A world of connections

Apr 26th 2007
From The Economist print edition

Belle Mellor

New wireless technologies will link not just people but lots of objects too. That will be tremendously useful, says Kenneth Cukier (interviewed here); but getting there will be tricky

THE radio is 110 years old this year and the microprocessor just under 50. As these two technologies move ever closer together, with wireless capabilities now being put on computer chips, something exciting is happening. All the benefits of the computing world—innovation, short development cycles and low cost—are being extended to wireless communications. As a result, a myriad of hitherto separate objects are becoming connected to networks, from televisions and cars to industrial machinery and farmland. Tiny devices are even being placed into the human body to perform useful tasks. The new technology enables control to be exercised from a distance and lets different devices interconnect to do something new.

So far the mobile phone has been getting all the attention. Around 2.8 billion are already in use, with a further 1.6m being added every day. The phones themselves are improving at a cracking pace. Yet this boom is also spilling over into other areas of wireless communications, used for linking machines, sensors and objects. “Everybody talks about the emerging markets being the big opportunity for the cellular industry in the next few years, but in the longer run there are going to be a lot more devices talking to each other,” says Paul Jacobs, the boss of Qualcomm, which makes mobile-phone chips.

This year around 10 billion microprocessors will be sold, embedded in anything from computers to coffee-makers. The vast majority of them will be able to “think” but not “talk”: they will perform specific tasks but cannot communicate. But this is now starting to change. The cost, size and power requirements of wireless functions are falling rapidly, so some unlikely candidates are now being connected to networks. For example, bridges and buildings are being monitored for structural integrity by small sensors. Farmland is being watched and irrigation systems are being switched on and off remotely.

In years to come, wireless communications will increasingly become part of the fabric of everyday life. David Clark, a computer scientist at the Massachusetts Institute of Technology who helped develop the internet, believes that in 15 or 20 years' time the network will need to accommodate a trillion devices, most of them wireless. To illustrate what that world might be like, Robert Poor, the co-founder of two wireless companies, Adozu and Ember, uses a modest example: light fixtures in buildings. If every one of them contained a small wireless node, people would not only be able to control the lighting more effectively but put them to many other uses too. If the nodes were programmed to serve as online smoke detectors, they could signal a fire as well as show its location. They could also act as a security system or provide internet connectivity to other things in the building.

Such applications are already being developed. For instance, Philips, an electronics firm, plans to introduce wirelessly controlled lighting systems for commercial buildings in around five years' time. And its researchers are working on making networked light fittings capable of monitoring the objects throughout a building, tracking equipment in hospitals or preventing theft in offices.

These ideas have been floating around for years, variously known as “ubiquitous computing”, “embedded networking” and “the pervasive internet”. The phenomenon “could well dwarf previous milestones in the information revolution”, according to a 2001 report entitled “Embedded, Everywhere” by America's National Research Council, part of the respected National Academy of Sciences. A report by a United Nations agency in 2005 called it “The Internet of Things”.

But now it is actually starting to happen. Even governments have taken notice. Japan and South Korea have incorporated wireless technology into national policies, their sprawling IT conglomerates marching in lockstep with the political leaders. The European Union and America (where defence money paid for many of the advances) have issued thick reports.

For all the excitement, it will be a while before machine-to-machine (M2M) communications and sensor networks become ubiquitous. Although the technology exists, different approaches do not as yet work well together. Unlike computer software, which can be deployed with a few mouse-clicks, each system still needs to be tailor-made. And the melding of communications and computing brings together two industries and engineering cultures that are generally at odds, slowing progress. Moreover, the business models to justify the time and cost of adding wireless services are embryonic.

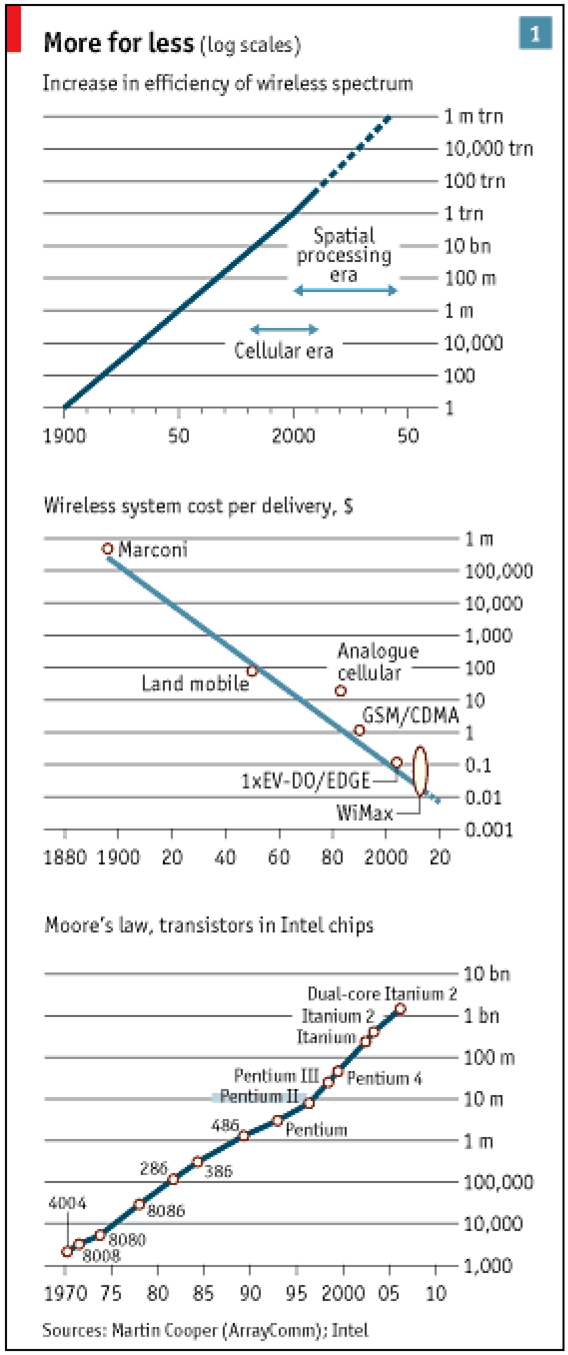
Still, the general direction is clear. In the years ahead new wireless technologies will appear in a plethora of devices, much as computer chips did in the second half of the 20th century. This survey will explain how this will come about, and why it will not be easy.

Marconi's brainwave

Apr 26th 2007
From The Economist print edition

Wireless technology is advancing by leaps and bounds—and there is much more to come

WHEN Guglielmo Marconi was granted patents on his “wireless telegraph” in 1897, the future of his invention looked modest. At the time radio signals could travel only a few kilometres, and only one receiver and transmitter could operate in any one area. Since 1900 “spectrum efficiency”—the amount of information that can travel over the same portion of radio waves—has improved perhaps a trillion times, estimates Martin Cooper of ArrayComm, who is hailed as the father of the mobile phone (see chart 1).



The invention of the transistor in 1947 and the microprocessor (which integrated transistors and other things onto a single chip) in 1958 changed the way radios function. The microprocessor helped to get rid of crystals, copper coils and vacuum tubes, putting the ingredients of a radio almost entirely on silicon. This costs less to make, takes up less space, consumes less power, makes the radio perform better and allows it to work more smoothly with the other electronics inside the device.

Innovation happens quickly. The processing power of chips doubles about every two years, according to Moore's law, named after Gordon Moore, a co-founder of Intel, the world's biggest chip company. As the billions of transistors on the chips get smaller, there is more room to add extra functions. Such chips do not just go faster, they also do more, and the cost of integrating new functions is relatively low.

Many of the functions of such chips are controlled by software, which means they can be continually upgraded at little cost. Moreover, chip technology has not only improved the performance and cost of the radio itself but other parts of the system too, from “smart” antennae to advanced power management for longer battery life. As a result, the cost of wireless communications has plummeted.

