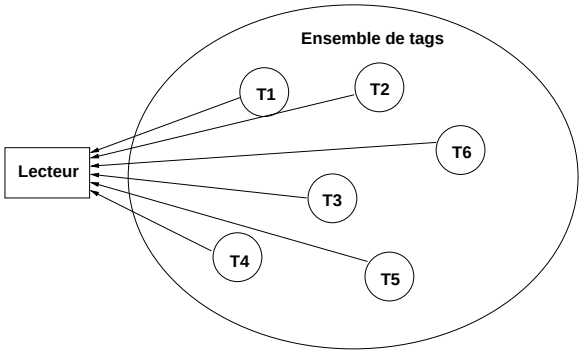

Fig. 2.4 – Réponses des tags

déterminée par le type de tag et donc par la fréquence d'utilisation. Les systèmes HF utilisent des protocoles probabilistes tandis que les systèmes UHF utilisent plutôt des protocoles déterministes. Nous passons en revue les deux principes.

Protocoles déterministes

La communication s'effectue au travers d'une série de messages (REQUEST(SNR), SELECT(SNR), READ_DATA). Les protocoles déterministes fonctionnent selon un algorithme de recherche dans un arbre binaire. Il en existe plusieurs, de complexité diverses, et nous en présentons un pour illustrer le principe. Les tags disposent d'un identifiant unique et statique (équivalent d'un numéro de série) inscrit par le fabriquant, à ne pas confondre avec l'identifiant de niveau applicatif qui peut dans certains cas être modifié dans des protocoles d'authentification avec identifiant dynamique. Si le numéro de série est de longueur l, il peut être désigné par la chaîne de bits $b_1 b_2 \dots b_l$. La figure 2.5 montre un arbre binaire de profondeur 3. Les numéros de série sur 3 bits correspondraient aux $2^3 = 8$ feuilles de cet arbre.

L'algorithme dit de *tree walking* permet au lecteur d'identifier les numéros de série des tags qui lui répondent au moyen d'une recherche récursive dans l'arbre. La racine correspond à la chaîne vide et chaque nœud de profondeur d est représenté par $b_1 b_2 \dots b_d$. Le principe de l'algorithme est le suivant : le lecteur part de la racine puis questionne récursivement les tags portant le préfixe $b_1 b_2 \dots b_d$. Les tags lui répondent avec le $(d+1)^{\text{e}}$ bit de leurs numéro de série. Si il y a collision, *i.e.* si un 0 et un 1 sont simultanément renvoyés, le lecteur recommence la procédure aux deux nœuds du niveau $d+1$ séparément. Si par contre un seul bit b_{d+1} alors seul le nœud correspondant est pris en compte et le sous-arbre correspondant à l'autre nœud est éliminé. Lorsque l'algorithme atteint une feuille, la séquence de bits correspond à un numéro de série d'un tag.

La figure 2.6 montre un exemple avec cinq tags présents dans le champ de lecture, représentés par des disques verts. Leur numéros de série respectifs sont 000, 010, 100, 110 et 111. L'algorithme parcourt l'arbre récursivement de gauche à droite, les collisions sont

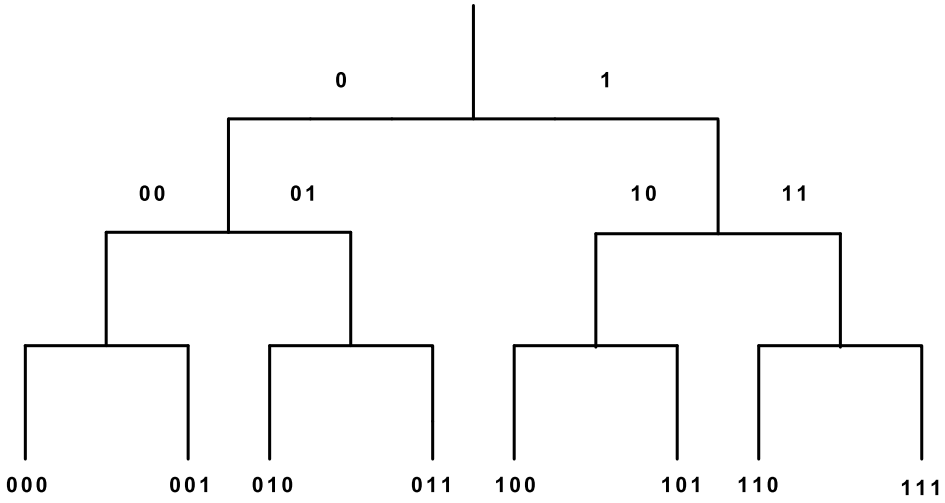

Fig. 2.5 – Arbre binaire des identifiants sur 3 bits

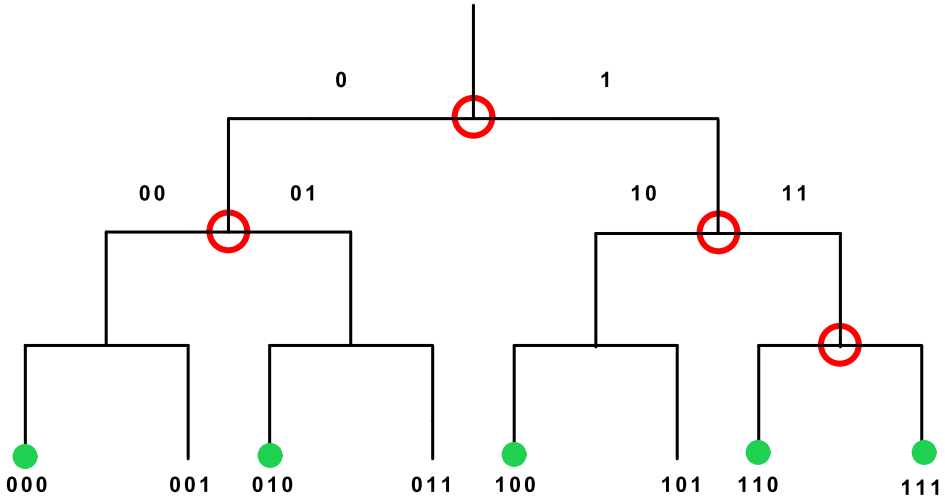

Fig. 2.6 – Exemple de déroulement du *tree walking*

représentées par des cercles rouges, là ou des numéros de série sont présents à la fois dans les sous-arbres gauche et droite. Ceci n'est qu'un exemple illustratif car en réalité l'arbre a une profondeur plus grande et un nombre de numéros de série possible bien supérieur. Nous verrons qu'un moyen de se prémunir contre la traçabilité a été imaginé à partir de cet algorithme (cf. *blocker tag* section 2.3.3)

Protocoles probabilistes

Les protocoles probabilistes sont souvent basés sur la procédure TDMA appelée *Aloha*[1], qui est en quelque sorte l'ancêtre des procédures CSMA utilisées par Ethernet et Wi-Fi (802.11) aujourd'hui. La méthode consiste à envoyer ses données sur le canal sans se préoccuper du fait qu'il soit libre ou non.

Les collisions dans ce cas se situent dans le temps et non sur le numéro de série. Une amélioration appelée *slotted Aloha* a été imaginée au moyen d'une discrétisation du temps en *time slots* ou intervalles de temps. De cette manière, les collisions ne peuvent avoir lieu que sur la durée d'un slot. Ce mécanisme est plus efficace, mais nécessite une synchronisation, chaque tag est contraint de répondre juste après le début d'un time slot. Le lecteur choisit un nombre de slots n. Si n est trop petit par rapport au nombre de tags, des collisions apparaîtront. Le tag recommencera la requête avec un autre n en ignorant les tags dont les numéros de série n'ont pas donné lieu à une collision par une commande de *muting* – technique de *switch-off*.

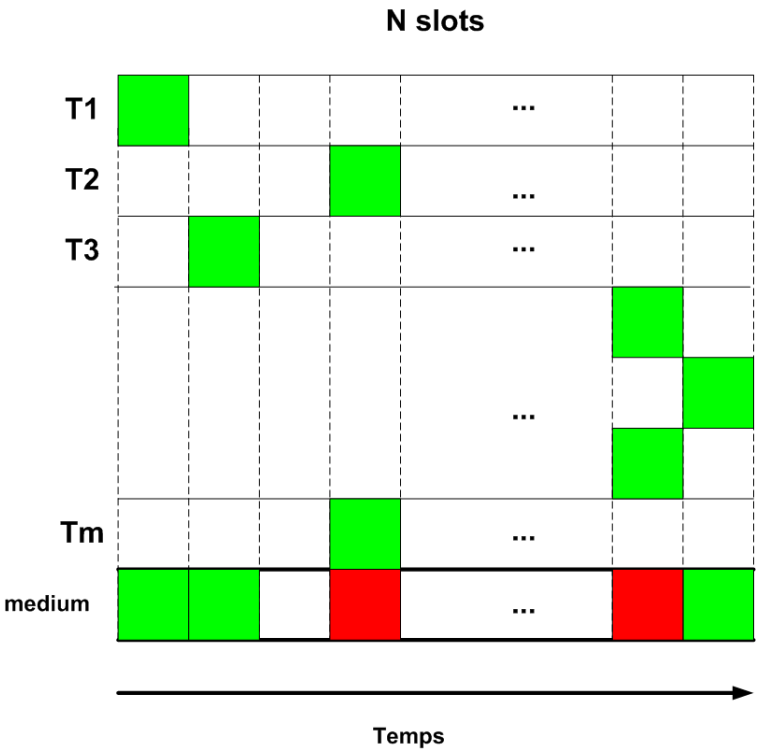

Fig. 2.7 – Slotted Aloha

Un exemple (figure 2.7) montre des collisions intervenant aux 4^{e} et $(n-1)^{e}$ slots. Le lecteur procédera à une nouvelle requête avec un n adapté en fonction des collisions

[1] en mémoire du réseau développé à l'Université de Hawaii dans les années 1970. Ce réseau avait la particularité d'utiliser un médium de transmission partagé pour la transmission.

précédentes et ignorera les tags n'ayant donné lieu à aucune collision. La technique est répétée jusqu'à ce que tous les tags soient identifiés.

Avoine souligne les lacunes de ces techniques dans [2] et montre qu'elles peuvent aussi mener à de la traçabilité.

2.2 Attaques

Après avoir vu les concepts des principaux protocoles, nous nous attardons sur les attaques possibles sur des systèmes RFID. L'accent est mis sur les attaques menaçant l'authentification qui peuvent mener à l'usurpation d'identité. L'attaque relai est étudiée en détail puisqu'elle motive les protocoles que nous étudierons au chapitre suivant. Nous n'aborderons pas les attaques sur le middleware et les niveaux supérieurs comme les débordement de tampons ou les injections SQL telles que décrites dans [48].

2.2.1 Le déni de service

Les attaques par déni de service ne sont pas l'apanage du domaine RFID mais concernent le monde des technologies de l'information dans son ensemble. Elles ont pour but de rendre une application incapable de répondre aux requêtes des utilisateurs. Ces attaques sont faciles à mettre en oeuvre et il est difficile de les prévenir dans les systèmes sans fil. On peut en recenser passablement, par exemple la destruction physique de tags ou un bruiteur qui introduit volontairement des interférences – *jamming* – afin de perturber le fonctionnement du système. D'autres dénis de service plus classiques peuvent être effectués au niveau logiciel par exemple sur les serveurs de bases de données EPC. Nous verrons qu'un déni de service a été exploité pour se prémunir d'attaques en bloquant le tag.

2.2.2 L'attaque *man-in-the-middle*

L'étude de la sécurité informatique et de la cryptographie classique nous enseigne que les échanges entre deux entités peuvent être sujets à une attaque du type *man-in-the-middle* perpétrée par une entité extérieure qui intercepte les messages échangés entre les victimes. Ce concept est général et englobe plusieurs types d'attaques possibles. Elles peuvent être *actives* – elles modifient alors les données échangées – ou *passives* en « écoutant » les informations qui transitent. Cette notion s'applique à la sécurité informatique dans son ensemble et pas uniquement aux systèmes pervasifs (ou diffus) comme RFID. Un mécanisme de défense utilisé dans les protocoles d'authentification se base sur un paradigme d'échange *challenge/response* (défi/réponse). Un défi est envoyé au tag qui renvoie une réponse dépendant du défi et pouvant aussi dépendre d'une clé partagée. Une parade efficace

contre ce type d'attaque réside dans l'implémentation d'un protocole d'authentification efficace, ce qui implique de fait une capacité suffisante au niveau des ressources du tag pour des opérations idoines.

2.2.3 Cas des systèmes RFID

Ces systèmes ont une particularité supplémentaire, une preuve de proximité est nécessaire pour valider l'authentification. En effet, en plus de la vérification qu'une entité est présente, il faut vérifier qu'elle est physiquement proche. Des attaques de type *man-in-the-middle* particulièrement pernicieuses peuvent être envisagées, et ce sans opération cryptographique supplémentaire. L'attaquant joue seulement le rôle de proxy qui relaie les informations sans être détecté, rendant ainsi l'attaque facile et transparente. On prend aisément conscience de l'ampleur de la problématique en présence d'applications sensibles qui utilisent la RFID.

Nous présentons les trois types d'attaques relatives à la distance comme elles sont mentionnées dans [7] et [40], évaluons l'importance de chacune d'elles et déterminons leur pertinence dans des systèmes RFID.

Définition 3 (Fraude sur la distance) *La fraude sur la distance met en œuvre deux entités : un tag malveillant $\bar{T}$ et un lecteur légitime L. Elle permet à $\bar{T}$ de faire croire qu'il est plus proche de L qu'il ne l'est réellement. Elle consiste donc à fausser l'information de la distance entre $\bar{T}$ et L uniquement au moyen du tag malveillant $\bar{T}$.*

La figure 2.8 illustre cette attaque. Elle concernerait plutôt les systèmes RFID actifs car

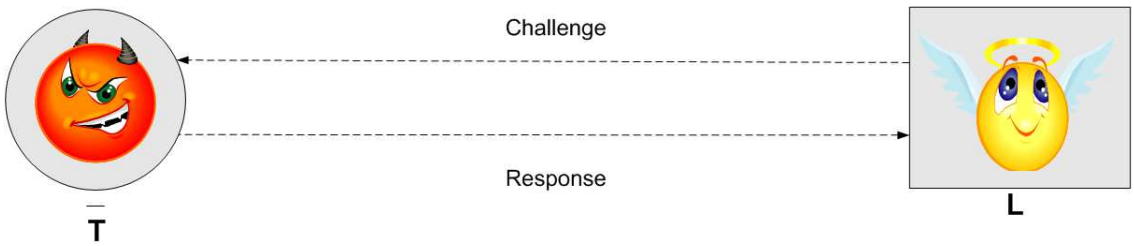

Fig. 2.8 – Fraude sur la distance

elle présuppose que le tag malveillant ait une connaissance précise des aspects temporels du protocole de vérification de distance du lecteur et soit capable de le fausser en les modifiant. Nous en étudierons une parade au chapitre 3.

Définition 4 (Attaque relai) *L'attaque relai fait intervenir trois entités. Un tag T et un lecteur L tous deux légitimes ainsi qu'un attaquant A qui relaie les informations entre T et L via un autre moyen de communication sans que T ni L n'en soient conscients.*

On rencontre souvent cette attaque sous la dénomination de *mafia fraud* dans la littérature. L'attaquant A peut être représenté par une paire $\{\bar{T}, \bar{L}\}$ qui jouent le rôle respectivement de tag et lecteur malveillant. $\bar{L}$ interagit avec le tag légitime T, transmet les données à $\bar{T}$ qui sera lu normalement par L comme s'il s'agissait du tag légitime T alors que celui-ci est situé à une plus grande distance. Ce type d'attaque (schématisé à la figure 2.9) constitue l'objet de la section suivante. Elle est plus redoutable que la précédente car réalisable même sur des tags passifs comme nous le verrons.

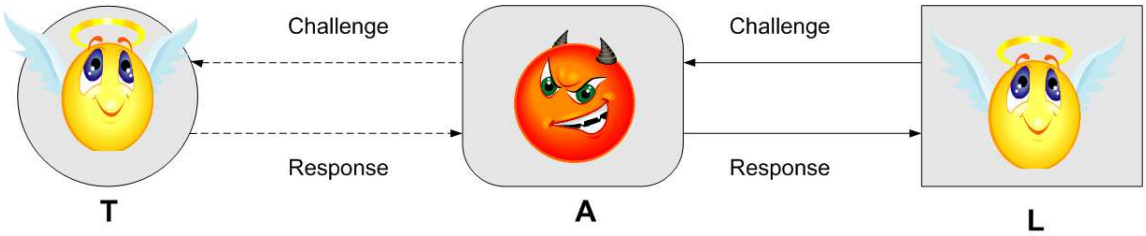

Fig. 2.9 – Attaque relai

Définition 5 (Attaque relai avec collusion) *L'attaque relai avec collusion s'effectue au moyen d'un tag malveillant $\bar{T}$ qui collabore avec un attaquant (relai) A situé près d'un lecteur légitime L afin de le tromper.*

Cette attaque, aussi nommée *terrorist fraud* (figure 2.10), est une combinaison des deux précédentes. Le tag malveillant $\bar{T}$ – qui peut être vu comme tag légitime agissant de manière préjudiciable – conspire avec l'attaquant pour tromper L. Elle est plus pernicieuse et plus difficile à contrer.

