NFC

Near Field Communication

19/11/2012

Aurèle Lenfant

Sommaire

- Introduction
- Fonctionnement
- Normes
- Codage
- Intérêts
- Usages
- Sécurité

Introduction

- Technologie de communication sans fil
  - Sans contact
- Simple d'utilisation
- Near Field : courte distance (cm)
- Extension de la norme définissant RFID
  - Compatible

Caractéristiques techniques

- Fréquence : 13.56 MHz
- Distance : <= 10cm
- Débit : de 106 à 420 Kbits/s
  - 848 Kbits/s ne respecte pas le standard ISO/IEC 18092

Fonctionnement

- Induction de champ magnétique
- Un initiateur et une cible
- Deux modes de communication existants
  - Passif
  - Actif

Fonctionnement

- L'initiateur est l'appareil qui souhaite communiquer
- La cible reçoit la requête et répond
- Permet d'empêcher l'envoi de données sans avoir établi une connexion
- Par défaut tous les appareils sont des cibles

Fonctionnement passif

- Un appareil initie la connexion
- Il fourni le champ magnétique
- L'appareil cible va moduler le champ existant
- Le champ magnétique peut être utilisé comme source d'énergie

Fonctionnement actif

- Les deux appareils génèrent des champs
- Alternatif
- Désactive la génération lors de l'attente
- Les deux appareils nécessites une source d'énergie propre

Normes

- Technologie ouverte de Philips et Sony
- Standardisée par ISO 18092
  - Vitesse de transfert
  - Méthode d'encodage
  - Modulation
  - Architecture des trames
  - Protocole utilisé

Normes

- ISO 14443
  - Définit la communication avec des circuits intégrés sans contact
- NDEF (NFC Data Exchange Format)
  - Définit le format d'échange

Communication : codage

- 1 bit envoyé par unité de temps
- Chaque unité est coupé en deux
- Utilise les pauses pour coder les bits

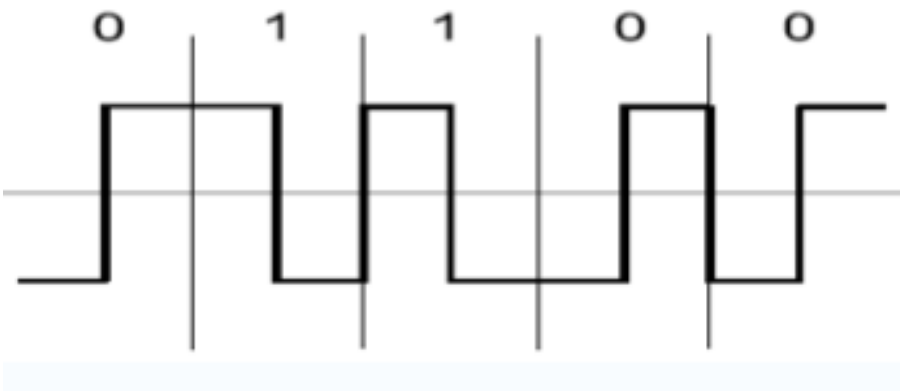
Débit	Appareil passif	Appareil actif
424 Kbits/s	Manchester,10%ASK	Machester,10%ASK
212 Kbits/s	Manchester,10%ASK	Manchester,10%ASK
106 Kbits/s	Modified Miller,100%ASK	Manchester,10%ASK

Modulation

- Modulation d'amplitude
- 100% : le signal radio est de 0 lors des pauses
- 10% : le signal radio est toujours présent lors de pause (82%)
- Influe sur la sécurité

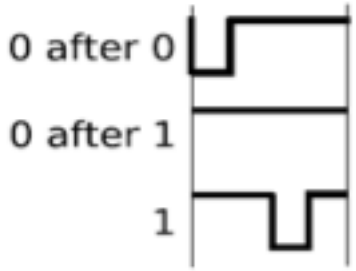
Manchester

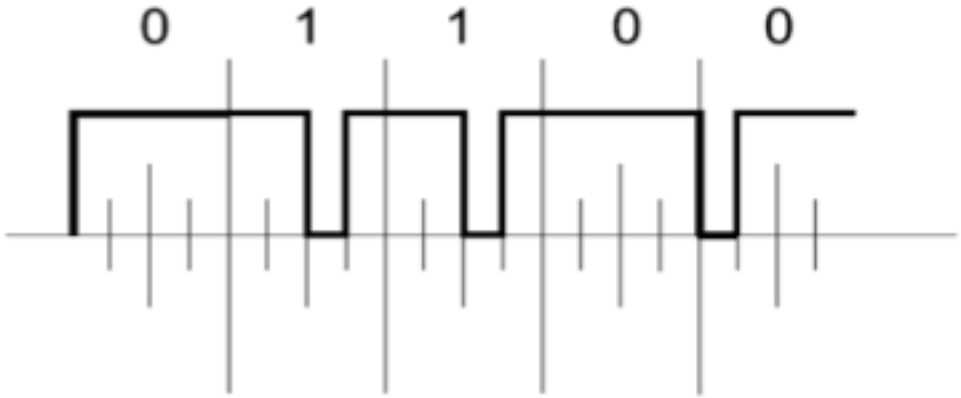
- Pause en première moitié → 0
- Pause en seconde moitié→ 1