The mobile-phone industry has both benefited from these developments and spurred them on. The industry as a whole—including handset-makers, software developers, network operators and so on—is reckoned to have revenues of around $1 trillion a year, according to Informa, a market-research firm. Traffic volume is soaring. By 2011 perhaps 4 billion people will be carrying a mobile phone.

Connecting things rather than people is far less advanced. Sales of wireless modules for devices, sensors and machines this year are forecast to reach a mere 33m, though they are expected to grow rapidly, to around 400m in 2011, according to Harbor Research. By then revenues for hardware and services, now $48 billion, may have grown to $200 billion—still a far cry from the mobile-phone industry.

Yet wireless communications in these areas are advancing rapidly at a time when the mobile-phone industry is approaching saturation point in rich countries and the average revenue per user is sagging. And they hold a lot of promise: there are far more things than people that can be wirelessly linked, from doors and windows to machines and trees.

Just as a milestone was reached in 1998 when the volume of global internet traffic through America overtook voice traffic, so a turning point will come when devices connected to the network overtake people, whether in number, bandwidth or calls. This may happen sooner than expected.

Stratton Scalvos, the boss of VeriSign, which operates part of the internet's address system, notes that around 12% of address traffic involves computers linking to other computers, without a person at either end. John Roese, the chief technology officer of Nortel, a telecoms-equipment vendor, expects the amount of machine-to-machine communication to pull ahead of human calls and web clicks some time between 2009 and 2011 as cameras, cars, utility meters, home security systems and the like continuously send data across the network. Vivek Ranadivé, the boss of Tibco, a software developer for corporate IT systems, says the number of computer transactions automatically started by other computers is already higher than that initiated by people.

Oddly enough, it is the success of mobile phones that has fuelled the rise of wireless communications among objects rather than people, promoting innovation and bringing down prices. Take Texas Instruments, which leads the market for chips in mobile phones on the GSM standard. In 2003 it began work on a single low-cost radio chip that included support for a digital music player, FM stereo radio, camera and colour display with a longer battery life. A prototype was built in 2004 and bulk production began in 2006. In the fourth quarter of last year alone the firm shipped 10m of these chips. The chips have dropped from $50 apiece to around $5, and a phone that would have cost $250 five years ago is now $25. But rather than become even cheaper, in future the chips will offer more features, says Greg Delagi, who heads TI's wireless unit.

Belle Mellor

Engineers have been able to apply such innovations and economies of scale to other wireless technologies. As a result, some radio chips—for example, those used for the Global Positioning System, say, or for Bluetooth wireless communications—now cost as little as $1 and are the size of a matchhead. Chips with a newer technology called Zigbee, used for short-range sensors, which currently cost around $4 and are the size of a fingernail, are expected to shrink down to a quarter of the price and size in five years. A far simpler kind of chip called a radio-frequency identification (RFID) tag, which sends a tiny quantity of data over a short range when activated, can already be manufactured for 4 cents apiece. Hitachi has a prototype chip that fits into the groove of a thumb-print. Last year 1 billion RFID chips were sold; this year the number may rise to 1.7 billion, according to IDTechEx, a consultancy.

All this means that many formerly self-contained things have become capable of communicating. For example, most big logistics companies in America and Europe now track their fleets with a combination of satellites and mobile-phone networks. Small wireless sensors monitoring equipment in large factories can provide early warning of impending breakdown. They can run on energy “harvested” from the heat or vibrations of the machinery.

Let device talk unto device

Apple's iPod and Nike's running shoes can interconnect so that the music player can select songs that match the jogger's pace. Large organisations such as retailers, hospitals and the armed forces are using RFID tags for managing stock levels. More robust versions of the technology are deployed in “contactless” bank cards, passports and public-transport passes.

Yet this is only the start. And although many of the initial technologies were championed by America's defence industry—which gave life to the internet in the 1970s—the most interesting applications are emerging in the private sector (again, as with the internet). Regulators are helping things along. Both Europe and America are considering proposals for fitting all cars with equipment that will automatically call the emergency services in the event of an accident. Some countries now require utility companies to read meters more regularly to promote energy conservation, giving a boost to wireless connections. Makers of medical devices are offering more home-monitoring products. And mobile operators are spending huge sums to upgrade their networks for high-speed access—and are looking for new sources of traffic for them.

One of the most important consequences of these new wireless technologies will be to increase visibility and accountability, says Jiro Kokuryo of Keio University in Japan. Economists today treat many items as indirect costs because there is no way to attribute the use of a resource to a particular individual. Wireless communications can change this, he says, by making it possible to base things like road tolls and car-insurance premiums on people's actual driving patterns. But that also raises privacy concerns on a far larger scale than hitherto.

Will the fridge really want to talk to the kettle? Probably not. But that is a detail. Wireless technology is akin to the electrical grid, which was originally intended for a particular use, the light bulb, but whose “killer application” turned out to be the power socket that allowed a multitude of new and unforeseen devices to draw energy from it. In time, the new wireless technologies will likewise reshape society in unpredictable ways.

On the radio

Apr 26th 2007
From The Economist print edition

Wireless takes many forms

RADIOS work by using the electromagnetic spectrum to send information. When an electrical current travels through a wire it creates an electromagnetic field, sending out waves in all directions—rather like light, which is also a part of the spectrum but at much higher frequencies. An antenna and extra power allow the signal to be transmitted over long distances. The frequency of the wave can be changed so that signals do not interfere with one another,
allowing more of the spectrum to be used.

Radio waves exist in nature, from sound and light to cosmic rays in space. The man-made sort can do things like transmit music or heat food in a microwave. At the low end of the spectrum are the frequencies used for things like television and mobile phones. The lower the frequency of the wave, the farther it can travel or penetrate physical objects. Thus FM radio at relatively high frequencies is used for local stations but does not travel far, whereas short-wave radio, at low frequencies, can stretch around the world.

Speaking in tongues 2

Main two-way wireless technologies*

	Data rate per second	Range	Cost†
Mobile WiMax	15Mb	5km	$8 in 2008
3G cellular (HSDPA/LTE)	14Mb	10km	$6
2G cellular (GSM/CDMA)	400k	35km	$5
Wi-Fi	54Mb	50-100m	$4
Bluetooth	700k	10m	$1
Zigbee	250k	30m	$4
UWB	~400Mb	5-10m	$5
RFID	1-200k	0.01-10m	4 cents

*Typical performance; actual figures vary
†Approx. device-chip cost at high volume

Sources: William Webb; Cambridge Consultants; OECD; Pyramid Research; Nokia; TI; CSR; Ember; Hitachi

Wireless technology can be split into five main sorts, roughly ranked by the distance that the signals travel. The top travellers are satellite communications such as the Global Positioning System (GPS). This is a constellation of 24 satellites, managed by the American armed forces, that constantly send out signals to devices on the ground. But the signals travel only one way, from satellite to device.

A little closer to home, and with signals going both ways, are “wide-area” mobile-phone technologies such as GSM or CDMA. Advanced “third-generation” (3G) versions include HSDPA and LTE, developed by the mobile-phone industry. A promising rival is WiMax, based on the internet standard and supported by the computer industry. A third category takes in shorter-range signals used to connect things in a building or room. Examples include the popular Wi-Fi standard to access the internet in hotels or airports, and Zigbee to link sensors. A new advance is ultra-wideband (UWB) technology, which uses very high frequencies at very short range to transmit huge amounts of data, as in sending video from an iPod-like device to a TV screen.

A fourth type connects things in a “personal-area network” or PAN. An example is Bluetooth, which is used to link mobile phones with earpieces. The last is near-field communications (NFC), where contact needs to be close, as in passes for buildings and public transport. A variant is radio-frequency identification (RFID) tags, used by retailers and others. When passed in front of a reader, the tags send back data stored on them. These radio systems are as different from each other as light is from sound, so satellites cannot track RFID tags, for instance. This means that some privacy worries are misplaced.

Radio has been cramming ever more information into the transmission, using techniques such as spreading it across the spectrum, dividing it up into portions and using “smart” antennae. As radio increasingly moves onto microchips, “software-defined radios” will be able to switch standards and frequencies as they go.

