Communication en champ proche

Table des matières

La communication en champ proche (CCP et en anglais near field communication, NFC) est une technologie de communication sans fil à courte portée et haute fréquence, permettant l'échange d'informations entre des périphériques jusqu'à une distance d'environ 10 cm[réf. nécessaire]. Cette technologie est une extension de la norme ISO/CEI 14443 standardisant les cartes de proximité utilisant la radio-identification (RFID), qui combinent l'interface d'une carte à puce et un lecteur au sein d'un seul périphérique.

1. La communication en champ proche

La communication en champ proche[1] est une technologie de communication sans-fil à courte portée et haute fréquence, permettant l'échange d'informations entre des périphériques jusqu'à une distance d'environ 10 cm. Cette technologie est une extension de la norme ISO/CEI 14443 standardisant les cartes de proximité utilisant l'identification par radiofréquence[2], qui combinent l'interface d'une carte à puce et un lecteur au sein d'un seul périphérique.

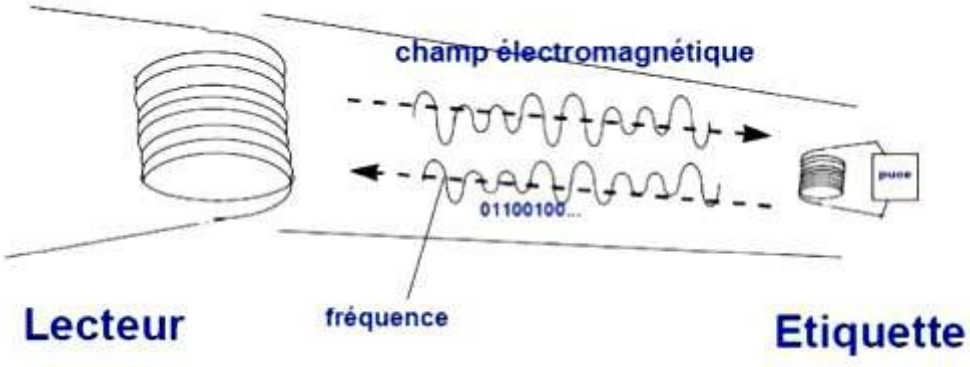
Un périphérique NFC est capable de communiquer avec le matériel ISO/CEI 14443 existant, avec un autre périphérique NFC ou avec certaines infrastructures sans-contact existantes comme les validateurs des transports en commun ou les terminaux de paiement chez les commerçants. La NFC équipe aujourd'hui des cartes utilisées dans les transports, dans le commerce ou pour l'accès à certains services publics et de plus en plus de terminaux mobiles.

En 2011, la NFC équipait en effet 50 millions de tablettes tactiles ou téléphones mobiles. Dotés d'un écran, d'un clavier et d'une connexion Internet, ces terminaux NFC ont un fort potentiel d'usages en favorisant les interactions entre les machines.

Au contraire d'autres techniques de radio-identification ou du bluetooth dont la portée est d'une dizaine de mètres, la technique NFC n'est utilisable que sur de très courtes distances (quelques centimètres). Elle suppose une démarche volontaire de l'utilisateur et normalement ne peut pas être utilisée à son insu. Mais cela n'exclut pas la collecte des données NFC par le système lui-même, qui reste capable d'historiser les usages de l'utilisateur avec cette technique de communication. En mai 2010, à l'occasion d'une visite des services sans contacts déployés à Nice, la CNIL[3] a du reste énoncé les grands principes pour que les services sans contact respectent les règles françaises en matière de protection des données personnelles.

2. Le fonctionnement de NFC/RFID

Une application d'identification automatique radio fréquence se compose donc d'un lecteur qui transmet un signal selon une fréquence déterminée vers une ou plusieurs étiquettes radio situées dans son champ de lecture. Celles-ci transmettent en retour un signal. Lorsque les étiquettes sont "réveillées" par le lecteur, un dialogue s'établit selon un protocole de communication prédéfini et les données sont échangées.



La technologie sans fil NFC est dite sans contact car elle nécessite une courte distance pour fonctionner de l'ordre d'une dizaine de centimètre maximum (aucune norme n'est définie à ce jour concernant les distances d'utilisation).

Les débits de communications vont de 106 à 848 kbits/s sur une gamme de fréquence de 13,56 MHz. La très courte portée suppose une démarche volontaire des utilisateurs et donc une résistance aux écoutes à leur insu.

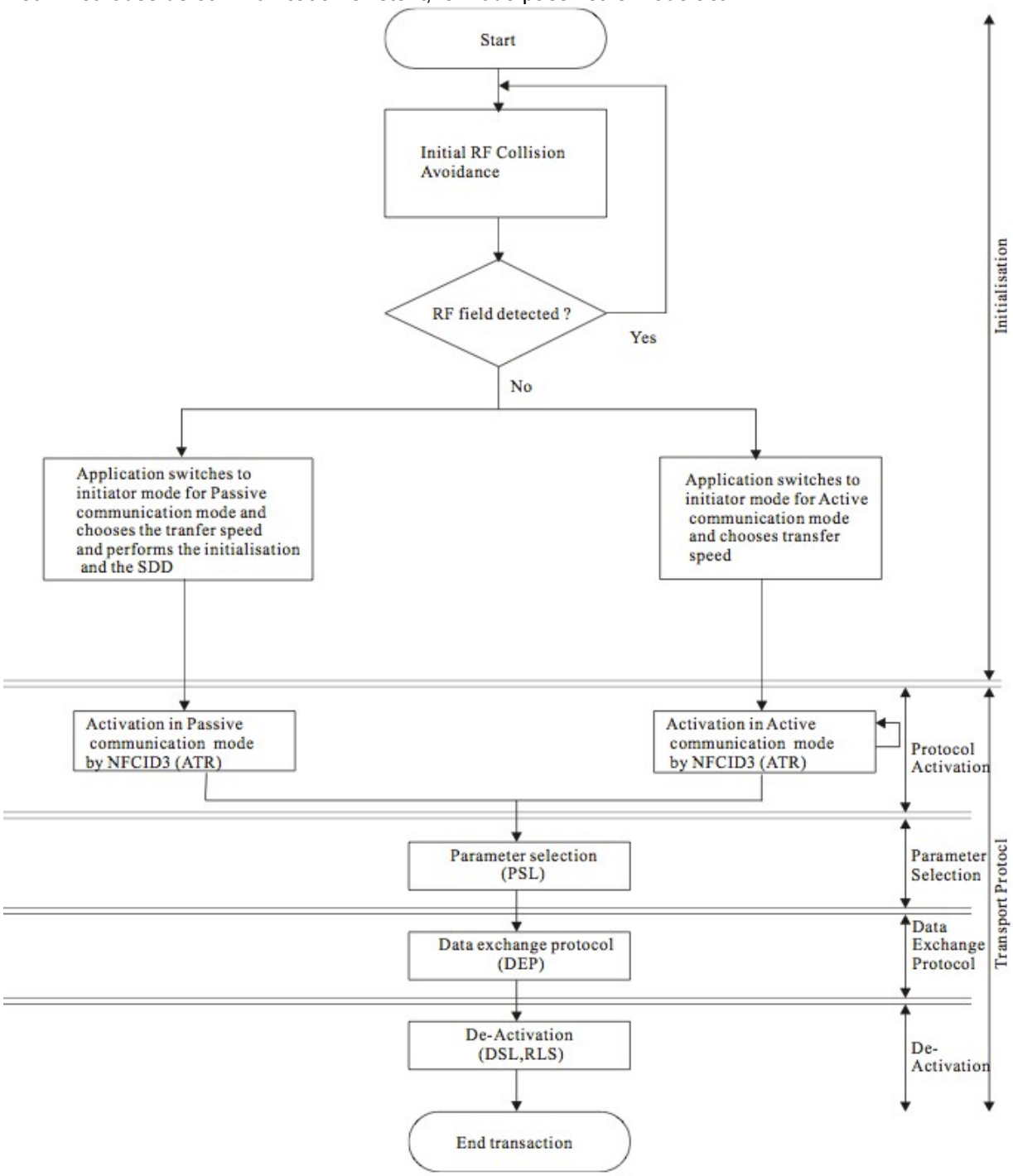
L'induction magnétique est le principe physique exploité par les solutions NFC/RFID:

1 Near Field Communication : NFC
2 Radio Frequency Identification : RFID
3 Commission Nationale Informatique et Liberté

- Un lecteur émet un faible courant électrique qui crée un champ magnétique entre les deux appareils. L'acteur démarrant la connexion est appelé initiateur.
- Un client reçoit le champ et le transforme en impulsion électrique qu'il peut traduire en bits de données. Cet acteur est appelé la cible.
- La manière dont la réponse est envoyée dépend du mode de fonctionnement

Par défaut, tous les appareils compatible NFC sont des clients potentiels et sont à l'écoute de champ magnétique. Avant d'initier une connexion, et dans le but de ne pas perturber d'autres communications NFC (collision avoidance), l'initiateur écoute systématiquement le médium avant de commencer l'émission. Le temps d'écoute est définit aléatoirement.

Deux méthodes de communication existent, le mode passif et le mode actif :



Remarques : Le tag RFID passif assisté par batterie (BAP : Battery Assisted Passive) comporte une alimentation embarquée (piles, batteries...). Cette dernière n'est pas utilisée pour alimenter un émetteur puisque le principe de communication reste la rétromodulation (comme pour le tag passif), mais pour alimenter le circuit électronique du tag ou tous autres circuits ou capteur connecté au circuit de base. Cette alimentation permet, en théorie, d'améliorer les performances. Ce tag est largement utilisé pour des applications nécessitant une capture d'information (température, choc, lumière, etc.) indépendante de la présence du lecteur.

L'étiquette électronique est un support d'informations qui combine le traitement d'un signal et le stockage des données. Elle est constituée d'un circuit électronique (ou « circuit intégré ») sur un circuit imprimé et couplé à une antenne.

Souvent appelées "transpondeur"[4] à cause de leurs fonctions de réponse et d'émission, l'étiquette radio ou tag répond à une demande transmise par le lecteur et concernant les données qu'elle contient. La mémoire d'un transpondeur comprend généralement une ROM[5], une RAM[6] ainsi qu'une mémoire programmable non volatile pour la conservation des données selon le type et le degré de complexité du produit. La mémoire ROM contient les données de sécurité ainsi que les instructions de l'OS[7] de l'étiquette en charge des fonctions de base telles que le délai de réponse, le contrôle du flux de données, et la gestion de l'énergie. La mémoire RAM est utilisée pour les stockages temporaires de données pendant les processus d'interrogation et de réponse. L'énergie nécessaire au fonctionnement du tag est fournie soit par une pile interne (ou batterie) pour les tags actifs ou semi-actifs, soit téléalimenté par le champ électro-magnétique émis par le lecteur (tags passifs).

2.1.Mode passif

La méthode de communication passif est utilisé par les tags NFC ou les systèmes devant économiser un maximum d'énergie. En effet, cette méthode permet à la cible de n'utiliser aucune source d'alimentation pour la transmission d'information.

La seule action qu'elle effectue est la modulation du champ pour transmettre des données prédéfinies, opération qui nécessite peu d'énergie comparé à l'émission d'un courant électrique. La cible utilise par ailleurs ce champ pour tirer l'énergie dont elle a besoin pour le moduler, la rendant totalement autonome d'un point de vue énergie, mais lui permettant de transmettre un nombre limité d'informations.

La technologie NFC utilise les communications passives pour deux modes de fonctionnement :

- Le mode émulation de carte permet à l'appareil de se comporter comme un tag RFID et de répondre ainsi aux lecteurs éventuels. NFC est ainsi compatible avec la norme RFID.
- Le mode lecteur permet de lire les tags RFID.

2.2. Mode actif

Avec cette méthode de communication les deux appareils génèrent des champs magnétiques. Il le font de manière alternative en désactivant la génération lors de l'attente. Les deux appareils nécessitent une source d'énergie qui leur est propre.

Le mode de fonctionnement associé à cette méthode de communication est appelé pair à pair (peer to peer). Deux appareils échangent de l'information qui n'est pas prédéfinies (carte de visite, photos, ...).

Jusqu'à récemment, le mode passif était le plus répandu, mais l'utilisation du mode actif avec les smartphones tend à se diffuser. Les fabricants de ces appareils font une promotion acharnée de cette nouvelle fonctionnalité dont l'objectif est d'étendre les possibilités de partage de données.

3. Les caractéristiques principales

Un système RFID permet donc d'écrire, de stocker et d'effacer de l'information sur la puce électronique du

4 TRANSmitter/resPONDER
5 Read Only Memory
6 Random Access Memory
7 Operating System

tag. En plus du transfert de données sans contact, la communication via l'antenne, permet également, des transferts sans visibilité entre le lecteur et l'étiquette au travers de matériaux opaques à la lumière, cette lecture pouvant s'effectuer simultanément sur plusieurs étiquettes.