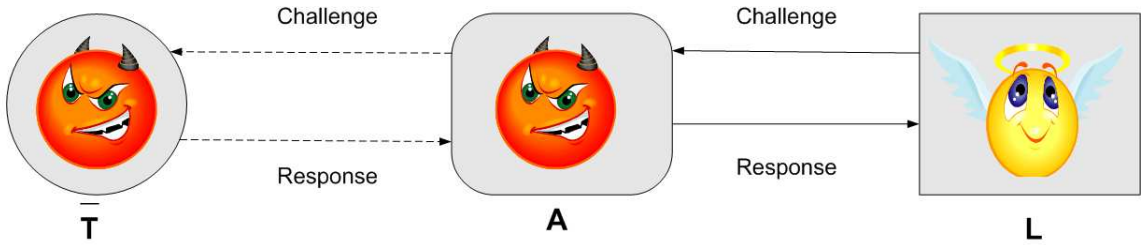

Fig. 2.10 – Attaque relai avec collusion

Dans les trois représentations de ces attaques (figures 2.8, 2.9 et 2.10), les flèches en trait continu impliquent une certaine proximité, *i.e.* la portée de lecture maximale et les flèches en traitillé une plus grande distance. Nous verrons avec l'attaque relai comment cette distance peut être théoriquement arbitrairement grande.

2.3 Attaque relai

L'attaque relai constitue le cœur de notre travail. Elle tire profit du fait que les tags peuvent être interrogés sans accord préalable de leur propriétaire, à fortiori si celui-ci n'est pas conscient qu'il en porte sur lui. Comme nous allons le voir, cette lacune ouvre la voie à une attaque sérieuse qui peut potentiellement faire des dégâts considérables.

2.3.1 Concept

L'attaque relai réside au niveau hardware (physique), ce qui la rend réalisable même si les protocoles des niveaux supérieurs utilisent des mécanismes d'authentification, si puissants que soient leurs algorithmes. La figure 2.11 en illustre le fonctionnement. Le

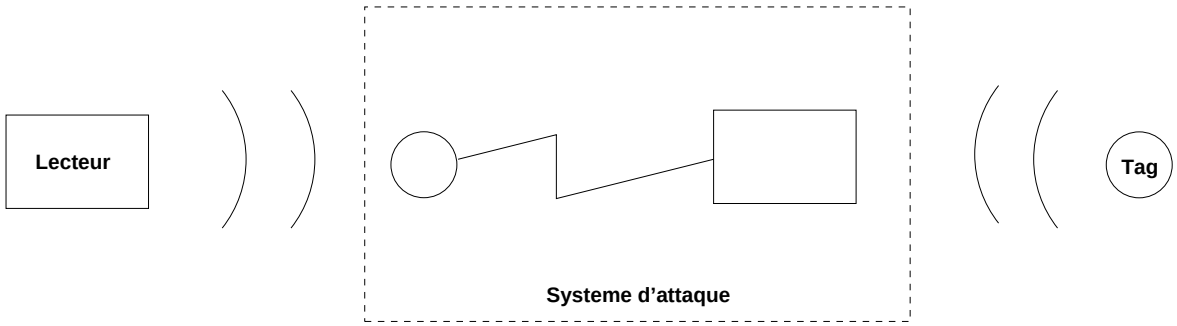

Fig. 2.11 – Attaque relai sur un système RFID

système d'attaque consiste en deux entités reliées par un média de communication rapide, typiquement un fil, pour la transmission des données. Une entité simule un tag auprès du lecteur d'origine et l'autre simule un lecteur auprès du tag d'origine. Les informations passent ainsi de manière transparente dans le système d'attaque. Cette technique crée donc une sorte de « rallonge » au système, permettant d'augmenter la distance entre tag et lecteur légitimes de manière considérable. Kfir et Wool dans [32] utilisent une terminologie qui illustre bien le concept. Ils parlent de *ghost* (fantôme) pour l'entité simulant le tag et de *leech* (sangsue) pour celle simulant le lecteur.

Un déroulement de l'attaque prend donc la forme suivante. Le lecteur envoie un message au fake tag, qui agit comme un tag normal et transmet les informations au fake lecteur qui les reçoit et trompe le tag légitime en lui transmettant le message. L'attaque est symétrique et s'effectue de de manière similaire dans le sens inverse en trompant le tag légitime. Dans ce cas le fake lecteur l'interroge, transmet les informations au fake tag qui trompe le lecteur en se faisant passer pour légitime. L'attaque relai décrite ci-dessus est passive *i.e.* elle ne modifie pas les données transmises, mais elle peut être active, ce qui permettrait à son auteur de stocker, puis de modifier les informations échangées, ouvrant la voie à de nombreuses actions malveillantes.

2.3.2 Impact et conséquences

La portée de lecture, paramètre essentiel, est faussé comme nous l'avons vu. Tags et lecteurs légitimes n'ont plus besoin d'être physiquement proches pour que la communication s'établisse et sont en quelque sorte leurrés. Voyons dans des cas concrets comment cette attaque peut prendre une dimension dramatique et répréhensible pénalement.

Passeports De nombreux gouvernements parlent d'introduire des tags dans les passeports. La possibilité de passer des contrôle sous l'identité d'une autre personne serait envisageable en consultant l'identité du passeport de la victime et en le restituant au contrôle (à supposer qu'aucune authentification ne soit nécessaire). Dans notre ère post 11 septembre, cela accentuerait la psychose et ne manquerait pas d'intéresser des terroristes éventuels qui pourraient passer outre les strictes réglementations de la CIA et de l'Union européenne en matière de données personnelles des usagers dans les aéroports. Avec relativement peu de moyens, le coup porté au *Patriot Act* des Etats-Unis serait non négligeable.

Contrôle d'accès L'accès limité à une salle, ou la preuve qu'une personne est physiquement présente à un certain endroit à un moment donné sont aussi vulnérables. A supposer que l'accès à son domicile puisse dans un future proche se baser sur un système RFID et remplace les clés traditionnelles, la perspective de voir un intrus pénétrer chez soi de manière discrète et non violente ne relève pas de l'utopie. En effet la seule restriction en pratique est la faible distance à laquelle doit se trouver le fake lecteur par rapport au tag légitime. En s'approchant suffisamment du tag de la victime pour l'activer l'attaquant peut ainsi relayer les informations à un complice à proximité du lecteur de la porte d'entrée permettant l'ouverture de celle-ci. Cette perspective n'est pas totalement imaginaire car des systèmes d'accès de ce style émergent peu à peu, en particulier avec des tags sous-cutanés.

Paiements automatiques De la même manière il est possible par ce moyen de débiter un porte-monnaie virtuel si celui-ci utilise la RFID. En plaçant les entités du système d'attaque de manière judicieuse, des achats peuvent être faits sur le compte d'autrui, entraînant le cauchemar des établissement bancaires qui devraient gérer des situations litigieuses nécessitant de nombreuses opérations d'extournes et de remboursements.

Dans la pratique, les seules contraintes sont une certaine proximité entre lecteur et fake tag ainsi qu'entre fake lecteur et tag. Ces distances peuvent être augmentées en agissant sur les paramètres physiques du système. Sorrels dans [52] montre comment de manière relativement simple, en agissant sur le diamètre des antennes ou le facteur de qualité, la portée peut être accrue. Pratiquement, avec une antenne dissimulée dans une mallette par exemple, il est possible de s'approcher suffisamment d'une victime pour déclencher l'attaque lorsque celle-ci se trouve dans un lieu public (file d'attente, magasin, banque, transport public etc). L'attaque relai est menaçante dans le sens qu'elle permet l'usurpation d'identité – ou *impersonation*. C'est son principal attrait pour un utilisateur malveillant. La pertinence de l'attaque est moindre dans le cas de simples systèmes d'identification.

2.3.3 Protections et moyens de parade

Plusieurs approches peuvent être imaginées pour se prémunir contre une attaque relai. La première consiste à circonscrire la distance entre tag et lecteur au moyen de protocoles dits de *distance bounding*. Ces protocoles fournissent une limite physique de distance en se basant sur un fait physique immuable bien connu : aucun signal ne peut se propager plus vite que la lumière. Nous ne les détaillons pas dans l'immédiat puisqu'ils font l'objet du prochain chapitre.

Le moyen le plus radical de se protéger est quelque peu radical puisqu'il consiste à détruire définitivement le tag. Cette solution est peu cohérente dans les systèmes d'authentification puisque toutes les possibilités se trouvent anéanties. La destruction de tag est plutôt destinée aux tags destinés aux chaînes d'approvisionnement et à l'identification. Une fois que l'objet correspondant a trouvé acquéreur, celui-ci ne peut plus faire l'objet de traçabilité. Mais une fois encore ce serait se priver d'avantages liés au service après vente par exemple. Cette solution présente donc peu d'intérêt.

Une autre approche vise à empêcher l'attaquant d'intervenir durant la phase d'authentification (défi/réponse) en isolant le système du reste du monde. Cette isolation est réalisable au moyen d'une cage de Faraday (figure 2.12) pour empêcher toute interférence électromagnétique extérieure. La solution est efficace, mais relativement laborieuse à mettre en œvre pratiquement et peu agréable à l'utilisation.

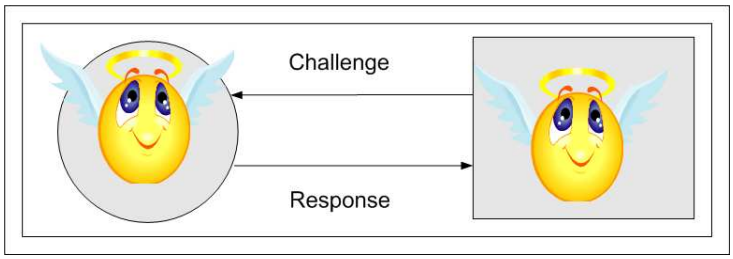

Fig. 2.12 – Isolement par une cage de Faraday

Les avantages de la technologie sont passablement affectés si chaque phase d'authentification nécessite une infrastructure matérielle ad hoc. De plus un investissement supplémentaire est nécessaire pour l'entité jouant le rôle de cage de Faraday et un problème pratique peut survenir selon la dimension de l'objet équipé du tag. Si celui-ci est imposant par rapport aux dimensions de la cage, la phase d'authentification sera délicate. Ce système est particulièrement adapté pour la protection des smartcards sans contact. Des entreprises[2] ont déjà commercialisé des protections de petite taille pour envelopper les cartes RFID qui seront probablement présentes dans de plus en plus de porte-monnaies.

[2]voir par exemple : `http://www.emvelope.com/`

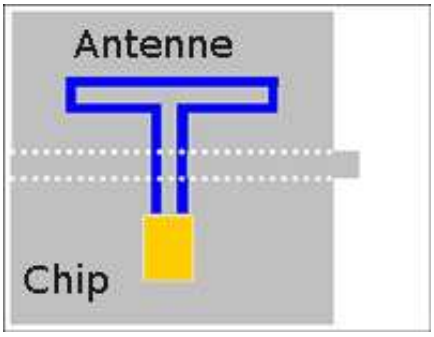

Fig. 2.13 – *clipped tag* d'IBM

Des systèmes hybrides ont aussi été imaginés. L'authentification peut se faire préalablement à l'échange des données par autre moyen de communication, typiquement l'infrarouge ou mieux une liaison filaire pour assurer la proximité tag/lecteur. De cette manière les conditions d'intégrité et de confidentialité sont assurées. Cependant, aussi bien le tag que le lecteur doivent être pourvus de fonctionnalités supplémentaires, ce qui augmenterait leur complexité et probablement leur taille, leur poids ainsi que leur prix. L'entreprise IBM propose des *clipped tags* (figure 2.13) qui offrent la possibilité de réduire la portée de lecture en enlevant une partie de l'antenne. Les avantages sont ainsi conservés avant et après l'acquisition du produit qui, une fois l'antenne raccourcie, est beaucoup moins sujet à traçabilité de par sa portée moindre. Ce système est un bon compromis qui permet de manière simple et accessible à tout le monde de tirer profit de la RFID dans les biens de consommation courante.

Weis imagine dans [54] un type de tag qui, pour être opérationnel, doit être activé par son propriétaire, ce qui permet de pallier au problème lié à l'initiation de la transmission à l'insu de celui-ci. La désactivation empêche *de facto* l'attaque relai. Cette méthode, comme la précédente est plus réaliste. Le porteur du tag gère son ou ses tag en les bloquant dans des endroits sensibles au moyen de codes PIN par exemple.

Une solution ingénieuse est proposée par Juels *et al.* dans [29] sous le nom de *Blocker tag*. Le concept est d'empêcher le lecteur de déterminer quels tags sont dans son champ de lecture en simulant tous les numéros de série possibles. Il constitue un déni de service qui agit sur le protocole d'anti-collision déterministe de *tree walking* vu à la section 2.1.3. Lorsque le lecteur interroge les tags le *blocker tag* crée intentionnellement des collisions de manière à ce que l'algorithme parcoure toutes les feuilles. Ces feuilles sont en nombre trop grand pour le lecteur qui se trouve saturé rapidement.

Les particularités de la RFID vis-à-vis de ces solutions proviennent de la légèreté du système. Leur aspect pratique dû à leur faible encombrement entraîne *in fine* des handicaps considérables. Une plus grande capacité de calcul leur permettrait de mieux se prémunir contre de telles attaques, mais leurs aspects intéressants en pâtiraient. Un bon compromis et un minimum de confiance sont donc de mise afin de tirer profit du système quel qu'il soit.

Pour conclure, notons que les superbes théories quantiques développées par Planck, Heisenberg, Bohr, Pauli et leurs collègues au cours du XX^{e} siècle ont mené à des applications intéressantes en cryptographie. Un flux de photons est inévitablement altéré par le simple fait d'être observé, car un état quantique ne préexiste pas à l'observation mais c'est cette observation qui le fait advenir[3]. Il serait donc théoriquement possible de se protéger contre les attaques relais. Cependant, ces expériences restent l'apanage des chercheurs et

[3]Schrödinger a illustré ceci dans son fameux paradoxe du chat

il faut des moyens considérables et onéreux pour les mettre sur pied. Le flux de photons nécessite une fibre optique pour transiter. Un déploiement dans la RFID à notre époque relève encore de la science-fiction.

2.3.4 Autres technologies

A l'instar de la RFID, de nombreuses autres technologies sans fil et d'environnements pervasifs peuvent être sujets à des attaques relais. Le cas de Bluetooth est abordé par exemple dans [36]. Les différences se situent au niveau de la topologie du système. Les réseaux PAN *Personal Area Network* utilisés par Bluetooth sont appelés *piconets*. Ils sont constitués de périphériques esclaves autour d'un périphérique maître et le rayon moyen est légèrement supérieur à la portée de tags RFID passifs. Bluetooth utilise la technique CDMA de *frequency hopping* adaptatif. Les sauts de fréquences sont générés par le maître pour éviter les interférences et le bruit. De plus, chaque périphérique Bluetooth est identifié par sa BD_ADDR (*Bluetooth device address*) sur 48 bits selon le standard 802 de IEEE. Ces adresses sont l'équivalent des adresses MAC dans une interface ethernet par exemple. L'attaque relai suppose donc un système avec possibilité d'ajuster la BD_ADDR et la connaissance des paramètres de sauts de fréquences.

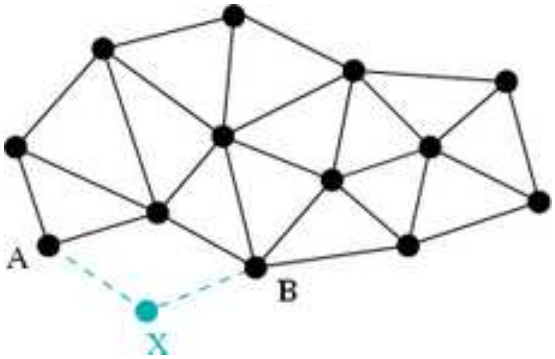

Fig. 2.14 – Wormhole dans un WSN

Dans le cas des réseaux ad hoc et les réseaux de senseurs WSN [31], les attaques revêtent un autre aspect puisque ces technologies disposent de protocoles de routage. Elles peuvent viser la manipulation des données ou la modification de la topologie et des tables de routage. L'attaque qui s'apparente à l'attaque relai est souvent désignée par le terme de *wormhole*. Elle consiste pour un nœud malveillant à enregistrer du trafic à un lieu A donné et le retransmettre à un autre endroit B non situé dans le voisinage immédiat de A. L'attaquant X reste transparent. Il n'est pas détecté par le protocole de routage et se contente de faire un tunnel entre A et B. Suivant la métrique utilisée par le protocole, e.g. la distance, la route du wormhole peut souvent être préférée car elle fournit une distance moindre.