The proliferation of wireless systems has pushed up the demand for spectrum and increased its value. There are hopes that “cognitive” radios may eventually alleviate the problem by sharing huge swaths of spectrum intelligently—but they have yet to be invented.

Overcoming hang-ups

Apr 26th 2007
From The Economist print edition

Belle Mellor

Mobile operators have more high-speed networks than they know what to do with

FROM a glass office on the 32nd floor of Samsung's R&D centre, an hour's drive from Seoul, the site of a huge property development known as “Ubiquitous City” is visible in the distance. Soon its grey concrete foundations will sprout a set of ultra-modern apartment blocks where everything is connected and controlled online. Samsung executives are proud of it because it ties together much of what their company is involved in, from home appliances and consumer electronics to mobile communications. Many other South Korean firms are also taking part, encouraged by the government. Joo Sik Lee, the head of new-business development at SK Telecom, the country's largest mobile operator, explains why such projects are so important. “Everyone already has a mobile phone,” he says. “We have to find new business models and new uses.”

SK Telecom has introduced mobile-payment technology and is experimenting with health-monitoring devices. It is adding RFID readers to its phones so people can get information about products. It is even co-ordinating activities with its parent company's construction arm to add wireless automation to around 120,000 homes in South Korea this year. For a monthly subscription of about $5 this will enable residents to check their thermostat, security system and fire alarm and switch their lights on and off from afar.

In Japan similar projects are under way. Tests are in progress on cars with wireless systems that will prevent collisions—seen as the next great innovation that will bring together the country's cherished IT and car industries. A private school in Tokyo has put wireless beacons on children's backpacks to keep track of where they are. At the Mitsukoshi department store in the chic Ginza district, RFID tags on cosmetics by Shiseido provide shoppers with more information about the products.

So far these sorts of wireless systems are relatively basic, admits Kazuo Murano, the president of Fujitsu Laboratories. But they mark the beginning of a new infrastructure that can be extended to many uses, just as new software on a PC enables it to do new things.

The enthusiasm for new wireless technologies in parts of Asia is mirrored in Europe and America. Mobile operators are investing billions of dollars in building new networks that provide fast internet access. 3G systems are being upgraded and an upstart technology called WiMax is being explored. Many executives hope that this will connect not just people and their phones but also gadgets, machines, pets, cars and homes.

But many problems remain to be resolved. There is no telling whether there will be any demand for such services because the technology is not yet in place, and nobody knows how to charge for such things. Cyber-security is a huge headache. And many of the uses envisaged involve short-range communications, such as dimming a light or transferring a video from one medium to another, that may never make use of the mobile network at all.

Worst of all, a world in which devices can join the network, do as they please while they are connected and leave again at will (like PCs logged on to the internet) runs counter to the telecoms industry's culture. It prefers to control customers' activities, both to ensure quality of service and to keep rates high. The same “walled garden” approach that prevents people from using Skype (a web-based telephone service) on their mobiles also ensures that they remain free of viruses. For the moment the vast majority of revenue comes from voice calls. As call rates drop, operators hope to make up their income by providing music and videos to the handsets.

Yet some mobile operators are trying to change their business models. Sprint Nextel's chief technology officer, Barry West, imagines a world in which someone who buys a television or washing machine from any shop and plugs it in can connect it to Sprint's network. The network itself will be open to the internet and users will be able to do what they like, rather than being funnelled to content providers with which the operator has a business relationship, as happens with most mobiles today. Mr West will be able to provide such freedom because he plans to change the way customers pay for his company's service. Instead of charging for every bit of communication—a call over a particular distance for a particular duration—he will use flat-rate pricing, the way that people pay for internet service.

A clever pipe

Will that not turn his wireless network into a “dumb pipe”, a mere commodity? “It's absolutely not dumb,” he insists. Sprint intends to charge a premium for special services, just as airlines charge more for a business-class seat, he says. Moreover, he plans to sell much of the information he has about his customers to advertisers. So, for example, interactive billboards at a bus stop may be tailored to young mothers at one moment and beer-guzzling sports fans the next. “We're migrating from a telecoms company to a media company,” he says.

Sprint is the first mobile operator to come up with a plan of action for a wireless internet world. Yet all operators are feeling the pressure of the internet. There is plenty of evidence that customers want to control their phones as they do their PCs, by adding new software, and pay for service at a flat rate as they do for the internet.

Pricing is critical. In Europe the average monthly airtime per user is under 250 minutes; in America it is more than 1,000. The most likely reason for the difference is the charging structure. When Japan's NTT DoCoMo introduced a flat fee for sending data such as photos from a phone, its network traffic was said to have risen many times over within days. Many people in America and Europe take pictures with their mobiles, but very few send them to other people because they are worried or uncertain about the cost. Sprint hopes to woo customers by simplifying the price and providing open internet access.

Sprint's business model echoes the internet approach in other ways too. For its new network the company chose WiMax, a technology that is supported by the computer industry, notably Intel, rather than by traditional telecoms vendors. WiMax uses the internet protocol to provide smooth online access, unlike mobile networks that carry the traffic over other protocols developed for phone calls. “If you try to use a phone or BlackBerry to access the web, it is a trying experience today at best,” grouses Paul Otellini, Intel's boss.

Industry experts argue over whether WiMax works better than enhanced 3G cellular systems, but most reckon that their performance will end up much the same. The difference is in the way the equipment is made and sold, notes Vanu Bose, the founder of Vanu, a wireless firm. The computing industry likes open standards so that any device can be replaced by any other, whereas the telecoms sector has long benefited from locking customers in with proprietary standards. And sometimes pieces of kit from different makers do not work smoothly together.

WiMax does away with this problem by establishing a standard that puts everyone on an equal footing. The hope is that this will bring costs down to a commodity level for wireless gear, just as it did for computers. The royalties that firms will need to pay to license the intellectual property is expected to be lower than at present. ABI Research estimates that just four firms own almost 60% of the patents in 3G technology, pushing licensing rates as high as 28.5% of the cost of the equipment. WiMax's patent pool is more evenly distributed among more firms, and rates are expected to be around 5%.

The network provider will not subsidise customers' devices, as mobile operators do at present to entice people into signing on for a year's subscription. So WiMax not only lowers operators' costs; it changes their approach to business. The problem is that it has barely got off the ground. Networks are still at the trial stage and mass-market devices are not expected until 2008.

For all the industry's lofty visions, it must confront uncomfortable realities. For instance, Samsung and LG, another big South Korean conglomerate, more often link their appliances with cables and power lines than with wireless technology. And for all the wizardry of SK Telecom's home-automation system, people in trials do not seem to use it much. The operator is considering bundling the service free with online entertainment packages. Even “Ubiquitous City,” some executives admit, is more hype than reality.

This is not the first time that the industry's plans have been delayed. In the lead-up to the 3G spectrum auctions in Europe in 2000, some carriers thought that linking machines and devices would account for around 12% of their revenue, notes David Benello of McKinsey, a consultancy. But in the event the industry decided to concentrate on people and phones, not factories and farm equipment.

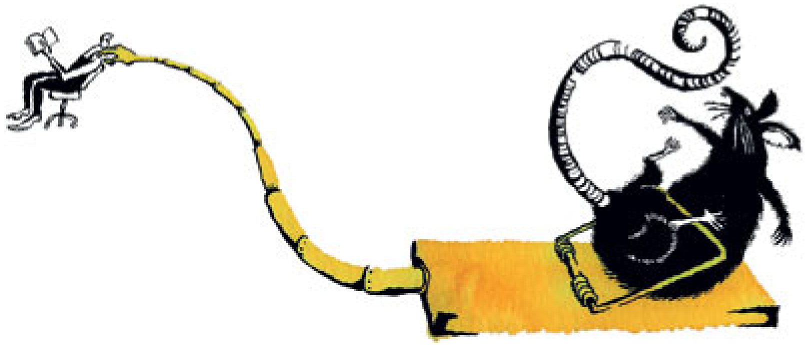
Now operators are having another go at machine-to-machine communications. Orange, a pan-European operator, has created a special business unit, M2M Connect. Other carriers have similar plans. Yet despite the talk, they are more interested in their mobile business than in pursuing M2M. That is a pity, because they have the customers, the expertise on network security and the experience in managing millions of devices that would allow them to develop the new market successfully.