Les différents systèmes RFID sont caractérisés principalement par leur fréquence de communication. Cependant, outre cette fréquence porteuse, d'autres caractéristiques définissent également les étiquettes RFID et constituent la base de leurs spécifications :

- l'origine et la nature de l'énergie ;
- la distance de lecture ;
- la programmabilité ;
- la forme physique ;
- la taille mémoire ;
- les propriétés du packaging (matériau) ;
- le nombre de tags lus simultanément (anti-collision) ;
- et bien sur le coût.

Débits de communication : 106, 212 ou 424 kbit/s (le débit 848 kbit/s n'est pas compatible avec la norme NFCIP-1) ;

Gamme de fréquence (classique) : 135 KHz ; 13,56 MHz ;

Distance de communication : maximum 10 cm ;

Mode de communication : half-duplex ou full-duplex.

	LF< 135 kHz	**HF13.56 MHz**	**UHF863 à 915 MHz**	**SHF2.45 GHz**
Capacité de données	De 64 bits lecture seul à 2kbits lecture-écriture	Classiquement tags lecture-écriture avec 512 bits de mémoire (max : 8kbits partitionné)	Classiquement tags lecture-écriture avec 32 bits de mémoire (max : 4kbits partitionné en 128 bits)	De 128 bits à 32 kbits partitionné
Produits disponibles	Read-only et read/write	Read-only et read/write	Read-only et read/write	Read-only et read/write, télé-alimenté et batterie assisté
Transfert de données	Faible taux de transfert : inférieur à l kbits/s (≈200bits/s)	Environ 25 kbits/s en général (existe en 100 kbits/s)	Environ 28 kbits/s	Généralement < à 100 kbits/s mais peu aller jusqu'à 1 Mbits/s
Distance de lecture	Typiquement du contact à 0.5 m pour les tags télé-alimentés, sinon ≈i 2 m	Pour les tags télé-alimenté de l'ordre du mètre	Pour les tags télé-alimenté de l'ordre du mètre	Qq dizaine de centimètre pour les passifs et qq dizaine de mètres pour les actifs
Mode de lecture	Les versions lecture unique et lecture multiple sont disponibles	Les versions lecture unique et lecture multiple sont disponibles	Lecture unique et lecture multiple, omni-directionnel	Lecture unique et lecture multiple

Limites de fonctionnement	- 40 à + 85 °C Peu sensible aux perturbations électro-magnétiques industrielles	- 25 à + 70 °C Faiblement sensible aux perturbations électro-magnétiques industrielles	- 25 à + 70 °C Sensible aux perturbations électro-magnétiques. Peut être perturbé par les autres systèmes UHF à proximité	- 25 à + 70 °C Fortement sensible aux perturbations électro-magnétiques réfléchies par le métal et absorbées par l'eau
Applications	Process de fabrication Identification de véhicules et de container Contrôle d'accès Identification animale	Suivi de flotte de véhicules Bagages Librairie Service de location Laveries automatiques Logistique	Logistique Suivi de flotte de véhicules	Automatisation d'entreprises Logistique militaire Contrôle d'accès Péage automatique

4. Le codage

4.1. Modulation

NFC utilise une modulation d'amplitude pour transmettre l'information : l'amplitude du signal est modifié pour permettre la représentation de bit. La manière dont elle varie est toujours la même, a savoir soit l'amplitude est maximal, soit elle est un pourcentage fixe de ce maximal (appelé pause).

Un bit est envoyé par unité de temps, chaque unité étant coupé en deux. L'amplitude du signal varie (ou non) à chaque demi-unité pour représenter un bit.

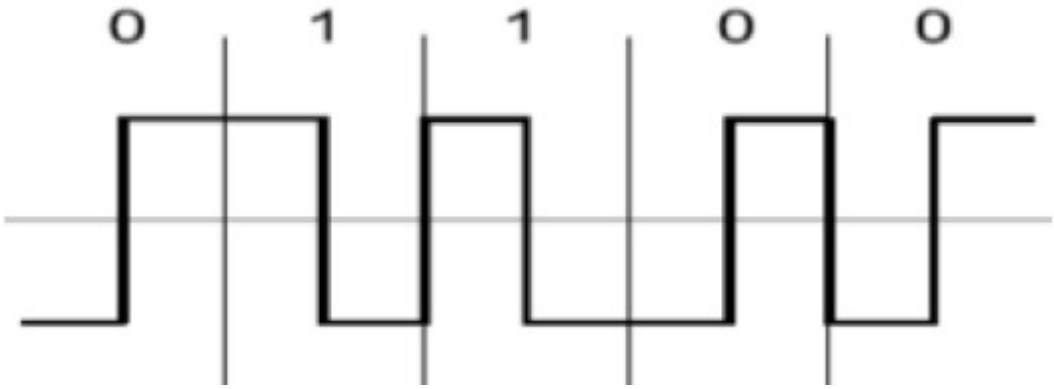
Le signal peut être codé de deux manières différentes avec deux amplitudes différentes pour les pauses en fonction de la méthode de communication choisie (active ou passive) et du débit :

Débit	Appareil passif	Appareil actif
424 Kbits/s	Manchester,10%ASK	Machester,10%ASK
212 Kbits/s	Manchester,10%ASK	Manchester,10%ASK
106 Kbits/s	Modified Miller,100%ASK	Manchester,10%ASK

Dans le cas d'une modulation (ASK) à 100%, aucun signal n'est émit pendant les pauses, alors qu'avec une modulation à 10% celui-ci est seulement diminué. Ce paramètre peut influe sur la sécurité.

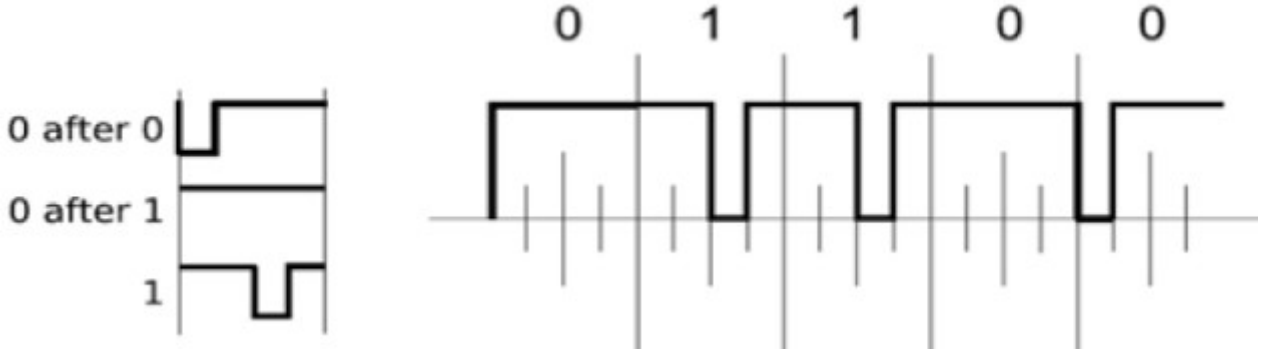
4.2. Codage Manchester

Le codage Manchester utilise systématiquement une pause par unité de temps pour définir la valeur du bit. Si la pause est effectuée pendant la première moitié un 1 est codé, si elle est effectuée pendant la seconde il s'agit d'un 0.