2.4 Aspects hardware

Hancke [22, 23] réalise un système complet d'attaque relai sur un système RFID HF. Il est assez performant puisqu'il parvient à relayer le signal sur 50 m. Le coût du matériel ne dépasse pas 100 £. Carluccio *et al.* [9] effectuent un montage similaire.

Pour les expériences pratiques, nous disposons d'un lecteur EM4094 de l'entreprise EM Microelectronic et d'un jeu de tags HF ISO 14443 type A (figure 2.15).

Fig. 2.15 – Kit RFID

Le manque de temps et de moyens ne nous ont pas permis d'effectuer un système d'attaque. Néanmoins, nous avons pu étudier les signaux transmis par le système au moyen d'une sonde fabriquée de manière assez rudimentaire, selon les paramètres explicités au chapitre précédent.

La sonde (figure 2.16) est constituée d'un circuit LC en parallèle, paramétré de manière à ce que sa fréquence de résonance vaille la fréquence de fonctionnement du système *i.e.* 13.56 Mhz dans notre cas. L'inductance est un fil de cuivre bobiné et la capacité est un condensateur ajustable à l'aide d'une molette de manière à pouvoir calibrer précisément C tel que :

$$\frac{1}{2\pi\sqrt{LC}} = 13.56\text{MHz}$$

Le tout est fixé sur une fiche mâle coaxiale de manière à pouvoir relier la sonde à un oscilloscope et, éventuellement, à une autre partie pour réaliser le système d'attaque.

Fig. 2.16 – Sonde

Parmi les mesures réalisées, nous en montrons deux intéressantes aux figures 2.17 et 2.18. Le signal du lecteur en présence d'aucun tag est sinusoïdal pur à $f = 13.56$ MHz.

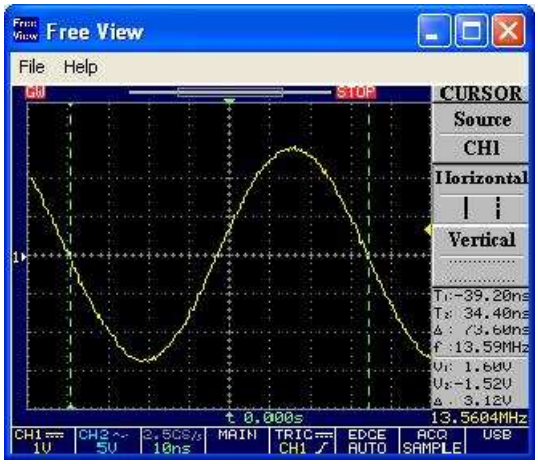

Fig. 2.17 – Signal du lecteur

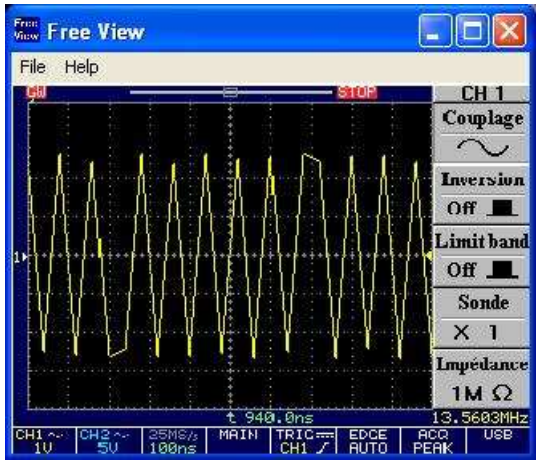

Fig. 2.18 – Signal avec saut de phase

L'autre figure représente de l'information codée dans le signal lors d'un échange entre tag et lecteur. On voit clairement les sauts de phase. Pour retrouver les bits il serait nécessaire d'utiliser un détecteur d'enveloppe.

Chapitre 3

Protocoles de borne sur la distance

« Those who sacrifice liberty for security deserve neither. »

B. Franklin (1706-1790)

Parmi les menaces qu'une attaque relai peut entraîner, il est un aspect qui ne peut être occulté : un attaquant ne peut éviter de causer un retard dans le système. Ceci provient d'un fait physique – ou métaphysique selon le point de vue – sur lequel Aristote, Hume et Kant s'étaient déjà penchés depuis l'Antiquité pour le premier : la causalité. Einstein dans sa théorie de la relativité restreinte, sous un angle plus scientifique, nous assure que *« tout effet a une cause et la cause précède l'effet dans tout référentiel galiléen*[1] *»*. Cela met en évidence qu'il existe une vitesse causale indépassable, faute de quoi, dans certains référentiels, l'effet aurait lieu avant la cause. Cette vitesse est celle des particules de masse nulle, en particulier de la lumière.

Une famille de protocoles a vu le jour pour se prémunir contre les attaques relai. Ils tendent à améliorer les protocoles d'authentification actuels en fournissant une limite sur la distance à laquelle se trouve l'élément interrogé – dans notre cas le tag. Il s'agit des *distance bounding protocols*, expression que nous avons traduit tant bien que mal par *protocoles de borne sur la distance*. La terminologie anglophone étant plus illustrative et plus répandue, nous l'utiliserons dans la suite.

La première section détaille leur fonctionnement général et la suivante présente les protocoles existants en analysant leur sécurité et leur efficacité. Leur analyse sous différents aspects constitue l'objet de la troisième section. Enfin dans la quatrième section nous pro-

[1] En physique, un référentiel galiléen est un référentiel dans lequel un objet isolé (sur lequel ne s'exerce aucune force ou sur lequel la résultante des forces est nulle) est soit immobile, soit en mouvement de translation rectiligne uniforme par rapport à ce référentiel. Cela signifie que le principe d'inertie, qui est énoncé dans la première loi de Newton s'applique. Source : `http://fr.wikipedia.org/`

posons une simulation informatique pour se faire une idée du principe de fonctionnement et des facteurs pouvant influencer les mesures.

3.1 Principe

Les distance bounding protocols concernent un sous-ensemble d'une large famille de protocoles qui recouvre la problématique de la localisation. A l'heure actuelle, on ne compte plus les domaines dans lesquels la localisation a une part prépondérante (la navigation, la construction, etc.). Diverses méthodes sont utilisées dont une sur laquelle nous nous penchons maintenant. Il s'agit de l'exploitation d'une mesure temporelle – *ToF Time of flight* – pour déterminer une distance.

3.1.1 Présentation du concept

L'authentification dans les systèmes RFID ou les réseaux ad hoc, comme nous l'avons vu nécessite une preuve supplémentaire en sus de la preuve d'authentification classique. Cette assertion concerne la distance à laquelle se trouve l'élément interrogé. Le lecteur doit pouvoir s'assurer que le tag ne se trouve pas au delà d'une certaine distance. Si ce n'est pas le cas, le tag doit être ignoré car cela implique que la distance et faussée et donc qu'une attaque relai peut être en cours. Cependant la seule information de distance ne suffit pas car le lecteur ne sait pas en cas de test de distance acceptable si le tag est légitime ou malveillant. Ainsi, les protocoles de distance bounding ne remplacent pas, mais étendent l'authentification, c'est pourquoi ils doivent comporter une phase utilisant les éléments de cryptographie comme les fonctions de chiffrement ou les clés secrètes pour une phase garantissant l'authentification.

Le principe consiste à mesurer le temps d'aller retour d'un signal envoyé par le tag au lecteur et renvoyé par ce dernier. Il s'agit donc d'une procédure de challenge response avec un *timer* qui est déclenché à l'envoi du challenge et arrêté à la réception de la réponse (figure 3.3). Le challenge C est décomposé en n bits $C_1C_2 \dots C_n$ où $C_i \in \{0, 1\}$. Nous considérerons parfois dans la suite C comme un élément (vecteur) d'un espace vectoriel de dimension n à valeurs dans $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$, *i.e* $C \in \mathbb{F}_2^n$. La forme de la réponse R dépend du protocole comme nous le verrons dans la section suivante.

Ce schéma représente uniquement la procédure utile au calcul du temps d'aller retour, elle ne forme donc qu'une partie d'un protocole de distance bounding, sans l'authentification. Elle s'effectue au niveau 1 (physique) et procède à un échange de bits rapides avec à chaque étape la mesure du temps d'aller retour au moyen du timer. La borne sur la distance est déterminée en multipliant le temps d'aller retour maximum par la vitesse de propagation du signal.

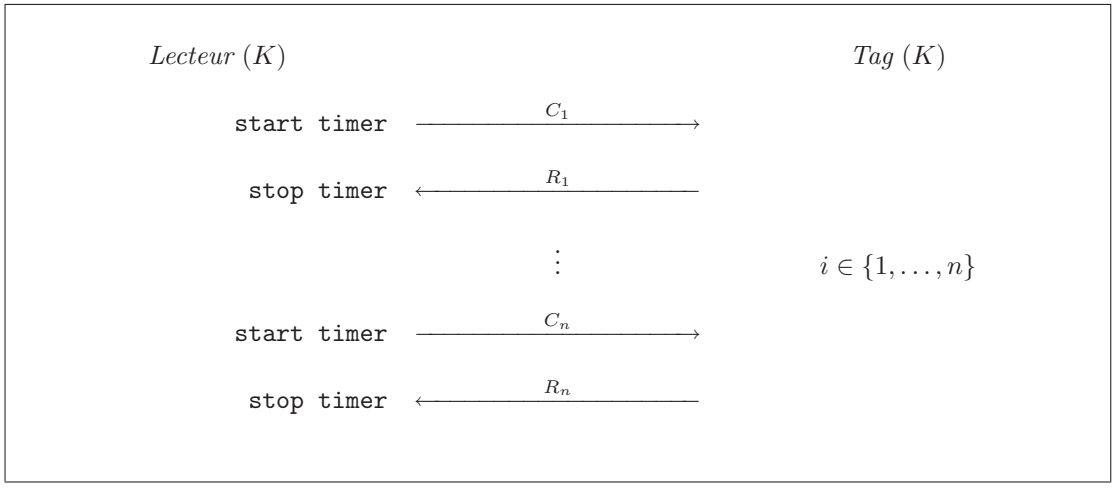

Fig. 3.1 – Détermination du temps d'aller retour des bits

Le temps d'aller retour ainsi mesuré n'est pas le temps de propagation *stricto sensu*. En effet, la procédure entraîne un temps de calcul pour traiter le signal et le renvoyer. Idéalement ce temps devrait être le plus court possible afin que le temps d'aller retour s'approche au plus du temps mesuré. Deux familles de signaux peuvent être utilisées :

1. Les *ultrasons* qui ont l'avantage d'être relativement lents. Le délai de traitement correspondant au temps de calcul peut être négligé par rapport au temps de propagation. Par contre la faille se trouve au niveau sécuritaire, les ultrasons se propagent plus vite dans certains milieux que dans l'air, un attaquant peut aisément effectuer des fraudes sur la distance. Il est alors difficile d'exclure sa présence dans le système.
2. Les *signaux électromagnétiques* qui se propagent à la vitesse de la lumière. Ce fait requiert une grande précision dans la mesure du temps d'aller retour. Une petite imprécision entraîne des fluctuations énormes sur le résultat. Cependant cette méthode donne, comme nous allons le voir, de meilleurs résultats.

3.1.2 Paramètres en jeu

Nous supposerons dans la suite que la borne sur la distance est mesurée avec des ondes électromagnétiques. La figure 3.2 illustre la mesure de la borne d, déterminée de la manière suivante :

$$d = c\left(\frac{t_m - t_d}{2}\right) \qquad \text{avec le RTT :} \qquad t_m = 2t_p + t_d$$

Les valeurs prises en compte sont :

- c la vitesse de la lumière ;
- t_p le temps de propagation ;
- t_d le délai de traitement ;

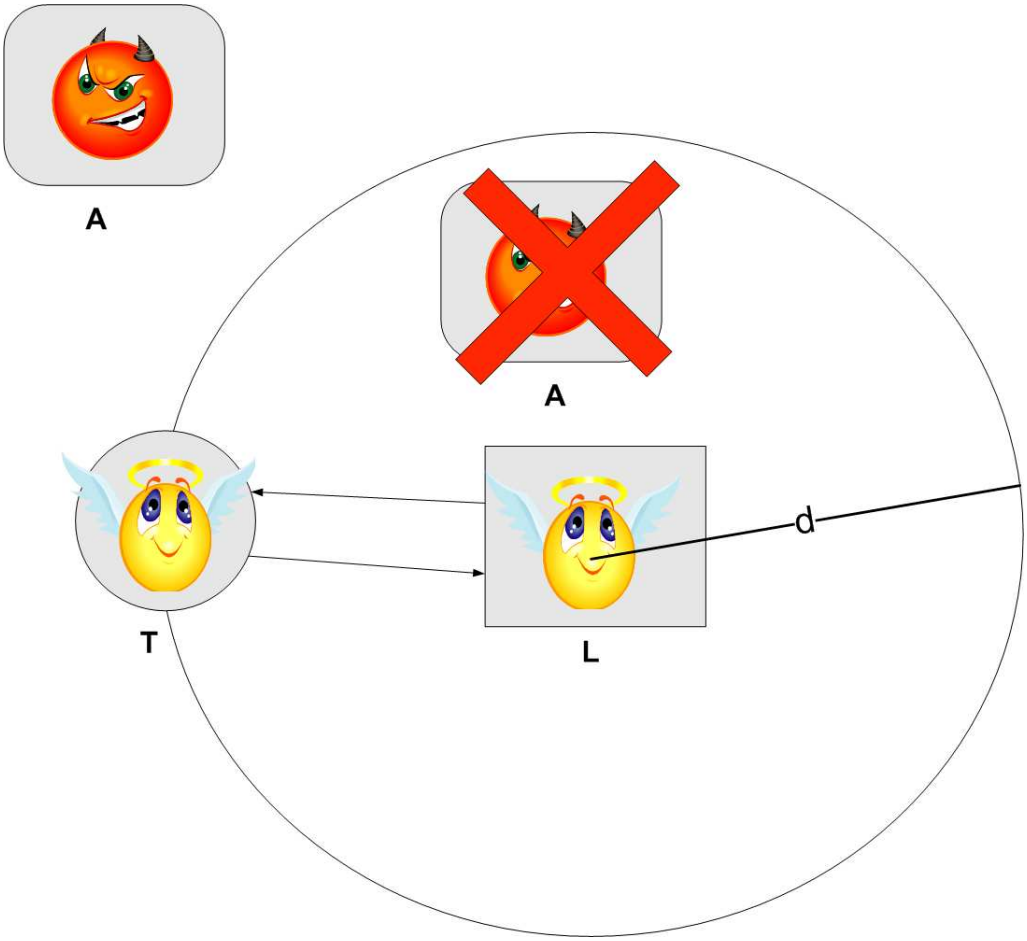

Fig. 3.2 – Borne sur la distance

- t_m le RTT (*Round Trip Time*) total.

Le fait que le signal se propage dans le vide à la vitesse de la lumière c implique qu'un attaquant A ne peux que faire croire qu'il se trouve plus loin qu'il ne l'est réellement car il retarde inévitablement la réponse. L'attaquant ne peut donc se trouver qu'en dehors du cercle de la figure 3.2. Dans ce cas le protocole détecte l'attaque relai.

Néanmoins cette méthode n'est pas complète et ne suffit pas à assurer une parade efficace à l'attaque relai – elle permet juste de déterminer d. En effet, ce processus étant effectué, le lecteur sait qu'un tag se trouve à une telle distance, mais ne sait pas lequel. Le tag distant peut très bien être malveillant mais dans ce cas il est aussi rejeté après la procédure d'authentification car il ne connaît pas les secrets partagés. C'est pourquoi les protocoles de distance bounding combinent la mesure de distance avec des considérations cryptographiques.

Les aspects temporels revêtent un aspect particulièrement important. Nous prenons conscience que les attaques relais ne peuvent pas être facilement détectables avec des protocoles opérant à la couche applicative car à ce niveau les informations temporelles

d'arrivée des messages ont déjà été passablement influencées par les synchronisations, évitement de collisions, détection d'erreurs et tous les processus implémentés dans les couches inférieures. On comprend alors pourquoi ce type de protocole dépend solidement de la couche physique, les notions de résolution et de synchronisation temporelles y sont fortement liées. Une légère imprécision sur une mesure de temps et la distance s'en trouve largement faussée, ceci à cause de la valeur de la constante c qui reste énorme comparée aux valeurs en jeu qui sont plus concevables à l'échelle humaine. Il est indispensable pour implémenter un protocole de distance bounding de disposer d'une base de temps suffisamment précise et c'est leur aspect problématique concrètement. La lumière parcourt 30 cm en une nanoseconde. Ce simple fait nous indique que l'implémentation physique ne sera pas triviale, car un niveau assez fin de précision sur d est souhaitable pour éviter les attaques relai dans les applications concrètes utilisant la RFID comme le contrôle d'accès. Dans l'absolu, pour que cette phase de détermination de distance soit optimale, il faudrait un système hardware indépendant du reste du tag, uniquement dédié à cette opération. Comme nous le verrons plus loin, les systèmes UWB (*Ultra Wide Band*) sont efficaces grâce à leur large bande passante et leur synchronisation précise. Le protocole de Hancke et Kuhn décrit dans [24] les préconise mais d'autres systèmes à consommation plus faibles sont déjà testés.

