Topical Issues: RFID

Part II

Dr Robert Harle

1 What is RFID?

What is RFID?

- Radio Frequency Identification
- An RFID tag is a device that can be identified without physical contact using electromagnetic phenomena
- Depending which newspapers/websites you read you could be forgiven for thinking RFID tags are the spawn of Satan
  - Unfortunately, the writers in the press are often rather ignorant and more than a little sensational!

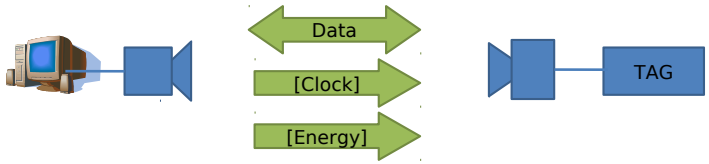
Note just how general the definition above is. Any device that uses radio to identify

itself is an RFID tag—even if it costs millions of pounds, is the size of a house and needs its own power station to run. Your phone fits that definition, along with a laptop and possibly a desktop.

Why bother?

- Lots of applications
  - **Industry**: supply chain management, personnel authorisation and tracking
  - **Individuals**: quick payments, automatic personalisation of devices and services, streamlined processes, ID
  - Internet of things
- Risks too
  - New legal challenges
  - Security concerns
  - Privacy concerns

Principles



Active: Tag is powered by its own source (battery)

Semi-active: Tag circuitry is powered by battery; comms powered by reader

Passive: Tag powered purely by reader

The broad definition of RFID means that there has to be a lot of flexibility in what is supported. So the reader might supply a clock signal, or not.

Active Tags

- Tags that have their own power source -

Disadvantages

- Not 'cool'
- Battery adds size
- Battery will run out eventually...
- Battery adds cost (harder to manufacture, more components)
- Battery adds weight

Advantages

- Reliable communications
- Better range (powered antenna)
- Better capabilities (powered processor)
- Stateful (can power memory)

An active tag is ay RFID device that requires local power identify itself. So your phone will fall into that category, as will most location systems (see the next lecture).

2 Coupling Techniques and Tag Types

2.1 Close Coupling Techniques

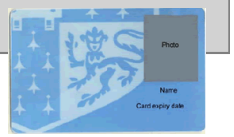
RFID Coupling

- Exactly how a reader and tag communicate depends on the coupling method in use. This is in turn determined by the intended range
- **Close**
  - Range ~1cm
  - Magnetic and capacitive coupling
- **Remote**
  - Range 1cm to 1m
  - Inductive coupling
- **Long range**
  - Range > 1m
  - Backscatter coupled

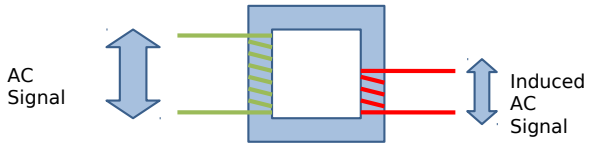
Capacitive Coupling

- Close range
- Communicate via capacitive effects between reader and tag
  - Reader and tag have conductive patches. When placed very close and parallel, the patches form a capacitor
  - Communication is possible through load modulation – one side measures the capacitance whilst the other varies the capacitance circuit to signal data
  - Need to ensure orientation so often have to *insert* card into reader
  - E.g. ISO 10536 smartcards

Magnetic Coupling



- Close range

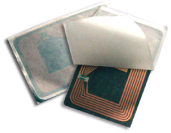


- *Ferrite core* gives good power transfer
- Tag must be put in the air gap, hence **1cm** range
- ~30MHz frequencies
- Communication possible through mutual inductance and load modulation. The tag connects/disconnects a coil to alter the induced current in the reader and transmit data

2.2 Remote Coupling Techniques

Inductive Coupling I

- Remote range



- Like magnetic, but we remove the ferrite core and the reader's magnetic flux propagates in free space
- Induces a current in the tag's coil, but much weaker than with the core. Hence power not as reliable and we can't do as much
  - E.g. usually can't support local memory

Inductive Coupling II

- Typical range is < 1m
- Range of signal frequencies used, including very low (<135kHz), but 13.56MHz the most common choice

The NFC Standard

- The big thing right now is the Near Field Communication (NFC) specification
  - This is really just a spec for an inductively coupled RFID system – 13.56MHz. In fact, NFC readers can read remote RFID tags that comply with the 13.56MHz ISO spec.
  - The standard allows for both active and passive tags
  - In reality NFC is just a rebadged remote RFID system that has been carefully designed for different applications.

NFC Security

- If you read the NFC news, you'll see they are often quoted as secure because they only have a range of a couple of cm.
- BUT the spec allows 20cm read ranges and we know it's possible to read up to 1m for inductive coupling
- Actually, it's been demonstrated that a read range of 20m is possible!
  - range depends on many factors:
    - reader's sensitivity, signal power, computational power, etc.
    - tag's orientation
- This is why most of the banking applications are still talking about needing a PIN...