4.3. Codage Modified-Miller

Avec un codage Modified-Miller, un 1 est toujours codé de la même manière, à savoir une pause pendant la seconde moitié de l'unité de temps. Le codage du zéro dépend par contre du bit précédent : si celui-ci était un 1, aucune pause n'est effectuée, dans l'autre cas une pause est effectuée pendant la première moitié de l'unité de temps.



5. Lecture seule ou lecture/écriture

Quelque soit la fréquence à laquelle le système RFID fonctionne, quelque soit le type d'étiquette passive ou active, on peut différencier les applications RFID suivant les possibilités de lecture et/ou d'écriture dans la mémoire de la puce embarquée sur l'étiquette. Le but de la RFID étant d'identifier de manière unique les objets portant des tags, la puce électronique doit au minimum contenir un identifiant numérique accessible par le lecteur. Ce numéro unique peut être celui gravé par le fondeur de la puce lors de la fabrication (TID). Si cette puce ne possède pas d'autre zone mémoire, on parle de puce en lecture seule. Toute l'information liée au produit portant l'étiquette est donc déportée sur des systèmes d'informations indexés par l'identifiant unique.

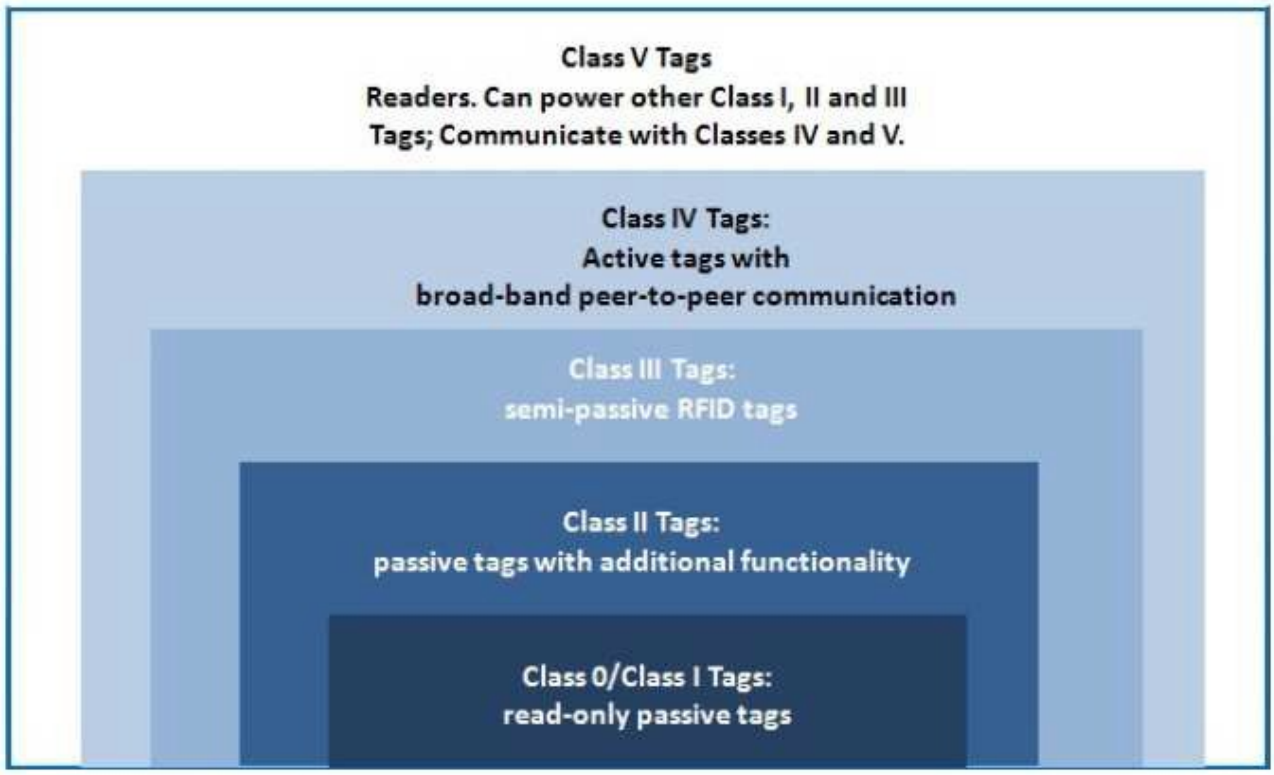
Dans certains cas, le numéro unique gravé par le fondeur de la puce n'est pas suffisant pour l'application finale. On peut donc trouver des puces possédant une zone mémoire vierge sur laquelle on puisse écrire un numéro particulier propre à l'utilisateur final du système RFID (UII[8] ou Code EPC[9] par exemple). Une fois ce numéro écrit, il ne peut plus être modifié. On parle alors de puce WORM[10].

D'autres types d'applications vont nécessiter la présence d'une zone mémoire accessible par l'utilisateur et réinscriptible. Cette zone, ne dépassant pas les quelques dizaines de kilo octets dans la majeure partie des cas, peut servir lorsque l'accès à une base de données centrale n'est pas garantie (lors d'opération de maintenance en zone isolée ou sur le théâtre d'opérations militaires). Les puces sont alors de type MTP[11] et possèdent de la mémoire généralement de type EEPROM.

8 Unique Item Identifier
9 Electronic Product Code
10 Write Once, Read Multiple
11 Multi Time Programmable

6. Les classes

- Classe 0 et classe 1 : tags passifs à lecture seule (on ne peut que lire l'identifiant unique du tag) ;
- Classe 2 : tags passifs à fonctions additionnelles (écriture mémoire) ;
- Classe 3 : tags passifs assistés par batterie ;
- Classe 4 : tags actifs. Communication large-bande du type « peer-to-peer » ;
- Classe 5 : interrogateurs. Alimentent les tags de classe 0, 1, 2 et 3. Communiquent avec les tags de classe 4.



