Pervasive tagging, sensors and data collection: A Science and Technology Review for the Foresight Project on Intelligent Infrastructure Systems

A. Tully

Abstract: In the coming years, we will see the deployment of pervasive computing where environments are saturated with computing and wireless communications capability, yet gracefully integrated with human users. Individual devices will be embedded in everyday objects, and connected to each other and to the Internet over wireless networks, harvesting energy from their environment. This Intelligent Infrastructure System (IIS) will not be developed *per se;* it will evolve from where we are now. This paper examines a range of technologies which are key to the success of the IIS and for each, postulates its likely trajectory. Advances in supply chain automation will deliver affordable radio frequency identification (RFID) while the competitive telecommunications environment will deliver systems beyond 3G using mobile *ad-hoc* networks at their periphery. New fabrication techniques will enable the production of smartdust devices incorporating novel sensors with the ability to process their data in the field. Finally, new software techniques will allow this data to be accessed wherever required without overloading the wireless communications network.

1 Introduction

The last 25 years has seen an incredible advance in computer-related technologies. From the first personal computers in the early 80s through the ubiquitous Windows PC to the mobile phone, technology has fundamentally changed the way people live their lives. The 21st century will see the deployment of pervasive computing, which is a concept based on a vision described by Mark Weiser in 1991.

> ‘The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it’ [1]

The essence of that vision was the creation of environments saturated with computing and wireless communications capability, yet gracefully integrated with human users. Pervasive computing is set to have an impact at least as great as preceding technologies and very likely much more.

An integral part of this pervasive computing vision is the sensor and actuator devices which form the bridge between the real world inhabited by humans and the virtual world beloved of computers. Individual devices will be embedded in everyday objects and connected to each other and to the Internet over wireless networks. Devices will harvest energy from the very environment with which they interact. Networks of devices will cooperate to achieve common goals while tolerating individual failures and changing patterns of ad hoc communication. Networked applications will be developed and deployed throughout the networks, increasing their resiliency and overcoming the communication bottlenecks inherent in conventional architectures based on back-office hosted applications. This intelligent infrastructure system (IIS) will not be developed per se; it will evolve from where we are now. If this evolution is to deliver Weiser’s vision, it must be managed carefully. Standards will guide evolution but commercial interests will drive it forward. It is essential that those with a strategic interest in IIS engage fully in this process through alliances with the independent and industrial research organisations at the heart of the vision.

For IIS to become a reality, many technological advances are still required; from the development of nano-scale science for sensors, through advances in MEMS for devices to a whole new field of sentient applications. There is an enormous and ever-expanding body of research aimed at achieving Weiser’s vision and a report of this size can only hope to scratch the surface. However, it is hoped that the report will inform its audience of the key constituent technologies and support the aims of the Foresight Programme.

2 Radio frequency identification

2.1 Overview

The history of radio frequency identification (RFID) can be traced back to the Second World War where the RAF pioneered the use of radio identification methods

IEE Proceedings online no. 20060002

doi:10.1049/ip-its:20060002

Paper received 2nd March 2006

The author is with the School of Computing Science, University of Newcastle upon Tyne, Claremont Tower, Newcastle upon Tyne, NE1 7RU, UK

