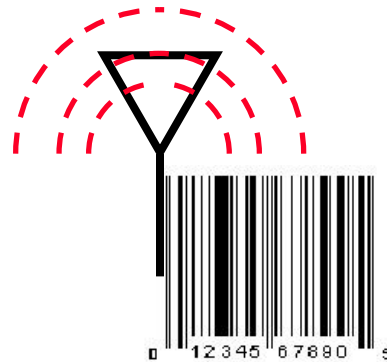


Radio Frequency Identification (RFID)



Raj Jain

Washington University in Saint Louis

Saint Louis, MO 63130

Jain@cse.wustl.edu

Audio/Video recordings of this lecture are available at:

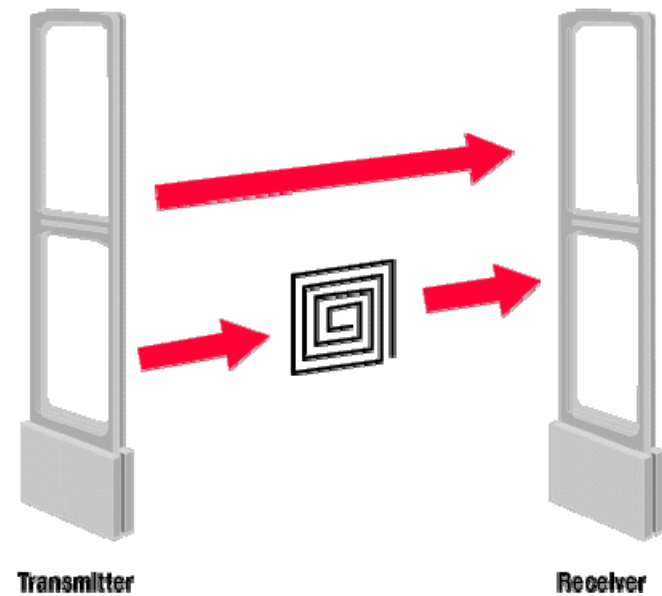
<http://www.cse.wustl.edu/~jain/cse574-08/>



- ❑ What is RFID?
- ❑ RFID: Applications
- ❑ RFID Tags and RFID Readers
- ❑ Reader-Tag Coupling
- ❑ RFID Standards
- ❑ Security Issues

What is RFID?

- ❑ Radio Frequency Identification
- ❑ Reader queries using RF, ID sends its ID using RF
- ❑ Competes with Bar Code, Magnetic stripes, Magnetic Ink Character Recognition (MICR) on Bank Checks



RFID: Applications

- ❑ Pioneered by British during World War II to identify aircrafts
- ❑ 1960's US Government started using RFID on nuclear and hazardous materials
- ❑ Garage door openers use RFID
- ❑ Implants in human, horses, fishes, animals
Animal ID Standards ISO 11784 and 11785 use RFID
- ❑ Automatic Toll Collection
- ❑ Access control, Equipment Tracking
- ❑ All shipments to DoD must be RFID tagged.
- ❑ Sensor+RFID can be used to monitor products inside sealed shipping containers

Applications (Cont)

- ❑ Warranty information on RFID tags
- ❑ Smart medical cabinets remind patients to take medications and call doctors if missed
- ❑ Retail loss prevention
- ❑ No need to unload grocery carts for checkout



RFID Tags

- ❑ Tag = Antenna, Radio receiver, radio modulator, control logic, memory and a power system
- ❑ **Power Source:**
 - **Passive Tags:** Powered by incoming RF. Smaller, cheaper, long-life. Approx range 5m.
 - **Active Tags:** Battery powered. Can be read 100 ft away.
More reliable reading.
 - **Semi-Passive tags:** Transmit using 'Backscatter' of readers' RF power. Battery for logic. Range like passive. Reliability like active.

Tags (Cont)

□ Size:

- Hitachi mu-chip is 0.4 mm on a side. Designed to be embedded in paper documents. Can be read within a few cm.
- Verichip makes tags the size of grain of rice. Designed to be implanted in humans. Identify patients.
- Semi-passive RFIDs used in E-Z Pass toll collection are paperback book size. 5-year battery.

