Mise en œuvre de la technologie RFID

Christian Perrot
Equipe MULTICOM
LIG – Laboratoire d'Informatique de Grenoble
Christian.Perrot@imag.fr

Résumé

Depuis quelques années l'équipe Multicom du LIG s'intéresse aux technologies RFID sur sa plateforme dédiée aux Usages des nouvelles technologies, en tant qu'outil de suivi de l'activité des sujets d'expérience, et en tant que dispositif d'interaction innovant.

Cet article rappelle le principe des RFID et présente un premier retour d'expériences de terrain qui se sont déroulées pendant plusieurs mois dans le cadre de notre activité culture.

Il sera détaillé les comportements des usagers en situation d'interaction au moyen des RFID et les écueils à éviter lors d'un déploiement.

Il sera abordé également l'indispensable dimension de respect de la vie privée et dans la mesure du possible, les aspects de normes sanitaires.

Mots clefs

RFID, Usages, Technologie

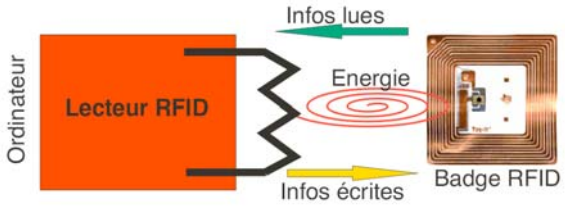
1 Rappels technologiques

La technologie mise en œuvre pour lire des badges Radio Fréquences, appelés badges RFID (Radio Fréquence IDentifier) ou encore « RFID tag » ou « étiquettes RFID », comporte deux parties :

- Un "Badge RFID" constitué d'une antenne en spirale connectée à une puce électronique
- Un "Lecteur RFID" pilotant une autre antenne. Le Lecteur RFID est connecté à un ordinateur.

1.1 Principe de lecture d'un badge RFID

Sur demande de l'ordinateur, le Lecteur RFID crée un champ magnétique au moyen de son antenne. Ce champ transfert de l'énergie à l'antenne incorporée dans le Badge RFID, ce qui "réveille" la puce électronique.



Cette dernière peut alors transmettre son identité et effectuer des opérations comme enregistrer des informations venant de l'ordinateur ou restituer des données inscrites dans sa mémoire. Lorsque le champ magnétique cesse, la "puce se rendort" et les informations restent stockées dans sa mémoire.

Les badges RFID ont en grande majorité des numéros d'identification (SID) uniques choisis dans une classe attribuée à chaque fabriquant et inscrits sur 32 bits en mémoire morte dans la puce. . Toutefois, il est possible, sur certains badges, de modifier le SID de manière à pouvoir remplacer des badges existants ayant disparu mais néanmoins indispensables à une chaîne de production par exemple.

1.2 L'anticollisions

On appelle « collision » la présence simultanée de plusieurs badges dans le champ de la même antenne créant ainsi des conflits dans le sens du dialogue badge vers lecteur. Divers algorithmes sont utilisés pour dialoguer en mode anticollision avec les badges présents :

- Par une gestion synchrone des collisions dans laquelle le lecteur sait décoder la superposition des informations spécifiques anticollision envoyées par les badges (le temps de réponse est fixe)
- Par une gestion probabiliste dans laquelle des tranches de temps successives sont alloués aux badges pour communiquer avec le lecteur (le temps de réponse dépend du nombre de badges)

Tous les lecteurs ne sont pas capables de gérer les collisions, en particulier pour les modèles bas de gamme de petite taille. En présence de plusieurs badges, ce type de lecteurs ne peut voir qu'un seul badge à la fois, et pas toujours le même d'une fois sur l'autre. Les lecteurs les plus évolués sont capables de lire plus d'une centaine de badges en quelques secondes. Les lecteurs RFID utilisent maintenant des circuits intégrés de plus en plus performants et de moins en moins chers (ASICs de Texas Instrument ou de STMicroelectronics), ce qui leur permet de supporter un plus grand nombre de protocoles, dont l'anticollision.

1.3 Originalités de la technologie RFID

Par rapport à des dispositifs plus classiques, comme le code à barre ou à l'infrarouge, le Badge RFID présente l'avantage d'être **réinscriptible** et d'être **invisible** s'il est enfoui dans un objet.