E-mail: alan.tully@ncl.ac.uk

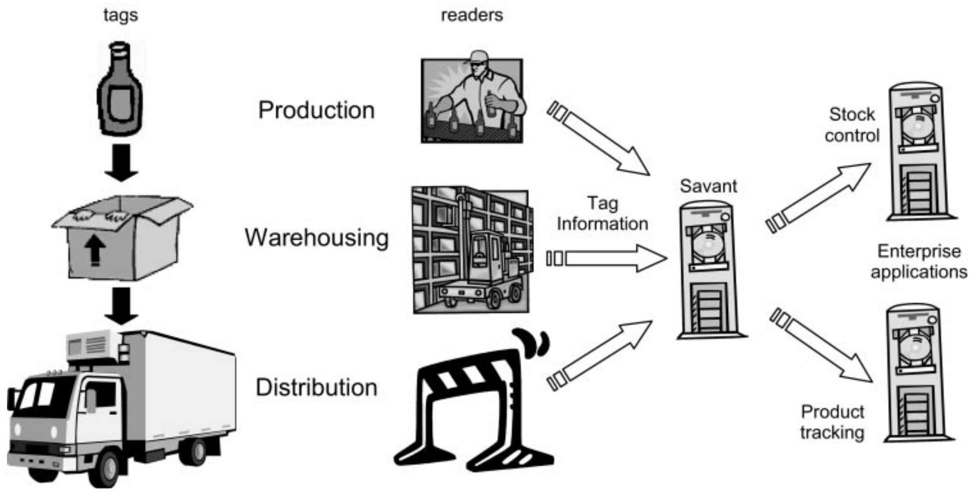

Fig. 1 *RFID in the supply chain*

to distinguish between friendly and enemy aircraft. In military applications, the cost of the technology was largely irrelevant. However, advances in the intervening 60 years have brought costs down to levels where commercial applications are viable.

Supply chain management has in the past relied on the use of barcodes to identify products. The use of 2D barcodes, which carry much more information, has extended their lifetime but reading is limited to line of sight at close range and is highly sensitive to ambient light conditions and barcode contamination [2]. In recent years, many large companies have introduced RFID technology. The transition from barcodes to RFID has required a large investment but companies such as Wal-Mart, Coca-Cola and Marks & Spencer have been prepared to invest to gain the benefits of reduced stock levels, less wastage or spoiling and better customer service. Walmart specified that its top 100 suppliers would have to put RFID tags on all their shipping crates and pallets by 1 January 2005 and the remaining suppliers by 1 January 2006. The resulting market for RFID tags created by the top 100 Walmart suppliers alone is estimated to be around 1 billion per annum [3]. This will have an enormous influence on standards while driving down costs from the current 20 cents per tag towards 1 cent per tag within 5 years. The benefits of cost reduction will not be limited to the supply chain industry but will open up new markets in areas for which RFID is currently uneconomic such as mass-transit ticketing.

RFID tags offer a number of advantages over barcodes; tags can be read at greater distances; several tags can be read at the same time; tags can hold more data; tags can be re-written as they move through the supply chain; some tags can even monitor their environment (e.g. US customs service container security initiative [4]).

2.2 System architecture

A typical RFID system consists of a host computer, a reader and a number of tags or transponders, as shown in Fig. 1. The reader emits a radio frequency (RF) signal which is received by all tags within the radio field which are tuned to that frequency. Tags respond by transmitting their stored data. The reader then transfers the data to the host computer. Anti-collision algorithms are used to allow a single reader to discriminate between many tags simultaneously passing through its radio field (up to 200 tags/s).

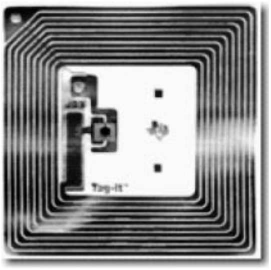

Fig. 2 *An RFID tag*

A reader typically contains a high frequency module (transmitter and receiver), a control unit and a coupling element to the transponder. In addition, many readers are fitted with an additional interface (RS 232, USB) to enable it to forward the data received to another system.

The transponder, which represents the actual data carrying device of an RFID system, normally consists of a coupling element and an electronic microchip (Fig. 2). In most cases, the transponder does not usually possess its own voltage supply (battery), and so when it is not within the range of a reader it is totally passive. The transponder is only activated when it is within range of a reader. The power required to activate the transponder is supplied to the transponder through the coupling unit (contactless) as is the timing pulse and data. Most RFID tags still generate their power directly from the incident wave and also use this carrier wave to ‘reflect’ data back to the reader. This process is known as backscatter.