Connecting machines requires giving up control to users, observes Tim Whittaker of Cambridge Consultants, which designs wireless systems. In fact, Orange M2M is criticised for trying to prevent customers from working with other operators. Thus even when mobile firms fall in love with M2M, the technology is suffocated by their embrace. Wireless innovation is more likely to come from smaller companies with a computing background. They are beginning to give machines eyes, ears and a voice.

What the mousetrap said

Apr 26th 2007
From The Economist print edition

Belle Mellor



Machines catch on to smart talk

MANY companies claim to have built a better mousetrap. Rentokil has actually done so. The British building-services firm added a small sensor and a wireless module to its traps so that they notify the building staff when a rodent is caught. This is a big improvement on traps that need to be regularly inspected. A large building might contain hundreds of them, and a few are bound to be forgotten.

Since June 2006 thousands of digital mousetraps have been put in big buildings and venues such as London's new Wembley Stadium. The traps communicate with central hubs that connect to the internet via the mobile network to alert staff if a creature is caught. The system provides a wealth of information. The data it collects and analyses on when and where rodents are caught enable building managers to place traps more effectively and alert them to a new outbreak.

Upgrading the humble mousetrap took a number of innovations to come together. Wireless chips have got smaller, better and less expensive. Sensors require less power. Batteries last longer. Many other companies too have woken up to these advantages, adding wireless features to objects and machines to enhance their performance and open up new revenue streams.

Such machine-to-machine communications can take many forms, from advanced utility meters that provide readings in real time to credit-card terminals at shops and restaurants. Most cash machines communicate wirelessly over a secure data network. Carmakers are exploring vehicle-to-vehicle communications to boost road safety. There are so many possibilities that the technology's champions sometimes get carried away. In 2003 the ARC Group, a British consultancy (since bought by Informa), forecast that by 2007 the market could be worth well in excess of $100 billion. In fact its value this year is likely to be around $25 billion, according to Juniper Research. Harbor Research reckons that the total may be as high as $48 billion if short-range wireless technologies, systems integrators and the like are included. What everyone agrees on is that the sector is now growing very rapidly.

And as prices fall—as much as 20% a year for mobile systems, according to Gartner Research— growth is accelerating.

Expectations were so high because much of the technology exists already. Yet it is being held back by non-technical factors: the lack of integration among different parts of the industry and the need for companies to change the way they operate. In the computing world the providers of networks, hardware and software work relatively smoothly together because of common standards, from the size of printer plugs to digital interfaces in the operating system. But wireless M2M systems have to start from scratch every time.

Reasons not to connect

Building the wireless chipsets into the machines in the first place requires know-how, time and money. Components from different firms may not work together, so systems integrators such as IBM, Accenture or Capgemini have to be called in. Mobile network coverage is inconsistent, so relying on just one operator is risky, and for movable things such as vending machines and cars, which may cross national borders, it is unthinkable. “Mobile virtual network operators” which resell airtime from scores of operators to M2M users could provide the required coverage, but they have been slow to emerge. Even trying to buy bulk airtime from individual carriers is difficult.

The list goes on. Back-office software to manage the system has to work with existing corporate software. Someone has to take care of billing and managing the devices. And as everyone takes their cut, the expense grows. “It is a very long value-chain for people to bring this together,” says Brian Tucker of Telit, which supplies cellular modules. Some consolidation is now taking place, and companies that bundle these functions are emerging in niches such as vehicle-fleet management. But integration remains a problem.

Vending machines are a striking example. At first sight giving them wireless connections seems an obvious improvement. It will allow their owners to check remotely on a machine's inventory, the amount of cash it contains and whether it is in working order, so staff can cut down on their visits for restocking, servicing and collecting the money. When the idea was put forward years ago, it seemed to epitomise the advantages of M2M.

But things have not gone as planned. In Japan, where much has been made of vending machines that accept payment via mobile phones, the vast majority are in fact unconnected. And in Europe only about half of the roughly 4m vending machines are reckoned to be worth upgrading with remote connections, which cost between $100 and $300 a go. Progress even on those is proving slow.

Part of the reason is the sheer difficulty of getting all the relevant businesses together. Vending machine companies have to employ specialist IT and wireless firms, which in turn have to find suppliers. One firm that works with the vending industry, Vianet, found that arranging wireless access from the plethora of mobile operators across Europe was so difficult that it decided to make this a business unit in its own right that supplies access to other M2M sectors.

The biggest obstacle, however, was not technology but the nature of the vending industry. Though the machines are stuffed with well-known brands from large companies, the firms that manage them are often small family businesses. Adding wireless technology means a lot of internal changes. What looks like improved efficiency on paper means a total reorganisation in practice, including job losses. Paul Green of Vianet recalls a conversation with the boss of a European vending-machine firm who stopped a programme promising cost savings of 30% because it was causing too much disruption.

Nice idea—if someone else pays

Another question that inhibits take-up, even among those who are interested, is who should pay for the installation. Putting a wireless terminal into a vending machine is attractive not just for inventory and maintenance but also because it will allow payment via mobile phone. But it is not clear who should pay, so no one does, says Anders Franzen of Wavecom, which sells cellular modules for machines.

Despite the difficulties, wireless vending machines are starting to emerge, but not in the way originally envisaged. Machines that sell pricey things such as iPods and DVDs are now being connected to the internet so companies can gather sales data and fine-tune the products on offer. Most importantly, the network connection also handles credit-card transactions, a necessity for higher-value items.

For mobile operators, moving into the M2M market makes perfect sense. It places low demands on the network. The average traffic load per device is around a quarter of a megabyte per month, estimates Paul Smith, the boss of Wyless, an M2M network provider. And corporate customers stick around for much longer than individuals do. Yet for customers, adding wireless connections to machines is risky because the technology is evolving so fast. And balancing the interests of everyone who has a stake in the system can be hard.

Certainly the car industry has found it so. Adding wireless features to cars has been under discussion for years. Some new cars in rich countries now come with satellite navigation; some have Bluetooth so that mobile phones and digital-media players can connect with the car's speakers. But long-range, two-way communications are being introduced only slowly. So far only 15m vehicles worldwide are connected, although numbers are expected to grow by 40% a year to more than 60m in 2011, according to Visant Strategies.

For the moment the technology is being used only in a few luxury cars and some rented cars and lorries. In Germany, lorries have had a GPS and mobile system to pay road tolls since 2005. Some regulators require telematics to ensure that lorry drivers are getting enough rest. Logistics firms themselves use such systems to communicate with drivers on the road.

General Motors in America offers a service called OnStar that can remotely diagnose engine trouble, contact emergency services after an accident and provide roadside assistance at the touch of a button. It already has more than 4m subscribers and an estimated revenue of more than $1 billion a year.

But getting wireless connections into cars on a large scale has proved difficult. Carmakers envisage vehicles communicating automatically with others nearby to signal road hazards or prevent accidents. Others see wireless as a source of new revenue from services such as traffic information. Regulators in Europe and America would like cars to contact emergency services automatically after an accident, and the police want to track suspects. (Tellingly, mobile operators are not keen on the idea. They are worried about liability if their network is not up to snuff.) Consumers could download maps, restaurant information and media content.

No escape

It is not easy to get agreement on who should pay for all this. Nevertheless, where it has started to happen, it has launched some innovative business models. For example, PassTime, an American company, leases cars to people with poor credit histories. The wireless device allows the company to switch off the ignition if payments are missed, and to find the car if it is stolen or has to be repossessed. Around half a million cars are already equipped with the system.