7. Protocoles TTF et ITF

Qui parle le premier : le tag ou le lecteur ?

Cette question, a priori anodine, prend tout son sens lorsque plusieurs étiquettes se trouvent simultanément dans le champ du lecteur où lorsque les étiquettes ne sont pas statiques et qu'elles ne font que passer dans le champ rayonné par l'antenne du lecteur.

Dans le cas, rencontré très souvent en RFID, où les étiquettes sont batteryless (sans source d'énergie embarquée), il est clair que la première chose à faire pour le lecteur est de transmettre de l'énergie à (aux) l'étiquette(s). Pour cela, le lecteur émet un signal à fréquence fixe (sans modulation).

À ce moment, la communication entre le lecteur et l'étiquette n'a pas débuté. Une fois la puce de l'étiquette alimentée, elle peut soit transmettre immédiatement une information au lecteur (protocole TTF[13]) ou répondre à une requête du lecteur (protocole ITF[14]).

Le choix d'un protocole ou de l'autre dépend fortement de la gestion de la ressource radio et de la gestion de la présence éventuelle de plusieurs étiquettes dans le champ rayonné par le lecteur (protocole d'anti-

12 Tag IDentifier
13 Tag Talk First
14 Interrogator Talk First

collision). Pour se faire une idée de l'implication sur la gestion des collisions du choix d'un protocole ou de l'autre, imaginons une salle de classe. L'enseignant joue le rôle du lecteur, les élèves celui des étiquettes RFID.

Pour les systèmes TTF, nous pouvons imaginer qu'en début de cours, chaque élève entrant dans la salle donne son nom. Les élèves arrivent en cours à l'heure et chacun donnant son nom quasiment en même temps, nous pouvons douter que l'enseignant (le lecteur) puisse comprendre chaque nom individuellement et identifier chacun des élèves (étiquettes). Pour essayer de palier ce problème, il est possible de demander aux élèves de ne donner leur nom qu'après avoir écouté et s'être assuré que personne d'autre n'a pris la parole. Cette variante du protocole TTF est appelée TOTAL[15].

Pour des systèmes ITF, c'est l'enseignant (le lecteur) qui pose la première question et demande aux élèves de donner leur nom. Tous les élèves présents dans la salle répondent alors à la requête de l'enseignant. Comme dans le cas précédent, il peut être difficile, voire impossible, à l'enseignant d'identifier chaque élève puisque ceux-ci répondront à la requête de façon simultanée.

Parmi les avantages du protocole TTF, on peut noter la rapidité avec laquelle il est possible d'identifier une étiquette quand celle-ci est seule dans le champ rayonné par le lecteur. On peut également noter que lorsque le lecteur ne communique pas avec des étiquettes, il ne fait que rayonner un signal RF sans modulation. Ce signal n'occupe donc qu'une faible partie du spectre électromagnétique. Cela permet de réduire le risque d'interférence avec d'autres émissions ou d'autres lecteurs. En ce qui concerne le protocole ITF, le principal avantage est que la communication est initiée (trigger) par le lecteur. Toutes les réponses des tags peuvent donc être facilement superposées pour une détection de collision au niveau « bit » ou facilement séquencées pour singulariser les étiquettes.

7. Sécurité

Comme toutes les technologies sans fil, le NFC est plus sensible aux attaques qu'un réseau câblé, un contact physique n'étant pas nécessaire. Cependant, elle dispose d'un très courte portée qui favorise sa sécurité.

7.1. Attaques possibles

Plusieurs types d'attaques sont possibles sur le NFC.

- Eaves Dropping

  Le Eaves Dropping ou "écoutes aux portes" est le fait de récupérer le signal radio émis par les appareils pour subtiliser des informations personnels. Cette attaque peut être effectué depuis plusieurs mètre avec l'utilisation d'une antenne spécifique.

  Un moyen simple de se protéger de cette attaque et de chiffrer les informations qui transitent entre les appareils NFC.

- Déni de Service

  L'attaque de déni de service (DOS) est la plus simple à réaliser, cependant elle ne permet pas de récupérer d'information mais uniquement de rendre impossible l'utilisation du NFC d'un appareil.

  L'algorithme de collision avoidance de NFC spécifie un temps d'attente avant toute émission, pendant ce temps, l'appareil écoute le canal et ne commence à émettre que s'il est libre. L'attaque DOS sur cette technologie requiert uniquement d'émettre sur la bande de fréquence du NFC (13,56 MHz). Aucune protection n'est possible contre ce type d'attaque si ce n'est de se trouver hors de porté de l'attaquant.

- Modification de données

  La modification des données envoyés par un appareil NFC vers un autres est possible mais extrêmement difficile. Pour cela l'attaquant doit modifier l'amplitude des ondes émises pour que la cible l'interprète autrement.

  Dans le cas d'une modulation avec un ratio de 10%, il faut laisser croire que les ondes reçues à

15 Tag Only Talk After Listening

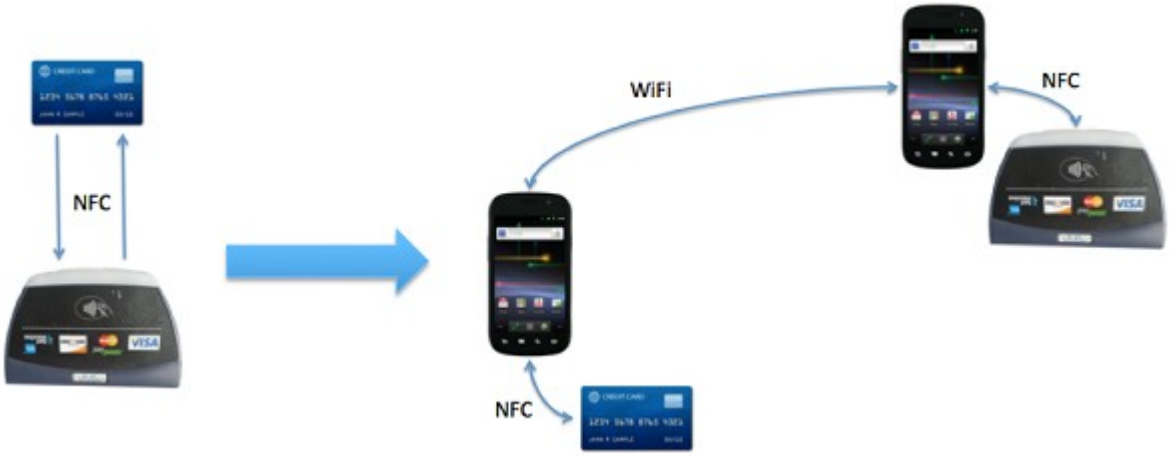
pleine amplitude sont en réalités des pauses pour inverser les bits. Pour cela, il faut intercepter toutes les ondes et augmenter l'amplitude maximale. Il est cependant impossible d'utiliser ce processus avec un ratio de modulation de 100% car les pauses, représentées par l'absence totale d'émission, ne peuvent pas être générées.

