ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/3437143

An introduction to RFID technology

Article *in* IEEE Pervasive Computing · February 2006

DOI: 10.1109/MPRV.2006.2 · Source: IEEE Xplore

CITATIONS
1,705

READS
36,908

1 author:

Roy Want
Google Inc.

144 PUBLICATIONS **18,240** CITATIONS

SEE PROFILE

All content following this page was uploaded by Roy Want on 15 August 2015.

The user has requested enhancement of the downloaded file.

HANSHOW-Ex. 1028
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

An Introduction to RFID Technology

RFID is at a critical price point that could enable its large-scale adoption. What strengths are pushing it forward? What technical challenges and privacy concerns must we still address?

Roy Want
Intel Research

In recent years, radio frequency identification technology has moved from obscurity into mainstream applications that help speed the handling of manufactured goods and materials. RFID enables identification from a distance, and unlike earlier bar-code technology (see the sidebar), it does so without requiring a line of sight.[1] RFID tags (see figure 1) support a larger set of unique IDs than bar codes and can incorporate additional data such as manufacturer, product type, and even measure environmental factors such as temperature. Furthermore, RFID systems can discern many different tags located in the same general area without human assistance. In contrast, consider a supermarket checkout counter, where you must orient each bar-coded item toward a reader before scanning it.

So why has it taken over 50 years for this technology to become mainstream? The primary reason is cost. For electronic identification technologies to compete with the rock-bottom pricing of printed symbols, they must either be equally low-cost or provide enough added value for an organization to recover the cost elsewhere. RFID isn't as cheap as traditional labeling technologies, but it does offer added value and is now at a critical price point that could enable its large-scale adoption for managing consumer retail goods. Here I introduce the principles of RFID, discuss its primary technologies and applications, and review the challenges organizations will face in deploying this technology.

About the Review Process

This article was reviewed and accepted before Roy Want became *IEEE Pervasive Computing*'s editor in chief. It went through our standard peer-review process and was accepted 28 Nov. 2005. —*M. Satyanarayanan*

RFID principles

Many types of RFID exist, but at the highest level, we can divide RFID devices into two classes: *active* and *passive*. Active tags require a power source—they're either connected to a powered infrastructure or use energy stored in an integrated battery. In the latter case, a tag's lifetime is limited by the stored energy, balanced against the number of read operations the device must undergo. One example of an active tag is the transponder attached to an aircraft that identifies its national origin. Another example is a LoJack device attached to a car, which incorporates cellular technology and a GPS to locate the car if stolen.

However, batteries make the cost, size, and lifetime of active tags impractical for the retail trade. Passive RFID is of interest because the tags don't require batteries or maintenance. The tags also have an indefinite operational life and are small enough to fit into a practical adhesive label. A passive tag consists of three parts: an antenna, a semi-

HANSHOW-Ex. 1028
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

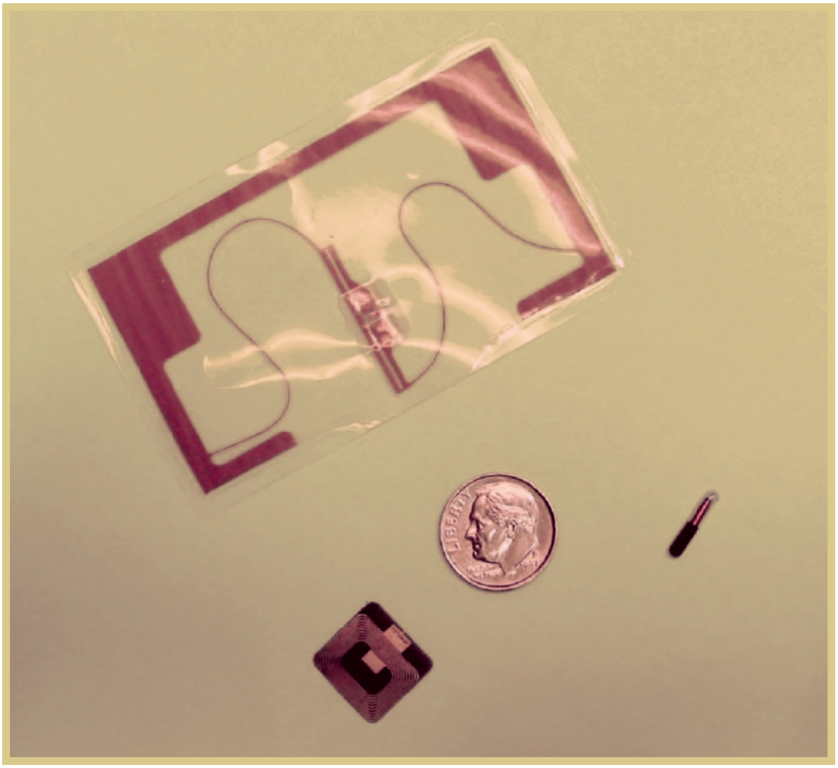


Figure 1. Three different RFID tags—they come in all shapes and sizes.

conductor chip attached to the antenna, and some form of encapsulation.