2.3 Tags

There are ANSI and International Organisation for Standardization (ISO) standards for tags [5] defined by five classes [6]:

- Class 0—factory programmed with a simple ID during manufacture which cannot be updated. Passive. Used for anti-theft applications.
- Class 1—user programmed with a simple ID in the field which cannot be updated. Passive. Used for stock control applications.
- Class 2—data can be written to the tag and re-written many times. Passive. Tags usually contain sufficient memory for data logging applications.

Table 1: Competing RFID frequency band allocations

	LF	HF	UHF	Microwave
Frequency range	<135 kHz	13.56 MHz	860–930 MHz	2.45 GHz
Standards	ISO 18000-2	ISO 18000-3	ISO 18000-6	ISO 18000-4
Read range	<0.5 m	1 m	5 m	1 m
Advantages	Works well through metals and liquids	Low cost	Long read range of many tags at once	Fast read rates of multiple tags at once
Disadvantages	Large antennae	Short read range of few tags at once	Poor through metals and liquids	Very poor through metals and liquids
Communication	Inductive coupling	Inductive coupling	Backscatter	Backscatter
Power source	Passive	Passive	Active/passive	Active/passive
Applications	Vehicle immobilizers	Access control Payment systems Baggage control	Pallet and box tagging Electronic tolling	Electronic tolling Real time tracking

- Class 3—tags contain on-board sensors for measuring temperature, pressure and motion. Active or battery-assisted as sensors must be monitored when no reader is present. Used for sensitive cargo.
- Class 4—tags can communicate with each other in the absence of a reader. Active. Can support ad-hoc networked applications.

Tags of classes 0–3 usually transmit to reader using inductive coupling (short range) or backscatter (longer range) techniques. Class 4 tags contain radio transmitters.

Tag information can be encoded to prevent access by unauthorised readers. Encryption can be performed by the reader for classes 0, 1 and 2 tags. Classes 3 and 4 tags must perform encryption locally using public-key cryptography [7]. Denial of service attacks (jamming) is possible using rogue tags deployed within the field of the reader or class 4 tag. Spread-spectrum radio technology may be used in future to mitigate against jamming.

RFID tags are typically deployed in a hierarchical manner [8] as shown in Fig. 1. Individual items carry class 0 or 1 tags while pallets or boxes carry class 2 or 3 tags. Class 4 tags are still relatively rare but can be carried by lorries to automatically generate advance shipping notices (ASNs) as they leave premises and tally with ASNs at their destination [9]. Container-level active tags were used during the Gulf War to hold manifests of the container's contents.

2.4 Communication between reader and tags

RFID generate and radiate electromagnetic waves; thus are classified as radio systems. The function of other radio services must under no circumstances be disrupted or impaired by the operation of RFID systems. It is particularly important to ensure that RFID systems do not interfere with nearby radio and television, mobile radio services (police, security services, industry), marine and aeronautical radio services and mobile telephones. For this reason, it is usually only possible to use frequency ranges that have been reserved specifically for industrial, scientific or medical applications or for short-range devices. These are the frequencies classified worldwide as ISM (industrial-scientific-medical) frequency ranges or SRD frequency ranges, and they can also be used for RFID applications.

Low frequency RFID (125 or 134 kHz) penetrates most packaging material but has short read range (<50 cm). High frequency RFID (13.56 MHz) is almost as good at penetrating packaging and has an increased read range (<3 m). Ultra high frequency (UHF – 915 MHz) has problems penetrating some materials but has a much better read range (<10 m). Microwave (2.45 GHz) is sometimes used for its high read rate but suffers degradation due to metals and liquids and has a poor read range (<1 m) (Table 1).

Table 2: The EPC code

Header	EPC manager	Object class	Serial number
01	0000B36	003BA1	00329DE12

The 13.56 MHz band is the only globally accepted frequency for RFID. Other frequency bands, particularly UHF, vary from one country to another according to local regulations. Within Europe, use of the UHF spectrum is regulated by CEPT [10].