2.3 Long Range Coupling Techniques

Back Scatter Coupling I

- Long Range
  - To exceed 1m without very specialist equipment we need to consider far-field EM waves
    - UHF (100s of MHz)
    - Microwave (GHz)
  - But radio transmitters kill batteries fast
    - And we don't even have a battery!
    - Use backscattering...

Back Scatter Coupling II

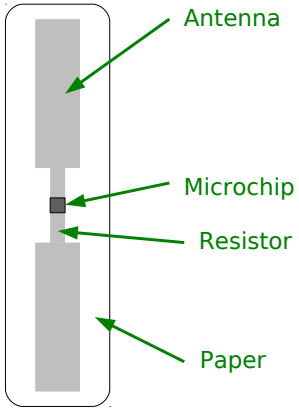
- The reader sends out a signal that hits the tag and induces a current
  - it siphons some power off for a chip
  - *reflects* the rest to act as a communication medium

Back Scatter Coupling III

- So each tag has a unique identifier
- When instructed by the reader, it spits out the serial number by encoding it on the reflected signal by switching its impedance (load modulation again).
- More advanced tags may support a small number of other commands such as “shut up” or “get data” (if the tag is advanced enough to carry extra data)

Back Scatter Coupling IV

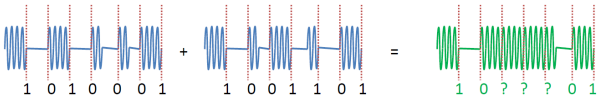
- Tags up to 3GHz exist (most use 900MHz)
- There isn't much to a tag so they can be very cheap (pennies or fractions of pennies in real bulk)
- Read ranges are usually around **3m** (10m for high powered directional antennas)
- Depends on environment and reader power



3 Finding Tags

Tag Enumeration ("Singulation")

- Most common task is to find all the tags that are within range.
- Since the tags use the same incident signal to 'talk', they all end up talking at the same time
- First trick is to use manchester encoding to spot the collisions



- This tells us the bit positions where collisions occur

Binary Tree Walking

- To actually enumerate, we usually use binary tree walking

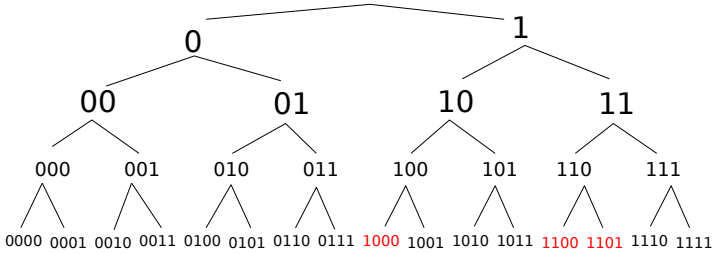
1. Request that all tags identify themselves
2. Detect collisions in the response
3. Now walk over a binary tree to figure out the collision bits

- All we need is a special reader command: **[REQ|bbbb]** : all tags with an ID less than bbbb (i.e. binary integer) should reply

This technique is also known as 'silent tree walking'.

Example

Tags: 1000 1100 1101



Here's another example: tags 111, 000, 101, 110. If we send out a query we get back

XXX (collisions in every position). So we explore the largest leftmost tree: i.e. 0??. This gets us one reply: 000—one tag found.

Now we explore the other tree: 1??. We get back 1XX, so we explore the left tree: 10?. We get back 101—second tag found.

Continue to explore the right tree: 11?. We get back 11X so we know both 110 and 111 are present—third and fourth tags found.

4 Long Range Tag Realities

Radio Power

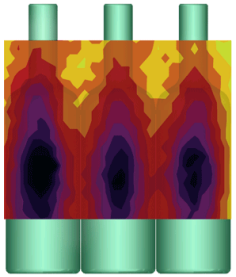
- A radio signal has to travel to the tag, and then back (having also lost power in the reflection) so we have to start with something quite powerful at the reader
- In fact, today's readers pump out as much as 4W of radio power
  - Wifi base stations are restricted to 100mW
  - A GSM 1800MHz phone handset is restricted to 1W
  - A DECT handset is restricted to 250mW
  - And these are peak powers (on average DECT produces 10mW); RFID readers have a constant power output...
  - *This might all be perfectly safe but it's not 100% clear - any volunteers to test?*

Radio Nulls

- Signals in real environments bounce around. A bounced signal can easily interfere with a direct signal
  - If the interference is destructive, the overall magnitude of signal at that point falls
  - We find lots of nulls, where there is no signal strength at all
  - Moving fractions of the wavelength can take us to a maximum
  - RFID at 800MHz has a wavelength of 37.5cm, so nulls come and go quickly, even when we expect a strong signal near the transmitter!