The tag reader is responsible for powering and communicating with a tag. The tag antenna captures energy and transfers the tag's ID (the tag's chip coordinates this process). The encapsulation maintains the tag's integrity and protects the antenna and chip from environmental conditions or reagents. The encapsulation could be a small glass vial (see figure 2a) or a laminar plastic substrate with adhesive on one side to enable easy attachment to goods (see figure 2b).

Two fundamentally different RFID design approaches exist for transferring power from the reader to the tag: magnetic induction and electromagnetic (EM) wave capture. These two designs take advantage of the EM properties associated with an RF antenna—the *near field* and the *far field*. Both can transfer enough power to a remote tag to sustain its operation—typically between 10 μW and 1 mW, depending on the tag type. (For comparison, the nominal power an Intel XScale processor consumes is approximately 500 mW, and an Intel Pentium 4 consumes up to 50 W.) Through various modulation techniques, near- and far-field-based signals can also transmit and receive data.[1]

RFID: From Obscurity to Wal-Mart

Ever since the advent of large-scale manufacturing, rapid identification techniques have helped speed the handling of goods and materials. Historically, printed labels—a simple, cost-effective technology—have been the staple of the manufacturing industry. In the 1970s, labeling made a giant leap forward with the introduction of Universal Product Code bar codes, which helped automate and standardize the identification process. Bar codes are also cheap to produce, but they have many limitations. They require a clear line of sight between the reader and tag, can be obscured by grease and nearby objects, and are hard to read in sunlight or when printed on some substrates. RFID is an alternative labeling technology that has also been around for decades.

The British employed RFID principles in World War II to identify their aircraft using the IFF (Identification Friend or Foe) system. In the 1960s, Los Alamos National Laboratory carried out work more closely related to modern RFID in its effort to explore access control. It incorporated RFID tags into employee badges to automatically identify people, limit access to secure areas, and make it harder to forge the badges. Niche domains have also used RFID in various applications, such as to identify animals, label airline luggage, time marathon runners, make toys interactive, prevent theft, and locate lost items.

Regardless of these applications, RFID technology remained relatively obscure for many years. Now, however, three major organizations are pioneering its large-scale adoption: Wal-Mart, Tesco, and the US Department of Defense. Each aims to offer more competitive pricing by using RFID to lower operational costs by streamlining the tracking of stock, sales, and orders. When used in combination with computerized databases and inventory control, linked through digital communication networks across a global set of locations, RFID can pinpoint individual items as they move between factories, warehouses, vehicles, and stores.

HANSHOW-Ex. 1028
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

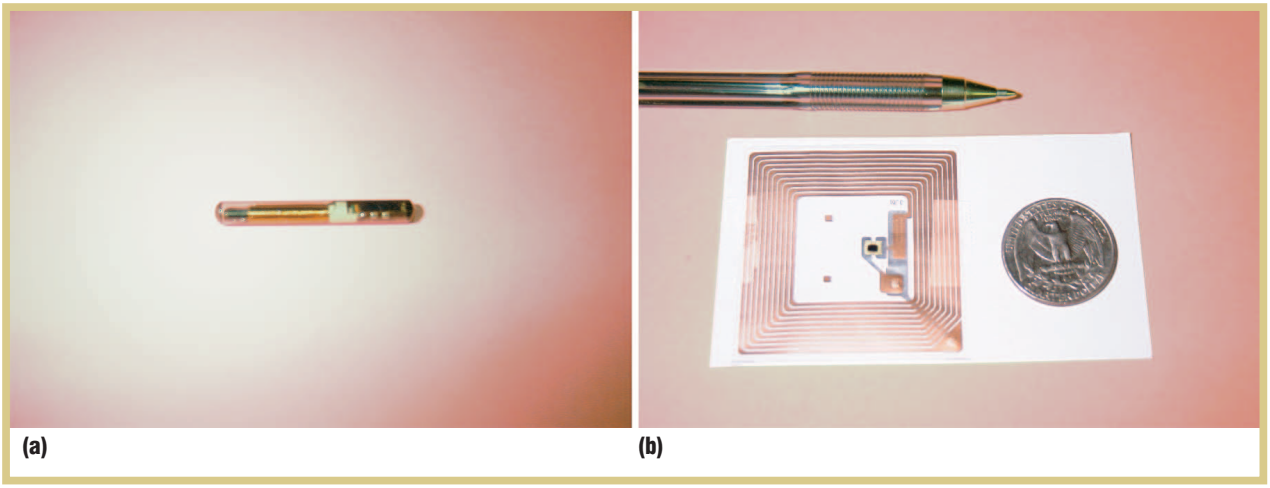


Figure 2. RFID tags based on near-field coupling: (a) a 128 kHz Trovan tag, encapsulated in a small glass vial that's approximately 1 cm long and (b) a 13.56 MHz Tiris tag (www.ti.com/rfid), which has a laminar plastic substrate (approximately 5 × 5 cm) with adhesive for easy attachment to goods.

