RADIO-FREQUENCY IDENTIFICATION (RFID)

Definitions

Radio-frequency identification (RFID) is an automatic identification method, relying on storing and remotely retrieving data using devices called **RFID tags** or transponders.

An **RFID tag** is an object that can be applied to or incorporated into a product, animal, or person for the purpose of identification using radiowaves.

Basics

Radio-frequency identification (RFID) is a technology that is a replacement for the barcode. The technology is used for automatically identifying a package or an item. To do this, it relies on RFID tags. These are small transponders that can transmit static information over a short distance, when they are asked to. The other piece to make use of RFID tags is an RFID tag reader.

An RFID tag is an object that can be applied to or incorporated into a product, animal, or person for the purpose of identification and tracking using radio waves. Some tags can be read from several meters away and beyond the line of sight of the reader.

Most RFID tags contain at least two parts. One is an integrated circuit for storing and processing information, modulating and demodulating a radio-frequency (RF) signal, and other specialized functions. The second is an antenna for receiving and transmitting the signal.

There are generally two types of RFID tags: active RFID tags, which contain a battery, and passive RFID tags, which have no battery.

Uses

RFID systems are used for the following:

- General Logistics, tracking a package, parcel; replacing barcodes
- Tracking vehicles for road pricing
- Many countries have started using RFID chips in passports
- Making products harder to falsify; currently proposed for drugs
- Tags in clothing, eg. in Jeans
- Sealing for containers (for the shipping industry). Not required yet.
- Identifying animals; used for tracking pets, but also for reasrch, eg. on turtles.
- Keys for vehicles. The vehicle key has an RFID tag inside; only the key with the right RFID tag can start the vehicle (this makes copying vehicle keys harder). Also used for locking/unlocking vehicles from a distance.

- Contactless smartcards, for example to regulate entry into certain areas; also used for ticketing, or public transport

Topics of Interest

Radio-frequency identification (RFID) is an automatic identification method, relying on storing and remotely retrieving data using devices called RFID tags or transponders.

An RFID tag is an object that can be applied to or incorporated into a product, animal, or person for the purpose of identification using radiowaves. Some tags can be read from several meters away and beyond the line of sight of the reader.

Most RFID tags contain at least two parts. One is an integrated circuit for storing and processing information, modulating and demodulating a (RF) signal and can also be used for other specialized functions. The second is an antenna for receiving and transmitting the signal. A technology called chipless RFID allows for discrete identification of tags without an integrated circuit, thereby allowing tags to be printed directly onto assets at lower cost than traditional tags.

Today, a significant thrust in RFID use is in enterprise supply chain management, improving the efficiency of inventory tracking and management. However, a threat is looming that the current growth and adoption in enterprise supply chain market will not be sustainable. A fair cost-sharing mechanism, rational motives and justified returns from RFID technology investments are the key ingredients to achieve long-term and sustainable RFID technology adoption.

History of RFID tags

In 1946 Léon Theremin invented an espionage tool for the Soviet Union which retransmitted incident radio waves with audio information. Sound waves vibrated a diaphragm which slightly altered the shape of the resonator, which modulated the reflected radio frequency. Even though this device was a passive covert listening device, not an identification tag, it has been attributed as the first known device and a predecessor to RFID technology. The technology used in RFID has been around since the early 1920s according to one source (although the same source states that RFID systems have been around just since the late 1960s).

A similar technology, such as the IFF transponder invented by the United Kingdom in 1939, was routinely used by the allies in World War II to identify airplanes as friend or foe. Transponders are still used by military and commercial aircraft to this day.

Another early work exploring RFID is the landmark 1948 paper by Harry Stockman, titled "Communication by Means of Reflected Power" (Proceedings of the IRE, pp 1196–1204, October 1948). Stockman predicted that "…considerable research and development work has to be done before the remaining basic problems in reflected-power communication are solved, and before the field of useful applications is explored."

Mario Cardullo's U.S. Patent 3,713,148 in 1973 was the first true ancestor of modern RFID; a passive radio transponder with memory. The initial device was passive, powered by the interrogating signal, and was

demonstrated in 1971 to the New York Port Authority and other potential users and consisted of a transponder with 16 bit memory for use as a toll device. The basic Cardullo patent covers the use of RF, sound and light as transmission medium. The original business plan presented to investors in 1969 showed uses in transportation (automotive vehicle identification, automatic toll system, electronic license plate, electronic manifest, vehicle routing, vehicle performance monitoring), banking (electronic check book, electronic credit card), security (personnel identification, automatic gates, surveillance) and medical (identification, patient history).

A very early demonstration of reflected power (modulated backscatter) RFID tags, both passive and semi-passive, was done by Steven Depp, Alfred Koelle and Robert Freyman at the Los Alamos Scientific Laboratory in 1973. The portable system operated at 915 MHz and used 12 bit tags. This technique is used by the majority of today's UHF and microwave RFID tags.

The first patent to be associated with the abbreviation RFID was granted to Charles Walton in 1983 (U.S. Patent 4,384,288).

RFID tags

RFID tags come in three general varieties: passive, active, or semi-passive (also known as battery-assisted). Passive tags require no internal power source, thus being pure passive devices (they are only active when a reader is nearby to power them), whereas semi-passive and active tags require a power source, usually a small battery.