3.2 Protocoles existants

Les protocoles imaginés à ce jour peuvent être considérés comme étant encore en phase de développement. En effet ils peuvent souffrir de la relative nouveauté du concept et du côté empirique des tentatives pour un adversaire de les déjouer. Nous en étudions trois dans les détails, lesquels sont applicables à des systèmes RFID tout en gardant à l'esprit que le concept s'applique à d'autres technologies.

3.2.1 Protocole de Brand et Chaum

Les pionniers dans le domaine de furent Stefan Brand et David Chaum qui publièrent [6] en 1993. Ils y présentent le premier protocole de distance bounding basé sur un échange de bits pour calculer le RTT dans un protocole d'authentification (figure 3.3).

Etape 1 Le lecteur L génère aléatoirement une suite de n bits $C_i \in \{0, 1\}$. Par convention nous dénoterons la concaténation de bits par le symbole $||$ dans la suite, autrement dit, les n bits générés forment la chaîne $C = C_1||C_2||\ldots||C_n$. De manière analogue, le tag T génère une suite R de n bits.

Etape 2 Cette étape correspond à l'échange de bits rapide, elle est effectuée au niveau physique. Les deux étapes suivantes sont répétées n fois.

– L enclenche son timer envoie C_i à T.

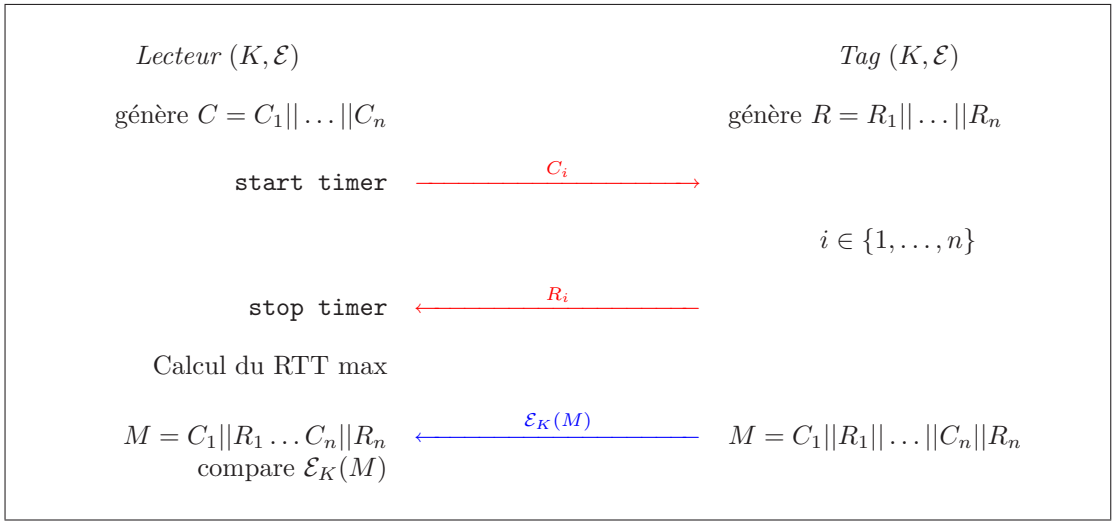

Fig. 3.3 – Protocole de Brand et Chaum version I

– T renvoie R_i immédiatement après avoir reçu C_i. L arrête le timer dès qu'il a reçu R_i en retour.

Etape 3 T concatène les $2n$ bits C_i et R_i pour former une chaîne N, qu'il signe au moyen d'une fonction de chiffrement $\mathcal{E}$ et de la clé secrète K.

L'authentification est réussie si et seulement si les deux conditions suivantes sont réunies : le tag est jugé suffisamment proche de L et la signature chiffrée reçue est correcte. De cette manière, le tag fournit une valeur chiffrée dépendant du challenge C et confirme qu'il est bien impliqué dans le protocole. De plus le tag prouve de manière sûre qu'il a reçu les C_i avant de renvoyer les R_i du fait de la structure de M.

Pour bien différencier les deux parties qui constituent le protocole, nous avons symbolisé la partie « lente » par des flèches bleues et la partie « rapide » par des flèches rouges. Le délai des échanges bleus est peu sensible et variable puisque le signal passe au travers toutes les couches, retardant ainsi sensiblement le processus. A l'opposé, un délai minimal est nécessaire lors des échanges rouges.

Ce protocole n'est néanmoins pas suffisant pour éviter une fraude sur la distance. En effet, nous pouvons remarquer que les bits R_i renvoyés par le tag ne dépendent pas des bits de challenge C_i reçus du lecteur. Cela implique qu'un tag $\bar{T}$ malveillant peut tromper L en envoyant prématurément ses bits de réponse R_i. Pour parer à cette éventualité, Brand et Chaum proposent une variante de leur protocole en y ajoutant une phase de *commitment*.

En cryptographie, un schéma de *commitment* peut être visualisé comme une transaction au moyen d'un coffre disposant d'une combinaison (figure 3.4).

Le tag place M dans un coffre c, le ferme et le transmet au lecteur. Quand le tag veut rendre M visible au lecteur, il lui suffit de lui transmettre le message d – pour *decommit* – qui correspond à la combinaison du coffre. Cette méthode a deux conséquences :

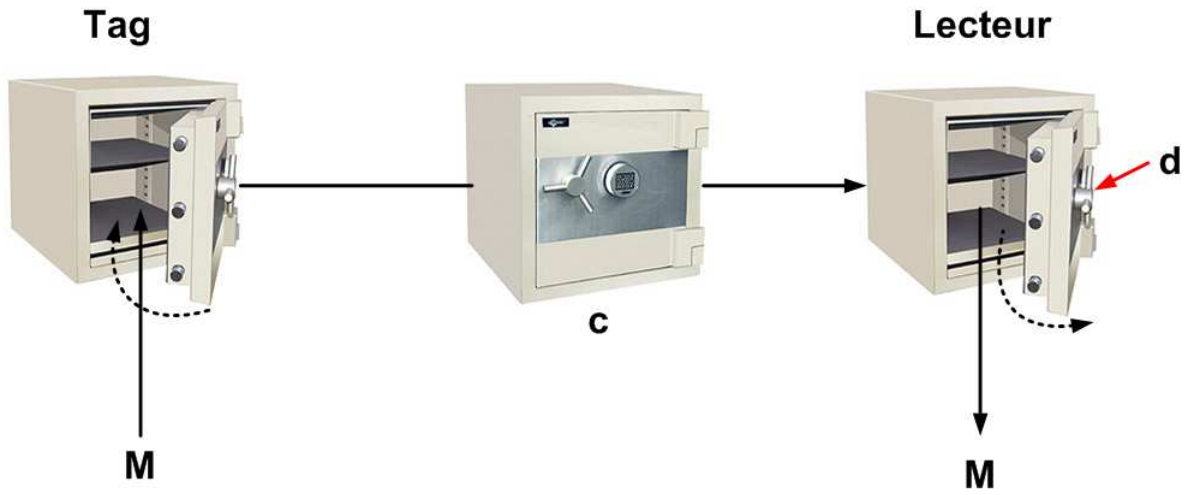

Fig. 3.4 – Schéma de *commitment*

- M ne peut pas être connu avant que c ne soit ouvert
- M peut pas être modifié après que c soit fermé

Pasini dans [41] propose les deux notations suivantes pour les algorithmes entrant en jeu dans cette phase de *commitment* :

$$(c, d) \leftarrow \mathsf{commit}(M) \qquad \text{et} \qquad M \leftarrow \mathsf{open}(c, d)$$

Le protocole de Brand et Chaum modifié est schématisé à la figure 3.5

Etape 1 L génère aléatoirement n bits C_i.

Etape 2 T génère aléatoirement n bits M_i, utilise un schéma de *commitment* et transmet c à L (une valeur hachée $h(M)$ peut faire l'affaire pour déterminer c, T doit alors disposer d'une fonction de hachage h).

Etape 3 L'étape bas niveau d'échange de bits a lieu comme précédemment à la différence près que cette fois L ne fait pas confiance à T qui peut anticiper les C_i en envoyant des bits $\widehat{C}_i$ (les bits peuvent aussi être altérés par du bruit).

Etape 4 T révèle d à L qui vérifie que les bits M_i sont bien conformes aux $\widehat{M}_i$ reçus. De plus, comme précédemment, T concatène les $2n$ bits C_i et R_i pour former une chaîne N, qu'il signe au moyen d'une fonction de chiffrement et de la clé secrète K.

En définitive dans l'étape 4, L vérifie que les bits qu'il a reçus sont bien conformes à ceux commités dans l'étape 2. De cette façon, il s'assure que le tag n'a pas anticipé les réponses. De plus, il s'assure que la signature chiffrée est correcte et ainsi détermine la borne d, condition d'acceptation de T.

Brand et Chaum proposent encore d'autres protocoles mettant en oeuvre des mécanismes asymétriques à clé publique. Ils nécessitent des ressources accrues, dépassant pour le moment celles des tags actuels. Ils sortent du cadre RFID de ce travail et nous renvoyons le lecteur intéressé à [6].

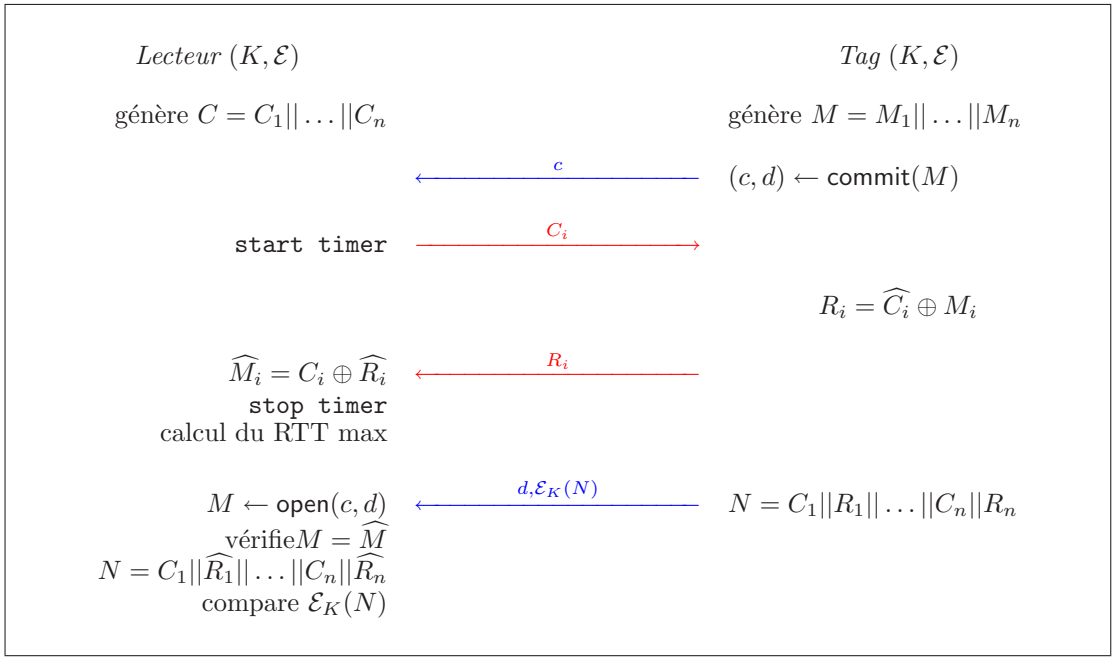

Fig. 3.5 – Protocole de Brand et Chaum version II

3.2.2 Protocole de Hancke et Kuhn

Hancke et Kuhn ont proposé dans [24] un autre protocole de distance bounding. Publié des années plus tard, il se démarque du précédent notamment parce qu'il est plus ciblé sur RFID au lieu de considérer des systèmes sans fil dans leur globalité. Pour l'implémentation pratique ils utilisent la technologie UWB que nous aborderons plus loin. Avant d'étudier leur protocole, voyons les hypothèses sur lesquelles se sont basées Hancke et Kuhn :

1. Le protocole est conçu pour détecter les attaques relais sans collusion uniquement. Il prouve au lecteur *et au lecteur uniquement* qu'un tag ne se trouve pas à une distance supérieure à d. Ainsi il ne fournit pas de non-répudiation sur la distance à une entité tierce ne faisant pas confiance au lecteur.
2. Pour les besoins du protocole, tag et lecteur partagent une clé secrète K et une fonction pseudo-aléatoire et une fonction de hachage h. L'attaquant n'a pas accès à celles-ci autrement qu'au niveau physique via l'interface radio.
3. Le tag est supposé être relativement faible au niveau des ressources. Le temps de calcul de la partie cryptograpique est nettement supérieur au temps d'aller retour maximum pour déterminer la distance.

Voyons le déroulement de leur protocole à la figure 3.6. La flèche en bleu symbolise la phase non critique au niveau du temps, elle peut être effectuée avant et indépendamment la phase d'échange de bits symbolisée par des flèches rouges.

Etape 1 La première étape consiste pour le lecteur à générer aléatoirement n bits C_i et à envoyer au tag un nonce r. T calcule $R = h(K, r)$ au moyen de la fonction de hachage pseudo-aléatoire h et de la clé secrète partagée K. Le résultat R n'est pas utilisé tout de suite mais stocké dans deux registres à décalage de n bits chacun.

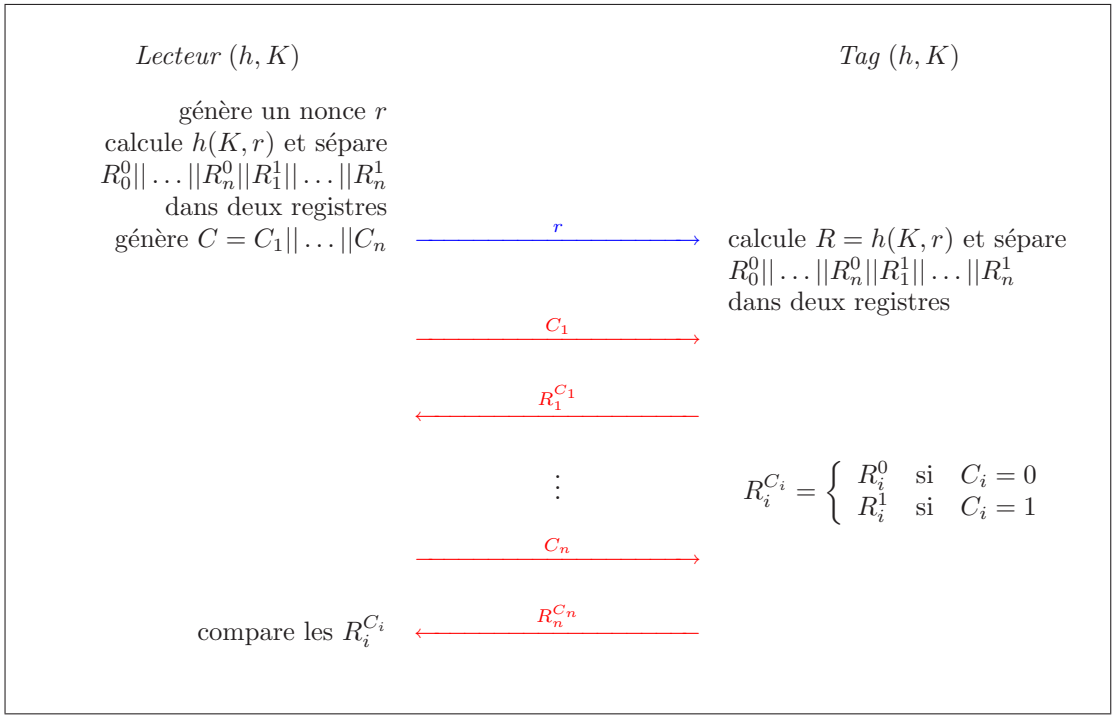

Fig. 3.6 – Protocole de Hancke et Kuhn

Etape 2 La phase d'échange de bits rapide commence ensuite. L envoie un par un les bits de challenge C_i auxquels T répond par $R_i^{C_i}$ qui dépendent de la valeur de C_i selon la règle suivante :

$$R_i^{C_i} = \begin{cases} R_i^0 & \text{si} \quad C_i = 0 \\ R_i^1 & \text{si} \quad C_i = 1 \end{cases}$$

C_i détermine le registre duquel est renvoyé le bit de réponse R_i. De cette manière seule la moitié des bits de R est révélée. La borne sur la distance est déterminée de la même manière que précédemment, en prenant le maximum des RTT mesurés.

Ce protocole a néanmoins un inconvénient majeur, si l'attaquant interroge $2n$ fois le tag avec le même nonce r avant l'étape 2, il obtient les $2n$ bits de R de façon sure et son attaque réussit. Il est donc nécessaire de générer 2 nonces r et s respectivement par le tag et le lecteur. Ainsi R sera déterminé par $R = h(K, r, s)$. La figure 3.7 montre le début du protocole en tenant compte de ce changement, la phase d'échange de bits rapide se fait de manière similaire et n'est pas représentée.