Interference

- An attached object can affect the quality of the tag response. The image below shows responses measured at the Auto-ID research labs in Cambridge
- Passive tags were attached to cases of wine at various points (three bottles illustrated)
  - Yellow – good response
  - Black – little or no response
- Factor of four in the read distance depending on position of tag!
- A difference in tag position of just 1cm can halve the read range..!



Orientation

- It turns out that the orientation of the inexpensive passive tags strongly affects the strength of the reflected beam to the reader

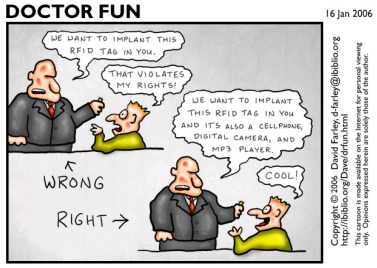
> *"Tag orientation also impacts read range. Whenever possible, try to vertically orient dipole tag antennas. Horizontal orientations are prone to miss-reads..."*
>
> *Alien whitepaper.*

- This means a random assortment of tagged items (as per a shopping trolley) is very unlikely to be read 100% and this can be serious
  - Who is responsible if you walk out with a 50" plasma and the system misses the tag..?
  - For some apps you can control the orientation (e.g. baggage in airports or on palettes of goods).
    - Reports suggest 99% accuracy possible with lots of fine tuning
    - What about that other 1%..!

RFID in Use...

Privacy

- The press always concentrate on the privacy implications (perhaps rightly)
- RFID tags are not like wifi-enabled laptops: they're limited in capabilities, meaning many standard crypto solutions are out.
- There have been some suggestions for how to address the issue...

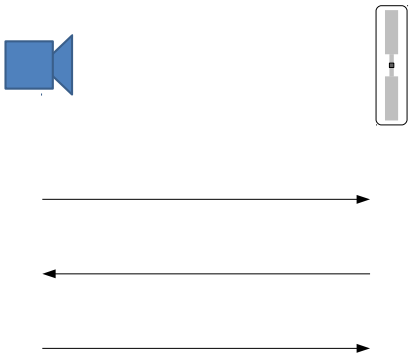


Kill Command!

- Classic solution: implement a tag command that results in self-destruction (burn out the radio circuit or similar)
- AutoID Center [sic] did this – you supplied a hardcoded password to fry your tag.
- Dramatically reduces the user benefits of the technology!

Hash-lock

- Allows the reader to authenticate to the tag



The idea is that a tag has a default 'locked' where it will only responds to one command (an ID request). The basic protocol here is:

1. Tag ID, k, not stored on the tag, but rather h(k) where h() is a one-way hash function
2. Reader receives h(k) and looks up the value of k
3. Reader transmits k to tag, which computes h(k) to verify it and is then 'unlocked' i.e. will respond to other commands

Of course, this does nothing for an attacker that just wants to know which tag is there (h(k) is just as good as k as an identifier), but at least prevents them from arbitrarily accessing more sensitive data on the tag. Unfortunately nothing stops an attacker from listening in on a valid transaction and getting the info that way!

Selective Blocker Tag

- Remember our binary tree walk to enumerate tags? The technique has a tag that responds with collisions (i.e. sends both a 0 and a 1) for certain pars of the tree
- E.g. set up a tag such that it sends 0000XXX. This prevents a reader from finding any tags in the subtree represented by the last three bits

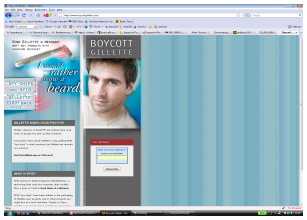
5 Deployments

Walmart

- **2003** – Walmart announces 100 top suppliers will use RFID tags to tag pallets by Jan 2005. All at own cost – not popular.
- **2007** – Wall street journal suggests that the pilot isn't going too smoothly. Walmart denies.
- **2007** – Walmart announces change of focus. Now only tracking specific items for specific parts of distribution.
- **2009** – Proctor & Gamble pull out, implying that Walmart is not doing what it should with the RFID info
- Overall, not that clear how successful, although one study suggests that RFID reduces the number of out-of-stock items on the shelves by 16%.

Gillette

- Gillette order 500 million tags from Alien for Mach 3 blades. Aim: Keep the shelves stacked with their latest product. Initial target Walmart.
- Tested in Tesco in Cambridge, UK. Guardian headline: “Tesco Tests Spy Chip Technology”. Turns out they hid a small camera and used the RFID to detect when someone picked up a razor (apparently Gillette razors are top of the thieving list).
- Abandoned after protests. www.boycottgillette.com still exists



6 Conclusions

Conclusions

- RFID is really an umbrella-term for many related technologies
- The applications have/can/will change the world
- BUT don't always believe the hype!