Near-field RFID

Faraday's principle of magnetic induction is the basis of near-field coupling between a reader and tag. A reader passes a large alternating current through a reading coil, resulting in an alternating magnetic field in its locality. If you place a tag that incorporates a smaller coil (see figure 3) in this field, an alternating voltage will appear across it. If this voltage is rectified and coupled to a capacitor, a reservoir of charge accumulates, which you can then use to power the tag chip.

Tags that use near-field coupling send data back to the reader using *load modulation*. Because any current drawn from the tag coil will give rise to its own small magnetic field—which will oppose the reader's field—the reader coil can detect this as a small increase in current flowing through it. This current is proportional to the load applied to the tag's coil (hence load modulation).

This is the same principle used in power transformers found in most homes today—although usually a transformer's primary and secondary coil are wound closely together to ensure efficient power transfer. However, as the magnetic field extends beyond the primary coil, a secondary coil can still acquire some of the energy at a distance, similar to a reader and a tag. Thus, if the tag's electronics applies a load to its own antenna coil and varies it over time, a signal can be encoded as tiny variations in the magnetic field strength representing the tag's ID. The reader can then recover this signal by monitoring the change in current through the reader coil. A variety of modulation encodings are possible depending on the number of ID bits required, the data transfer rate, and additional redundancy bits placed in the code to remove errors resulting from noise in the communication channel.

Near-field coupling is the most straightforward approach for implementing a passive RFID system. This is why it was the first approach taken and has resulted in many subsequent standards, such as ISO 15693 and 14443, and a variety of proprietary solutions. However, near-field communication has some physical limitations.

The range for which we can use magnetic induction approximates to $c/2\pi f$, where c is a constant (the speed of light) and f is the frequency. Thus, as the frequency of operation increases, the distance over which near-field coupling can operate decreases. A further limitation is the energy available for induction as a function of distance from the reader coil. The magnetic field drops off at a factor of $1/r^3$, where r is the separation of the tag and reader, along a center line perpendicular to the coil's plane. So, as applications require more ID bits as well as discrimination between multiple tags in the same locality for a fixed read time, each tag requires a higher data rate and thus a higher operating frequency. These design pressures have led to new passive RFID designs based on far-field communication.

Far-field RFID

RFID tags based on far-field emissions (see figure 4) capture EM waves propagating from a dipole antenna attached to the reader. A smaller dipole antenna in the tag receives this energy as an alternating potential difference that appears across the arms of the dipole. A diode can rectify this potential and link it to a capacitor, which will result in an accumulation of energy in order to power its electronics. However, unlike the inductive designs, the tags are beyond the range of the reader's near field, and information can't be transmitted back to the reader using load modulation.

The technique designers use for commercial far-field RFID tags is *back scattering* (see figure 5). If they design an

