What is RFID?

- Radio Frequency IDentification
RFID

- **ADC** (automated data collection) technology that uses radio-frequency waves to transfer data between a reader and a movable item to identify, categorize, track...
- RFID is fast, reliable, and does not require physical sight or contact between reader/scanner and the tagged item
- A close cousin to sensor network technology
- Generally, RFID tags are cheaper, but less “intelligent” than sensor nodes
- As things evolve the line between the two technologies is blurring

Some Historical Background

- **Identification Friend or Foe (IFF)** Used by Allied bombers during World War II
- In 1948, concept of **passive RFID** systems introduced by Harry Stockman
- In 1972, Kriofsky and Kaplan designed and patented an “inductively coupled transmitter-responder” (2 antennas)
- In 1979, Beigel designed/patented “identification device” which combined both antennas into one
- In the 1970s, a group of scientists at the Lawrence Livermore Laboratory (LLL) build a handheld receiver stimulated by RF power for secure access to nuclear facilities
RFID Systems

Main components:
- **Tags** (transponders)
  - Microchip & antenna
- **Tag reader**
  - Decoder & antenna
  - RFID reader sends pulse of energy and waits for response
  - Can be on all the time or activate only in response to external event

Variations:
- **Memory**
  - Size (16 bits - 512 Kbytes)
  - Read-Only, Read/Write or WORM
- **Arbitration (Anti-collision)**
  - Ability to read/write one or many tags at a time
- **Frequency**
  - 125KHz - 5.8 GHz
- **Price**
  - $0.10 to $250
- **Physical Dimensions**
  - Thumbnail to Brick sizes
“Mission Impossible”

Tiny Tags

- 2007 Hitachi produced RFID device measuring 0.05×0.05 mm, and thin enough to be embedded in a sheet of paper. The data contained on them can be extracted from as far away as a few hundred meters. Human hair comparison.
## Active versus Passive

<table>
<thead>
<tr>
<th></th>
<th>Active RFID</th>
<th>Passive RFID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tag Power Source</td>
<td>Internal to tag</td>
<td>Energy transferred using RF from reader</td>
</tr>
<tr>
<td>Tag Battery</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Required signal strength</td>
<td>Very Low</td>
<td>Very High</td>
</tr>
<tr>
<td>Range</td>
<td>Up to 100m</td>
<td>Up to 3-5m, usually less</td>
</tr>
<tr>
<td>Multi-tag reading</td>
<td>1000’s of tags recognized – up to 100mph</td>
<td>Few hundred within 3m of reader, about 3 sec per read =&gt; at most 3 mph.</td>
</tr>
<tr>
<td>Data Storage</td>
<td>Up to 512 KB</td>
<td>16 bits – 1 KB</td>
</tr>
</tbody>
</table>

## Frequency Ranges

<table>
<thead>
<tr>
<th>FREQUENCY BAND</th>
<th>CHARACTERISTICS</th>
<th>TYPICAL APPLICATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOW 100-500 KHz</td>
<td>SHORT TO MEDIUM READ RANGE INEXPENSIVE LOW READ SPEED</td>
<td>ACCESS CONTROL ANIMAL IDENTIFICATION INVENTORY CONTROL</td>
</tr>
<tr>
<td>HIGH 10-15MHz</td>
<td>SHORT TO MEDIUM READ RANGE POTENTIALLY INEXPENSIVE MEDIUM READ SPEED</td>
<td>ACCESS CONTROL SMART CARDS</td>
</tr>
<tr>
<td>ULTRA-HIGH 2.4-5.8 GHZ</td>
<td>LONG READ RANGE HIGH READING SPEED LINE OF SIGHT REQUIRED EXPENSIVE</td>
<td>RAILROAD CAR MONITORING TOLL COLLECTION SYSTEMS VEHICLE IDENTIFICATION</td>
</tr>
</tbody>
</table>
Active Tag

- Greater range: 20-200m
- 10 yr. Life
- Limited sensor capabilities
- "Self-powered" uses interrogator RF beam for wake-up and communication

Passive Tag

- Limited range: <10m (frequency dependent)
- Communication & power from interrogator RF beam
Low Frequency: Load Modulation

1. An integrated circuit sends a signal to an oscillator, which creates an alternating current in the reader's coil.

2. That current, in turn, generates an alternating magnetic field that serves as a power source for the tag.

3. The field interacts with the coil in the tag, which induces a current that causes charge to flow into a capacitor, where it is trapped by the diode.

4. As charge accumulates in the capacitor, the voltage across it also increases and activates the tag’s integrated circuit, which then transmits its identifier code.

5. Variations in the resistance of the circuit, as a result of the transistor turning on and off, cause the tag to generate a varying magnetic field, which interacts with the reader's magnetic field. In this technique, called load modulation, magnetic fluctuations cause charge to flow from the reader to its coil in the same pattern as the ones and zeros transmitted by the tag.

6. The variations in the amplitude of the reflected signal, in what is called backscatter modulation, correspond to the pattern of the transistor turning on and off.

7. The variations in current flow in the reader coil are sensed by a device that converts this pattern to a digital signal. The reader’s integrated circuit then decodes the tag’s identifier code.

High-Frequency: Backscatter Modulation

1. An integrated circuit sends a digital signal to a transceiver, which generates a radio-frequency signal that is transmitted by a dipole antenna.

2. The electric field of the propagating signal gives rise to a potential difference across the tag’s dipole antenna, which causes current to flow into the capacitor, the resulting charge is trapped there by the diode.

3. The voltage across the capacitor turns on the tag’s integrated circuit, which sends out its unique identifier code as a series of digital high- and low-voltage levels, corresponding to ones and zeros. The signal moves to the transistor.