Modified Miller

- 1 est toujours codé de la même manière
- 0 dépend du bit précédent

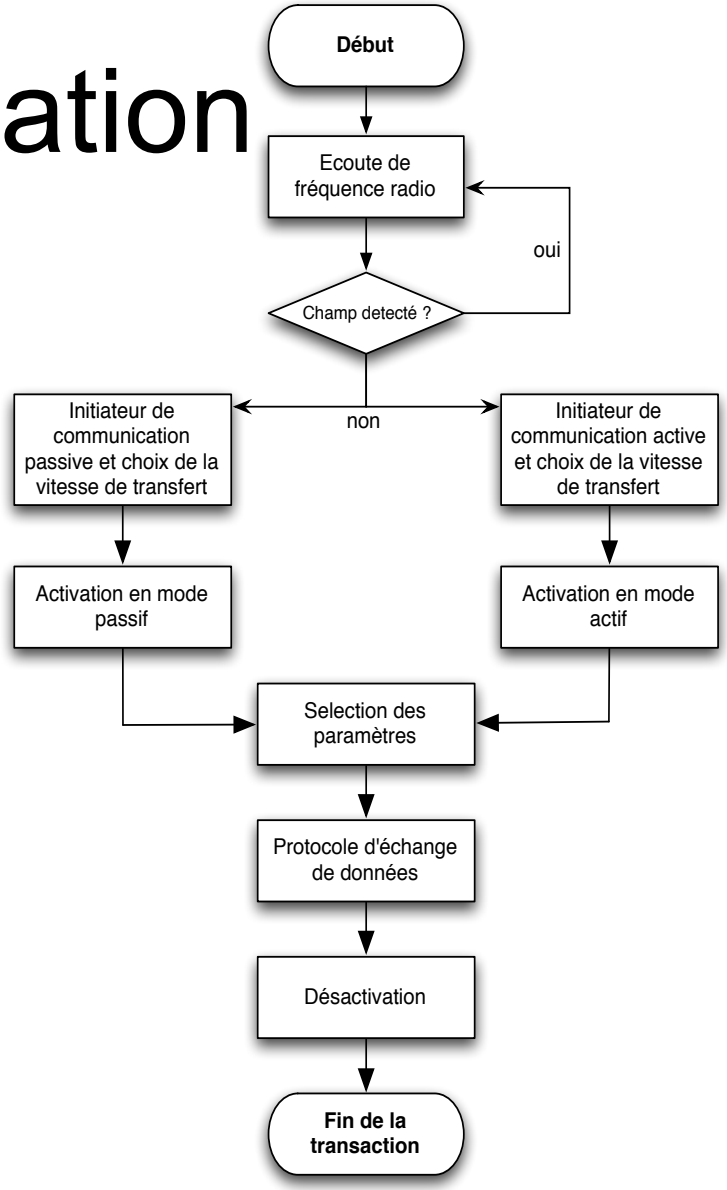




Collisions

- Rares (faible portée)
- Collision avoidance
  - Ecoute avant d'émettre
  - Attend tant qu'une émission est en cours
  - Commence l'émission une fois le canal libre et après un temps de garde

Communication



Interêts

- Faible portée
  - Sécurité
  - Utilisation naturelle
- Mode passif
  - Economie d’énergie

Comparaison : NFC / RFID

- NFC englobe les fonctionnalités de RFID
  - Emulation de tag RFID
- Possibilité de P2P (communication active)

Comparaison : NFC / Bluetooth

- Portée : 10cm / 10m
- Temps d'établissement de la connexion
  - <0.1s / 6s
- NFC propose mode actif / passif
- Débit : 424 Kbits/s / 2.1 Mbits/s
- Utilisation différente

Usages

- Paiement : carte bancaire NFC / téléphone
- Billetterie : transport / spectacle
- Lecture d'information : transport / magasin
- Contrôle d'accès
- Carte de visite électronique
- Appairage Bluetooth, clé wifi