“Pay-as-you-drive” insurance schemes are also gaining ground. Last year Norwich Union and Royal & Sun Alliance, two British insurance firms, began offering car insurance based on driving patterns, made up of a modest fixed rate and a variable element depending on where and when the customer drives. The car is fitted with GPS and a mobile connection. Under Norwich Union's plan, driving down a motorway (where accidents are rare) on a Sunday afternoon costs a penny a mile; cruising on a suburban road (where mishaps are more frequent) on a Saturday night is a hefty £1. The driver benefits because he has some control over what he pays. Insurance companies benefit by creating an incentive for drivers to avoid risky situations. The system can also track the car if it is stolen and pinpoint its location if it breaks down.

Robin Duke-Woolley of Harbor Research reckons that such new business models, which he calls “smart services”, will be a good reason for companies to add wireless technology to machines. Not everything lends itself to this treatment: aeroplane engines, for example, are too hot, so they have wired sensors, and printing presses usually sit deep inside buildings, so they use fixed-line access. But for many things—even simple mousetraps—wireless is just the job.

A sense of things to come

Apr 26th 2007
From The Economist print edition

Sensors can keep a remote eye on almost anything

Belle Mellor

THE military uses for wireless technology are persuasive. For example, pilots can fly above a war zone and drop thousands of small wireless sensors, the size of a small pebble and costing a dollar apiece, over the terrain. As soon as they settle the devices start communicating with each other, weaving themselves into a dense digital mesh. They pick up vibration and sound, so they can identify advancing troops. The sensors can also detect the presence of nuclear, chemical or biological agents. The information they pick up is relayed to a satellite. For power, they “scavenge” energy from the environment, using solar energy or temperature changes.

The civilian uses are equally impressive. Forest rangers can drop the sensors from aeroplanes to detect fires, showing their exact location and how fast and in what direction they are spreading. Smaller versions the size of grains of rice can be used by airlines in the innards of aircraft to check for the presence of large insects or rodents that might interfere with the wiring. Still smaller versions the size of specks of salt can be added to paint, turning entire surfaces into wireless sensors that can detect motion or act as smoke alarms or security systems.

The trouble is that as yet such sensors do not exist. But a lot of practical work is already going into making them a reality. A version of the military scenario above, for instance, was rehearsed in an experiment in March 2001 at an American Marine Corps base in California. Around a dozen nodes the size of a matchbook were released by a miniature unmanned aircraft. They were able to measure the speed and direction of vehicles from ground vibrations. This proved that the technology, although still at an early stage, was viable.

The military experiment was supported by America's Defence Advanced Research Projects Agency (DARPA) and arose from a programme called “smart dust” at the University of California at Berkeley in the 1990s. It created some of the technical foundations needed for sensor networking, such as a pared-down computer operating system, database and protocol for sensors to send traffic (but “sleep” as much as possible to prolong battery life). The technologies are open standards, so may be used freely by other firms, just as the underlying protocol of the internet is open.

With DARPA's early support a gaggle of companies have emerged, such as Dust Networks, Arch Rock and Moteiv (from research at Berkeley) and Ember (based on work at MIT). Other companies, such as Crossbow Technology, Millennial Net, Sensicast, Tranzeo and MicroStrain, are applying the innovations to their existing technologies. Wireless-sensor technology is now moving out of military testing grounds and into the commercial world. It is used for things like monitoring and controlling industrial machinery, automatic temperature regulation in buildings and keeping tabs on the environment.

Whereas M2M communications generally involve wireless devices attached to equipment such as cars or vending machines that link up to the cellular system, sensor networks use small chips that are often embedded into the device and use a local-area network that may never connect to a larger one such as the cellular system or the internet. For the moment the sensors are not yet widely deployed: the technology is still maturing and customers need convincing that it is worth having. But the idea is gaining momentum. Once the volume goes up, prices will come down and follow-on innovation will speed its adoption.

A good place to get a glimpse of new wireless technologies in action is BP's Cherry Point Refinery in Blaine, Washington. Built in 1971 on almost four square miles (10 sq km), it has a daily throughput of 225,000 barrels of crude oil. The site also produces 8% of the world's calcined coke, which finds its way into one out of every six aluminium cans. Modernising the plant to keep it efficient is costly; BP says it has spent nearly $500m on this over the past ten years. Fields of tanks need to be monitored for operational, safety and environmental purposes. But snaking wires across such a huge area is expensive.

New wireless technologies are critical, explains Tim Shooter, who works on future technology at BP. They allow more operations to be monitored and controlled and save money at the same time. The average refinery has around 3,000 “instrumentation points” where data on things like temperature, flow, humidity and vibration are collected; managers would be even happier with 10,000 points if only they were less pricey. The cost of the basic monitoring devices ranges from $1,000 to $10,000 apiece. Although adding wireless functions to these sensors almost doubles that cost, it reduces the price of installation by 50-90%—and installation makes up most of the total cost. By upgrading some processes to wireless systems, Mr Shooter believes each refinery will be able to save at least $1m a year.

Getting better all the time

Until a few years ago wireless technology was not up to the job. The “big leap forward”, says Mr Shooter, is that the new technologies are far more reliable in hostile industrial conditions and the communications protocols are more intelligent.

One notable innovation is “ad-hoc mesh networking” in which each node on the network—eg, a sensor on a water pump—is both a transmitter and a receiver and can join the network whenever required. Earlier wireless technologies assumed that sensors would send data to a specific receiver, in a hub-and-spoke fashion. This had many drawbacks. For a start, it made the system inflexible. If you added a new node, the whole system had to be reconfigured and the network became harder to manage. And if a central receiver failed, the whole system collapsed.

The newer technology remedies these faults. Each node can relay traffic to other devices, creating an interlocking web. It needs less power because the data travel only a small distance to another node. It is self-organising and self-healing. If one node goes down, the system finds an alternative path for the traffic. And the more devices are attached, the more efficient and resilient the network becomes.

Factory controls like those at BP are obviously useful, but they do not add up to a volume business. A good example of a large-scale application is building management. Thanks to wireless communications, lighting, heating and air-conditioning can be controlled centrally to keep energy bills down. So when a guest checks out of a hotel the receptionist can adjust the air-conditioning to stop it needlessly chilling the furniture. This could also be done through a wired system, but wireless technology offers lower installation costs and greater flexibility.

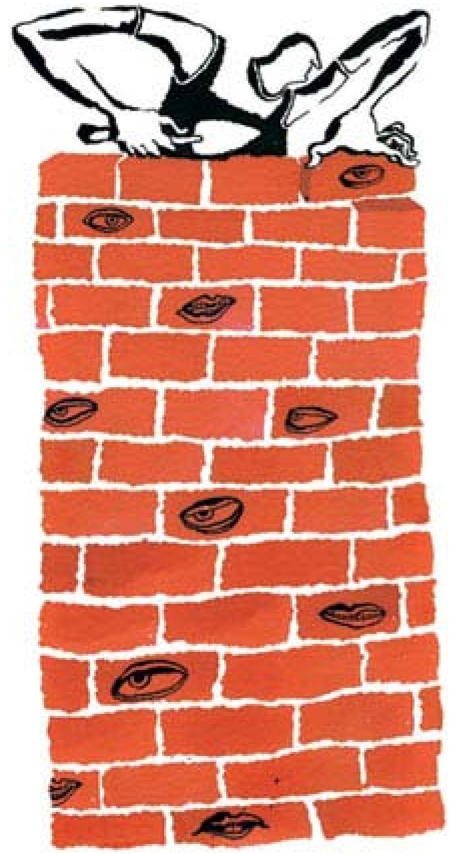
Guest appearance

Some firms are installing such systems in older buildings as well as integrating them into new ones. Riga Development, a wireless-technology firm in Toronto, has worked with hotels in Canada and the United States to replace ageing analogue thermostats with digital ones that are around 35% more energy-efficient. It wirelessly links the new temperature-control panels with heating and air-conditioning units, at a cost of around $350 per room. Each room can also be controlled from the front desk. And thanks to the wireless mesh network, the panel in each room also acts as a relay for the data traffic from other rooms back to a central control point.