HANSHOW-Ex. 1028
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

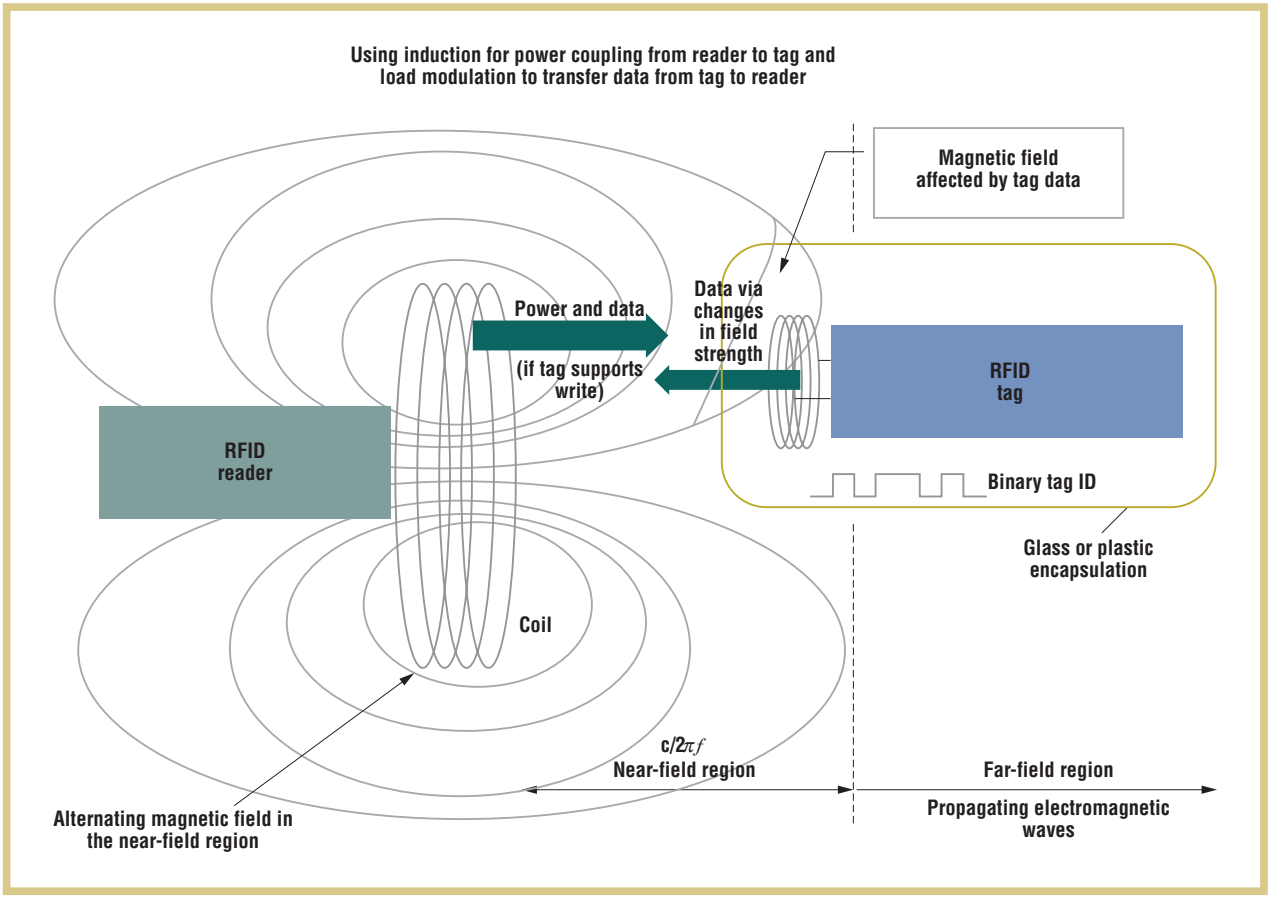
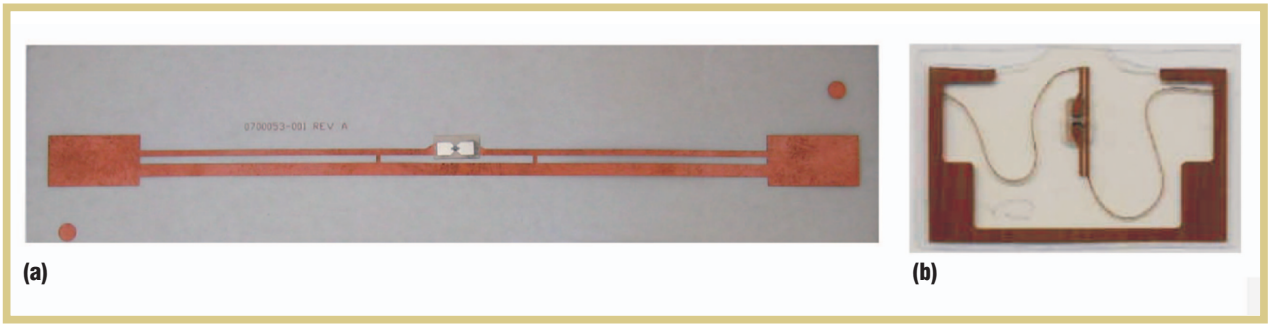


Figure 3. Near-field power/communication mechanism for RFID tags operating at less than 100 MHz.

antenna with precise dimensions, it can be tuned to a particular frequency and absorb most of the energy that reaches it at that frequency. However, if an impedance mismatch occurs at this frequency, the antenna will reflect back some of the energy (as tiny waves) toward the reader, which can then detect the energy using a sensitive radio receiver. By changing the antenna's impedance over time, the tag can reflect back more or less of the incoming signal in a pattern that encodes the tag's ID.

In practice, you can detune a tag's antenna for this purpose by placing a transistor across its dipole and then turning it partially on and off. As a rough design guide, tags that use far-field principles operate at greater than 100 MHz typically in the ultra high-frequency (UHF) band (such as 2.45 GHz); below

Figure 4. RFID tags based on far-field coupling: (a) a 900-MHz Alien tag (16 × 1 cm) and (b) a 2.45-GHz Alien tag (8 × 5 cm).