L'interaction avec le lecteur est transparente contrairement à l'usage de la traditionnelle douchette codes à barres. Il fonctionne sans pile et sa durée de vie est quasi-illimitée. Les badges RFID ont diverses formes, depuis le plus petit inséré sous la peau d'un animal, jusqu'au plus grand format carte postale que l'on peut fixer sur des colis. Son épaisseur est rarement supérieure à un millimètre.

Les dispositifs électroniques « Lecteur RFID »ont des dimensions de quelques dizaines de centimètres pour les plus complexes à la taille d'une boite d'allumettes pour les plus petits, jusqu'à l'intégration à l'intérieur d'un téléphone portable pour les prochaines générations en cours de développement. L'interfaçage avec l'ordinateur hôte est effectué par une ligne série (RS232, RS422, USB) ou Ethernet, bus PCMCIA, bus SDcard. Aucune norme n'existe quant à la définition du dialogue entre le lecteur et son ordinateur hôte.

La distance d'interaction maximale va de 2 mètres à quelques millimètres, distance essentiellement dépendante de la dimension des antennes du Lecteur, de la taille du Badge RFID et de la puissance d'émission.

Technologie	Distance max	Débit max	Exemples d'applications
125 KHz	Quelques mètres	Quelques 10 Kbits/sec	Automobile, Animaux, Anti-intrusion
VHF – 13,56 Mhz	Moins de 2 mètres	Quelques 100 Kbits/sec	Logistique, Inventaire, Salons, Porte-monnaie, Cartes d'abonnement
UHF – 860 Mhz	Une ou deux dizaines de mètres	Quelques Mbits/sec	Logistique, commerce
UHF - 2,4 GHz, 5,8 GHz	Plusieurs dizaines de mètres	Quelques Mbits/sec	Peu utilisé en France

Note : Multicom n'a pas testé sur sa plateforme les technologies 125 KHz car elles commencent à dater à cause de leur faible débit, et les RFID à 2,4 Ghz ou 5,8 GHz qui sont peu répandus. Les badges actifs ont été exclus car ce sont plutôt des télécommandes radio à piles pour lesquels il existe une grande variété de protocoles et un marché de niche pour les tags.

Les antennes des badges 13,56 MHz sont refermées sur elles-mêmes car elles se comportent principalement comme la boucle secondaire d'un transformateur dont le primaire serait l'antenne du lecteur.

Les antennes des badges UHF (860 MHz) sont constituées de dipôles car elles fonctionnent principalement comme un récepteur. radio.

1.4 Standards et normes de lecture des badges

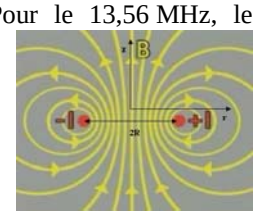
Les industriels ont cherché très tôt à assurer la compatibilité de leurs lecteurs avec les badges les plus répandus du marché. Pour faire un choix, la démarche conseillée est celle de l'architecte de système d'information privilégiant les normes ouvertes de l'ISO. Voici ci-dessous un tableau non exhaustif des standards propriétaires les plus courants et des normes ISO. Les lecteurs modernes supportent en général plusieurs protocoles, et les fabricants ont au catalogue des badges supportant divers protocoles, dont les ISO.

Fabriquant ou Organisme de normalisation	Standard ou norme	Remarques
ISO - SC17 Format carte de crédit	14 443	Faible distance "Proximity"
	15 693	Plus grande distance "Vicinity"
ISO - SC31 Autres formats	18 000 & 15 963	Couvre toutes les gammes de fréquences du 125 KHz au 5,8 GHz
EPC Global Initiative USA	GEN2	UHF approuvé par l'ISO -> cf ISO 18 000
NFC Forum Near Field Communications		Vise à unifier toutes les communications sans fil à courte distance
Texas	Tag-It & ISO	
Philips	Icode & ISO	
Tagsys	Tags souples et rigides	France

2 Modes d'interaction

2.1 Paramètres influençant la distance de détection

Du fait de la nature physique du couplage entre l'antenne du badge et celle du lecteur, la RFID est sensible à l'environnement. Pour le 13,56 MHz, le modèle de comportement est plutôt celui de la mutuelle inductance d'un transformateur dont le primaire serait l'antenne du lecteur et le secondaire l'antenne du badge. Pour l'UHF, le modèle de comportement est plutôt celui de la réception radio avec tout ce que cela implique de réflexions.