4. The transistor gets turned on or off by the highs and lows of the digital signal, alternately causing the antenna to reflect back or absorb some of the incident radio-frequency energy from the reader.

5. The reader's transceiver detects the reflected signals and converts them to a digital signal that is relayed to the integrated circuit, where the tag’s unique identifier is determined.
Codes

RFID tag

Bar code

Bar Code

Manufacturer Code

Product Code

Number System Character

3 Guard Bars

Check Digit

0 12345 67890 5
EPC: Electronic Product Code

The Electronic Product Code

S-GTIN: 01.000389.000162.00169740

- Header (8 bits)
  - Identifies the EPC's version number and allows for the evolving of different lengths or types of EPC.
- EPC Manager (28 bits)
  - Identifies the manufacturer of the product which it derives from the company's prefix.
- Object Class (24 bits)
  - Refers to the exact type of product which is the GTIN without the prefix or the item reference.
- Serial Number (36 bits)
  - The specific serial number of the individual item.

Communication and Collisions

- Very simple packet formats
  - General structure:
    - Sync
    - Header
    - Command
    - Data
    - CRC
  - Usually reader-to-tag and tag-to-reader format somewhat different.
  - Typically 2 byte CRC
Collisions

- All tags receiving query will respond: collisions!
- Many readers feature “simultaneous read” capabilities (resolve collisions)
- No “carrier sense” possible

Approach 1: Slotted Aloha

- One of the earliest and simplest medium access control protocols
- Aloha: access medium whenever ready to transmit
- Slotted Aloha: only access medium at beginning of slot (can reduce occurrence of collisions)
- Tags choose random backoff (reader can acknowledge tag ID and that tag will not send anymore)
Approach 2: Binary Tree Algorithm

- Poll tags bit-by-bit
- Example (figure):
  - Query "x": 7 tags respond: collision
  - Query "0x": 3 tags respond: collision
  - Query "00x": 1 tag responds
  - Query "01x": 2 tags respond: collision
  - Query "010x": 2 tags respond: collision
  - Query "0100x": 1 tag responds
  - Query "0101x": 1 tag responds
  - Query "011x": no response
  - Query: "1x": 4 tags respond: collision
  - Query: "10x": 1 tag responds
  - Query: "11x": 3 tags respond: collision
  - ...

Application Scenarios

- Track the movement of consumer product goods
- Animal identification/tracking/counting
- Toll collection
- Implantation of RFID chips into people, e.g., Alzheimer patients
Applications

- Keyless entry
- Proximity cards
- Supply chain management

Implants

- It is the most controversial application
- Small glass cylinders approximately 2 or 3mm wide and between 1 and 1.5cm long
- Consists of a microchip, a coiled antenna, and a capacitor
- Implanted typically under the skin of arm or the back of the neck
Instant Checkout?

“Chip to remove shopping blues”
—Post-Courier, January 1994

“1.5¢ electronic bar code announced”
—San Francisco Chronicle

“Scanning range of four yards”
—NY Times

“Checkout in one minute”
—The Times, London

“Tiny microchip identifies groceries in seconds.”
—Chicago Tribune

Concerns

- Clandestine tracking
- Inventorying

Mr. Jones in 2020...

- Replacement hip medical part #439552
- Wig model #4456 (brown polyester)
- Dan Kapital and Communist-party handbook
- 1500 Euros in wallet
- Serial numbers: 597387, 389473
- 30 items of lingerie
Security/Privacy Issues and Solutions

- **Unauthorized Reading:**
  - Scan closed boxes and find out what is inside
  - Read RFID enabled credit card or ID (metal foil in passports)

- **Unauthorized Writing:**
  - Can change UPC/price of an item
  - Can kill a tag

- **RFID Zapper:**
  - Can burn a tag using overcurrent

- **RSA Blocker Tag:**
  - Placed near another RFID; prevents its reading

- **Put Tag to Sleep:**
  - Can wake up later; reuse tags

- **Re-label Tag and Dual-Use Tag:**
  - Customer sees differed info or can over-write tag with useful information

- **Authentication:**
  - Reader has to know PIN

Near-Field Communication (NFC)

- **NFC,** is one of the latest wireless communication technologies. As a short-range wireless connectivity technology, NFC offers safe yet simple communication between electronic devices.
- It enables exchange of data between devices over a distance of 4 cm or less.
- NFC operates at 13.56 MHz and rates ranging from 106 kbit/s to 848 kbit/s.
How NFC Works

• NFC is based on **RFID technology** that uses magnetic field induction between electronic devices in close proximity.

• For two devices to communicate using NFC, one device must have an **NFC reader/writer** and one must have an **NFC tag**. The tag is essentially an integrated circuit containing data, connected to an antenna, that can be read or written by the reader.

How NFC Works

• The technology is a simple extension of the ISO/IEC14443 proximity-card standard (contactless card, RFID) that **combines the interface of a smartcard and a reader into a single device**

• An NFC device can **communicate with both existing ISO/IEC14443 smartcards and readers, as well as with other NFC devices**, and is thereby compatible with contactless infrastructure already in use for public transportation and payment

• NFC is primarily aimed at usage in **mobile phones**

• 2015: ~600 million NFC-equipped phones in use (estimate that 5% are used at least once a month)
NFC Applications

There are currently three main uses of NFC:

- **Card emulation**: The NFC device behaves like an existing contactless card
- **Reader mode**: The NFC device is active and reads a passive RFID tag, for example for interactive advertising
- **P2P mode**: Two NFC devices communicating together and exchanging information

NFC Applications

- **Mobile payment**
- **Mobile/electronic ticketing**
- **Smart objects**
- **Electronic keys**
- **P2P data transfers**
- **NFC can be used to configure and initiate other wireless network connections such as Bluetooth or Wi-Fi**
Future of RFID and NFC