18-759: Wireless Networks
Lecture 29: RFID

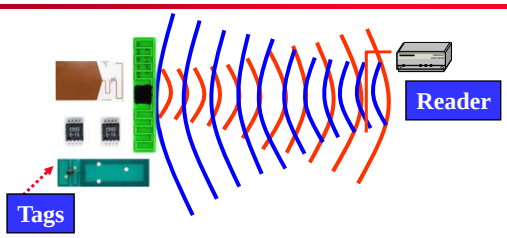
Peter Steenkiste
CS and ECE, Carnegie Mellon University

Peking University, Summer 2016

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 write 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 detect a radio frequency signal from a reader 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) that store information, which can be transmitted wirelessly in an automated fashion
- Readers (or interrogators) both stationary and hand-held read/write information from/to tags

Internet of Things

- Objects in our environment equipped with networking capabilities
- Interaction types
  - » between objects: Wireless Sensor/Actuator Networks
  - » of a user or infrastructure with a (passive) object: reader device (dedicated device or mobile phone) and RFID tags
- Requires unique addressing scheme
  - » Electronic Product Code:
    "unique across all physical objects in the world, over all time, and across all categories of physical objects"
    - – urn:epc:id:sgtin:0614141.012345.62852
      10cc Syringe #62852 (trade item)

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

Linear Bar Code

CMB
Contact Memory Button

2D Symbol
QR Code

Smart Card/CAC

OMC
Optical Memory Card

RFID - Active
Radio Frequency ID

STS
Satellite-Tracking Systems

RFID- Passive
Radio Frequency ID

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 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 inventory control
- Now used in increasingly larger set of applications

Standards

- Passive tags operate in the LF, HF, and UHF unlicensed spectrum
- Transmission consists of a bit stream and a CRC
- Many standards exist, mostly incompatible
  - » Early standards mostly defined by the ISO
- 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

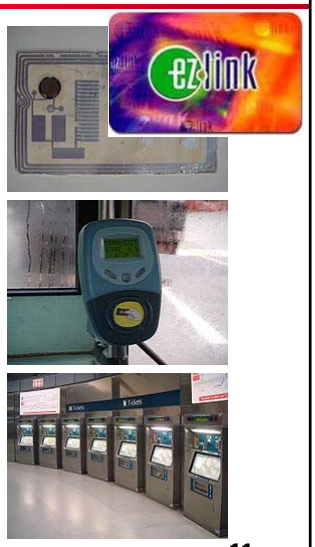
Identification and Localization

- 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)**



Example: NFC Shopping Zone

Three month trial in Seoul

- **Payments in shops**
- **Smart ordering in restaurants: tap a tag to order a drink**
- **Smart posters to download coupons and advertising information**
- **Movie ticket purchasing and ticket checking**
- **Bus timetable information and real-time service status**
- **Loyalty stamps from a store**
- **Electronic receipts delivered directly to NFC phones as a legal replacement for paper receipts**

Near Field Communication (NFC)

- Combines the functionality of
  - an RFID reader device
  - and an RFID transponder into one integrated circuit.
- Integral part of mobile devices (e.g. mobile phones), NFC components can be accessed by software to
  - act as a reading/writing device …
  - or to emulate a RFID tag.
- 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").
- Projected (2008): in 2012 20% of phones NFC enabled
  - Driven by NFC Forum (founded by Nokia, Philips, and Sony in 2004)
  - http://www.nfcworld.com/nfc-phones-list/#available

N-Mark trademark of NFC Forum

NFC Devices

Modes of operation

- Smart Card emulation (ISO 14443):
  - phone can act as a contactless credit card

Example: contactless payment applications
Sony FeliCa, Asia
MIFARE, Europe
Google Wallet

(c) Google

- Peer-to-peer (ISO 18092)
  - transfer electronic business cards between devices
- Read/Write
  - allows NFC devices to access data from an object with an embedded RFID tag
  - enables the user to initiate data services such as the retrieval of information or rich content (e.g. trailers and ring tones).

Comparison: Main Applications

RFID

- Retail
- Logistics
- Supply chain management
  - » accurate inventories
  - » product safety and quality

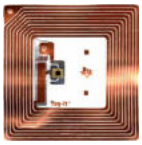
NFC

- mobile payment
- mobile ticketing
- pairing of devices (esp. Bluetooth devices)
- download of information from "smart posters"

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

What information does an RFID tag contain?



Gen 2 tags have four memory banks

Bank 0	Bank 1	Bank 2	Bank 3
Reserved Memory •32-bit Kill Password •32-bit Access Password *(64 bits)*	EPC Memory •16-bit CRC •16-bit Protocol Control •96-bit EPC *(128 bits)*	Tag Identification Memory * •8-bit Class Identifier •12-bit Tag Designer •12-bit Tag Model Number •32-bit Serial Number (optional) *(0, 32, or 64 bits)*	User Memory * •User-defined format *(0 or more bits)*

The CBP "GDTI-96" bit unique number

A 64-bit TID memory bank contains a tag serial number that uniquely identifies a tag.

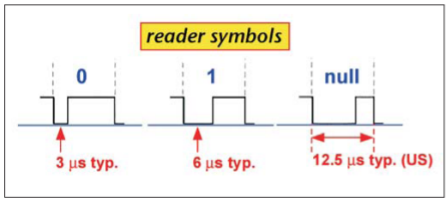
* *TID and User Memory banks are not initialized on some Gen 2 tags*

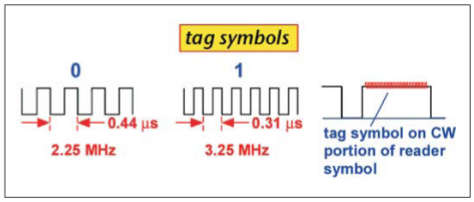
Passive RFID Tags

- **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

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

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

Binary Tree Resolution

- Send requests to tags with ids that start with a certain string
- Narrow down search until one tag responds