Les paramètres qui influencent la distance de détection sont les suivants :

- Puissance d'émission de l'antenne du lecteur
- Distance entre le badge et l'antenne, dont la sensibilité varie comme l'inverse du carré de la distance
- Taille de l'antenne du lecteur
- Taille de l'antenne du badge
- Accord de l'antenne avec son environnement
- Intelligence de traitement embarquée dans le lecteur permettant de reconnaître un signal dégradé
- Fréquence utilisée
- Orientation du badge par rapport à l'antenne

On dit souvent que l'ordre de grandeur de la distance de détection est égal à la diagonale de l'antenne, pour un badge de taille moyenne (taille carte de crédit par exemple)

Lorsque l'environnement est absorbant, il est préférable de prévoir un accord fin de l'antenne. Il faut éviter de déplacer des masses autour des lecteurs (réserves d'eau, masses métalliques)

Le meilleur couplage est obtenu en 13,56 MHz lorsque les lignes de champ de l'antenne traversent perpendiculairement le plan du badge, comme quelqu'un qui voudrait remplir son verre à une fontaine placerait le col du verre perpendiculairement au jet.

Le couplage en UHF dépend des réflexions dans l'environnement, et augmenter la puissance n'est pas toujours la meilleure solution. Un grand handicap de l'UHF est de se situer à 860 MHz dans la bande d'absorption de l'eau, donc du corps humain. Ainsi, il sera très difficile de détecter un badge si le porteur le serre dans sa main ou le place dans une poche contre son corps. Un conditionnement permettant d'écarter le badge du corps humain d'un centimètre suffit pour restituer un fonctionnement acceptable (surépaisseur, collier autour du coup n'incitant pas à le mettre dans une poche, badge caché dans un jouet ou dans un gadget,…)

2.2 Interaction et usages

En termes d'usages, on distinguera deux types d'interactions :

- L'interaction volontaire
- L'interaction transparente (involontaire)

L'interaction **volontaire** est le mode le plus classique consistant à « badger ». Dans un groupe, une personne qui « badge » est une personne qui s'identifie, désigne sans ambiguïté sa volonté d'interaction aux yeux de tous. Par contre, contrairement aux technologies classiques qui font du bruit (« crac », « slap »…etc…

et j'en passe) le lecteur RFID est silencieux. Ce sublime raffinement technologique qui ravit l'ingénieur, déroute l'utilisateur. On voit, par exemple, des usagers des transports en commun frotter nerveusement leur carte sur le lecteur comme si le mouvement facilitait l'interaction. Pour matérialiser l'interaction aux yeux de l'utilisateur, il faut donc, comme pour toute situation d'interaction en dialogue personne-système, prévoir un retour d'action (visuel, sonore, sensitif,…).

Il faut également que le badge RFID soit « porteur de sens » pour l'usager, c'est-à-dire qu'il identifie clairement quel avantage en tirer et comment s'en servir. A titre d'exemple, pour donner du sens à sa carte d'abonné RFID, la compagnie de transports publics grenoblois a dessiné dessus une image de puce à contact pour carte bancaire alors que l'analogie n'a rien à voir techniquement ;

L'interaction **transparente** est encore plus complexe en termes d'usages, si l'on choisit de la mettre en œuvre avec des antennes de grande dimension pour des distances de détection de l'ordre du mètre. Inutile de dire que hors contexte précis d'usage et sans l'accord implicite de l'usager, ce dispositif sera immédiatement perçu comme une surveillance policière et au même titre que l'antivol d'un magasin.

Si cette méthode est utilisée pour identifier des passages, voir faire des études de parcours de visiteurs comme le fait Multicom dans les musées avec l'accord explicite des visiteurs, cela ne pose pas trop de problèmes. Par contre, comment signifier à un visiteur particulier dans un groupe que le système s'adresse à lui, alors que cette personne n'a fait aucune action d'identification perceptible par ses voisins ? Comment traiter la réponse à une présence multiple ? C'est là qu'intervient la nécessité d'étudier soigneusement les scénarios d'usage et leur contexte de façon à rajouter des « implicites » dans la communication ou bien prévoir un dialogue « multimodal » enrichi avec d'autres capteurs.

2.3 Maîtriser le dialogue

Pour être satisfait en contexte commercial, un usager souhaite obtenir une réponse efficace à sa requête. Il ne poursuivra la négociation avec le système que si il est satisfait rapidement, sinon il prendra une autre voie pour obtenir ce qu'il recherche.