The ISO defines the *air interface* standards to be used for communication between reader and tag [11, 12].

When multiple tags are within range of the same reader at the same time, there is potential for collisions to occur between the response messages of the tags. This is solved by implementing an anti-collision algorithm. Such algorithms are specified in the standards governing communication and are based on well-known algorithms such as binary tree search and the Aloha protocol used in long-distance radio networks and satellite communication. The first phase of the algorithm establishes an order for reading the tags. The reader then interrogates each tag in turn to read or write tag data.

2.5 Electronic product code

In 1999 Massachusetts Institute of Technology Auto-ID Centre in the US collaborated with a number of industrial companies to develop the electronic product code (EPC). The EPC is the electronic equivalent of the Universal Product Code used in barcodes and is set to become the international standard for RFID. Although there are many stovepipe implementations of RFID which do not mandate or even require the use of EPC, the adoption of technology using EPC would benefit from the economies of scale. The Auto-ID Centre closed in 2003 and transferred its technology to a private company called EPCglobal Inc. [13].

The EPC code consists of 64–256 bits divided into the 4 fields shown in Table 2.

The header defines the EPC code type which in turn defines the lengths of the remaining fields. The EPC manager identifies the manufacturer of the product the tag is attached to, the object class identifies the type of product while the serial number uniquely identifies the product. The EPC code may be used by Middleware (called Savants) to obtain information on the product via the Internet from a back-end database or even update that information based on reader location or sensor data read from the tag, as shown in Fig. 1. In this way, other applications such as product tracking and stock management can trace the product and its condition by querying the database alone. It is the combination of tag, reader, Middleware and back-end database, which enables the fine-grained supply chain management demanded by companies such as WalMart [14].

2.6 Privacy

The widespread adoption of RFID and similar technologies has the potential to allow the tracking of individuals through the items that they carry. This has enormous implications on privacy (Fig. 3). Benetton withdrew its plans to deploy RFID in 2003 [15] after a threat to boycott its products. It was claimed that although the Benetton tags supplied by Philips Electronics [16] would be disabled at the point of sale, they could be reawakened at a later date.

Marks & Spencer learned from the Benetton experience when they embarked on their RFID trials and have been careful to placate customer privacy concerns. Instead of embedding tags in the garments, Marks & Spencer embedded the tags in the garment labels. Thus it is claimed, all the benefits of automated stock control are achieved while the customer is assured that they cannot be tracked as the label and tag are removed at the point of sale [17].

2.7 Security

The protocols used for communication between a tag and its reader may incorporate security measures such as encryption to encode the identity of both the user and the transaction. However, there is a trade-off between security and performance [18]. The shorter the key used for the encryption, the easier it becomes to compromise. There are already instances of commercial tag codes being broken. In January 2005, a team from John Hopkins University and RSA Labs [19] successfully compromised an RFID tag from Texas Instruments and were able to buy petrol [20] and turn-on a car's ignition [21].

The US State Department is investigating the use of RFID in passports to speed the passage of travellers through security checks. However, opponents claim that this would allow tracking of individuals who carry a passport at other times which has implications for Civil Liberties and would allow US citizens to be targeted by terrorists (Fig. 4). The US Government has agreed to reconsider the design [22]. The new design will use encryption to protect the holder's identity, nationality and other personal information and the tag will be shielded by protective metal sheets when the passport is closed.

The European Central Bank (ECB) has proposed to embed small RFID tags in Euro banknotes as a tracking mechanism for law enforcement agencies. This has raised a number of security and privacy concerns [7]. The ECB is not disclosing the technology it intends to use but experience shows that information will eventually leak into the public domain (Fig. 5). Any mechanisms it uses must therefore assume this leak so security and privacy must rely on the use of public key encryption.