3.2.3 Autres protocoles

Bussard [7] ainsi que Reid *et al.* [46] proposent des protocoles de distance bounding pour contrer les attaques relai avec collusion dans lesquelles un tag malveillant conspire avec l'attaquant proxy. Le premier requiert beaucoup de ressources et il est peu concevable de l'appliquer au monde RFID. Le deuxième, par contre est basé sur des clés symétriques et

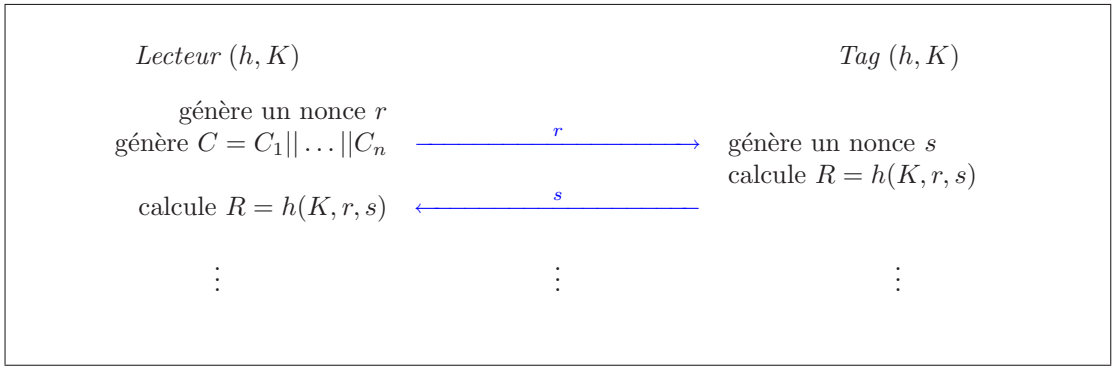

Fig. 3.7 – Protocole de Hancke et Kuhn amélioré

son implémentation est imaginable sur RFID. Il améliore en quelque sorte le protocole de Hancke et Kuhn en utilisant des concepts de [7] afin de le rendre résistant aux attaques relai avec collusion. La seule hypothèse qu'ils font est que le secret partagé K n'est jamais dévoilé. En effet l'attaque est trivialement réussie si l'attaquant le connaît et la distinction entre tag et attaquant n'est plus nécessaire. Ils constitueraient la même entité d'un point de vue cryptographique.

Nous rappelons que la collusion est la participation d'un tag $\bar{T}$ agissant de manière complice de l'attaquant A pour tromper le lecteur L en lui révélant des informations utiles. Le danger supplémentaire vient du fait que les informations secrètes de $\bar{T}$ peuvent être utilisées à des fins différentes que celles que préconise le protocole. Une fois de plus, c'est l'indépendance entre la phase d'authentification et celle d'échange rapide des bits qui rend l'attaque réalisable. Le lecteur ne peut savoir si le tag qui effectue la première est bien le même que celui qui effectue la seconde. Il est seulement convaincu que l'entité qui a effectué l'échange rapide est à proximité et que l'entité qui a effectué l'authentification connaît K. Dès lors, comment être sûr que ces deux entités forment un seul et même tag ? La collusion s'explique par le fait suivant : le tag $\bar{T}$ complice de A est à même de se faire accepter par le protocole en utilisant un tag légitime T pour l'échange de bits rapide.

L'idée de Reid *et al.* est d'introduire volontairement de la dépendance entre les deux phases du protocole de manière à pouvoir assurer le lecteur qu'il a affaire à un et un seul T. Pour ce faire, une clé supplémentaire dite clé de session est introduite. Le protocole fait ainsi intervenir une clé à usage unique ξ de durée de vie limitée à un déroulement du protocole, et un texte chiffré η obtenu à l'aide de ξ et d'une fonction de chiffrement $\mathcal{E}$. La clé ξ est déterminée à l'aide d'une KDF – *key derivation function* – et elle utilisée pour le chiffrement du secret partagé K. La figure 3.8 montre le déroulement du protocole. La phase d'échange de bits rapide est similaire à celle du protocole de Hanke et Kuhn à l'exception des valeurs retournées dans $R_i^{C_i}$. cette fois, elles sont constituées de bits ξ_i ou η_i selon la valeur de C_i. C'est là le principal changement qui garantit une parade à la collusion. Les bits de réponses dépendent de la clé privée du tag.

Pour que le protocole aboutisse à l'acceptation du tag $\bar{T}$ par le lecteur, $\bar{T}$ connaître ξ et η que seul T peut générer. De plus la connaissance de ξ et η implique la connaissance

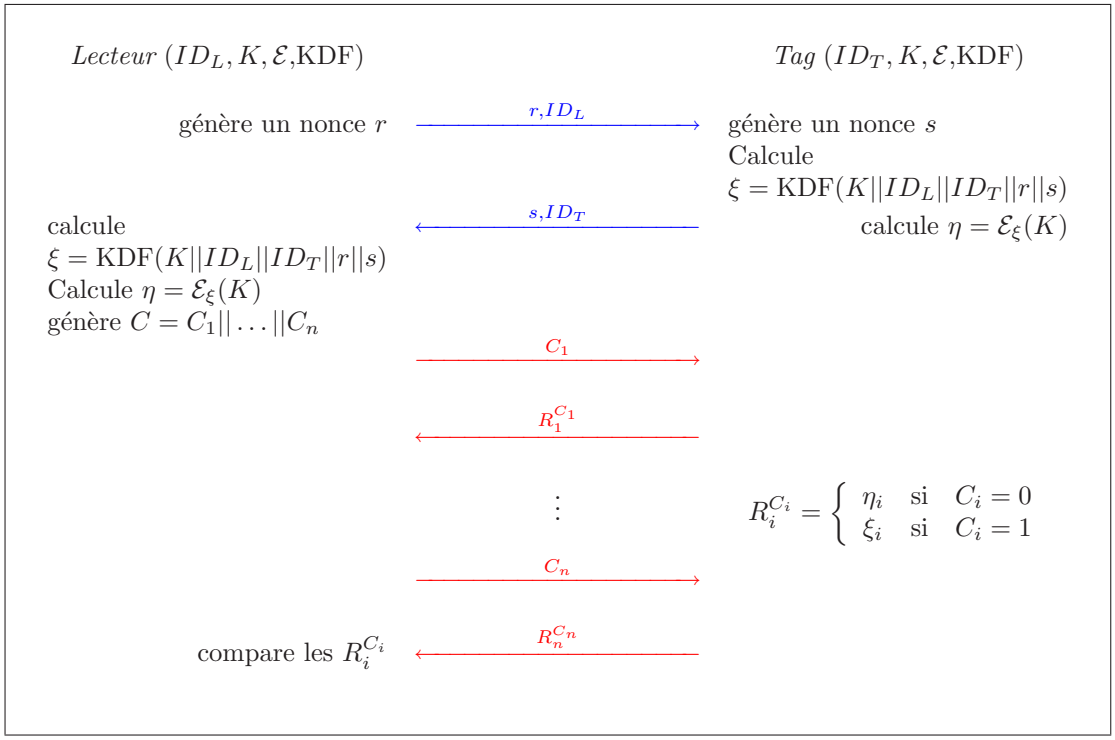

Fig. 3.8 – Protocole de Reid *et al.*

de la clé secrète $K = \mathcal{E}_\xi^{-1}(\eta)$ que $\bar{T}$ ne connaît pas. Il se trouve donc rejeté.

Pour conclure nous pouvons encore citer le protocole de Capkun et Hubaux [8] basé sur celui de Brand et Chaum que nous ne détaillerons pas car il est destiné et optimisé pour les réseaux de senseurs. A l'inverse des précédents, il garantit l'authentification mutuelle entre les nœuds.

3.3 Analyse des protocoles

Nous désignerons dorénavant le protocole de Brand et Chaum par (BC) , celui de Hancke et Kuhn par (HK) et celui de Reid *et al.* par (RE) . Avant d'aborder des aspects d'efficacité et de sécurité, résumons leur comportement vis à vis des attaques définies au chapitre précédent dans un tableau (3.1).

Protocole	Fraude distance	Attaque relai	Att. relai avec collusion
(BC)	✔	✔	✖
(HK)	✔	✔	✖
(RE)	✔	✔	✔

Tab. 3.1 – Protocoles étudiés

3.3.1 Vulnérabilité

Imaginons que l'attaquant interroge le tag au moyen d'un challenge $\widehat{C}$. En d'autres termes, il essaie de deviner le challenge C. Si le système est protégé par (BC) alors l'attaque réussit avec une probabilité de $(\frac{1}{2^n})$. En effet, le choix de chaque bit se restreint à $\mathbb{F}_2$ le corps à deux éléments et les bits sont supposés être aléatoires donc indépendants entre eux. On a alors :

$$\Pr(C_i = \widehat{C}_i) = \frac{1}{2} \qquad \forall i \in \{1, \ldots, n\} \qquad \Longrightarrow \qquad \Pr(R = \widehat{R}) = \left(\frac{1}{2}\right)^n$$

Dans le cas de (HK) , l'attaquant peut connaître de façon sure la moitié des R_i en envoyant un challenge $\widehat{C}$ au tag avant la phase d'échange de bits rapide. Ainsi, quand le lecteur envoie son challenge C, l'attaquant connaît une réponse sur deux et répond de manière aléatoire à l'autre. Cela a pour conséquence une probabilité de réussite de $\left(\frac{3}{4}\right)^n$ car en détail :

$$\Pr(R_i = \widehat{R_i}) = 1 \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} = \frac{3}{4} \qquad \forall i \in \{1, \ldots, n\}$$

Les probabilités de succès de l'attaque dépendent donc uniquement de la taille des chaînes de bits envoyées et diminuent exponentiellement à mesure que n grandit (figure 3.9).

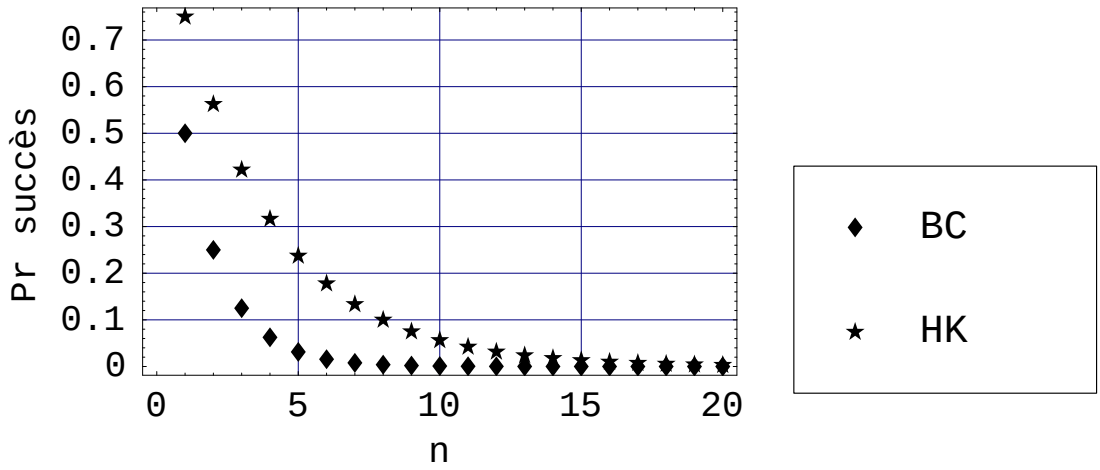

Fig. 3.9 – Probabilités de succès

Le graphique logarithmique en figure 3.10, plus illustratif, montre que, à nombre de bits égal, la probabilité de réussite est moindre avec (BC) .

Du strict point de vue de la résistance à cette attaque (BC) est donc meilleur que (HK) . Cependant, en prenant en considération d'autres paramètres c'est le constat inverse qui s'impose. En effet (HK) ne comporte pas de phase de commitment et de signature – processus qui prend un temps considérable – après l'échange de bits rapides. La phase d'authentification de (HK) prend donc sensiblement plus de temps que dans (BC) . D'après le tableau 3.2 on constate qu'en prenant une longueur n assez grande mais raisonnable,

n	Pr(succès) (BC)	Pr(succès) (HK)	ΔPr(succès)
1	0.5	0.75	0.25
5	$3.13 \cdot 10^{-2}$	$23.73 \cdot 10^{-2}$	$20.6 \cdot 10^{-2}$
10	$9.76 \cdot 10^{-4}$	$5.63 \cdot 10^{-2}$	$5.53 \cdot 10^{-2}$
15	$3.05 \cdot 10^{-5}$	$1.33 \cdot 10^{-2}$	$0.33 \cdot 10^{-2}$
20	$9.53 \cdot 10^{-7}$	$3.17 \cdot 10^{-3}$	$3.17 \cdot 10^{-3}$
30	$9.31 \cdot 10^{-10}$	$1.78 \cdot 10^{-4}$	$1.78 \cdot 10^{-4}$

Tab. 3.2 – Probabilités de succès

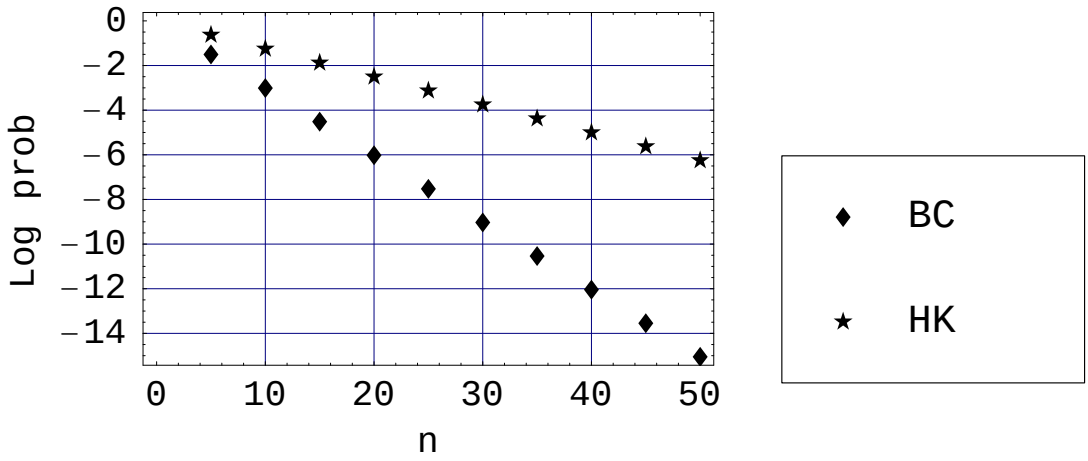

Fig. 3.10 – Log-probabilité de succès

la probabilité de succès devient négligeable. De plus nous n'avons pour l'instant considéré que le cas d'un canal « idéal » c'est-à-dire sans bruit. En pratique les choses changent passablement. En présence de bruit, les messages C et R peuvent devoir être retransmis en même temps que la signature dans (BC) .

3.3.2 Environnement bruité

Munilla dans [40] propose une modification pour (HK) . Elles consiste à générer une chaîne de bits P en plus de R au moment du hachage. Concrètement $R = h(K, r, s)$ et $R = R_0||R_1||P$. Le vecteur P est connu par le lecteur et le tag et a pour rôle de déterminer si l'attaquant connaît la réponse ou la devine pour chaque bit de challenge (selon la valeur de V_i). Si $P_i = 1$ alors le tag considère que l'attaquant connaît C_i tandis que si $P_i = 0$ le challenge C_i n'est pas envoyé et le tag essaie donc de le deviner. Par exemple si $P = 001101$, seuls les bits C_3 C_4 et C_6 sont envoyés. Plus généralement deux cas de stratégies sont envisageables pour l'attaquant :

- Il connaît les bits R_i en avance – entre l'authentification et l'échange de bits rapide

– et réussit son attaque avec la probabilité :

$$\Pr(\text{succès}) = \left(\frac{1}{2}\right)^n \text{ dans le cas où } P = \underbrace{11\ldots11}_{n \text{ fois}}$$

- Il ne connaît pas les bits en avance et essaie de deviner les challenges envoyés. Ce cas comporte davantage de possibilités de vecteurs P à considérer. En effet, il y a $\binom{n}{k}$ possibilités de vecteurs P de longueur n avec le bit 1 représenté k fois.
  – La probabilité de deviner k bits correctement vaut $\frac{1}{2^k}$.
  – Elle est à multiplier par la probabilité[2] d'avoir k bits 1 dans P qui vaut :

$$\Pr(\text{k bits à 1}) = \binom{n}{k}\left(\frac{1}{2}\right)^k\left(\frac{1}{2}\right)^{n-k} = \binom{n}{k}\frac{1}{2^n}$$

  En prenant en compte les deux points précédents et en considérant tous les k possibles, la probabilité de succès s'en déduit.

$$\Pr(\text{succès}) = \frac{1}{2^n}\sum_{k=0}^{n}\binom{n}{k}\left(\frac{1}{2}\right)^k = \frac{1}{2^n}\left(\frac{3}{2}\right)^n = \left(\frac{3}{4}\right)^n$$

Le résultat coïncide avec celui de (HK) , mais seulement dans un cas non bruité. Munilla montre que dans un environnement réél, son protocole est plus performant. En effet, moins de bits échangés entraînent moins de possibilités d'erreurs à la réception. Le bruit est considéré dans (HK) par l'introduction d'un seuil d'erreur au delà duquel la probabilité d'erreur de transmission est jugée trop grande. Au delà de ce seuil, le tag est rejeté.