To communicate, tags respond to queries generating signals that must not create interference with the readers, as arriving signals can be very weak and must be told apart. Besides backscattering, load modulation techniques can be used to manipulate the reader's field. Typically, backscatter is used in the far field, whereas load modulation applies in the nearfield, within a few wavelengths from the reader.

Passive RFID tags have no internal power supply. The minute electrical current is induced in the antenna by the incoming radio frequency signal,it provides just enough power for the CMOS integrated circuit in the tag to power up and transmit a response. Most passive tags signal by backscattering the carrier wave from the reader. This means that the antenna has to be designed to both collect power from the incoming signal and also to transmit the outbound backscatter signal. The response of a passive RFID tag is not necessarily just an ID number; the tag chip can contain non-volatile, possibly writable EEPROM for storing data.

Unlike passive RFID tags, **active RFID tags** have their own internal power source, which is used to power the integrated circuits and broadcast the signal to the reader. Active tags are typically much more reliable (i.e. fewer errors) than passive tags due to the ability for active tags to conduct a "session" with a reader. Active tags, due to their onboard power supply, also transmit at higher power levels than passive tags, allowing them to be more effective in "RF challenged" environments like water (including humans/cattle, which are mostly water), metal (shipping containers, vehicles), or at longer distances, generating strong responses from weak requests (as opposed to passive tags, which work the other way around). In turn, they are generally bigger and more expensive to manufacture, and their potential shelf life is much shorter.

Semi-passive tags are similar to active tags in that they have their own power source, but the battery only

powers the microchip and does not broadcast a signal. The RF energy is reflected back to the reader like a passive tag. An alternative use for the battery is to store energy from the reader to emit a response in the future, usually by means of backscattering.

The **antenna** used for an RFID tag is affected by the intended application and the frequency of operation. Low-frequency (LF) passive tags are normally inductively coupled, and because the voltage induced is proportional to frequency, many coil turns are needed to produce enough voltage to operate an integrated circuit. Compact LF tags, like glass-encapsulated tags used in animal and human identification, use a multilayer coil (3 layers of 100–150 turns each) wrapped around a ferrite core.

Current uses passports, transportation payments, product tracking, animal identification.

Potential uses: replacing barcodes, telemetry (remote measurement and reporting of information), patient identification.

Cancer risk On September 8, 2007, veterinary and toxicology studies spanning the last ten years surfaced indicating that RFID chips induced malignant tumors in laboratory animals. The U.S. Food and Drug Administration, the agency that approved the use of the chips in the United States, refused to respond to questions from the media about their awareness of the studies. VeriChip Corp. maintains that the chips are completely safe and that they were unaware of the studies. The studies were somewhat limited in scope, lacking control groups that did not receive chips and failing to test large animals such as dogs, cats, or primates. As a result, most of the studies included cautionary language against making assumptions about the chips causing cancer in humans based on the study results.

Security concerns: A primary security concern surrounding technology is the illicit tracking of RFID tags. Tags which are world-readable pose a risk to both personal location privacy and corporate/military security. Such concerns have been raised with respect to the United States Department of Defense's recent adoption of RFID tags for supply chain management. More generally, privacy organizations have expressed concerns in the context of ongoing efforts to embed electronic product code (EPC) RFID tags in consumer products.

Viruses: Ars Technica Reported in March 2006 an RFID buffer overflow bug that could infect airport terminal RFID Databases for baggage, and also Passport databases to obtain confidential information on the passport holder.

Passports: In an effort to make passports more secure, several countries have implemented RFID in passports. However, the encryption on UK chips was broken in under 48 hours. Since that incident, further efforts have allowed researchers to clone passport data while the passport is being mailed to its owner. Where before a criminal had to secretly open and then reseal the envelope, now it can be done without detection, adding some degree of insecurity to the passport system.

Protection against RFID interception: Various methods can be used to protect against RFID data interception:

RFID shielding: A number of products are available on the market in the US that will allow a concerned carrier of RFID-enabled cards or passports to shield their data. In fact the United States government

requires their new employee ID cards to be delivered with an approved shielding sleeve or holder. There are contradicting opinions as to whether aluminum can prevent reading of RFID chips. Some people claim that aluminum shielding, essentially creating a Faraday cage, does work. Others claim that simply wrapping an RFID card in aluminum foil, only makes transmission more difficult, yet is not completely effective at preventing it.

Privacy

How would you like it if, for instance, one day you realized your underwear was reporting on your whereabouts? — California State Senator Debra Bowen, at a 2003 hearing.

The use of RFID technology has engendered considerable controversy and even product boycotts by consumer privacy advocates such as Katherine Albrecht and Liz McIntyre of CASPIAN who refer to RFID tags as "spychips". The two main privacy concerns regarding RFID are:

- If a tagged item is paid for by credit card or in conjunction with use of a loyalty card, then it would be possible to indirectly deduce the identity of the purchaser by reading the globally unique ID of that item (contained in the RFID tag).

Source : http://www.juliantrubin.com/encyclopedia/electronics/rfid.html