Fig. 3 *The Benetton protest*

Fig. 4 *An RFID passport*

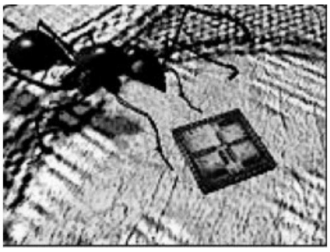

Fig. 5 *An RFID banknote*

2.8 Future trajectory

The commercial drive behind the deployment of RFID technology is massive. The significant benefits to be gained from its adoption within the supply chain mean that large companies with logistics operations will invest heavily. The resultant drop in the cost of the technology brought about by increased competition and improvements in production processes will be passed on to all sectors which use it. Any future IIS is likely to rely on RFID at its core. Where there is a need for large-scale deployment of dumb sensor technology, RFID will provide a cost-effective solution. Current RFID developments are aimed primarily at driving down the cost of low-end tags and their associated readers. While this trend will surely continue, there will also be a drive towards hierarchical RFID architectures ranging from 1c tags which merely identify their host to $1 tags which can sense their environment, log their findings and communicate with other similar tags and with a telecommunications infrastructure such as that promised by fourth generation (4G).

3 Telecommunications

3.1 Overview

The explosion in the ownership of personal communications devices has led to the deployment of vast mobile telephone networks which cover most of the UK. Telecom operators are keen to grow their share of this lucrative market through the delivery of an ever-increasing range of sophisticated services which place great demands on these telephone networks. This technological demand is fuelling the advances in network technologies and standards which we see today. These advances can be exploited to enable ubiquitous communication with vehicles on the move, delivering services and gathering sensor information on a scale which would not be possible using any proprietary solution. In the longer term this may have implication for mobile information provision to individuals within and outside their vehicles; on-road-user charging solutions; vehicle-to-vehicle communications and the wide range of applications that will require vehicle-to-infrastructure communications.

3.2 Towards 3G ubiquity

The prevalent technology for mobile communications in Europe today is still the global system for mobile communications (GSM) which is a second generation (2G) system using digital communications. The only form of packet data transmission is the short message service (SMS) at 14.4 kbps (see Table 3). Many European telecom operators have deployed general-purpose packet radio system (GPRS) or enhanced GPRS (EGPRS) technology within their GSM network to allow the transmission of data packets across their circuit-switched infrastructure at 115.2 or 384 kbps, respectively. This is often referred to as 2.5G. The mobile device obtains an Internet Protocol (IP) address from a gateway GPRS support node (GGSN) giving it an Internet presence.

We are now beginning to witness the roll-out of third generation (3G) systems which will support the real-time transmission of multimedia data using the universal mobile telecommunication system (UMTS) [23].

Transmission rates of up to 2 Mbps are possible for static terminals but drop to EGPRS or even GPRS rates as the velocity of the terminal is increased. Phase 1 of this roll-out [24] uses a virtual home environment to ensure that users are presented with a common interface to services located outside the 3G network wherever the user is located and whatever the characteristics of the mobile device. The mobile device obtains an IP address from a GGSN as with 2.5G. Phase 2 of this roll-out sees the introduction of Mobile-IP. Mobile terminals can now directly negotiate communication with services outside the 3G network.

3.3 Future trajectory

Attention of the research community is now focused on 4G systems. 4G systems will begin by integrating a number of existing technologies such as 3G [25–27], digital audio broadcast [27–29] and wireless LAN (WLAN) [30–34] into heterogeneous wireless networks to provide access to an ever-increasing range of services [24]. 4G will then evolve by incorporating evolutionary advances in the constituent technologies as well as new high bandwidth local radio technologies [36] and high altitude platforms [24, 37]. Data will be transported through 4G networks using packets which conform to the Internet Protocol version 6 (Ipv6) standard. Mobile devices will be able to connect to a 4G network through the nearest WLAN hot-spot access point (AP). The ability for mobile devices to access services via WLANs will mean that users become totally independent of the mobile network operator. Local authorities and transport operators favour this technology as a short-to-medium term for personal communications provision over LAN distances.