3.3.3 Eléments cryptographiques

Les protocoles étudiés mettent en oeuvre des fonctions cryptographiques de différentes nature pour leur phase d'authentification, nous en rappelons les principaux concepts.

Définition 6 (Fonction de hachage) *Une fonction de hachage est une fonction qui associe à un vecteur de longueur arbitraire un vecteur de longueur fixe caractéristique de celui-ci.*

De nombreuses fonctions de hachage existent en pratique (MD5, SHA-1 etc.). Les conditions suivantes doivent être remplies par h pour qu'elle soit considérée comme sûre :

- *Résistance à la préimage :* il est très difficile de trouver x à partir de $h(x)$, en d'autres termes de calculer h^{-1}.
- *Résistance à la deuxième préimage :* pour tout x dont on connaît $h(x)$, il est très difficile de trouver y tel que $h(x) = h(y)$.

[2] Calculée en considérant une variable aléatoire binomiale $\mathcal{B}(n,p)$ avec $p = \frac{1}{2}$

- *Résistance aux collisions :* il est très difficile de trouver deux messages aléatoires x et y qui donnent la même signature (*i.e.* $h(x) = h(y)$).

La notion de « très difficile » n'est pas mathématiquement formelle. On entend par là « impossible pratiquement » de manière algorithmique ou matérielle.

Un autre type de fonction rencontré est la fonction de chiffrement $\mathcal{E}$. Elle produit un vecteur chiffré à partir d'une clé secrète K et d'un vecteur de longueur arbitraire à transmettre. Combinée avec une fonction de hachage, elle donne lieu à un HMAC *keyed-hash message authentication code*, qui constitue la signature du message. La clé requise pour vérifier la signature est aussi utilisée pour la créer. De par sa plus petite taille, elle sera moins sujette à erreur lors de la transmission en comparaison à un simple chiffrement.

Enfin mentionnons encore que le protocole (RE) utilise une KDF *key derivation function* qui est une fonction de hachage particulière dont le rôle est de fournir une clé secrète à partir d'autres informations (secrètes ou non).

3.3.4 Efficacité et sécurité

Les tags passifs actuels ont une capacité de stockage de quelques milliers de bits. L'ALU comporte entre 5'000 et 10'000 portes logiques dont une partie est consacrée aux tâches de sécurité comme le chiffrement ou le hachage. Cela reste relativement modeste et la question de la détermination de fonctions de hachage et de chiffrement pour l'implémentation n'est pas triviale.

Nous essayons dans cette section de comparer les protocoles étudiés au niveau de l'efficacité et de la sécurité. En premier lieu nous constatons que les trois protocoles sont réalisés dans l'optique de minimiser le délai de traitement correspondant au renvoi des R_i dans la phase d'échange de bits rapide. (BC) effectue une opération rapide et peu coûteuse XOR ($\oplus$) pour calculer la réponse alors que (HK) et (RE) calculent les R_i préalablement. Ces derniers répondent aux challenges en effectuant une sélection du premier bit d'un des deux registres, ce qui correspond aussi à une opération peu coûteuse.

Pour effectuer une synthèse et distinguer les trois protocoles étudiés, nous nous concentrons du côté du tag. En effet, c'est de cette partie du système que dépendra leur distinction. Le défi relève de l'implémentation des outils nécessaires avec les faibles ressources disponibles. Les trois aspects suivants sont à prendre en considération :

- les calculs et opérations réalisées par le tag ;
- la quantité d'information échangée et de quelle manière se fait l'échange de messages ;
- le stockage des informations.

Les tableaux 3.3, 3.4 et 3.5 résument les caractéristiques précitées.

Pour être efficaces, les nonces générés ne doivent pas être prédictibles, il est donc

Protocole (BC)	
Outils	▷ Fonction de chiffrement $\mathcal{E}$ ▷ Clé secrète K ▷ Générateur pseudo-aléatoire ▷ Fonction de hachage pour le *commitment*
Opérations	▷ Une génération de nonce (n bits) ▷ Un chiffrement de $2n$ bits ▷ n ou exclusifs XOR ▷ Un hachage pour le *commitment*
Messages	▷ n réponses R_i pendant la phase bas niveau d'échange de bits ▷ Un chiffrement et un hash pour la signature
Stockage	▷ $3n$ bits pour les messages ▷ Fonctions $\mathcal{E}, h$ et clé K

Tab. 3.3 – Overview de (BC)

Protocole (HK)	
Outils	▷ Clé secrète K ▷ Générateur pseudo-aléatoire ▷ Fonction de hachage
Opérations	▷ Une génération de nonce ▷ n recherches dans les registres ▷ Un hachage
Messages	▷ n réponses R_i pendant la phase bas niveau d'échange de bits ▷ Un nonce
Stockage	▷ $2n$ bits pour les messages, stockés dans deux registres ▷ Fonction h et clé K

Tab. 3.4 – Overview de (HK)

indispensable qu'ils soient générés de manière aléatoire. En toute rigueur il faudrait dire de manière pseudo-aléatoire car il sont créés à l'aide d'un clock de manière algorithmique. Une étude approfondie et au cas par cas de différents tags permettrait d'envisager un choix pour les fonctions de hachage et de chiffrement. Faldhofer *et al.* [17, 14] proposent des exemples avec une fonction de hachage SHA-256 ou un chiffrement par bloc AES en

Protocole (RE)	
Outils	▷ Clé secrète K ▷ Générateur pseudo-aléatoire ▷ Fonction de chiffrement $\mathcal{E}$ ▷ Key derivation function KDF
Opérations	▷ Une génération de nonce ▷ n recherches dans les registres ▷ Une génération de clé ▷ Un chiffrement de clé
Messages	▷ n réponses R_i pendant la phase bas niveau d'échange de bits ▷ Un nonce
Stockage	▷ $2n$ bits pour les messages, stockés dans deux registres ▷ Fonctions $\mathcal{E}$, KDF et clés K, ξ, η

Tab. 3.5 – Overview de (RE)

montrant qu'ils sont adaptés aux tags RFID de par leur relativement faible gourmandise en ressources.

(BC) se distingue de (HK) et (RE) du fait que la signature est envoyée après l'échange de bits rapide. Comme nous l'avons vu, cela peut poser problème en cas de bruit qui entraînerait une altération du HMAC. Au niveau temporel, le protocole doit effectuer un chiffrement après l'échange de bits et en plus du *commitment*, ce qui entraîne un délai supplémentaire, car ces opérations se font au niveau applicatif. La quantité d'information échangée pour l'authentification est au moins deux fois supérieure à (HK) . De plus le volume de données à stocker sur le tag est supérieur. (BC) souffre peut-être de son âge mais il a le mérite d'avoir posé les jalons dans le domaine et servi de point de départ à ses successeurs.

(RE) est sensiblement plus lourd que (HK) en terme de stockage et de calculs. Cela est en partie dû au fait qu'il offre la possibilité de se prémunir de l'attaque avec collusion, ce qui offre une niveau de sécurité plus élevé. L'attaque avec collusion est cependant moins probable que l'attaque relai qui représente la grande menace comme nous l'avons vu.

L'échange des messages se fait de manière entrelacée. Les messages échangés vont ainsi alternativement dans un sens puis dans l'autre mais il faut bien garder à l'esprit la nature et le but des messages qui diffère selon la phase d'authentification ou d'échange de bits. Au niveau temporel, le laps de temps entre les messages diffère de par l'indépendance des procédures. Nous avons vu que la période entre les deux phases ouvrait la voie à des attaques dans (HK) .

Une amélioration à apporter à (HK) serait de commencer la phase d'échange de bits rapide dès que les deux parties ont calculé $h = (K, r, s)$. L'envoi d'un *acknowledgement* par le tag pourrait être envisageable, afin de prévenir le lecteur qu'il est prêt. Cette confirmation devrait dépendre du secret K afin que seul un tag légitime puisse l'envoyer. On pourrait par exemple prendre $h(K, r \oplus s)$. De cette manière, le tag confirme qu'il est prêt et déclenche immédiatement l'envoi des challenges C_i du lecteur. Cependant une opération de hachage supplémentaire serait alors nécessaire, ce qui signifie plus de stockage et plus de temps de calcul. Encore une fois le gain d'un côté se traduit en perte de l'autre.

L'hypothèse la plus forte de ces protocoles est le fait que les *nonces* doivent être pseudo-aléatoires, utilisés qu'une seule fois et ne peuvent être déterminés par une tierce personne. Sans cette garantie, les efforts mis en oeuvre deviennent caducs.

Nous essayons de résumer les aspects fondamentaux pour la conception d'un protocole de borne sur la distance efficace et sûr :

1. Minimiser la taille de l'information échangée dans la phase de calcul du temps. Le bit, unité atomique, est la meilleure solution. Cette contrainte exclut la communication de paquets ou de Bytes qui prennent trop de temps à traiter. Cela exclut aussi la correction d'erreurs et se limite au niveau physique. Cette exigence est indispensable pour une détermination acceptable de la distance. Une partie dédiée et indépendante du reste du tag est nécessaire.
2. Considérer un médium de communication dans lequel la vitesse de propagation se rapproche le plus possible de c. Cela exclut les ultrasons et pose des limitations quant aux transmissions filaires.
3. Pour la partie cryptographique, choisir une fonction de hachage résistante aux collisions et une générateur pseudo-aléatoire de nombres. Limiter la partie haut niveau au début du protocole, sans signature après l'échange de bits rapide. Le tag doit donc être pourvu d'une mémoire de type EEPROM pour le stockage.

3.3.5 Ultra Wide Band

Pour conclure cette section expliquons pourquoi la technologie *ultra wide band* sort du lot pour des mesures de temps suffisamment fines. La résolution en distance d'un canal de communication se détermine par la formule $r = \frac{c}{B}$ où c est la vitesse de la lumière et B la bande passante du canal. Un bref calcul suffit à se convaincre que des systèmes à très large bande sont requis pour obtenir des résolutions acceptables. Pour leur implémentation, Hancke et Kuhn utilisent la fréquence de la porteuse comme base de temps pour synchroniser la communication, puis des impulsions UWB pour le calcul du temps, sur un système hardware indépendant du reste du tag.

3.4 Simulation

L'implémentation de systèmes permettant des mesures temporelles si précises se révèle délicate avec les moyens dont nous disposons. Afin d'illustrer les différents aspects temporels et leur importance, nous effectuons une simulation de la partie des protocoles qui détermine la mesure de la distance (*i.e.* l'échange de bits rapide). Par analogie et avec un petit effort d'abstraction, nous pourrons aisément transposer ceci au monde RFID. Nos simulations sont implémentées à plus haut niveau et utilisent le modèle de communication TCP/IP, nous allons donc mesurer des RTT différents dans l'absolu que ceux que nous obtiendrions avec UWB ou des ultrasons.

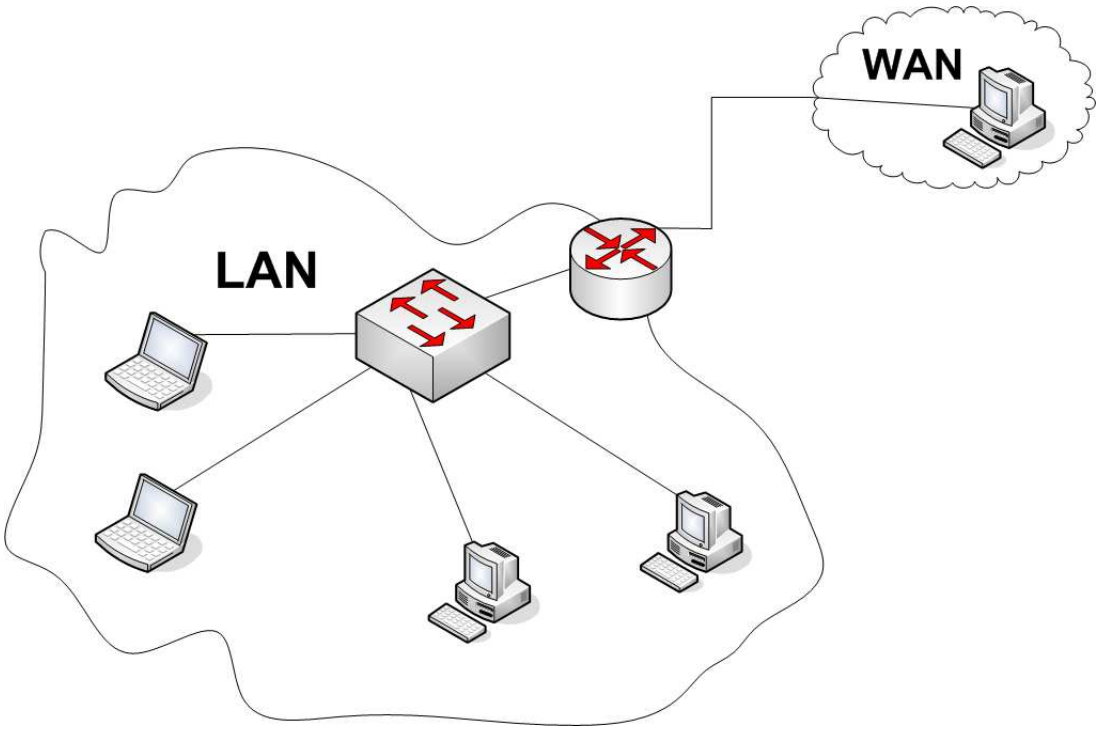

Fig. 3.11 – Schéma de la simulation

La simulation se déroule comme suit (figure 3.11) : une machine représentant le lecteur envoie un paquet challenge à une autre machine qui joue le rôle du tag. Celui-ci renvoie immédiatement le paquet. Le but est d'accepter ou de rejeter la machine distante selon que le RTT est inférieur ou supérieur à une valeur de seuil donnée. Le calcul de la distance n'est pas effectué car les RTT sont de l'ordre de quelques millisecondes, et le calcul de la distance n'a par conséquent pas trop de sens. De plus le RTT comporte une partie de temps de traitement t_d qui est non négligeable par rapport au temps de propagation t_p. Nous verrons la différence des temps de traitement dans deux implémentations différentes en les appliquant à des mêmes machines. La borne sur la distance sera dans nos simulations une borne sur le temps.

3.4.1 Script Bash

Cette première simulation mesure le RTT au moyen d'une commande `ping`, *i.e.* par le protocole ICMP. Le script prend l'adresse de la machine distante en paramètre, lui envoie 10 requêtes `echo`, mesure le RTT moyen et génère un graphe des RTT avec gnuplot. Un test est ensuite effectué pour déterminer si la machine distante se trouve dans le LAN ou le WAN selon la valeur du RTT moyen comparée à la valeur seuil du RTT (définie et modifiable dans le script).

```
#!/bin/sh
#Nbre de requetes a envoyer
count=10
#limite (threshold) sur le temps pour determiner WAN ou LAN
limit=20

echo "Envoi d'une requete PING sur $1"
ping -c $count $1 > ping.tmp
echo "Traitement en cours ..."
echo "Calcul moyenne RTT..."
#enregistrement des donnees dans un fichier temporaire
cat ping.tmp | grep icmp | cut -d " " -f7 | sed s/time=/""/g >
    vector.tmp

#somme des RTT
octave -q << EOF
v1=dlmread("vector.tmp");
somme=sum(v1);
dlmwrite("sum.tmp",somme);
EOF
sum=$(cat sum.tmp)

#calcul de la moyenne
bc -q << EOF > avg.tmp
scale=3
$sum/$count.0<$limit
quit
EOF

avgbool=$(cat avg.tmp)
bc -q << EOF > avg.tmp
scale=3
$sum/$count.0
quit
EOF
#test de la valeur et affichage WAN/LAN
```

```
avg=$(cat avg.tmp)
echo "Moyenne RTT=$avg"
if [ $avgbool ];then
        echo "PC distant sur LAN"
else
        echo "PC distant sur WAN"
fi

#graphe RTT avec Gnuplot
cat ping.tmp | grep icmp | cut -d " " -f5,7 | sed s/[icmp_seq=,
   time=]/""/g > ping.plot
gnuplot << EOF
set autoscale
set ylabel "RTT(ms)"
set xlabel "ICMP_SEQ"
set output "ping.plot.eps"
set terminal postscript eps color
plot './ping.plot' using 1:2 title 'Statistique RTT' with line
EOF
#rm -f vector.tmp avg.tmp sum.tmp ping.tmp ping.plot
gv ping.plot.eps
#rm -f ping.plot.eps
```

3.4.2 Programmes Python

La deuxième simulation mesure le RTT en établissant une connexion au moyen de sockets UDP sur une machine client et une machine serveur. Le client envoie un Byte de données renvoyé immédiatement par le serveur. Le RTT est calculé au moyen d'un timer.