Cette attaque nécessite un matériel coûteux (récepteur, antenne) et est détectable car modifie l'amplitude du signal.

- Relais

  L'attaque par relais cible essentiellement les cartes de paiement sans contact et consiste à utiliser un proxy NFC. Deux appareils sont donc nécessaire : le premier sera à l'écoute de la carte, le second près du terminal de paiement. Ce dernier va initier le paiement à la borne et transmettre toute la communication via une connexion wifi au complice. La communication va ensuite être transmise à la carte NFC qui va répondre comme si elle était en contact avec le terminal.

  Cette attaque est simple à mettre en œuvre, nécessite uniquement deux smartphone NFC et aucune connaissance du protocole utilisé par les cartes. En effet, le trafic passe par la connexion Wifi sans être altéré.



Pour se protéger de cette attaque, la mise en place d'un code PIN sur la carte est nécessaire, ce dernier n'est pas demandé dans certains Pays.

7.2. Protection

Le NFC étant sensible au Eaves Dropping, il est primordial de sécuriser les échanges. C'est ce qui est fait pour la carte Navigo qui ne contient aucune données personnelles (l'identifiant de la carte étant différent de l'identifiant de l'utilisateur) et dont le contenu est chiffré. Le passeport RFID est lui aussi chiffré et nécessite par ailleurs une combinaison de lecteur optique et RFID pour que le contenu soit lu.

Ces sécurités ne sont pourtant pas en place pour les cartes de paiement NFC, qui disposent d'information bien plus sensible. Aucun chiffrement ni authentification n'est en place dans leurs puces NFC. Il est ainsi possible de récupérer certaines informations personnels simplement en approchant un lecteur (smartphone) d'une carte :

- Nom, Prénom, Sexe
- Numéro de compte
- Date d'expiration
- Contenu de la bande magnétique
- Historique des transactions

Seul le code de sécurité n'est pas disponible (3 chiffres au dos de la carte).

Ces informations permettent cependant d'utiliser la carte sur certains site de e-commerce ne demandant pas

le code de sécurité. Elle permettent aussi d'effectuer une attaque DoS de la carte en saisissant 3 mauvais code PIN. Il est aussi possible de cloner la bande magnétique et de l'utiliser.

Lecture d'une carte sous Android

Lecture d'une carte sous GNU/Linux

8. Exercices d'application

Sur un objet, on peut désormais installer une étiquette contenant des données d'identification et des informations en tout genre, que des lecteurs reçoivent et décodent automatiquement à distance.

C'est ce que l'on appelle la technique d'identification par radiofréquences (RFID). Elle est utilisée par exemple dans les systèmes de contrôle d'accès aux transports en commun, type passe pour le métro.

Les étiquettes, « souvent pas plus grosses qu'un grain de riz » sont constituées d'une « puce de silicium et d'un bobinage d'antenne encapsulés dans un module de verre ou de plastique ». Elles sont placées sur les passes des abonnés, tandis que les lecteurs sont fixés dans le bâti des portes automatiques.

Lorsque l'usager approche son passe à moins de 10 cm du lecteur, l'étiquette reçoit l'onde électromagnétique, de fréquence égale à 13,56 MHz, émise par le lecteur. Cette onde « sert de source de courant pour l'étiquette », qui ne nécessite donc pas de piles. Le courant produit par la réception de cette onde dans la bobine, charge un condensateur. « La tension à ses bornes augmente et active le circuit intégré de l'étiquette, qui transmet alors son code identificateur » au lecteur, toujours par onde électromagnétique. Le lecteur identifie alors le code et actionne le mécanisme d'ouverture de la porte.

Par rapport au système classique du ticket, l'usager gagne en simplicité, et la rapidité de l'opération permet de mieux réguler le trafic, surtout en cas d'affluence.

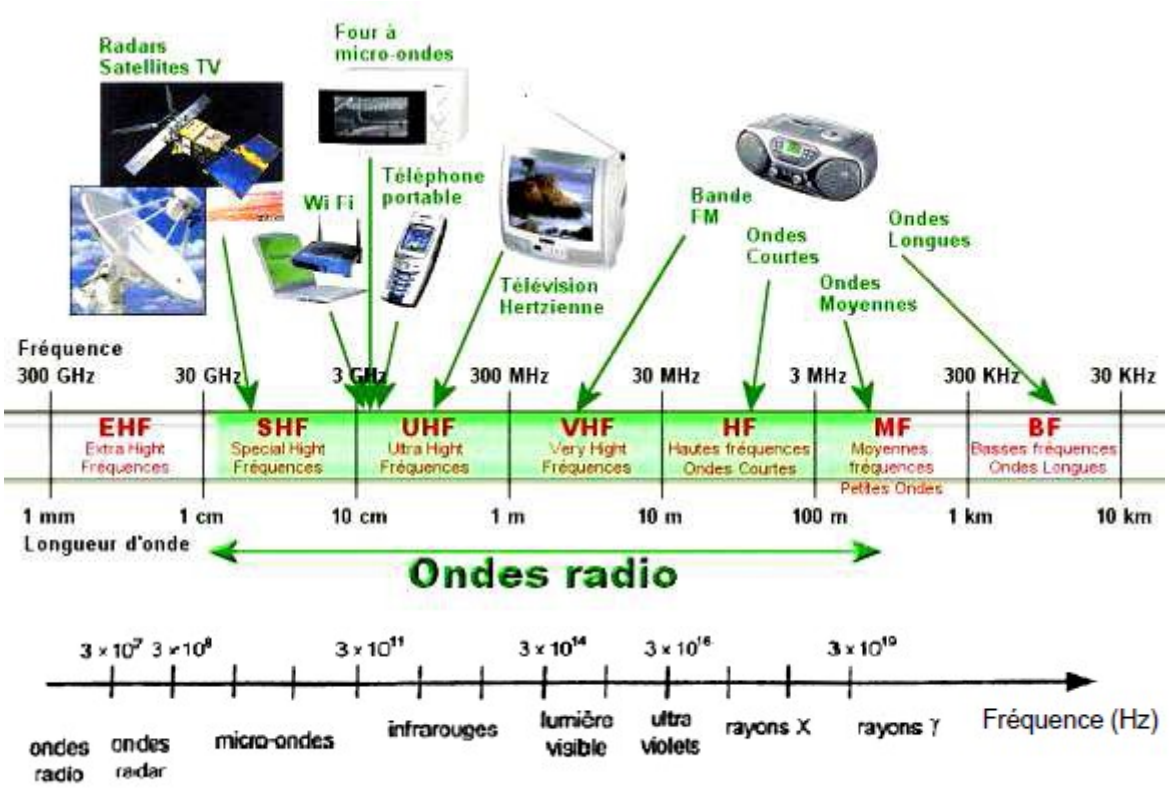
Dans cet exercice, on étudie le mode de communication entre le lecteur et l'étiquette. On modélise ensuite une partie du circuit électronique de l'étiquette, et on vérifie la validité de ce modèle expérimental en comparant son temps de réponse à celui d'un passe.

