18-452/18-750
Wireless Networks and Applications
Lecture 23: RFID and NFC

Peter Steenkiste
CS and ECE, Carnegie Mellon University

Spring Semester 2017
http://www.cs.cmu.edu/~prs/wirelessS17/

Plan, outline

• RFIDs
  » Concept and applications
  » EPC and backend processing
  » PHY and MAC
  » Security
• Near Field Communication

What is RFID?

• Radio Frequency IDentification (RFID) is a method of remotely storing and retrieving data using devices called RFID tags and RFID Readers
• An enabling technology with many applications
  » Data can be stored and retrieved from the tag automatically with a Reader
  » Tags can be read in bulk
  » Tags can be read without line of sight restrictions
  » Tags can be read once read many (WORM) or rewritable
  » Tags can require Reader authentication before exchanging data
  » Other sensors can be combined with RFID
• Technology has been around for a long time
• Also has critics, e.g. privacy concerns

How Does It Work?

How does it operate?

• RFID tags are affixed to objects and stored information may be written and rewritten to an embedded chip in the tag
• Tags can be read remotely when they receive a radio frequency signal from a reader and use the energy to respond
• Can operate over a range of distances
• Readers display tag information or send it over the network to back-end systems

What is RFID?

• A means of identifying a unique object or person using a radio frequency transmission
• Tags (or transponders) store information, that can be retrieved wirelessly in an automated fashion
• Readers (or interrogators), either stationary and handheld, can read/write information from/to the tags
Applications

- **Operational Efficiencies**
  - Shipping and Receiving
  - Warehouse management
  - Distribution
  - Asset management

- **Total Supply Chain Visibility**
  - Inventory visibility in warehouses
  - In-transit visibility, asset tracking
  - Pallet, case level
  - Item, instance level

- **Shrinkage, counterfeit**
  - Reduce internal theft
  - Reduce process errors
  - Avoid defensive merchandizing
  - Product verification
  - Origin, transit verification

- **Security, Regulations**
  - Total asset tracking
  - Defense supplies
  - Container tampering
  - Animal Tracking

Automated Identification Technology Suite

<table>
<thead>
<tr>
<th>Linear Bar Code</th>
<th>CMB Contact Memory Button</th>
</tr>
</thead>
<tbody>
<tr>
<td>2D Symbol QR Code</td>
<td>Smart Card/CAC</td>
</tr>
<tr>
<td>OMC Optical Memory Card</td>
<td>RFID - Active Radio Frequency ID</td>
</tr>
<tr>
<td>STS Satellite-Tracking System</td>
<td>RFID - Passive Radio Frequency ID</td>
</tr>
</tbody>
</table>

RF ID Types

- **Passive Tags:** rely on an external energy source to transmit
  - In the form of a reader that transmits energy
  - Relative short range
  - Very cheap

- **Active Tags:** have a battery to transmit
  - Has longer transmission range
  - Can initiate transmissions and transmit more information
  - A bit more like a sensor

- **Battery Assisted Passive tags are a hybrid**
  - Have a battery transmit
  - But need to be woken up by an external source

A Bit of History

- **Early technology was developed in the 40s**
  - Originally used as eaves dropping devices
  - Used reflected power to transmit (transponder), e.g. the membrane of a microphone

- **First RF IDs were developed in the 70s**
  - Combines transmission based on reflected energy with information in memory – can now distinguish devices

- **Dramatic growth in last decade as a result of mandates**
  - Big organizations (DOD, Walmart) requiring the use of RFIDs from their vendors for easy inventory control

- **Now used in increasingly larger set of applications**
Standards

- Passive tags operate in the LF, HF, and UHF unlicensed spectrum
  - 30-300 KHz, 3-30 MHz, 300-3000 MHz
  - Distance drop with frequency
- Transmission consists of a bit stream and CRC
- Many standards exist, mostly incompatible
  » Early standards mostly defined by the ISO
  » Widely used standard: ISO/IEC14443
- In 2003 EPCGlobal was formed to promote RFID standards
  » Defined a standard for the Electronic Product Code (EPC)
  » Also defined standards for coding and modulation