HANSHOW-Ex. 1028
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

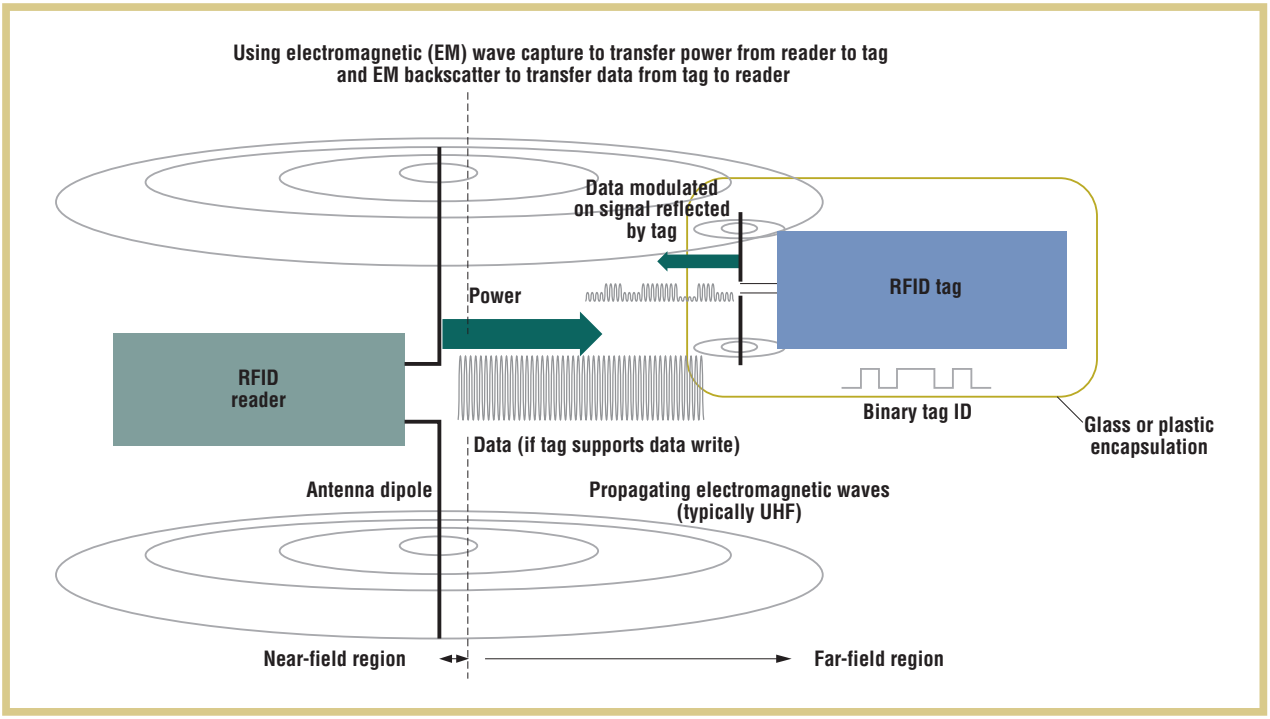


Figure 5. Far-field power/communication mechanism for RFID tags operating at greater than 100 MHz.

this frequency is the domain of RFID based on near-field coupling.

A far-field system's range is limited by the amount of energy that reaches the tag from the reader and by how sensitive the reader's radio receiver is to the reflected signal. The actual return signal is very small, because it's the result of two attenuations, each based on an inverse square law—the first attenuation occurs as EM waves radiate from the reader to the tag, and the second when reflected waves travel back from the tag to the reader. Thus the returning energy is $1/r^4$ (again, r is the separation of the tag and reader).

Fortunately, thanks to Moore's law and the shrinking feature size of semiconductor manufacturing, the energy required to power a tag at a given frequency continues to decrease (currently as low as a few microwatts). So, with modern semiconductors, we can design tags that can be read at increasingly greater distances than were possible a few years ago. Furthermore, inexpensive radio receivers have been developed with improved sensitivity so they can now detect signals, for a reasonable cost, with power levels on the order of –100 dBm in the 2.4-GHz band. A typical far-field reader can successfully interrogate tags 3 m away, and some RFID companies claim their products have read ranges of up to 6 m.

EPCglobal's work was key to promoting the design of UHF tags (see www.epcglobalinc.org), which has been the basis of RFID trials at both Wal-Mart and Tesco (see the sidebar for more information about the trials). EPCglobal was originally the MIT Auto-ID Center, a nonprofit organization set up by the MIT Media Lab. The center later divided into Auto-ID labs, still part of MIT, and EPCglobal, a commercial company. This company has defined an extensible range of tag standards, but its Class-1 Generation-1 96-bit tag is the one receiving the most attention of late. This tag can label over 50 quadrillion (50×10^{15}) items, making it possible to uniquely label every manufactured item for the foreseeable future—not just using generic product codes. This isn't necessary for basic inventory control, but it has implications for tracing manufacturing faults and stolen goods and for detecting forgery. It also offers the more controversial post-sale marketing opportunities, enabling direct marketing based on prior purchases. (I discuss the related privacy concerns later on.)

Adopting a standard: The Near-Field Communication Forum

An important recent development opens up new possibilities for more widespread RFID applications. Since 2002, Philips has pioneered an open standard through EMCA International, resulting in the Near-Field Communication Forum (www.nfc-forum.org). The forum sets out to integrate active signaling between mobile devices using near-field coupling, and it uses an approach that is compatible with reading existing passive RFID products. The new NFC standard aims to provide a mechanism by which wireless mobile devices can

HANSHOW-Ex. 1028
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

communicate with peer devices in the immediate locality (up to 20 cm), rather than rely on the discovery mechanisms of popular short-range radio standards. These standards, such as Bluetooth and Wi-Fi, have unpredictable propagation characteristics and might form associations with devices that aren't local.