8.1. Communication entre le lecteur et l'étiquette du passe

La lumière, les rayons gamma, les infrarouges, les micro-ondes, les ondes radio, etc… font partie de la famille des ondes électromagnétiques. Les figures ci-dessous, précisent les différents domaines de

fréquence de ces sous-familles.

Question 1 : en vous aidant des figures et du texte ci-dessus, vérifier que les ondes passant entre le lecteur et l'étiquette appartiennent bien au domaine des ondes radio.



13,56 MHz appartient bien au domaine des ondes radio (HF).

Question 2 : calculer la valeur de la longueur d'onde du signal radio lorsque celui-ci se propage dans l'air (que l'on assimilera au vide).

La longueur d'onde est l'équivalent spatial de la période temporelle. En effet, la longueur d'onde est la distance parcourue par l'onde au cours d'une période. Si on appelle c la célérité de l'onde et T sa période temporelle, on a :

$$\lambda = c.T = \frac{c}{f} = \frac{3.10^8}{13{,}56.10^6} = 18{,}115\,m$$

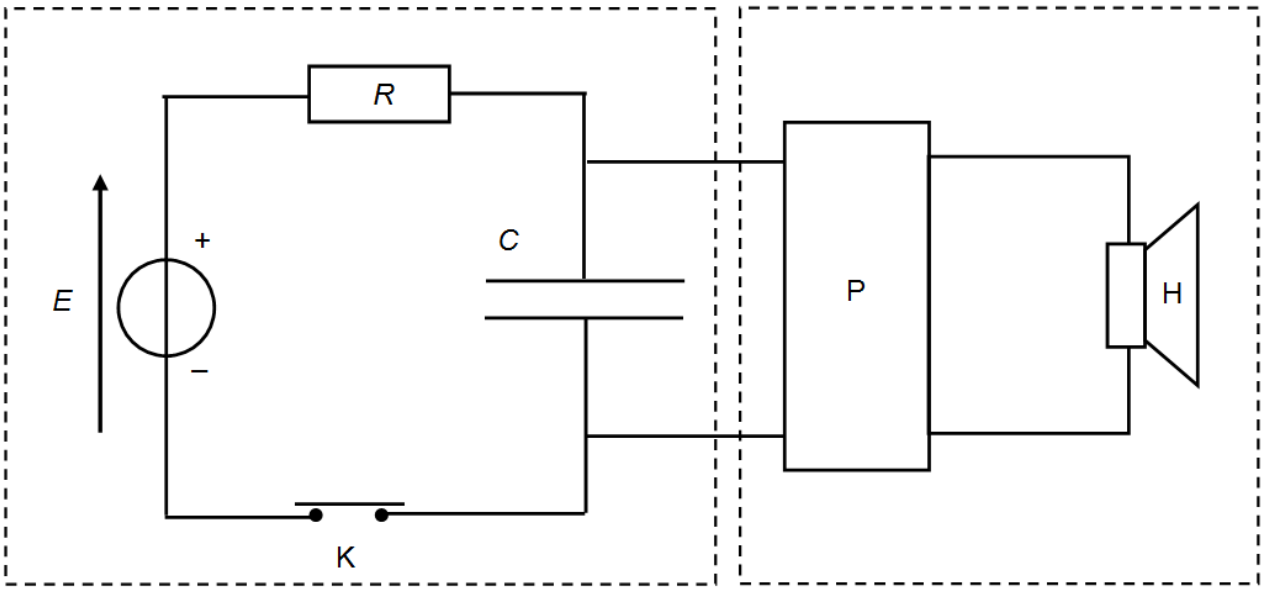
On peut modéliser le circuit de l'étiquette selon le schéma donné ci-dessous. Le bobinage d'antenne de l'étiquette qui reçoit l'onde radio et dans lequel naît le courant est modélisé, par souci de simplification, par un générateur idéal de tension E.

La résistance R du circuit représente la résistance de l'étiquette et vaut R = 1 MΩ.

Lorsque le passe de l'usager est suffisamment proche du lecteur, un courant prend naissance dans le circuit, ce qui correspond à la fermeture de l'interrupteur K à la date t_0 = 0, et charge le condensateur de capacité C.

Quand la tension aux bornes du condensateur devient supérieure à une tension seuil, notée U_S, le composant électronique P (qui correspond au circuit intégré de réponse de l'étiquette) alimente le haut-parleur H qui émet un son.

Ainsi la réponse du modèle n'est donc pas une onde radio comme pour l'étiquette, mais une onde mécanique sonore.



Question 3 : Retrouver la ou les bonnes propositions, parmi les suivantes :

a) Un milieu matériel est nécessaire à la propagation d'une onde mécanique et d'une onde électromagnétique telle que la lumière.

b) Une onde mécanique, tout comme une onde électromagnétique, se propage dans le vide.

c) Une onde mécanique nécessite un milieu matériel pour se propager, alors qu'une onde électromagnétique peut se propager dans le vide.