The pervasive computing community is addressing issues which are pertinent to the establishment of any IIS. Pervasive computing will embed data processing devices in everyday objects. As the density of such computing devices increases, so does their need for communications. Despite advances in 3G cellular networks, they are not scaleable indefinitely and will never provide sufficient bandwidth to support truly pervasive computing due to the high cost of infrastructure and the limited capabilities of embedded devices. Even the envisaged 4G networks have their limitations; WLANs are used as single-hop bridges to Internet APs so the extension of the edge of the Internet is limited by the transmission range of the technology.

Any future IIS will almost certainly use 4G networks to provide the bridge between deployed infrastructure and the Internet. The always-on model of 3G networks will be extended through the incorporation of WiFi to provide 4G networks with a national reach. It is unlikely that it would be cost-effective for IIS to deploy alternatives to 4G except in a small number of heavily subscribed urban networks. The investment costs of introducing and maintaining a network and keeping pace with advances in technology would far outweigh any savings on data transmission charges. The data-oriented model of 3G, where users pay only for the quantity of data they transmit and receive will continue into 4G and the mobile network operators will provide a service for IIS. Operation of fixed term franchises will ensure that IIS reaps the benefits of their economies of scale.

Table 3: Wireless communication technologies

Technology	Data rate	Range	Coverage	Frequency
2G SMS	14.4 kb/s	5 km?	National	900 MHz/1800 MHz/1900 MHz
2.5G GPRS	115.2 kb/s	5 km?	National	900 MHz/1800 MHz/1900 MHz
2.5G EGPRS(EDGE)	384 kb/s	5 km?	National	900 MHz/1800 MHz/1900 MHz
3G UMTS	100 kb/s (mobile) 2 Mb/s (fixed)	5 km?	National?	2 GHz
4G WW Phase 1	2 Mb/s (mobile) 20 Mb/s (fixed)	2 km?	National?	5.8 GHz
4G WW Phase 2	50 Mb/s (mobile) 200 Mb/s (fixed)	2 km?	National?	60 GHz?
WLAN (IEEE802.11a)	54 Mb/s	100 m	Local	5 GHz
WLAN (Hiperlan2)	54 Mb/s	300 m	Local	5 GHz
Bluetooth	1 Mb/s	10 m	Personal	2.4 GHz ISM Band
IrDA	16 Mb/s	2 m line of sight	Personal	IR
MANETs	250 kb/s	300 m	Local	2.4 GHz

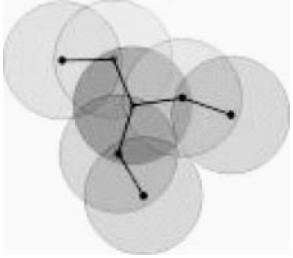

Fig. 6 *A MANET*

4 Mobile ad hoc networks

4.1 Overview

A Mobile Ad hoc NETwork (MANET) is a collection of mobile computing devices which cooperate to form a dynamic network without using fixed infrastructure (Fig. 6). In 4G networks, WLANs are used to provide a single hop access to the Internet when a mobile device is within range of an AP. In MANETs, devices themselves provide routing services so that a device can access the Internet even where no direct wireless connection exists between the device and an AP.

One consequence of adopting a MANET architecture is that computing nodes themselves become an integral part of the communications infrastructure, bypassing traditional network operators and allowing unfettered third-party access to mobile devices and their users. MANETS can be constructed using a wide range of computing devices and communications technologies such as IEEE802.11WiFi, Bluetooth and wireless sensors.

MANETs are not a new concept; they have been widely used by the military since the 1970s. However, commercial interest is a relatively recent phenomenon. A working group [38] has been set up by the Internet engineering task force to standardize MANET routing protocols and provide the basis for extending the IP into the MANET domain.