□ Security:

- **Promiscuous Tag:** Can be read by any reader. Most tags.
- **Secure Tag:** Need reader authentication. Usually manual passwords.

Tags (Cont)

□ Components:

- Simple tags with Serial #. 96-bit block of read-only storage (ROM).
- Read-write memory.
- Tags may have embedded sensors (tire pressure sensor)

□ **Kill Feature:** Special code causes the chip to stop responding.

□ Multiple tags can interfere

⇒ Need a **singulation** protocol

⇒ Reader interrogates one tag at a time.

RFID Readers

- ❑ Sends a pulse of radio energy and listens for tags response
- ❑ Readers may be always on, e.g., toll collection system or turned on by an event, e.g., animal tracking
- ❑ Postage stamp size readers for embedding in cell phones
Larger readers are size of desktop computers
- ❑ Most RFID systems use License-exempt spectrum
- ❑ Trend towards high-frequency

Band	Frequency	λ	Classical Use
LF	125-134.2 kHz	2,400 m	Animal tagging and keyless entry
HF	13.56 MHz	22 m	
UHF	865.5-867.6 MHz (Europe) 915 MHz (USA) 950-956 MHz (Japan)	32.8 cm	Smart cards, logistics, and item management
ISM	2.4 GHz	12.5 cm	Item Management

Reader-Tag Coupling

- ❑ Passive tags have capacitor to store energy for replying (TDD)
 - Can respond on another frequency while reader is still transmitting (FDD)
- ❑ Near-Field = Within a few wavelength
Far-field = Beyond a few wavelengths
- ❑ Low-Frequency (large λ) system operate in near-field
High-Frequency and UHF system operate in far-field

1. **Inductive Coupling:** In near-field

- Both Antennas are coils (like transformers)
- Reader sends a AM/FM/PM modulated wave.
- Tag responds by varying its load on the reader.



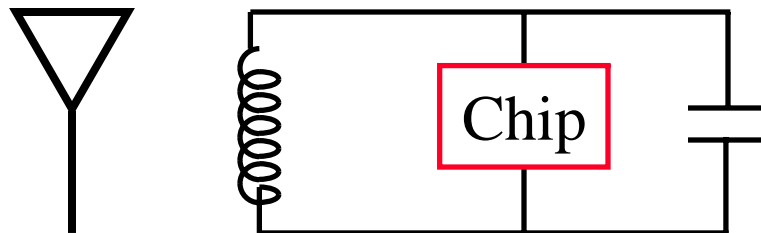
Coupling (Cont)

2. **Back Scatter:** In far-field

- Reflecting the energy back.
- Tag changes its reflection to respond.

3. **Capacitive Coupling:**

- Charged plates as antennas on readers and tags
- Can be easily printed.



RFID Range

- ❑ Reading range depends upon the transmitted power, antenna gains, frequency, reader receiver sensitivity.
- ❑ Affected by the environment: Metal objects (aluminum foil), Water (Wetness, salt water)



RFID Standards

- ❑ ISO/IEC JTC1/SC31/WG4
 - Automatic Identification and Data Capture Techniques
 - ISO (International Organization for Standardization) and
 - IEC (International Electro-Technical Commission)
 - Joint Technical Committee number one, JTC 1 (ISO/IEC)
 - Subcommittee SC 31
- ❑ Electronic Product Code (EPCGlobal) - Industry consortium
- ❑ JTC 1/SC 17 Identification Cards and related devices
- ❑ ISO TC 104 / SC 4 Identification and communication
- ❑ ISO TC 23 / SC 19 Agricultural electronics
- ❑ CEN TC 278 Road Transport and Traffic Telematics
 - Comité Européen de Normalisation
(European Committee for Standardization)

RFID Standards (Cont)

- ❑ CEN TC 23/SC 3/WG 3 Transportable Gas Cylinders - Operational Requirements - Identification of cylinders and contents
- ❑ ISO TC204 Transport Information and Control Systems
- ❑ American National Standards Institute (ANSI) X3T6: RF Identification
- ❑ European Telecommunications Standards Institute (ETSI)
- ❑ ERO European Radio communications Office (ERO)
- ❑ Universal Postal Union
- ❑ ASTM International (Testing Materials)

Security Issues

- ❑ Unauthorized Reading:
 - Competitors can scan closed boxes and find out what is inside
 - Someone can read your RFID enabled credit card
- ❑ Unauthorized Writing:
 - Can change UPC/price of an item
 - Can kill a tag
- ❑ Solution: Reader authentication.
 - Passwords can be sniffed.