Réponse : c

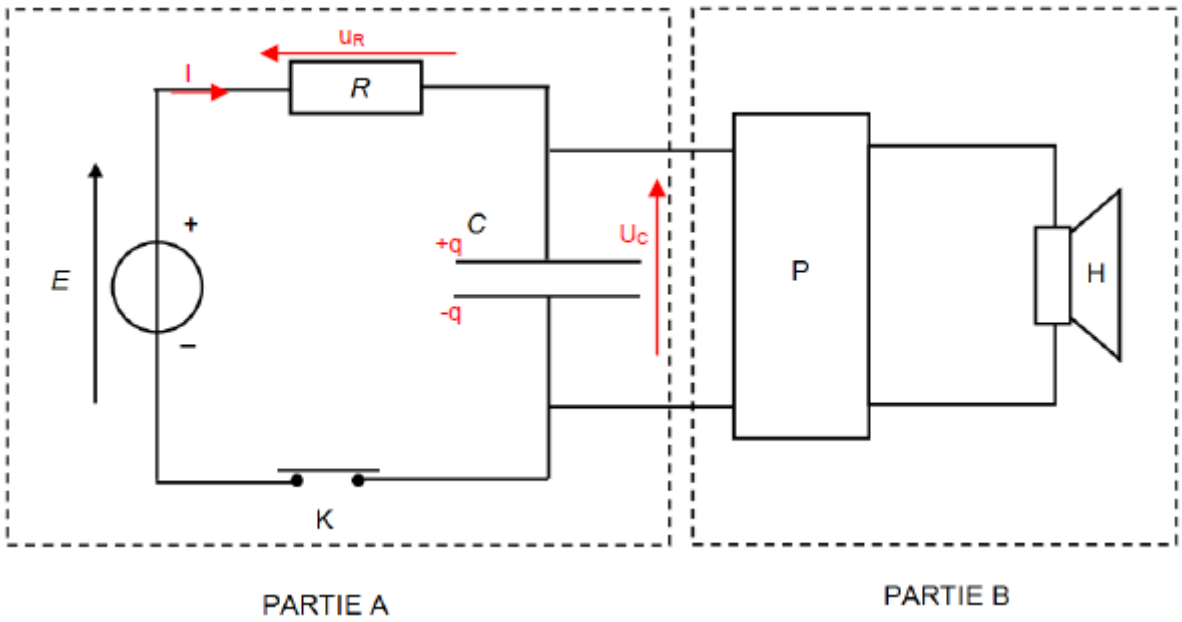
Question 4 : Quelle grandeur physique l'onde radio transfère-t-elle pour permettre à l'étiquette RFID de fonctionner sans piles ?

La grandeur physique que l'onde radio transfère est un champ magnétique.

8.2. Étude du temps de réponse du modèle expérimental

Question 5 : compléter le schéma du circuit (PARTIE A) en représentant :

1. le sens de circulation du courant électrique dans la portion du circuit qui contient le condensateur lorsque l'interrupteur K est fermé. Pour la suite, vous choisirez ce sens comme sens positif du courant.
2. les charges +q et - q des armatures du condensateur.
3. la flèche de la tension Uc aux bornes du condensateur et la flèche de la tension U_R aux bornes de la résistance.

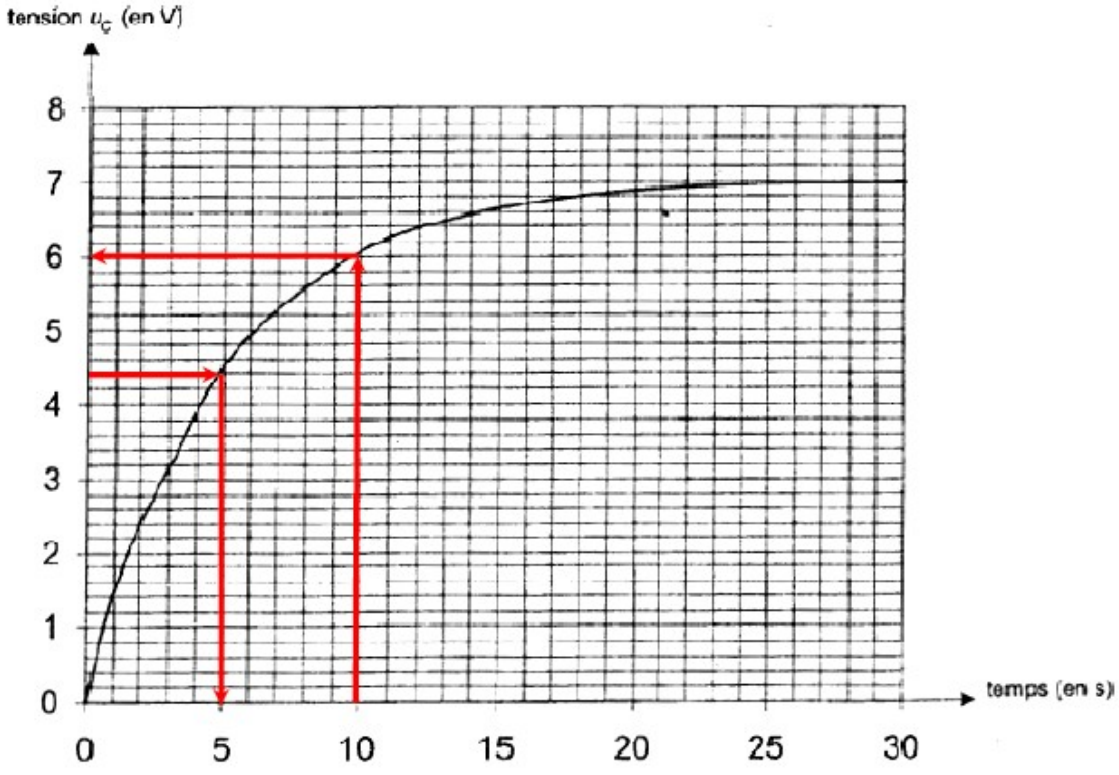


Question 6 : Pour un condensateur, donner la relation entre la charge Q et la tension Uc, en précisant les unités des grandeurs utilisées.

Q = C.Uc

- Q : quantité d'électricité en coulombs (C)
- C : capacité en farads (F)
- Uc : tension en volts (V)

Question 7 : au cours de la charge, l'évolution temporelle de la tension Uc est représentée sur la figure ci-dessous.



Indiquer la valeur vers laquelle tend Uc pour un temps de charge très long.

Uc tend vers E

En déduire graphiquement la valeur de E.

E = 7V

Question 8 : déduire graphiquement la valeur de « τ ». Faire apparaître la construction graphique sur la figure.

τ = 5 s

Question 9 : on constate que le composant électronique P n'alimente le haut-parleur H qu'au bout d'une durée égale à 2τ , que l'on appelle temps de réponse du circuit.

En déduire graphiquement la valeur de la tension seuil Us.

Us = 6V

Le condensateur est-il complètement chargé au bout de 2τ ?

Le condensateur n'est pas totalement chargé au bout de 2τ.

Peut-on dire que le temps de réponse du modèle est vraisemblable dans le cas de l'usage du « passe métro » ?

Le temps de réponse du modèle n'est pas vraisemblable.