The NFC standard aims to streamline the discovery process by passing wireless Media Access Control addresses and channel-encryption keys between radios through a near-field coupling side channel, which, when limited to 20 cm, lets users enforce their own physical security for encryption key exchange. The forum deliberately designed the NFC standard to be compatible with ISO 15693 RFID tags operating in the 13.56-MHz band. It also allows mobile devices to read this already popular tag standard and to be compatible with the FeliCa and Mifare smart card standards, widely used in Japan.

In 2004, Nokia announced the 3200 GSM cell phone, which incorporates an NFC reader (see figure 6). Although the company hasn't published an extensive list of potential applications, the phone can make electronic payments (similar to a smart card) and place calls based on the RFID tags it encounters. For example, you could place your phone near an RFID tag attached to a taxi-stand sign, and your phone would call the taxi company's coordinator to request a taxi at that location.[2] This model offers a close link between the virtual representations within a computer's memory, such as the positions of taxis being tracked by the dispatch computer, and the physical world, such as signs and people with cell phones. Furthermore, it is a key enabling technology for implementing Mark Weiser's vision of ubiquitous and pervasive computing.[3]

A complication for broad adoption of the NFC standard is that state-of-the-art EPCglobal RFID tags are based on far-field communication techniques, working at UHF frequencies. Unfortunately, NFC and EPCglobal standards are fundamentally incompatible.

Figure 6. The Nokia 3200 cell phone features a Near Field Communications reader. From the front, it looks like an ordinary cell phone, but on the back, you can see the reader coil molded into the housing. (figure courtesy of Nokia)

Reading colocated tags

One commercial objective of RFID systems is to read, and charge for, all tagged goods in a standard supermarket shopping cart as it is pushed through an instrumented checkout aisle. Such a system would speed up the checkout process and reduce operational costs.

Even if the RF reading environment for an RFID tag is ideal, it's still an engineering challenge to support multiple colocated tags. Consider two tags situated next to each other and equidistant from the reader. On hearing the reader's signal, both would acquire enough power to turn on and transmit a response back to the reader, resulting in a collision. The data from both tags would be superimposed and garbled.

In CSMA (carrier sense multiple access)-based communication networks, such as Ethernet, this is an old problem that an anticollision protocol can resolve. In its simplest form, the protocol inserts a random delay between the beginning of the interrogation signal and the tag's response. But a collision might still occur, so the reader must initiate several rounds of interrogation until it hears all the tags in that area with high probability. The number of rounds used, number of tags present, and duration of each tag reply can be used to calculate the probability of all tags being detected. By modifying the number of rounds, we can adjust the probability to suit typical operation conditions. We can further enhance this protocol by preventing tags that have already been heard by the reader from responding on the next round until the current interrogation cycle ends.

Using another anticollision approach, the EPCglobal class-1 standard implements an algorithm based on a Query Tree protocol. The reader starts an interrogation cycle by asking which of the ID space's top branches (modeled as a binary tree) contain tags. The algorithm recursively repeats for each subtree branch, but if a particular subtree doesn't generate a reply, the reader won't consider any of its branches and subtrees in the remaining search space. In other words, that branch is pruned from the binary tree. After a short time, all tags present will respond to the reader in depth-first-search order. EPCglobal systems using this anticollision algorithm can potentially read 500 colocated tags per second.

Enabling a distributed memory revolution

Another distinguishing feature of modern RFID is that tags can contain far more information than a simple ID. They can incorporate additional read-only or read-write memory, which a reader can then further interact with.

Read-only memory might contain additional product details that don't need to be read every time a tag is interrogated but are available when required.

HANSHOW-Ex. 1028
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

For example, the tag memory might contain a batch code, so if some products are found to be faulty, the code can help find other items with the same defects.

Tag memory can also be used to enable tags to store self-describing information. Although a tag's unique ID can be used to recover its records in an online database, communication with the database might not always be possible. For example, if a package is misdirected during transportation, the receiving organization might not be able to determine its correct destination. Additional destination information written into the tag would obviate the need and cost of a fully networked tracking system.

Other RFID applications take advantage of read-write memory available in some tag types. Although the size of these memories is currently small—typically 200 to 8,000 bits—it's likely to grow in the future and be used in creative ways. These tags could lead to a distributed memory capability embedded in our surroundings. If locations in a city were tagged with RFID,[4] a reader could write messages directly into the tag. This might be used for historical data or for updates about nearby services.

Additionally, tags in commercial products could contain ownership history. For example, a tag attached to secondhand consumer goods might tell you about the previous owners and when and where the product changed hands. This is similar to the providence documentation that often accompanies antiques of value; using RFID to extend this kind of tracking to everyday items could provide consumers with greater confidence in their secondhand purchases.