Usages

- En France : uniquement pour le transport dans neuf villes
- Aux Etats-Unis : transport / paiement (Google, Amazon, Paypal)
- Corée / Japon : très développé

Eavesdropping

- Récupérer les fréquences radio émises
- Distance de quelques mètres (avec matériel)
  - 10m actif
  - 1m passif

Denial of Service

- Occuper la canal de fréquence radio
- Envoyer des données à un appareil
  - Si NFC est activé il lira tous les messages

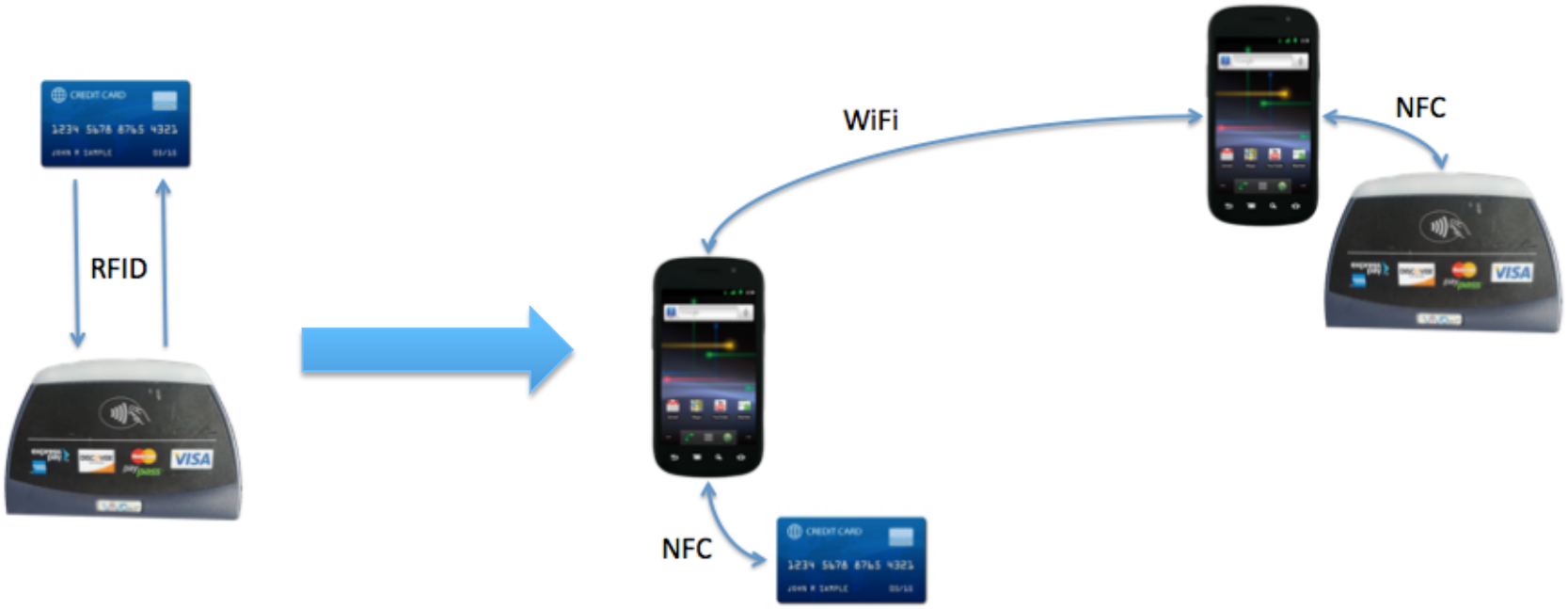
Modification des données

- Très difficile
- Efficacité dépend de la modulation utilisé
  - Modified Miller, 100% : certains bits
    - Génération de pause impossible
  - Manchester, 10% : tous les bits
- Détectable

Relai

- Utilisation d'un proxy RFC
- Nécessite deux appareils NFC
- Un lit les informations de la victime
- Le second les transmets
- Aucune connaissance du protocole nécessaire

Relai



Sécurité actuelle

- Navigo : Pas de données personnel, chiffrement, authentification
- Passeport RFID : Chiffrement, lecture RFID + optique
- Carte Paiement : Pas de chiffrement, pas d'authentification

Données des cartes de paiement

- Données disponible:
  - Nom, prénom, sexe
  - Numéro de compte
  - Date d'expiration
  - Données de la bande magnétique
  - Historique des transactions
- Code de sécurité non disponible

Attaques possibles

- Lecture des données et utilisation en e-commerce → Code de sécurité optionnel
- DoS (3 mauvais PIN)
- Clonage de la bande magnétique
- Récupération de données personnelles

Questions ?