Privacy

What can you do to prevent others from reading your RFID after you purchase the item?

- ❑ Kill the tag. Need authentication.
- ❑ Put the tag to sleep. Used for reusable tags. Libraries. Authentication to put to sleep and to awaken.
- ❑ Re-label: Customer can overwrite customer specific information. Manufacturer specific information can remain.
- ❑ Dual Labeling: One tag with customer specific information. One with manufacturer specific information.
- ❑ PIN: The reader needs to provide a PIN. The user can change the PIN.
- ❑ Distance-Sensitive: Tag is designed so that the information provided depends upon the distance
- ❑ Blocker: A device that generates random signal and prevents others from reading your RFIDs. Use aluminum foil.

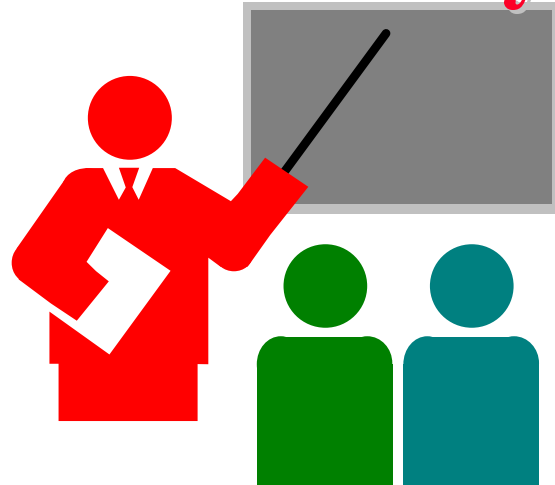
Range of Attacks

- ❑ Nominal reading range: Standard power reader
- ❑ Rogue reading range: More powerful readers can read from longer distance
- ❑ Tag-to-Reader Eavesdropping Range: Passively listen to response with a more sensitive receiver
- ❑ Reader-to-tag Eavesdropping Range: Passively listen to query with a more sensitive receiver. Can do this from very far.
- ❑ Detection Range: Can just detect the presence of a tag or a reader. Important in defense applications where important weapons or targets are tagged.

Types of Attacks

- ❑ Sniffing and eavesdropping: Passively listening with very sensitive readers. Competition can find what you are shipping/receiving
- ❑ Spoofing: Copy tag for use on other items
- ❑ Replay: Unauthorized access by recording and replaying the response. Garage door openers.
- ❑ Denial of Service: Frequency jamming
- ❑ Blocking: Aluminum foils

Summary



1. Three types: Passive, Active, Semi-Passive
2. Kill feature, secure and promiscuous tags
3. Low/High/Ultra High Frequency, ISM band
4. Near field and far field
5. Three Couplings: Inductive, Backscatter, Capacitive
6. Wireless security and privacy issues are even more severe with RFID due to limited tag capability.

Reading Assignment

- ❑ C. Jechlitschek, “A Survey Paper on RFID Trends,”
<http://www.cse.wustl.edu/~jain/cse574-06/rfid.htm>
- ❑ Introduction to Radio Frequency Identification (RFID),
<http://www.aimglobal.org/technologies/rfid/resources/RFIDPrimer.pdf>
- ❑ Radio Frequency Identification,
http://www.technology.gov/reports/2005/RFID_April.pdf
- ❑ How RFIDs Work,
<http://electronics.howstuffworks.com/smart-label.htm>
- ❑ How Anti-shoplifting Devices Work,
<http://electronics.howstuffworks.com/anti-shoplifting-device.htm>