Time stamps can also be stored in an RFID memory alongside other data that has been written there. For example, if two writes occur sequentially but separated in time, the second write must have occurred after the first write. If a reader were trying to forge the writing time of the second write, the first write at least constrains when the forgery has occurred to after the first time stamp. Unfortunately, passive RFID doesn't have the continuous power needed to support an onboard clock, so time stamps couldn't be derived from the tag itself. However, the readers—powered from the infrastructure or from batteries in a handheld unit—could contain an electronic clock and write time stamps alongside other data written into the tag.

Another application of RFID sensing is in relation to perishable goods. An RFID temperature sensor could both identify goods and ensure they remain within a safe temperature range.

RFID that incorporates sensing

One of the most intriguing aspects of modern RFID tags is that they can convey information that extends beyond data stored in an internal memory and include data that onboard sensors created dynamically.[5] Commercial versions of RFID technology can already ensure that critical environmental parameters haven't been exceeded. For example, if you drop a package on the floor, the impact might have damaged the enclosed product. A passive force sensor can supply a single bit of information that can be returned along with an RFID tag's ID, alerting the system about the problem.

Another application of RFID sensing is in relation to perishable goods. Typically, items such as meat, fruit, and dairy products shouldn't exceed a critical temperature during transportation or they won't be safe for consumption. An RFID temperature sensor could both identify goods and ensure they remain within a safe temperature range. The KSW TempSens RFID tag was designed explicitly for this purpose (see www.ksw-microtec.de/www/startseite_en.php).

Antitamper product packaging is another application domain for RFID sensing. Most modern consumable products are protected by a packaging technology that clearly shows customers if the product has been tampered with. A simple binary switch (sensor) can be incorporated into an RFID tag, perhaps a thin loop of wire extending from the tag through the packaging and back to the tag. If tampering occurs, the wire breaks and shows up as a tamper bit when the tag is read during checkout. In this way, a store can ensure that it only purveys tamper-free items. Furthermore, at each point in the supply chain, you can check individual products for tamper activity, making it easier to find the culprits.

Privacy concerns

RFID has received much attention in recent years as journalists, technologists, and privacy advocates have debated the ethics of its use. Privacy advocates are concerned that even though many of the corporations considering RFID use for inventory tracking have honorable intentions, without due care, the technology might be unwittingly used to create undesirable outcomes for many customers.

The inherent problem is that radio-based technologies interact through invisible communication channels, so we don't know when communication is occurring. Consider a clothing store that labels its garments with RFID tags. From the store's perspective, this improves

HANSHOW-Ex. 1028
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

inventory stock checks, because employees can quickly catalog the contents of various racks and bins, even when customers have mixed up the clothes. Also, employees can perform fast periodic stock checks to detect thefts, which isn't usually an easy task.

However, if the store fails to remove a tag at the point of purchase, it's possible to track customers every time they wear the tagged clothing. Vendors—including vendors other than the original seller—could learn where the customer shops to better target the person with direct-marketing techniques. Even more troubling, a criminal might track consumers, judging their wealth based on purchases, possibly targeting them for theft.

Although the potential for RFID misuse is high, undesirable scenarios can be turned into potentially useful ones. For example, if clothes were tagged, washing machine manufacturers could integrate RFID readers into the doors of their machines, making them aware of all items selected for washing. The machines could then choose the appropriate washing cycle and possibly warn you about incompatible garments that might result in color runs.

The current focus, however, remains on the potential for misuse. A growing cloud of public and media concern forced Benetton, a well-known clothing store, to hastily retreat after it announced plans to use RFID tags in its stores.[6] Concern also surfaced when the US government announced plans to put RFID tags into passports to make them easier to check at borders and harder to forge. Privacy advocates argued that covert readers might steal the information, enabling identity theft.[7] The passport scheme is still going forward, but the government is modifying its implementation to address public concerns.

EPCglobal has addressed some of these concerns by designing a *kill switch* in their tags that lets vendors permanently disable a tag at the point of sale. Vendors then wouldn't have to remove the tag itself, which might be woven into a garment and (deliberately) difficult to remove. Of course, concerns still exist that vendors might become complacent and that not all stores would be vigilant about disabling the tags. An insidious number of tags could still become part of our daily activities, which could later be exploited for criminal purposes.

RSA's proposed solution is the concept of a *blocker tag*[8]—a modified RFID tag that takes advantage of EPCglobal's anticollision protocol. The blocker tag responds to each interrogation such that it appears that all possible tag IDs are present, so the reader has no idea what tags are actually nearby. Perhaps having simple countermeasures to prevent tag misuse is exactly what we need to overcome privacy concerns.

The press and civil libertarians have raised some genuine concerns, so it's important that we proceed cautiously to incorporate safeguards that address the potential for RFID misuse.