Primary Application Types

Identification and Localization
- Readers monitoring entering and exiting a closed region
  » security (RFID in identification cards)
  » automatic ticketing (NFC on mobile phone)
- Readers tracking an RFID-tagged object
  » business process monitoring (RFID tags on pallets)
- Tags marking a spatial location
  » an NFC enabled mobile phone passes tags in the infrastructure whose location is known

Example: Smart Card

Public transport system in Singapore
- FeliCa Smart Card
- 2001 – 2009
- faster boarding times
- Other uses
  » small payments retail
  » identification
- Replaced by contactless card (RFID)

Plan, outline

- RFIDs
  » Concept and applications
  » EPC and backend processing
  » PHY and MAC
  » Security
- Near Field Communication
Electronic Product Code (EPC)

• "A Universal identifier for physical objects"
  » EPC is designed to be unique across all physical objects in the world, over all time, and across all categories of physical objects.
  » It is expressly intended for use by business applications that need to track all categories of physical objects, whatever they may be.
  » urn:epc:id:sgtin:0614141.012345.6285210cc Syringe #62852 (trade item)

• Combine
  » EPC data located on the RFID tag
  » Reader’s middleware
  » locate EPC Information Services (EPCIS), using Web Services like SOAP and WSDL

EPC Network Concept (2001)

What information does an RFID tag contain?

Passive RFID Tags

• Power supply
  » passive: no on-board power source, transmission power from signal of the interrogating reader
  » semi-passive: batteries power the circuitry during interrogation
  » active: batteries power transmissions (can initiate communication, ranges of 100m and more, 20$ or more)

• Frequencies
  » low frequency (LF): 124kHz – 135 kHz, read range ~50cm
  » high frequency (HF): 13.56 MHz, read range ~1m
  » ultra high-frequency (UHF): 860 MHz – 960 MHz (some also in 2.45GHz), range > 10m
**Frequency Bands**

**Passive RFID Tags**

**Electromagnetic Spectrum**

- **Radio Waves**
- **Infrared**
- **Visible Light**
- **Ultra-Violet**
- **X-Rays**
- **Gamma Rays**
- **Cosmic Rays**

**The "RFID" Frequencies**

- **VLF**: 125-134 kHz
- **LF**: 13.56 MHz
- **HF**: 860-930 MHz
- **VHF**: 2.45 and 5.8 GHz

**Standards**

- ISO 18000: multipart standard for protocols in LF, HF, and UHF bands
- For example, HF:
  - ISO 14443 (A and B) for "proximity" RFID
  - ISO 15693 for "vicinity" RFID (basis for ISO 18000 part 3)
- Two classes:
  - Class 0: read only
  - Class 1: read/write, can for example be used for tracking

**Transmission methods**

- **LF and HF**: inductive coupling
  - coil in the reader antenna and a coil in the tag antenna form an electromagnetic field
  - tag changes the electric load on the antenna.
- **UHF**: propagation coupling: backscatter
  - tag gathers energy from the reader antenna
  - microchip uses the energy to change the load on the antenna and reflect back an altered signal
  - Different modulations used by reader and tag

**PHY Layer**

- Depends on the frequency band used
- Different modulations used by reader and tag
  - Different constraints, e.g. power and complexity
  - E.g. cannot used amplitude modulation for HF tag (why?)
- Example of EPCGlobal symbols for UHF

From: [http://www.highfrequencyelectronics.com/Archives/Aug05/HFE0805_RFIDTutorial.pdf](http://www.highfrequencyelectronics.com/Archives/Aug05/HFE0805_RFIDTutorial.pdf)
What does an RFID tag look like inside a card?