En contexte culturel, le visiteur a un comportement ambivalent. Il présente par moments un comportement ludique dans lequel tout l'étonne (ou le comble de ravissement)même si le dispositif n'a pas vraiment compris la subtilité de ses requêtes. Ces requêtes peuvent être volontaires avec un badge ou déclenchées par des informations d'ambiance et de contexte. Le scénographe et l'ingénieur ne sont donc pas trop contraints dans cette situation. Par contre, le visiteur peut changer brusquement d'attitude pour se mettre en situation de recherche d'information car son intérêt a été piqué au vif. Le système doit donc pouvoir s'adapter à ce nouveau comportement. Il est alors très difficile de conceptualiser de telles situations et c'est là que les études ergonomiques et les tests sur plateforme s'avèrent utiles.

3 Respect de la vie privée

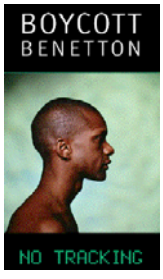
La technologie RFID introduit des risques potentiels d'atteinte à la vie privée que les responsables du déploiement ne peuvent pas ignorer. Ces aspects ont été évoqués longuement par Multicom lors de ses rencontres avec les professionnels des musées et lors du déploiement de RFID dans l'exposition "Ni vu ni connu" au Muséum du Rhône en partenariat avec la CNIL (Commission Nationale Informatique et Libertés).

De par la nature de leur activité scientifique, il serait difficile de prêter l'intention aux professionnels des musées de vouloir attenter à la vie privée de leurs visiteurs pour en tirer un quelconque profit commercial. Par contre, les titres d'accès aux expositions munis de badges RFID et les serveurs de contenu accessibles par l'Internet sont des cibles potentielles aux agressions extérieures pouvant présenter une atteinte à la vie privée des visiteurs. Par exemple, il est techniquement possible qu'une personne puisse se faire voler à son insu le contenu de sa carte d'abonnement à un musée à l'occasion de son passage à proximité du portique d'un centre commercial peu scrupuleux.

Aussi, il y aura lieu de prendre un certain nombre de précautions pour installer une technologie RFID pérenne dans une institution culturelle. Voici quelques suggestions applicables à d'autres contextes :

3.1 Précautions techniques

- Collecter des informations en les rendant autant que possible anonymes à la source
- Ne collecter que le minimum d'informations pertinentes et effacer les informations personnelles lorsque l'objectif du traitement est atteint
- Isoler les serveurs collectant des informations personnelles, en particulier en les rendant inaccessibles de l'Internet
- Si des informations personnelles sont inscrites dans un titre d'accès au musée, il y aura lieu de les crypter.
- Utiliser des dispositifs permettant au visiteur de désactiver les badges RFID momentanément pendant les expositions et surtout en dehors du musée (porte-badges métalliques).



- Utiliser des protocoles et des formats de données ouverts (dont les spécifications sont publiées par des organismes de normalisation comme l'ISO) de manière à maîtriser la manière dont l'information est traitée et stockée. En effet, en utilisant des protocoles appartenant à des sociétés privées qui ne les publient pas, dans un contexte de transactions en réseau on n'est plus en mesure de vérifier que les

informations ne sont pas détournées à d'autres fins.

- Délicate question des attaques relais avec des lecteurs tolérants sur le temps de réponse des badges (voir revue MISC, références ci-dessous)

3.2 Communiquer avec son public

- Informer le public sur les objectifs du projet en présentant les avantages qu'il peut en tirer en termes de personnalisation
- Mettre à disposition du public un dispositif (borne interactive par exemple) lui permettant de consulter les informations personnelles le concernant en lui donnant le droit de les corriger ou de les effacer. Cette démarche sous-entend que la présentation du contenu soit «compréhensible» et que cette démarche s'effectue dans la confidentialité par rapport aux autres visiteurs.
- Afficher clairement la situation physique exacte des lecteurs RFID dans les scénographies (afficher leur activité par des petits voyants sur les lecteurs, et installer des pictogrammes).