Programme côté client

```
#!/usr/bin/python2.4
from socket import *
import sys
import timeit
import math

host=sys.argv[1]            #adresse IP du serveur passe au
   parametre au script
port=12345                  #port de destination
```

```
threshold=sys.argv[2]    #seuil pour acceptation du temps passe
    en parametre

#creation sockets UDP
UDPsocket_send = socket(AF_INET,SOCK_DGRAM)
UDPsocket_rec = socket(AF_INET,SOCK_DGRAM)
UDPsocket_rec.bind(('',12345))

#fonction qui envoie un Byte
def f_envoi():
        UDPsocket_send.sendto("b",(host,port))
        while 1:
                data=UDPsocket_rec.recv(1)
                if(data):
                        break
t=timeit.Timer('f_envoi()','from __main__ import f_envoi')
time=(t.timeit(1))*1000
print "RTT= "+str(time)+" ms" #calcul du RTT
if time<threshold:            #test LAN ou WAN
        print "Machine sur LAN"
else:
        print "Machine sur WAN"
```

Programme côté serveur

```
#!/usr/bin/python2.4
from socket import *
import sys

port=12345
UDPsocket_send = socket(AF_INET,SOCK_DGRAM)
UDPsocket_rec = socket(AF_INET,SOCK_DGRAM)
UDPsocket_rec.bind(('',12345))

#se met en attente sur un port et renvoie des qu'il recoit
    quelque chose
#sur le port 12345
while 1:
        data=UDPsocket_rec.recvfrom(1)
        host = data[1][0]
        UDPsocket_send.sendto(data[0],(host,port))
```

3.4.3 Analyse et comparaison

Voici le résultat obtenu avec le script shell à l'adresse `http://www.google.ch` avec un seuil RTT fixé à 10 ms. La figure 3.12 représente le graphe des RTT.

Script bash

```
leo@perlon:~/memoire\$ ./script.sh www.google.ch
Envoi d'une requete PING sur www.google.ch
Traitement en cours ...
Calcul moyenne RTT...
Moyenne RTT=20.140
PC distant sur WAN
```

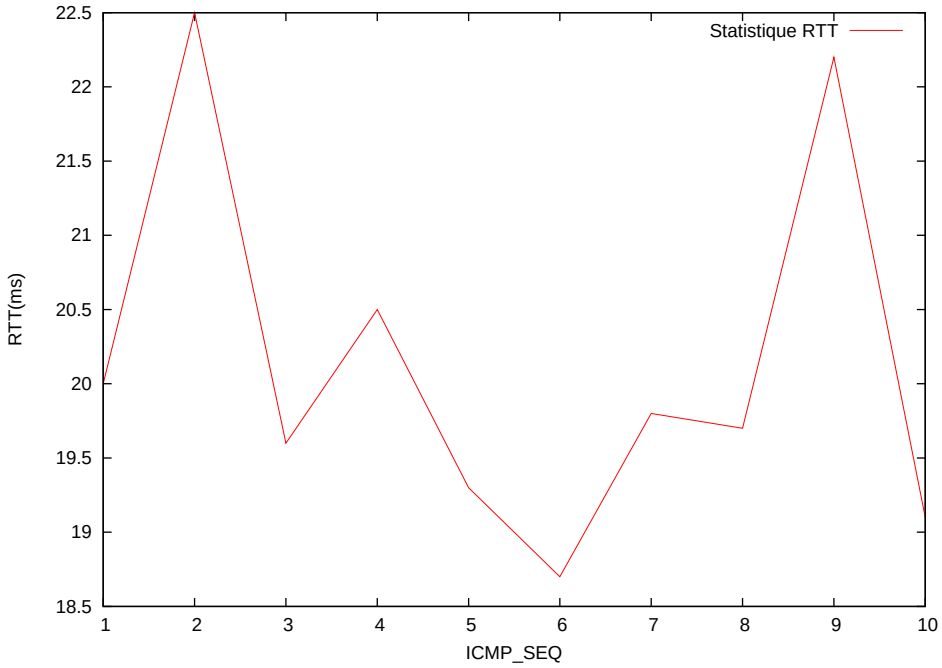

Fig. 3.12 – Visualisation des RTT vers Google

Cette simulation s'éloigne quelque peu de l'échange de bits rapide des procédures vues précédemment. En effet un échange de bits n'est pas possible si on considère les encapsulations successives des données introduites à chaque couche du modèle OSI. Un message ICMP est encapsulé dans une trame Ethernet ou 802.3 avant d'être transmise physiquement. Cette encapsulation entraîne l'adjonction de *headers*, donc de données supplémentaires. Ce processus introduit du temps de traitement qui dans certains cas peut être supérieur au temps de transmission proprement dit. C'est l'inconvénient de cette simulation par rapport à une mesure directe au niveau physique.

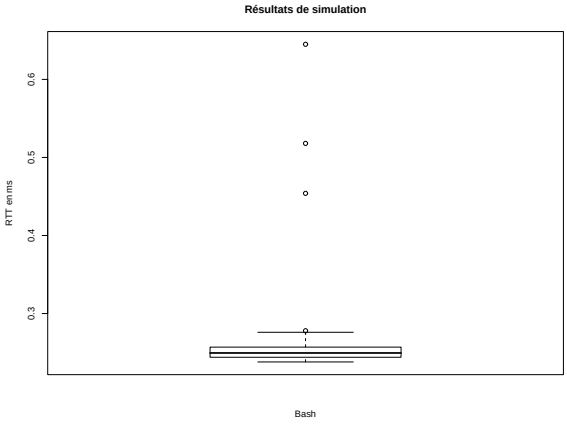

Fig. 3.13 – RTT avec `ping`

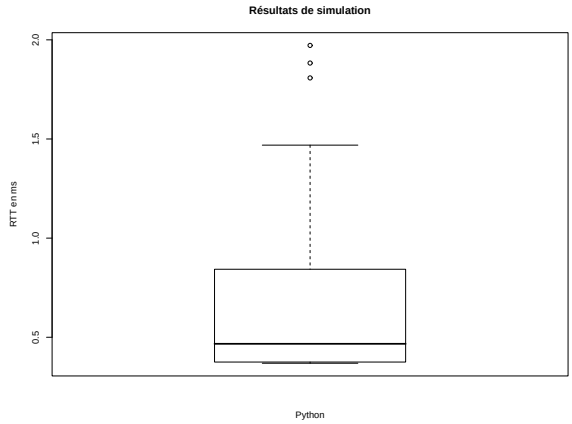

Fig. 3.14 – RTT avec UDP

Dans le cas du programme python ce sont des datagrammes UDP qui sont envoyés. L'implémentation est donc effectuée à la couche transport et par conséquent même si un seul Byte est envoyé, les *headers* ajoutés aux niveaux 3 et 2 respectivement aux couches réseau et liaison augmenteront sensiblement la taille des données qui transitent au niveau physique. Cela entraîne une influence sur le RTT mesuré.

Pour comparer nos deux méthodes de mesure du RTT, appliquons les à une même machine du même *subnet* d'adresse IP `10.192.51.80` afin de cerner les différences. Nous effectuons trente mesures, l'équivalent d'un challenge à 30 bits dans les protocoles de distance bounding. Le programme python `recv.py` doit être lancé côté serveur (machine distante). Le programme `envoi.py` prend deux paramètres : l'adresse du serveur et le seuil RTT en millisecondes pour le test.

Programme python

```
leo@perlon:~/memoire\$ ./envoi.py 10.192.51.80 20.0
RTT= 0.392913818359 ms
Machine sur LAN
```

Les deux figures 3.13 et 3.14 sont appelées *boîtes à moustaches*. Elles ont été obtenues avec le logiciel de statistiques R et ont le grand avantage de fournir une vue d'ensemble ainsi que des informations intéressantes sur les données. Le rectangle s'étend du premier au troisième quartile et il est coupé par la médiane. La longueur des « moustaches » vaut 1.5 fois l'écart interquartile. Les données dites atypiques sont illustrées par les petits cercles.

Les calculs de moyenne et de variance donnent $\bar{x} = 0.279$, $\sigma^2 = 0.008$ pour la mesure avec `ping` et $\bar{x} = 0.703$, $\sigma^2 = 0.241$ pour celle avec les paquets UDP. Nous constatons immédiatement que la mesure avec la requête `ping` est inférieure à celle avec le programme python. De plus les mesures sont moins dispersées. La différence peut avoir plusieurs causes. Premièrement le protocole ICMP se situe une couche en dessous d'UDP qui se

trouve à la couche transport, le temps de traitement s'en trouve donc diminué. De plus il se peut qu'un paquet UDP soit perdu et que le timer du programme python ne s'arrête qu'avec la réception du suivant, ce qui entraîne de nouveau des délais. Pour une simulation de ce type, la méthode de calcul du RTT via ICMP est donc à préconiser.

Chapitre 4

Conclusions et perspectives

« Chronologiquement, aucune connaissance ne précède en nous l'expérience et c'est avec elle que toutes commencent. »

E. Kant (1724-1804)

Cette étude nous a permis d'aborder le concept de preuve de proximité dans un processus d'authentification. Dans les réseaux conventionnels, l'authentification est basée sur une connaissance (mot de passe), un objet possédé (e.g. une smart-card) ou une donnée intrinsèque au sujet dans le cas de la biométrie. La preuve de proximité – condition nouvelle due à la multiplication des entités dans l'informatique diffuse – s'avère indispensable pour contrer des attaques relativement simples à mettre en oeuvre et potentiellement dangereuses. Les protocoles abordés permettent une flexibilité vis-à-vis de ces attaques et offrent une bonne alternative aux méthodes plus radicales d'isolement du système qui vont à l'encontre de la philosophie et de la finalité de la technologie.

Des études plus approfondies peuvent être envisagées, nous en proposons quelques idées dans ce chapitre.

4.1 Points à approfondir

4.1.1 Attaque relai

Le manque de connaissances en électronique, le manque de temps et la complexité du circuit à réaliser ne nous ont pas permis de réaliser pratiquement une attaque relai. La

véritable évaluation du danger aurait été possible sur un système grand public commercialisé comme celui dont nous disposons. Un aspect à étudier avec attention concerne le *time out* du lecteur, le délai au delà duquel le lecteur n'attend plus la réponse et refuse l'authentification. Selon la durée de ce délai, des autres médias de transmission entre fake tag et fake lecteur pourraient être imaginés. L'attaque relai gagnerait en discrétion et donc en dangerosité si par exemple les données pouvaient transiter par du Wi-Fi.

4.1.2 Protocoles de distance bounding

L'implémentation hardware des protocoles afin de les tester se trouve être difficile avec les moyens dont nous disposons. Des travaux récents sur l'ultra wide band [13] ont permis la réalisations de prototypes de pulseurs. Une étude de faisabilité serait intéressante en vue d'une intégration sur des tags RFID. Une très large bande passante est la condition *sine qua non* à une réalisation plausible. C'est là que le bât blesse puisque les systèmes requis sont encore peu développés et encore au stade de la recherche. Pour l'instant le concept du calcul du temps de réponse du tag est un bon moyen de parade mais les lois de la physique le rendent peu viable en pratique.

La simulation software réalisée permet de saisir la problématique, mais reste relativement éloignée d'une démonstration fiable pour convaincre les acteurs du domaine du bien-fondé des protocoles.

Ces protocoles ouvrent néanmoins la voie à des améliorations de plusieurs sortes :

- Une évolution possible serait la garantie d'authentification mutuelle. Nous n'avons abordé que des cas de tags malveillants et donc implicitement considéré que les lecteurs étaient toujours honnêtes. Il se peut néanmoins que des lecteurs malveillants interviennent et que le besoin d'une authentification simultanée des deux parties s'impose.
- L'information de distance pourrait aussi être exploitée pour de la localisation. Si le protocole est effectué par plusieurs lecteurs, l'information sur la position du tag peut être affinée. L'intersection de trois cercles par exemple définirait la zone dans laquelle se situe le tag. Des nuances supplémentaires sont à prendre en compte. Le protocole est-il effectué trois fois indépendamment les unes des autres ou une fois par les trois lecteurs simultanément en mode *broadcast* ? Le deuxième cas est préférable pour garantir une synchronisation entre lecteurs et une détection efficace d'un éventuel attaquant qui introduirait le même délai pour les trois lecteurs.

4.2 La norme NFC

A l'heure où nous rédigeons ces lignes, un consortium initié par Sony, Nokia et Philips pour la promotion de la communication en champ proche – *near field communication* – fait de plus en plus parler de lui. Les grandes entreprises de matériel de télécommunications semblent vouloir intégrer cette technologie dans leurs produits que tout le monde est en passe de posséder. Ainsi, il sera possible de profiter de la technologie avec son PDA ou son portable GSM. Le *NFC Forum*[1] promeut ce déploiement pour l'obtention d'information diverses en tout lieu, le paiement de biens et de services par porte-monnaie virtuel ou l'accès à des transports publics. Si le concept connaît l'essor attendu, il sera indispensable d'assurer un niveau de sécurité suffisant et les protocoles vus dans ce travail revêtiront une importance capitale.

4.3 Impacts économiques

Faute de temps, l'impact économique n'a pas été abordé. Une prise de contact avec des industriels afin d'obtenir des informations sur la faisabilité et la mise en oeuvre dans une production de masse aurait pu être envisagée. Pour l'heure les contraintes de largeur de bande sont encore un peu difficiles à satisfaire et un déploiement à court terme semble compromis. Ceci dit, le concept est tout à fait viable et il est possible qu'il fasse un jour son apparition dans le monde RFID, avec lequel il faudra à l'avenir indéniablement cohabiter.

[1] `http://www.nfc-forum.org`

Annexe A

Journal de travail

Semaine 1, du 19 au 22 septembre 2006

- présentation à l'aula ;
- initialisation du projet ;
- lecture documents.

Semaine 2, du 25 au 29 septembre 2006

- installation et tests du set EM 4094 ;
- commande deuxième set EM 4094 ;
- mise en place de la forme générale du mémoire ;
- rédaction Chapitre 1 ;
- prise de contact avec Gildas Avoine.

Semaine 3, du 2 au 6 octobre 2006

- forum HES-SO Fribourg ;
- rédaction Chapitre 1.

Semaine 4, du 9 au 13 octobre 2006

- rédaction fin Chapitre 1 ;
- rédaction Chapitre 2 ;

Semaine 5, du 16 au 20 octobre 2006

- téléphone avec Gildas Avoine ;
- prise de contact avec Cédric Candolfi pour monter le dispositif nécessaire à l'attaque relai ;

– script bash simulant un protocole de distance bounding.

Semaine 6, du 23 au 27 octobre 2006

– programmes Python pour simulation du calcul du RTT avec des datagrammes UDP ;
– rédaction Chapitre 2.

Semaine 7, du 30 octobre au 3 novembre 2006

– rédaction Chapitre 2 ;
– contact avec Jérôme Vernez pour documentation UWB.

Semaine 8, du 6 au 10 novembre 2006

– contact Jeremy Briod pour montage hardware ;
– rédaction Chapitre 2 et début Chapitre 3.

Semaine 9, du 13 au 17 novembre 2006

– tests des programmes de simulation, établissement des statistiques

Semaine 10, du 20 au 24 novembre 2006

– téléphone avec Gildas Avoine pour questions ;
– rédaction Chapitre 3.

Semaine 11, du 27 novembre au 1er décembre 2006

– étude et comparaison des protocoles ;
– rédaction Chapitre 3.

Semaine 12, du 4 au 8 décembre 2006

– finalisation et mise en page ;
– relecture et corrections.

Annexe B

Cahier des charges

B.1 Résumé du problème

Les tags RFID commencent à être utilisés en masse. Dans les prochaines années on attend à ce que plusieurs milliards de tags soient en fonction, voire même quelques trillions. Ils sont surtout utilisés dans les chaînes de production (alimentation, textiles,...) et sont présents sur divers objets, y compris, éventuellement, dans nos corps. Dans ce projet il s'agira de faire une recherche sur les moyens disponibles pour préserver la confidentialité des données d'une personnes portant des objets munis de tags RFID et de faire des propositions raisonnables d'amélioration pour préserver sa sphère privée. Il faudra aussi faire mettre sur pied un répertoire d'attaques possibles avec démonstrations éventuelles. Les problèmes potentiels concernent des applications diverses : paiements dans les péages, passeports, librairies, implants humains,..

B.2 Travail à effectuer

L'identification par radiofréquence (RFID) est une technologie qui permet d'identifier à distance des objets sans contact physique ni visuel. Elle nécessite pour cela des transpondeurs à bas coût, appelés tags qui sont apposés sur les objets à identifier ; des lecteurs qui permettent d'interroger ces tags par radiofréquence ; et un système de traitement de données, qui peut être centralisé ou distribué dans chaque lecteur. On l'utilise pour la traçabilité dans les chaînes logistiques, pour les abonnements aux transports publics, pour les clefs de démarrage des voitures, pour les badges de contrôle d'accès, pour les passeports électroniques, etc.