At a medium-sized office park in Las Vegas, wireless temperature controls were installed in a few buildings containing around 200 offices, says the media-shy maintenance manager (who did not want his or the company's name to be used). Temperatures in the Nevada desert tend to extremes and landlords are responsible for energy bills, so managing a building's climate makes a difference to the bottom line. The new wireless thermostats allow rooms to be controlled centrally on a PC or over the web. The adjustments that tenants themselves are able to make can be controlled too, so that heating or air-conditioning is not used to excess. The system was cheap to put in, mainly because it required very little installation, the manager explains. Tenants are happier and the savings on the energy bills have been considerable, he says; “conservatively 25%”.

These uses of wireless are just the beginning. Sensors are not only being added to devices that already have electronics on them, but being put on to things that were formerly bare of any technology at all. For example, they are being fitted to buildings, bridges and roads to monitor their structural integrity. The sensors can identify stress and early cracks that need attention. Sensors are also being used to monitor the environment. Scientists now use them to measure the climate in areas that would have been impractically small when sensors were more costly—say under individual plants rather than in a thicket.

Belle Mellor



Wireless sensors are also cropping up on farms, to measure temperature, moisture and light on tracts of land where wired sensors cannot easily go. Among the first big users are vintners, because their crop is particularly valuable and even small variations in climate can ruin it. Ranch Systems, for instance, supplies equipment and software to a dozen vineyards in Northern California. A fleet of sensors allows growers to monitor wind, water and soil and air temperature. This helps them set the watering schedule to suit the different needs of each part of the vineyard and manage frost, disease and pests, explains Jacob Christfort, the founder. “It is a little like da Vinci and the helicopter,” he says, referring to the artist's famous sketches that presaged later inventions. “These things were conceptually possible all along, but some mundane advances are required before it all comes together and somebody actually does it.”

The technology has become so accessible that it is sparking a cottage industry of small entrepreneurial firms. Moteiv is putting sensors on firemen's uniforms to relay information about the fire and let their colleagues know exactly where they are. The system can even provide the firemen with information such as floor plans, projected onto their masks. Other applications now on sale include wireless home-security systems and wireless beacons for sailors to tell the crew when someone has fallen overboard.

Yet the very diversity of its uses highlights one of the barriers to the development of the technology: they all have to be put together in a bespoke fashion. Wireless technology is so new that it has yet to be simplified and standardised, as most technologies are over time, notes Monica Paolini of Senza Fili Consulting.

Another complication is that nobody really knows how much stress a collection of wireless sensors will put on a network, other than that it will probably be different from what happens on the internet. Much internet traffic is asymmetric, with computers at the edge of the network receiving hundreds or thousands of times more traffic than they send. A single mouse-click to request a file brings a massive

YouTube video in return. With sensor networks this traffic asymmetry is inverted: they send far more data than they receive. Although each individual consignment of data is tiny, they add up. And some sensors send out a steady heartbeat, if only to say “I'm still here!”, which sets off a communications session throughout the network.

What worries engineers most is how to deal with all the data produced by the sensors. “The good news is that you can get all these data; the bad news is that you have to do something with them,” says Kris Pister, the co-founder of Dust Networks. Efforts are under way to increase the processing power of the sensors so that they can analyse the information themselves rather than just collecting it and passing it on.

But this wealth of information creates opportunities as well. Teruyasu Murakami of Nomura Research Institute believes that having things continuously connected to a network will open up new markets and new ways of living. And Bob Karschnia of Emerson Process Management, which designs and builds factory automation systems such as the one at BP's Cherry Point Refinery, digs through the mountains of data to find new ways for businesses to operate. At times, he philosophises about what the technology means. The interconnected machines are akin to the brain's neural pathways, he suggests. “If we are computing and connecting like the brain, we should be able to emulate memory,” he says. “How do you create ‘memories' in the processes of a factory?”

As machines talk to other machines, they may uncover facts and relationships that are not apparent to people. That may enable factories to “learn” and find ways to become more efficient. What happens on the factory floor will make its way, in a different form, to office buildings and homes. The next step is for wireless technology to enter human beings themselves.

Cutting the cord

Apr 26th 2007
From The Economist print edition

Wireless energy makes wireless devices look easy

THE most ubiquitous accessory for wireless devices is the wire used to power them. That limitation could be overcome by using electromagnetic waves to transfer energy. The idea has been around since soon after their discovery: Michael Faraday found in the 1830s that changing a magnetic field induces an electrical current in a nearby wire. One of the first patents registered in the 1890s by Nikola Tesla, one of Edison's former assistants, was for “radiant energy”. The pioneers of radio were also those of electricity; the two disciplines were initially one.

Much of the research on wireless energy transfer lay fallow for a century. It was difficult and dangerous, and there was no immediate need. But the proliferation of small wireless devices has sparked new interest in the idea. “Nobody wants to have to change the batteries in their door,” says Tim Fowler of Cambridge Consultants, a wireless engineering firm.

There are several kinds of wireless energy transfer. One, dubbed “radiative”, involves generating an electromagnetic field. A special receiver picks up a bit that has not naturally dissipated in the air and converts it to electricity. The energy can travel nearly three metres (ten feet) to keep a small battery charged, but most of it is lost before it gets to the receiver and the power supplied is extremely low. The technology, pioneered by Powercast in Philadelphia, will be deployed for the first time this year by Philips, for lights on things like Christmas decorations.

A second technique relies on magnetic fields. It is still at an experimental stage and works using resonance. When two objects resonate at the same frequency, they transfer energy well—just as a child easily maintains momentum on a swing when he uses his legs to move in synch. The use of magnetic resonance allows energy to be transferred in useful quantities and almost entirely to the device. But again it can travel only a few metres. Even so, ever since its inventor, Marin Soljacic of MIT, presented his work at a conference last autumn he has been besieged by calls from venture capitalists.

Another way of transferring energy, called “inductive coupling”, is not so much wireless as plugless. Power is sent on almost direct contact, for example, with a mat on which gadgets can be placed to recharge. This system, with a few variations, is used by start-ups such as Splashpower in Britain and WildCharge and Fulton Innovation in America. It avoids the need for cables and connectors to charge gadgets and can be built into many surfaces, such as car dashboards or office furniture.

It helps that computer chips now need much less power than they used to. Gene Frantz at Texas Instruments calculates that the power requirements of a chip of a given capacity roughly halve every 18 months, a less-noticed corollary to Moore's law. Despite the advances, power consumption remains a serious constraint. The amount of energy a battery can store per unit volume is increasing by 8% a year, but the needs of ever more powerful electronic devices are going up more than three times as fast.

Another method is to “harvest” energy from the environment, converting heat, light or vibrations that occur naturally. For example, sensors in a skyscraper could be powered by the normal sway of the structure. And certain materials are “piezoelectric”, meaning that they naturally become deformed by heat or vibrations, generating an electrical current that can be captured and stored. The technology is young but advancing fast. Commercial products are already being sold by a host of companies such as Perpetuum in Britain and Ferro Solutions, Midé Technology, KCF, TPL and MicroStrain in America. The hiccup is that very little energy is generated and the harvesting mechanisms are sometimes larger than the devices they power.

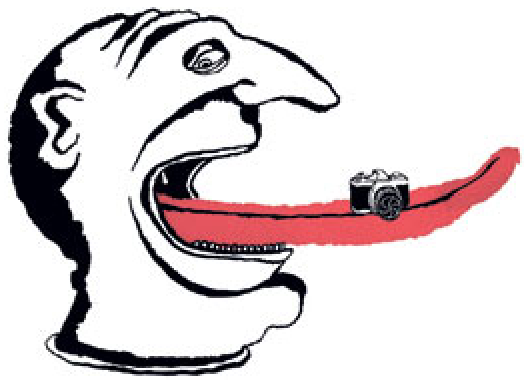
Yet another solution could be fuel cells. Unlike batteries, which simply store energy, fuel cells actually generate it from volatile stuff such as hydrogen or methanol. Basic versions of the technology already exist to recharge devices such as mobile phones. But just try getting on board an aircraft with a full-fledged fuel cell in your laptop.