MAC Layer

- Typically assumed that only one reader is present, i.e. no need for MAC on the reader
- MAC for tags is a challenge: very high concentrations of tags are present in many contexts
  - And tags are dumb, i.e. cannot have sophisticated protocols
- Two types of schemes used (standard):
  - Binary tree resolution: reader explores a tree of relevant tag values
  - Aloha: tags transmit with a random backoff

General Security Concerns

- RFID tags raise a number of security concerns:
  - Privacy risks, e.g., eavesdropping
  - Cloning and forging of tags
- Specific disadvantages due to tag limitations
  - Encryption algorithms are too complex to be implemented on tags
- But also specific advantages:
  - Tags are slow to respond, maximum no. of read-out operations
  - Adversary has to be physically close
### Privacy Concerns

- **Tracking**
  - Depends only on unique id (even if random)
  - Today:
    - automated toll-payment transponders
    - loyalty cards
  - Future: pervasive availability of readers

- **Inventorying**
  - Invisible items become visible
  - Libraries
  - Passports
  - Human implants: VeriChip
    - Medical record indexing
    - Physical access control
  - Future: pervasive availability of readers

### Privacy for Business Networks

- **Major concern for industry:**
  - Supply chain visibility
  - Supply chains and business networks are business assets
  - Example provenance checking: competitors may be able to get a lot of information
    - Where an object and its parts were manufactured
    - When it was manufactured
    - By which sub-contractors
  - Who are the suppliers of a company
  - Which companies are the customers of a company

### Reading Ranges

- Controlling reading range can limit privacy risk
- Nominal read range (RFID standards and product specifications):
  - 10cm for contactless smartcards (ISO 14443)
- Rogue scanning range: sensitive reader with more powerful antenna or antenna array
  - 50cm
- Tag-to-reader eavesdropping range: need to power the tag limits range for passive RFIDs
  - Eavesdropping on communication while another reader is powering the smartcard: > 50cm
- Reader-to-tag eavesdropping: readers transmit at much higher power

### Use for Authentication

- **RFID tags** uniquely identify objects
- Many proposals to use tags for authentication
  - Passport or driver's licence
  - Identification of stolen goods
- Counterfeiting attack
  - Scanning and replicating tags
- Possible options
  - EPC:
    - Simple bitstring
    - No access-control
  - VeriSign:
    - Digital signing
    - Against forging but not cloning
Plan, outline

• RFIDs
  » Concept and applications
  » EPC and backend processing
  » PHY and MAC
  » Security
• Near Field Communication

Near Field Communication (NFC)

• One device combines the functionality of
  » An RFID reader device
  » An RFID transponder (tag)
  » Bit rates ranging from 106 Kbs to 424 Kbs
• Integral part of mobile devices (e.g. mobile phones)
  NFC components can be accessed by software to
• Operates at 13.56 MHz (High frequency band)
  and is compatible to international standards:
  » ISO/IEC 18092 (also referred to as NFCIP-1),
  » ISO/IEC 14443 (smart card technology, "proximity coupling devices")
  » ISO/IEC 15693 ("vicinity coupling devices").
• Use of NFC is growing fast
  » Driven by NFC Forum (founded by Nokia, Philips, and Sony in 2004)
  » http://www.nfcworld.com/nfc-phones-list/#available

NFC Devices

Modes of operation
• Smart Card emulation (ISO 14443):
  » Phone can act as a contactless credit card
  » Information can be generated rather than pre-stored
• Reader mode
  » Allows NFC devices to access data from an object with
    an embedded RFID tag
  » Enables the user to initiate data services, i.e., retrieval of
    rich content, advertisements, ...
• Peer-to-peer (ISO 18092)
  » Allows two way communication between NFC devices
  » NFC can act as smart tag, i.e., generates information

Active and Passive Communication Modes

• Passive communication: one device acts as a
  reader and the other as a tag
  » Reader generates a field while the other responds
  » The second device can be a tag or another NFC device
• Active communication: both devices
  alternatively act as readers
  » Allows fairly general two way communication
  » Both devices must have a battery
• Since NFC devices can read and write, they
  must check for collisions
  » Compare received signal with transmitted signal
## Comparison: Main Applications

<table>
<thead>
<tr>
<th>RFID</th>
<th>NFC</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Retail</td>
<td>• Mobile payment</td>
</tr>
<tr>
<td>• Logistics</td>
<td>• Mobile ticketing</td>
</tr>
<tr>
<td>• Supply chain management</td>
<td>• Pairing of devices (esp. Bluetooth devices)</td>
</tr>
<tr>
<td>» accurate inventories</td>
<td>• Download of information from &quot;smart posters&quot;</td>
</tr>
<tr>
<td>» product safety and quality</td>
<td></td>
</tr>
</tbody>
</table>