NFC

Jonathan Windle

University of East Anglia

J.Windle@uea.ac.uk

June 6, 2017

Overview I

Intro

- A method of wireless data transfer.
- Low range communication.
- Connections established by "touching" devices.
- Effective operating range of approx $<$ 10cm.
- Little/no setup required.
- Relatively secure.
- Difficult to perform "Man in the middle" attack.

Fundamentals

- NFC tags (tansponders) store data.
- NFC readers (initiators) read data from the tags (clients).
- Tags are often **passive** (unpowered) devices.
  - Powered by the reader wirelessly.
  - Store data in small amount of memory (typically $<$ 2kb(.
  - Readers can often emulate tags.
- Readers are always **active** (powered) devices.
- E.g. Smartphones, card readers etc.
- May alternate between passive and active mode to send/receive data between devices (half-duplex network).

Types of NFC Tags

- Tag 1:
  - Read and re-write capable
  - 96 bytes of memory, expandable to 2KB.
  - 106kb/s transmission rate.
  - **No data collision protection**.
- Tag 2:
  - Read and re-write capable.
  - 96 bytes of memory, expandable to 2KB
  - 106kb/s transmission rate.
  - **Anti-collision support**.

Types of NFC Tags - Cont

- Tag 3:
  - Read and re-write capable
  - Up to 32KB of memory.
  - 212 or 424kb/s transmission rate.
  - Anti-collision support.
- Tag 4:
  - Read and re-write capable.
  - Up to 32KB of memory.
  - 106,212 or 424kb/s transmission rate.
  - Anti-collision support.

Transfer Modes

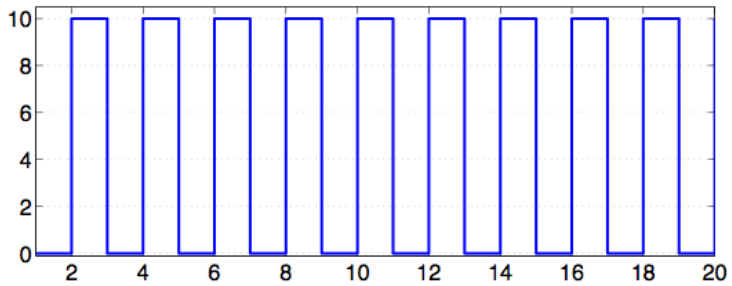
- Carrier signal frequency is **13.56MHz**.
- Passive data transfer:
  - Reader is powered, client is not.
  - Reader powers client using a magnetic field: air-cre transformer.
  - Client uses load modulation to send data to reader using readers magnetic field.
  - Simplex data transfer.
- Active data transfer:
  - Both devices are powered.
  - Sends data by modulating own magnetic field.
  - Allows half-duplex and full-duplex data transmission.
  - Gives a better performance.
  - Transponder (tag) only generates the subcarrier sgnals and actively transmits through own magnetic field.
  - The signal requires less energy because both devices are powered.

Powering Devices

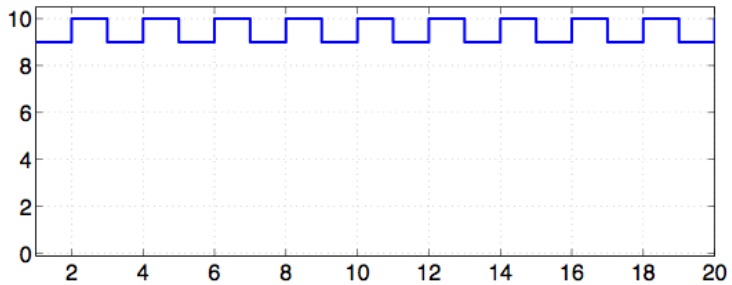
- Reader device powers passive device by magnetic induction air-core transformer.
- Reader induces a magnetic field by passing voltage through a coil (carrier signal)
- Passive device uses similar coil to cnvert magnetic field back to electric impulses.
- Voltage is rectified (AC to DC) to serve as a power supply.

Signal Coding

- NFC uses ASK to send data:
  - Manchester coding
  - Modified Miller coding.
- Modulation ratio: The ratio of signal level between high and low bits.
  - Given a signal with a dynamic range of 0-10 a 100% modulation ratio would represnt a zero bit as 0 and 1 as 10, whilst for 10% modulation ratio, a zero bit would be represented by 9 and 1 as 10.
- Two modulation ratios used: 10% and 100%.



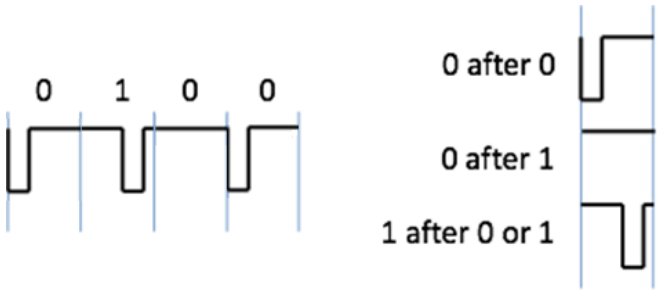
100%



10%

Signal Coding Methods

- Manchester coding:
  - low-high transition = 0
  - high-low transition = 1
- Modified Miller cding (delay encoding)
  - Bit inversion **during** period denotes change in symbol.
  - Type of transition depends on location of inversion.
  - Beneficial as non-positive signal duration are short ensuring power transfer during data transmission.
  - Singal energy does not stay low for long.



Configurations

- Depends on the capability of the tag:

Speed	Active	Passive
424kb/s	Manchester (10% modulation)	Manchester
212kb/s	Manchester	Manchester
106kb/s	Modified Miller (100% modulation)	Manchester

- Modfied Miller coding gives best protection against external modification.
- Can only modify low-high transitions and so only 0 after 0 or 1 after 1 may be affected.

Summary

- NFC tags store data, NFC readers read the data from the tags.
- Simplified network stack.
- NFC is a standard of very short-range data transmission.
- Active devices may power passive devices.
- Operation very similar to other wireless network standards (i.e. IEEE 802.11).
- Collision avoidance (half-duplex)
- Carrier sense for existing RF field.

The End