Wireless incorporated

Apr 26th 2007
From The Economist print edition

Gizmos are starting to be slipped inside people

Belle Mellor



THE Baja Beach Club in Barcelona is an unlikely demonstration model for wireless technology. Bikini-clad waitresses serve drinks to guests as a DJ mixes music from a motorboat perched above the dance floor. But the club made headlines three years ago when it introduced a unique form of entry ticket to its VIP area: a microchip implanted in the patron's arm.

Slightly larger than a grain of rice and enrobed in glass and silicon, the chip is used to identify people when they enter and pay for drinks. It is injected by a nurse with an intimidating syringe under a local anaesthetic. In essence, it is an RFID tag. If a special tag-reader is waved near the arm, a radio signal prompts the chip to transmit an identification number which is used to call up information about the wearer in a computer database. Otherwise the chip is dormant. The “intelligence” of the system is in the computer, not the capsule.

It is the first time that chips have been placed in humans as a means of identification and payment, gushes Conrad Chase, the club's co-owner, who came up with the idea and was the first volunteer to be “tagged”. “I know a lot of people have fears about it,” he says. But he points out that many people already have piercings and tattoos. “Having a radio-transmitting chip under your skin makes you very unique,” he says wryly.

All this for a *mojito* might seem a bit extreme—which for a night club is precisely the point. Even so, take-up has been low: only 94 people have been tagged in Barcelona and 70 at another Baja club in Rotterdam. But as go the bohemians, so, eventually, go the rest of us.

CityWatcher.com, an American firm that provides video surveillance in cities, has experimented with tagging two employees to give them access to areas where sensitive data are stored. VeriChip, another American company that sells chips and readers, provides it to hospitals to manage patients (though only around 200 people have so far raised their arm to get one). The idea of tagging immigrant workers in the United States has been brought up in Congress.

There is much more to come. As wireless technology improves, it is not only getting attached to machinery and embedded in the environment, but slipping under people's skin as well. And RFID capsules are small fry. There are far more advanced wireless medical devices that measure body functions and transmit the information from the skin surface or from inside the body. As the huge cohort of baby-boomers grows older and becomes more interested in preventive medicine, people now aged

50 or younger are quite likely to have some form of wireless gizmo attached or implanted in their lifetime.

Wireless technology has been used in medicine for decades. Pacemakers rely on a basic wireless system to set a stable heartbeat. Ultrasound and X-ray technologies are wireless. But as microchips become more powerful, devices shrink and battery life is extended, a host of companies are vying to take wireless technology deep into the human body.

Some wireless devices are ingested. Others are implanted. Some are attached to the body and linked to a network. It is still early days, but the systems are improving fast. “The basic technology to make these things happen exists; the big issue is how to make this economically viable,” says Maarten Barmentlo, the chief technology officer of Philips's consumer health-care division.

Inside story

Already a gaggle of gadgets is available for specialised uses. Take the PillCam, developed by Given Imaging in Israel, a tiny two-sided camera the size of a very large pill which patients swallow. It has been used in more than half a million gastro-intestinal endoscopy tests since 2001. One version is used to diagnose disorders of the oesophagus and another for those of the small intestine. It snaps a pre-set number of pictures per second and sends them wirelessly to a data recorder worn on the patient's waist. The images are downloaded to a computer for diagnosis. The $450 capsule passes through the bowel naturally and is flushed down the toilet.

This method lets people go about their normal business for most of the eight-hour test, during which up to 50,000 images are generated. It marks a vast improvement on an older technique that involves pushing a long tube through a patient's digestive tract. Although that procedure allows doctors to take tissue samples, it is uncomfortable and risks irritating the tract. Now Given Imaging is in clinical trials with a wireless camera for inspecting the colon, and is developing another for the stomach. The company faces competition from Olympus, a Japanese camera-maker, which is using similar technology.

Other wireless systems are implanted in the body. Medtronic, a large medical-device-maker, is developing many products that use wireless communications. Last year it won regulatory approval for an implantable defibrillator that links up with hospital equipment or a home monitoring device. Along with three other companies—CardioMEMS, St Jude Medical and Remon Medical Technologies—Medtronic is racing to market a device for congestive heart failure, which afflicts many millions of people worldwide. Once implanted, the device will measure pressure and fluid inside a patient's heart and wirelessly send the data to an external unit. With regular monitoring, patients will be alerted to abnormalities at an early stage.

There are two ways of making the wireless work, marking a division in the industry about the future of wireless technology in health care. Medtronic and St Jude currently make large-matchbox-sized devices—in essence, miniaturised computers—that are implanted in the chest and connected to the heart with leads, but can be interrogated wirelessly from outside the body by a reader at close quarters.

A more novel approach involves either radio waves or ultrasound technology. CardioMEMS uses radio-frequency technology, activating the chip in the implanted device by a reader that sends a burst of energy (like an RFID tag) to which the device responds with the heart-pressure information. Remon relies on a form of ultrasound that transmits energy to power the chip and prompt it to send back its pressure readings. Because the electromagnetic frequencies it uses are low, the reader can be farther away.

All four companies' heart-failure devices are still at the trial stage. In March Medtronic suffered a setback when a panel at America's Food and Drug Administration rejected its device, called Chronicle, because the trial data showed it to be insufficiently effective. Meanwhile, Remon is applying its technology to what it calls “intra-body wireless communications”. By dividing up the signal, this allows several devices inside the body to relay information to each other or to a receiver without interference, just as a radio can be tuned to different stations. So an implanted glucose-level reader in one part of the body could communicate with an implanted insulin-pump elsewhere, says Hezi Himelfarb, the boss of Remon.

Such scenarios are not so far from being realised. Sensors for Medicine and Science (SMSI) is developing a glucose sensor to be placed just under the skin of the forearm that connects to a watch-like wireless reader. This will probably become the most common way of deploying the technology: not by surgery deep into the body, but by inserting a sensor below the skin that can last for months or years, and having a wireless reader nearby.

This is the method used by Thomas Ferrell of the University of Tennessee, who has developed an implantable capsule that measures ethanol concentration in the blood. He says it could be used by alcoholics who volunteer for monitoring as an alternative to prison. The technology, funded by the National Institute on Alcohol Abuse and Alcoholism, is currently being tested in animals. Dr Ferrell expects it to become available commercially within two years.

Listen to me

Earlier Dr Ferrell spearheaded a DARPA initiative to create a tiny chip that would fit into a person's ear and monitor vital signs such as body temperature, pulse and blood pressure. The work was put on ice five years ago because of the huge cost of developing the technology that was available at the time. But now that the cost has fallen and the technology improved, the project is becoming feasible. Later this year the work is due to be resurrected by a start-up, Senior Vitals, to produce sensors for monitoring elderly people.

The technology to monitor people's vital signs already exists: NASA does it for astronauts in flight. But for the moment there is no business model for applying it on the ground, no IT system to manage it and no company that could carry out the work. As with M2M communications, any system would have to be tailor-made, which would make it very expensive. And as with other wireless devices, powering the electronics is a problem.

But companies are beginning to show interest in the sector. Adi Gan of Evergreen Venture Partners, a venture-capital fund in Israel, says that numerous business plans in this area have crossed his desk in recent months. He sees a lot of promise. For example, a doctor might implant a sensor during surgery to offer far better post-operative monitoring and care. When the patient comes for a follow-up visit, the doctor's reader would power the chip, which would provide medical information. Tiny devices could even be used for treating diseases. They might be powered wirelessly to, say, burn new cancer cells in an area that had previously been treated.

Belle Mellor

Such uses of wireless seem far removed from the mobile phones which vast numbers of people carry with them at all times. But there is a connection. As the use of wireless medical devices grows, the best way of collecting the data and sending them to a remote monitoring centre may turn out to be the patient's mobile phone, which will be close enough to receive data from the low-powered implanted device. It could be the critical bit of infrastructure between wireless communications in the body and the global internet. Just when people are starting to think of the mobile phone as a wallet, they find that it is becoming the family doctor too.