3.3 Disposition réglementaire et recommandations des organismes publics

- Faire une déclaration à la CNIL (Commission Nationale Informatique et Libertés)
- Interdire tout recoupement avec des informations de contexte extérieures, d'autres bases de données ou d'autres dispositifs de capture, comme les caméras ou les portillons (Demande de la CNIL).
- Le traitement nominatif doit être « légitime et proportionné aux nécessités de l'objectif final » (Demande de la CNIL).
- De manière plus générale, la multiplication de traces anonymes issues de dispositifs hétérogènes non corrélés présente de plus en plus un danger pour le respect de la vie privée. En effet, une multitude de traces anonymes regroupées créent un profil tellement pointu et contextualisé dans le temps et l'espace qu'il ne peut finalement que pointer sur une seule personne, qu'il sera alors possible de solliciter sans avoir besoin de la nommer.
- Offrir la possibilité de "brûler" la puce d'un badge RFID avec une confirmation visible sur la carte (Demande de la Communauté européenne)

4 Aspects sanitaires

Les inquiétudes du public rejoignent celles concernant les téléphones portables, le WiFi, les fours à Micro-ondes, les antennes relais GSM, …etc.

En 13,56 Mhz, il est difficile de trouver des informations pertinentes sur les puissances maximales admissibles. Il me semble que moins de 300 mW pour la détection de proximité suffisent et se limiter à 4 W pour le "long range" paraît intuitivement raisonnable. En particulier, il n'est pas nécessaire d'appliquer le champ sur les antennes que de manière continu, mais procéder par brèves impulsions, ce qui est largement suffisant pour détecter des piétons.

En UHF à 860 Mhz, nous sommes précisément, comme nous l'avons déjà vu, dans le spectre d'absorption maximal de l'eau du corps humain. C'est certainement pour cette raison qu'une récente recommandation évoque une limite de puissance UHF à 4 watts Toutefois en France, l'autorité de régulation des télécommunications (ARCEP), ayant libéré une bande de fréquence encore utilisée par les militaires limite la puissance à 2 W (500 mW dans un rayon de 20 Km autour des camps militaires).

Sujets testant les RFID sur la plateforme Multicom

5 Annexe

5.1 Applications possibles en contexte académique

Peut-on transposer cette technologie en milieu universitaire ou dans des labos de recherche ? Connaissant mal les services d'aide à la vie quotidienne des étudiants et des chercheurs, je ne me livrerai pas à l'exercice périlleux de concevoir des applications nouvelles. Je suggère juste les pistes de réflexion suivantes pour le monde académique basées sur la personnalisation du profil de la personne :

- Informations générales dans la langue
- Dates d'examens
- Carte de cantine sous forme de porte-monnaie électronique
- orientation personnalisée vers les salles de cours sur des « Pictobornes ». Ce sont des afficheurs simplifiés avec 4 directions sous forme de pictogrammes lumineux indiquant à l'étudiant la direction à suivre (tout droit devant, gauche, droite, demi-tour)
- Contrôles d'accès (c'est classique et existe sur le marché)
- Gestion d'un parc d'appareils en prêt (vidéo-projecteurs par exemple) avec anti-vol et traçabilité des retours en maintenance (c'est classique et existe sur le marché)
- Gestion des entrées dans les congrès scientifiques et de la trace de passage dans les stands avec poster (c'est classique et existe sur le marché)

6 Références

1. Communauté européenne - « Document de travail sur les questions de protection des données liées à la technologie RFID » - WP 105 - Article 29 - Groupe de travail Protection des données
2. CNIL - La radio-identification - "Communication de M. Philippe Lemoine relative à la Radio-Identification (Radio-Tags ou RFIds)"
3. http://www.cnil.fr/
4. ISO/IEC 18000 - RFID Air Interface Standards
5. http://www.hightechaid.com/standards/18000.htm
6. RFID Journal mai/juin 2005 Article « Privacy & profits »
7. Revue MISC Sept_Oct 2007 RFID « Sécurité ou surveillance »
8. Revue IEEE Spectrum mars 2007
9. Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions - L'identification par radiofréquence (RFID) en Europe: vers un cadre politique
10. http://ec.europa.eu/information_society/policy/rfid/doc/rfid_fr.pdf
11. EPC Global France
12. http://www.eannet-france.org/fille/b/b46.htm#10
13. ARCEP, mot clé « RFID » puissances émission et bandes UHF
14. http://www.arcep.fr
15. Lettre de l'OCIM n° 99 mai/juin 2005
16. « Apport de la technologie RFID en museographie » (Christian Perrot)
17. Lettre de l'OCIM
18. => prochain article sur l'analyse des traces des visiteurs dans les musées (Nadine Mandran, Multicom)
19. Les diapos RFID des JRES2007 sur le blog de l'auteur :
20. http://www-clips.imag.fr/multicom/User/christian.perrot/SPIP-v1-7/