La RFID fait face à de nombreux problèmes de sécurité, difficiles à résoudre en rai-

son des faibles ressources des tags. Elle doit se prémunir des dénis de service, des fuites d'information, des problèmes de vie privée et de l'usurpation d'identité. L'une des technique permettant d'usurper l'identité d'une personne (par exemple dans le cadre d'un contrôle d'accès physique) est de pratiquer une attaque relais, c'est-à-dire de faire croire à un lecteur qu'un tag légitime est à sa proximité, alors qu'il est en fait en dehors de son champs opérationnel. Pour cela, le pirate, avec l'aide d'un complice, joue le rôle d'une « rallonge »entre le lecteur et le tag : il suffit que le pirate soit proche du lecteur et son complice proche du tag au moment même de l'attaque. L'attaque est totalement transparente pour la victime car le tag répond à toute sollicitation sans demander l'accord de son porteur. Les conséquences d'une telle attaque peuvent être très importantes, en particulier dans le cadre du contrôle d'accès ou du paiement électronique. Les techniques pour éviter ce type d'attaques reposent sur la mesure du temps de réponse du tag : un temps de réponse trop important implique le rejet du tag. Ces techniques sont appelées *distance bounding protocols*.

Le but de ce projet est d'étudier la faisabilité de l'utilisation en RFID de *distance bounding protocols*. Cette étude, qui portera aussi bien sur les aspects théoriques que sur les aspects techniques et économiques de telles solutions, a pour objectif ultime de démontrer que les *distance bounding protocols* ont, ou n'ont pas, d'intérêts pour les industriels. Selon le profil de l'étudiant, l'avancée dans le projet et les collaborations extérieures, les aspects suivants pourront être développés :

- Etude de l'impact et de la pertinence des attaques par relais. Le but de cette partie est de convaincre que les attaques par relais doivent être considérées sérieusement. Pour cela, l'étudiant proposera entre autres des exemples d'applications où les attaques par relais sont possibles et en analysera les conséquences. Dans quels types d'applications ces attaques ne sont pas pertinentes ? Comparaison entre RFID et autres technologies. Selon le matériel à disposition de l'étudiant et de ses connaissances, une attaque sur de vrais tags pourrait être considérée.
- Etude des solutions envisageables. L'étudiant proposera entre autres une classification des différentes approches qui permettent d'éviter les attaques par relais. Mis à part les *distance bounding protocols*, ces approches reposent sur l'intervention du porteur du tag lorsque celui-ci est interrogé (par exemple les tags proposés par IBM qui nécessitent d'être pressés pour répondre). Quelle approche est appropriée à quelle application ? Quelles sont les techniques proposées aujourd'hui ? Quelles sont les particularités de la RFID vis-à-vis des solutions envisageables.
- Analyse technique et scientifique des *distance bounding protocols* existants. L'étudiant devra analyser les protocoles existants en considérant aussi bien les aspects liés à la sécurité que les aspects liés à l'efficacité. Il proposera une sélection d'algorithmes cryptographiques appropriés (choix d'une fonction de hachage, d'un générateur pseudo-aléatoire, etc.) et devra estimer les ressources nécessaires au niveau du tag. Cette analyse constituera une partie importante du projet et pourra éventuellement déboucher sur une partie orientée "recherche" où l'étudiant aura pour objectif d'améliorer les solutions proposées et d'évaluer leur sécurité.

- Analyse de la faisabilité des *distance bounding protocols* du point de vue électronique. L'étudiant devra apporter la preuve que le concept consistant à calculer le temps de réponse du tag est viable ou ne l'est pas. Il devra également montrer comment peut se faire l'intégration d'un tel protocole dans le modèle de communication.
- Communication des résultats techniques. Si l'utilisation de *distance bounding protocols* sur des tags RFID est techniquement envisageable, alors l'étudiant pourra réaliser une simulation permettant d'en convaincre les autres acteurs de la RFID. Le choix de la plate-forme pour réaliser cette simulation sera déterminé en fonction des connaissances de l'étudiant et du matériel à sa disposition.
- Etude de l'impact économique des *distance bounding protocols*. Cette phase s'effectuera en collaboration avec les industriels afin d'évaluer l'intérêt de la mise sur le marché de système utilisant ces protocoles.

Bibliographie

[1] Manfred Aigner and Martin Feldhofer. Secure symmetric authentication for RFID tags. In *Telecommunication and Mobile Computing – TCMC 2005*, Graz, Austria, March 2005.

[2] Gildas Avoine. *Cryptography in Radio Frequency Identification and Fair Exchange Protocols*. PhD thesis, EPFL, Lausanne, Switzerland, December 2005. 17, 22

[3] Gildas Avoine and Philippe Oechslin. RFID traceability : A multilayer problem. In Andrew Patrick and Moti Yung, editors, *Financial Cryptography – FC'05*, volume 3570 of *Lecture Notes in Computer Science*, pages 125–140, Roseau, The Commonwealth Of Dominica, February–March 2005. IFCA, Springer-Verlag. 15

[4] Lejla Batina, Jorge Guajardo, Tim Kerins, Nele Mentens, Pim Tuyls, and Ingrid Verbauwhede. An elliptic curve processor suitable for RFID-tags. Cryptology ePrint Archive, Report 2006/227, 2006. 18

[5] Lejla Batina, Jorge Guajardo, Tim Kerins, Nele Mentens, Pim Tuyls, and Ingrid Verbauwhede. Public key cryptography for RFID-tags. Printed handout of Workshop on RFID Security – RFIDSec 06, July 2006. 18

[6] Stefan Brands and David Chaum. Distance-bounding protocols (extended abstract). In *Theory and Application of Cryptographic Techniques*, pages 344–359, 1993. 36, 38

[7] Laurent Bussard. *Trust establishment protocols for communicating devices*. PhD thesis, Thesis, Oct 2004. 23, 40, 41

[8] S. Capkun, L. Buttyan, and J. Hubaux. Sector : Secure tracking of node encounters in multi-hop wireless networks, 2003. 42

[9] Dario Carluccio, Timo Kasper, and Christof Paar. Implementation details of a multi purpose ISO 14443 RFID-tool. Printed handout of Workshop on RFID Security – RFIDSec 06, July 2006. 29

[10] Dario Carluccio, Kerstin Lemke, and Christof Paar. Electromagnetic side channel analysis of a contactless smart card : first results. Printed handout of Workshop on RFID Security – RFIDSec 06, July 2006.

[11] Claude Castelluccia and Gildas Avoine. Noisy tags : A pretty good key exchange protocol for RFID tags. In Josep Domingo-Ferrer, Joachim Posegga, and Daniel Schreckling, editors, *International Conference on Smart Card Research and Advanced Applications – CARDIS*, volume 3928 of *Lecture Notes in Computer Science*, pages 289–299, Tarragona, Spain, April 2006. IFIP, Springer-Verlag. 18

[12] Christy Chatmon, Tri van Le, and Mike Burmester. Secure anonymous RFID authentication protocols. Technical Report TR-060112, Florida State University, Department of Computer Science, Tallahassee, Florida, USA, 2006. 18

[13] James Colli-Vignarelli. Emetteur et récepteur ultra wide band. Technical report, Laboratoire pour les communications informatiques et leurs applications, EPFL, 2006. 58

[14] Sandra Dominikus, Elisabeth Oswald, and Martin Feldhofer. Symmetric authentication for RFID systems in practice. Handout of the Ecrypt Workshop on RFID and Lightweight Crypto, July 2005. 47

[15] Martin Feldhofer. An authentication protocol in a security layer for RFID smart tags. In *The 12th IEEE Mediterranean Electrotechnical Conference – MELECON 2004*, volume 2, pages 759–762, Dubrovnik, Croatia, May 2004. IEEE. 18

[16] Martin Feldhofer, Sandra Dominikus, and Johannes Wolkerstorfer. Strong authentication for RFID systems using the AES algorithm. In Marc Joye and Jean-Jacques Quisquater, editors, *Workshop on Cryptographic Hardware and Embedded Systems – CHES 2004*, volume 3156 of *Lecture Notes in Computer Science*, pages 357–370, Boston, Massachusetts, USA, August 2004. IACR, Springer-Verlag. 18

[17] Martin Feldhofer and Christian Rechberger. A case against currently used hash functions in RFID protocols. Graz, Austria. 47

[18] Klaus Finkenzeller. *RFID handbook : fundamentals and applications in contactless smart cards and identification*. WILEY, second edition, 2003. 1

[19] Kenneth Fishkin, Sumit Roy, and Bing Jiang. Some methods for privacy in RFID communication. In Claude Castelluccia, Hannes Hartenstein, Christof Paar, and Dirk Westhoff, editors, *European Workshop on Security in Ad-hoc and Sensor Networks – ESAS 2004*, volume 3313 of *Lecture Notes in Computer Science*, pages 42–53, Heidelberg, Germany, August 2005. Springer-Verlag.

[20] Xingxin (Grace) Gao, Zhe (Alex) Xiang, Hao Wang, Jun Shen, Jian Huang, and Song Song. An approach to security and privacy of RFID system for supply chain. In *Conference on E-Commerce Technology for Dynamic E-Business – CEC-East'04*, pages 164–168, Beijing, China, September 2005. IEEE, IEEE Computer Society.

[21] Simson Garfinkel, Ari Juels, and Ravi Pappu. RFID privacy : An overview of problems and proposed solutions. *IEEE Security and Privacy*, 3(3) :34–43, May-June 2005.

[22] Gerhard Hancke. A practical relay attack on ISO 14443 proximity cards. Manuscript, February 2005. 29

[23] Gerhard Hancke. Practical attacks on proximity identification systems (short paper). In *IEEE Symposium on Security and Privacy*, Oakland, California, USA, May 2006. IEEE, IEEE Computer Society Press. 29

[24] Gerhard Hancke and Markus Kuhn. An RFID distance bounding protocol. In *Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm 2005*, Athens, Greece, September 2005. IEEE. 36, 39

[25] Jaap-Henk Hoepman, Engelbert Hubbers, Bart Jacobs, Martijn Oostdijk, and Ronny Wichers Schreur. Crossing borders : Security and privacy issues of the european e-passport. Manuscript in submission, 2006.

[26] Yang Jeongkyu. Security and privacy on authentication protocol for low-cost radio frequency identification. Master thesis, Information and Communications University, Daejeon, Korea, December 2004. 18

[27] Ari Juels. Minimalist cryptography for low-cost RFID tags. In Carlo Blundo and Stelvio Cimato, editors, *International Conference on Security in Communication Networks – SCN 2004*, volume 3352 of *Lecture Notes in Computer Science*, pages 149–164, Amalfi, Italia, September 2004. Springer-Verlag. 18

[28] Ari Juels. RFID security and privacy : A research survey. Manuscript, September 2005.

[29] Ari Juels, Ronald Rivest, and Michael Szydlo. The blocker tag : Selective blocking of RFID tags for consumer privacy. In Vijay Atluri, editor, *Conference on Computer and Communications Security – ACM CCS*, pages 103–111, Washington, DC, USA, October 2003. ACM, ACM Press. 28

[30] Ari Juels and Stephen Weis. Defining strong privacy for RFID. Cryptology ePrint Archive, Report 2006/137, 2006.

[31] Chris Karlof and David Wagner. Secure routing in wireless sensor networks : Attacks and countermeasures. In *First IEEE International Workshop on Sensor Network Protocols and Applications*, pages 113–127, May 2003. 29

[32] Ziv Kfir and Avishai Wool. Picking virtual pockets using relay attacks on contactless smartcard systems. In *Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm 2005*, Athens, Greece, September 2005. IEEE. 25

[33] Ilan Kirschenbaum and Avishai Wool. How to build a low-cost, extended-range RFID skimmer. Cryptology ePrint Archive, Report 2006/054, 2006.

[34] Heiko Knospe and Hartmut Pohl. RFID security. *Information Security Technical Report*, 9(4) :39–50, November–December 2004.

[35] Mikko Lehtonen, Thorsten Staake, Florian Michahelles, and Elgar Fleisch. From identification to authentication - a review of RFID product authentication techniques. Printed handout of Workshop on RFID Security – RFIDSec 06, July 2006. 18

[36] Albert Levi, Erhan Çetintas, Murat Aydos, Çetin Kaya Koç, and M. Ufuk Çaglayan. Relay attacks on bluetooth authentication and solutions. In *ISCIS*, pages 278–288, 2004. 29

[37] Tobias Lohmann, Mattias Schneider, and Christoph Ruland. Analysis of power constraints for cryptographic algorithms in mid-cost RFID tags. In Josep Domingo-Ferrer, Joachim Posegga, and Daniel Schreckling, editors, *International Conference on Smart Card Research and Advanced Applications – CARDIS*, Lecture Notes in Computer Science, Tarragona, Spain, April 2006. IFIP, Springer-Verlag.

[38] David Molnar. Security and privacy in two RFID deployments, with new methods for private authentication and rfid pseudonyms. Master thesis, University of California Berkeley, Berkeley, California, USA, 2006. 18

[39] David Molnar and David Wagner. Privacy and security in library RFID : Issues, practices, and architectures. In Birgit Pfitzmann and Peng Liu, editors, *Conference on*

Computer and Communications Security – ACM CCS, pages 210–219, Washington, DC, USA, October 2004. ACM, ACM Press.

[40] Jorge Munilla, Andres Ortiz, and Alberto Peinado. Distance bounding protocols with void-challenges for RFID. Printed handout of Workshop on RFID Security – RFIDSec 06, July 2006. 23, 44

[41] Sylvain Pasini. Secure communications over insecure channels using an authenticated channel. Master's thesis, Swiss Federal Institute of Technology (EPFL), 2005. `http://lasecwww.epfl.ch/`. 38

[42] Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan Estevez-Tapiador, and Arturo Ribagorda. LMAP : A real lightweight mutual authentication protocol for low-cost RFID tags. Printed handout of Workshop on RFID Security – RFIDSec 06, July 2006. 18

[43] Selwyn Piramuthu. HB and related lightweight authentication protocols for secure RFID tag/reader authentication. In *Collaborative Electronic Commerce Technology and Research – CollECTeR 2006*, Basel, Switzerland, June 2006.

[44] Damith Ranasinghe, Daniel Engels, and Peter Cole. Low-cost RFID systems : Confronting security and privacy. In *Auto-ID Labs Research Workshop*, Zurich, Switzerland, September 2004.

[45] Damith Ranasinghe, Daniel Engels, and Peter Cole. Security and privacy : Modest proposals for low-cost RFID systems. In *Auto-ID Labs Research Workshop*, Zurich, Switzerland, September 2004.

[46] Jason Reid, Juan Gonzalez Neito, Tee Tang, and Bouchra Senadji. Detecting relay attacks with timing based protocols. QUT ePrint, Report 3264, 2006. 40

[47] Melanie Rieback, Bruno Crispo, and Andrew Tanenbaum. RFID guardian : A battery-powered mobile device for RFID privacy management. In Colin Boyd and Juan Manuel González Nieto, editors, *Australasian Conference on Information Security and Privacy – ACISP'05*, volume 3574 of *Lecture Notes in Computer Science*, pages 184–194, Brisbane, Australia, July 2005. Springer-Verlag.

[48] Melanie R. Rieback, Bruno Crispo, and Andrew S. Tanenbaum. Is your cat infected with a computer virus ? In *PERCOM '06 : Proceedings of the Fourth Annual IEEE International Conference on Pervasive Computing and Communications (PERCOM'06)*, pages 169–179, Washington, DC, USA, 2006. IEEE Computer Society. 22

[49] Sanjay Sarma, Stephen Weis, and Daniel Engels. RFID systems and security and privacy implications. In Burton Kaliski, Çetin Kaya ço, and Christof Paar, editors, *Cryptographic Hardware and Embedded Systems – CHES 2002*, volume 2523 of *Lecture Notes in Computer Science*, pages 454–469, Redwood Shores, CA, USA, August 2002. Springer-Verlag.

[50] Tom Ahlkvist Scharfeld. An analysis of the fundamental constraints on low cost passive radio-frequency identification system design. Master thesis, Massachusetts Institute of Technology (MIT), Massachusetts, USA, August 2001. 1

[51] Youngjoon Seo and Kwangjo Kim. Scalable and untraceable authentication protocol for RFID. In *International Workshop on Security in Ubiquitous Computing Systems – Secubiq 2006*, Lecture Notes in Computer Science, Seoul, Korea, August 2006. Springer-Verlag. 18

[52] Peter Sorrels. Optimizing read range in RFID systems. *EDNmag*, pages 173–184, December 2005. 26

[53] István Vajda and Levente Buttyán. Lightweight authentication protocols for low-cost RFID tags. In *Second Workshop on Security in Ubiquitous Computing – Ubicomp 2003*, Seattle, WA, USA, October 2003. 18

[54] Stephen Weis. Security and privacy in radio-frequency identification devices. Master thesis, Massachusetts Institute of Technology (MIT), Massachusetts, USA, May 2003. 28

[55] Pengyuan Yu, Patrick Schaumont, and Dong Ha. Securing RFID with ultra-wideband modulation. Printed handout of Workshop on RFID Security – RFIDSec 06, July 2006.

Index

U