Mobile-phone operators understand the potential. South Korean and Japanese carriers are experimenting with technologies that let people monitor their heart rate, blood pressure and other vital signs with home devices and transmit the data using a phone. Philips and GE are adding wireless technology to patients' home-monitoring devices. Yet today's mobile networks are not sufficiently reliable for anything other than non-critical uses, according to a study in 2005 from the University of Massachusetts in Amherst. And the operators' current pricing models are a major barrier, says Matt Welsh of Harvard University, who is developing sensors for the continuous monitoring of vital signs.

For now the advances are largely coming from the IT industry, not the medical sector, which is noted for its conservatism. Whereas pharmaceutical firms are starting to use RFID tags on medicine packages as an anti-counterfeiting measure, other companies are working to put RFID tags onto individual pills. In January Kodak filed for a patent on an edible RFID tag which could be used, for example, to examine the digestive tract or check whether a patent has taken his medication.

It all seems a long way from the Baja Beach Club, where Mr Chase goes about his nightly routine. He reviews images from security cameras, some of which are wireless, and then locks an office with keys using a wireless ID system that records who enters where and when. The geeky stuff is his doing, but then he has form. Back in the 1980s, long before opening his nightclub, he served in the US Army Signal Corps, working on the ARPANET, the military precursor to the internet.

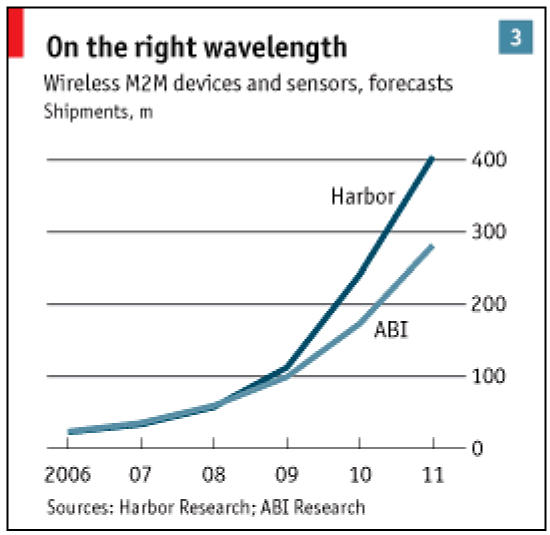
The hidden revolution

Apr 26th 2007
From The Economist print edition

What you don't see will need careful watching

MACHINES, buildings, fields and human bodies have a lot to say, if only they are given a chance to talk. “The previous information revolution was IT, which was basically: take all the paper and turn it digital to share. What we provide [now] is a bridge to the physical world,” says Joy Weiss, the boss of Dust Networks, which makes wireless chips.

Yet dealing with lots of wireless gadgets everywhere is an unpractised art. Security must be assured and privacy protected. All those radio waves raise health worries. There may not be enough radio spectrum to go around as demand grows. And in the longer term disparate systems may converge and become interconnected, bringing up a whole host of new questions.



What is already clear is that the infrastructure required to support wireless communications will have to be massive. Already, tens of billions of e-mails, mobile text messages and instant messages are being sent through the world's public networks each day, not to mention quasi-closed networks used by stock exchanges, flight-reservation systems and the like. Each CDMA mobile phone communicates with a cell tower 800 times a second just for its power management.

VeriSign, which manages networks such as the internet's address system, the global RFID registry and mobile text messages, is spending $200m-300m on its system to handle a peak load of 4 trillion internet-address queries a day by 2010. Cyber-attacks are expected to grow at a rate of 50% a year. The design of the new systems will be critical and the penalties for failure severe. For example, faulty RFID infrastructure in the initial stages of the Iraq war in 2003 resulted in supplies to the value of $1.2 billion being lost during transport, according to the US General Accounting Office. Projects to embed robust RFID chips into passports and national ID cards around the world are beset with delays.

The issue is trickier than many people appreciate. As wireless systems become common in homes, businesses and public spaces, says Lee McKnight of Syracuse University and the founder of Wireless Grids Corp, they will eventually integrate and work together on the fly, in the same way that today a property website might choose to overlay Google maps on its listings. Moreover, the streams of data from devices and sensors are different in kind from what most people are used to: the information is “probabilistic” rather than definitive, explains Martin Illsley of Accenture. And the systems are vulnerable to being hacked into.

The way we look at privacy protection will need to be overhauled. Today it works like a minuet, with a defined set of partners and parameters, says Elliot Maxwell, a technology-policy guru and former official at America's commerce department. But M2M and sensor networks change the tune: the systems are more decentralised and interwoven. Who keeps an audit trail? How are the data verified? Who gives consent to whom? Today's privacy rules presume a relationship between citizen and government or consumer and company. But the way in which information will be generated and shared may involve so many parties that the minuet will turn into a punk rock concert.

The issues feel new because the technology is only just beginning to be deployed. Where it is already in use, with RFID chips, it has generated controversy. American Express has patented a technique to track people in public places based on the RFID tags in their clothing and products they carry, but has agreed not to use it without disclosing the fact, after pressure from privacy advocates. Last year a Wisconsin legislator proposed a law to ban any mandatory microchip implants in humans (although nothing of the kind exists as yet), or embedding a chip in a person without the recipient's knowledge. The European Commission is set to issue guidelines on privacy and security standards for RFID technology later this year.

Silent chips

“The ‘silence of the chips' must be preserved as a fundamental right of citizens,” says Bernard Benhamou of the Institute of Political Science in Paris, who was a member of the French delegation at UN meetings on internet governance in 2003-06. Mobile phones, he believes, should be able to pick up the presence of sensors. People should be able to read basic RFID tags—and destroy them too to preserve their privacy. Such rights, he says, will become more important as wireless technologies become small enough to be invisible.

Yet the technology cuts both ways. Prisons in America are experimenting with bracelets that have wireless chips embedded in them to keep track of inmates. It sounds Big Brotherish, but prison officials say that violence among prisoners has decreased. Guards are also tagged, so prisoners may feel safer from abuse.

A 2004 report for the European Parliament on the effects of new wireless technologies on health and the environment argued for the “precautionary principle”: holding back until any adverse effects have become clear. But in practice that is hard to do. The report recommended that technology products be sold with factual labels, rather like processed foods, so consumers will know how much radiation they emit, how much energy they use and so on. The report did not cover privacy, but there should probably be disclosure of the presence of wireless systems too.

Another possibility is to separate the data. Adam Greenfield, in his book “Everyware: The Dawning Age of Ubiquitous Computing”, published last year, makes an impassioned plea for “seamfulness”. Whereas the computer industry strives to make things as “seamless” (that is, integrated) as possible, he advocates keeping some networks and data apart.

Belle Mellor

Viktor Mayer-Schönberger of Harvard University's Kennedy School of Government has come up with a more innovative proposal: requiring information to be deleted over time. He describes this as a legal and technical version of human forgetting. Today's computer systems do not do that; tomorrow we may wish they did.

We are in the early stages of the creation of a new industry, reminiscent of computing in the early 1970s when companies began to adopt it in earnest. There was plenty of resistance. The systems were difficult to operate and seemed to be set up for nerds. The economic benefits were questioned. There were privacy and regulatory worries. Yet in time the rough edges were smoothed and everybody benefited.

Technology rarely evolves in the way that people think it will. When Marconi invented his wireless telegraph, he never imagined broadcast radio. A decade earlier Heinrich Hertz had famously declared: “I do not think that the wireless waves that I have discovered will have any practical application.” To the men at Bell Labs in 1947 the transistor was simply an efficient replacement for vacuum tubes; they had no inkling of its use in computers. Today these technologies are omnipresent: televisions in every home; computers in every office; phones in every pocket; radio towers looming overhead.

What is different about new wireless communications is that people will barely notice them. Machines will talk to machines without human intervention. But humans will nevertheless be laying the foundation of a new infrastructure which, like the electrical power grid, will become a platform for subsequent innovation. There is no saying how it will be used other than that it will surprise us.