Remaining challenges

Three main issues are holding back RFID's widespread adoption, the first of which is cost. Although RFID tags are now potentially available at prices as low as 13 cents each, this is still much more expensive than printed labels. (As of September 2005, Alien Technologies (www.alientechnology.com) could supply RFID tags for 12.9 cents each in quantities of 1 million.)

Market analysts can't agree on the price tipping point—will it be a 10-cent, 5-cent, or 1-cent tag? Consider a 50-cent candy bar—if you replace a bar code (which costs nothing because you can print it on the wrapper) with a 10-cent RFID tag, then you might not have any remaining profit. Consequently, RFID tags are likely to have their first deployments with high-profit items. Of course, when adoption does take hold, it could rapidly accelerate as mass production drives down prices.

Another important issue is design. We still need to engineer tags and readers so that they guarantee highly reliable identification. The solutions must be resilient to all tag orientations, packaging materials, and checkout configurations found in typical stores. Improved tag antenna design can solve some of these issues. Tag readers can also be designed to exhibit antenna diversity by multiplexing their signals between several antenna modules mounted in orthogonal orientations, or by coordinating multiple readers. In the latter case, we must avoid the *reader collision problem*,[9] as interrogation signals will interfere with each other. A strict time division scheme would allow multiple readers to be deployed.

The final issue is acceptance. The press and civil libertarians have raised some genuine concerns, so it's important that we proceed cautiously to incorporate safeguards that address the potential for RFID misuse. In 2003, Simson Garfinkel proposed "An RFID Bill of Rights,"[10] which laid down a set of guidelines that retailers should adhere to in order to protect citizens' rights. Currently, no laws regulate tag use, and legislation might be required to assure the public. In the meantime, early adopters such as Wal-Mart and Tesco could help defuse concerns by publicly adopting a similar proposal.

HANSHOW-Ex. 1028
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

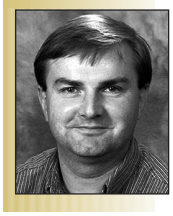
Despite these challenges, RFID continues to make inroads into inventory control systems, and it's only a matter of time before the component costs fall low enough to make RFID an attractive economic proposition. Furthermore, extensive engineering efforts are under way to overcome current technical limitations and to build accurate and reliable tag-reading systems. We might also start to see economic pressure from the larger distributors to modify product packaging and its associated materials to more effectively integrate RFID. Finally, at this delicate stage, while major corporations are trialing the technology, media reaction and outspoken privacy groups can influence the rules by which we use the technology. Given that legislation is now in place among most of the developed countries to protect our personal information held in computers at banks and other organizations, there is no reason why RFID data management can't acquire a similar code of conduct.

RFID's potential benefits are large, and we're sure to see many novel applications in the future—some of which we can't even begin to imagine. P

REFERENCES

1. K. Finkelzeller, *The RFID Handbook*, 2nd ed., John Wiley & Sons, 2003.
2. R. Want et al., "Bridging Real and Virtual Worlds with Electronic Tags," *Proc. ACM SIGCHI*, ACM Press, 1999, pp. 370–377.
3. M. Weiser, "The Computer for the 21st Century," *Scientific Am.*, vol. 265, no. 3, 1991, pp. 94–104.
4. T. Kindberg et al., "People, Places, and Things: Web Presence of the Real World," *ACM Mobile Networks & Applications J.*, 2002, pp. 365–376.
5. R. Want, "Enabling Ubiquitous Sensing with RFID," *Computer*, vol. 37, no. 4, 2004, pp. 84–86.
6. E. Batista, "'Step Back' for Wireless ID Tech?" *Wired News*, 8 Apr. 2003; www.wired.com/news/wireless/0,1382,58385,00.html.
7. R. Singel, "American Passports to Get Chipped," *Wired News*, 19 Oct. 2004; www.wired.com/news/privacy/0,1848,65412,00.html.
8. A. Juels, R.L. Rivest, and M. Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy," *Proc. 8th ACM Conf. Computer and Comm. Security*, ACM Press, 2003, pp. 103–111.
9. D.W. Engels and S.E. Sarma, "The Reader Collision Problem," white paper MIT-AUTOID-WH-007, Auto-ID Center, Nov. 2001.
10. S. Garfinkel, "An RFID Bill of Rights," *Technology Rev.*, Oct. 2002, p. 35.

the AUTHOR



Roy Want is a principal engineer at Intel Research in Santa Clara, California, and leader of the Ubiquity Strategic Research Project. His research interests include proactive computing, ubiquitous computing, wireless protocols, hardware design, embedded systems, distributed systems, automatic identification, and microelectromechanical systems. He received his PhD for his work on "reliable management of voice in a distributed system" from Cambridge University. He is a Fellow of the IEEE and ACM. Contact him at Intel Corp., 2200 Mission College Blvd., Santa Clara, CA 95052; roy.want@intel.com.

For more information on this or any other computing topic, please visit our Digital Library at www.computer.org/publications/dlib.

View publication stats

HANSHOW-Ex. 1028
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189