4.2 Future trajectory

MANETs are now the focus of attention of a large section of the research community [33, 39]. Areas receiving particular attention are routing, security, quality of service, internetworking and energy-efficiency.

- Routing in a MANET is made more complex due to their dynamic connectivity; algorithms which undertake multiple rounds of information exchange to establish network topology will fail.
- Security becomes an issue if denial of service attacks exploit the distributed nature of network management.
- Quality of service is difficult to guarantee in any network but is particularly elusive in such a dynamic, heterogeneous environment and ways are needed to ensure than MANET participants provide an equitable service to through-traffic.
- Internetworking protocols are necessary to link MANETs to the Internet infrastructure.
- Energy-efficiency is paramount if new generations of portable and embedded devices are to be ergonomic.

The PACE project (Protocols for Adhoc Collaborative Environments [40]) is concerned with the development of lightweight middleware protocols which can support collaboration among mobile users over an ad hoc network. The availability of a suite of middleware protocols simplifies the development of collaborative applications; since the topology of an ad hoc mobile network is not static, at least the services of a group membership protocol would be essential. PACE will develop a message communication model that accurately captures the characteristics of ad hoc networks. It will combine the best aspects of known models and seek to avoid the worst. It will then design and implement middleware protocols and evaluate their robustness against known group mobility models. IIS will need the services offered by MANET protocols to enable large distributed applications to be deployed on an ever-changing and potentially unreliable network infrastructure.

5 Smartdust

5.1 Overview

At the edge of the integrated communications infrastructure promised by 4G and augmented by MANETs will be wireless sensor networks. Large pervasive networks of simple devices will be deployed to gather information about the environment. Such networks have been termed as follows:

> ‘a *macroscope* that enables us to observe and interact with physical phenomena in real time and at a fidelity that was previously unobtainable’ [41].

Each device will contain a microprocessor, a two-way radio link and a number of sensors to measure light level, temperature, pollution levels or vehicle movement. The devices will autonomously form networks, forward each other’s information and act as a bridge to the roadside wired or wireless infrastructure. These devices are indistinguishable from class 4 RFID tags.

Over the last few years many different versions of wireless sensor devices (motes) have been designed and built by various companies and institutions. The size of these motes varies from the size of a box of matches to the size of a pen tip. The ultimate aim is to implement a mote that fits into a volume of one cubic millimetre. These motes have been nicknamed *Smartdust*. Current motes communicate in the ISM bands using proprietary protocols but standards are emerging (e.g. IEEE 802.15.4 Zigbee [42]) which will eventually allow motes and sensors from different manufacturers to be combined in the same network [43].

5.2 RF mote

The RF mote [23] was an early mote version which was finished in the first part of 1999. The device was designed by Seth Hollar at UC Berkeley. It consisted of an Atmel AT90LS8535 processor, a 916 MHz RF transceiver and 5 sensors (temperature, light, barometric pressure, a 2 axis accelerometer and a 2 axis magnetometer). It operates on a 3V lithium coin cell battery that can sustain a mote for 5 days of continuous operation or 1.5 years at a duty cycle of 1%. The mote used a single radio carrier frequency to transmit data and so only one device is able to transmit at any one time. The RF mote had a communication range of about 5–30 m at a rate of 5 Kbps depending on conditions. The RF mote was designed to use a serial operating system where only a single task can occur at any one time.

5.3 Laser mote

The laser mote [44] uses active laser communication to send sensor data over long distances. The mote runs off two AA batteries and contains humidity, light, temperature and pressure sensors. The laser transmitter, a laser module from a laser pointer, needs to be manually pointed towards the receiver. These motes can only send data back to a base station as they have no receiver module on board. These motes have been shown to transmit weather data over a distance of 21 km in the San Francisco Bay area. In this experiment a CCD camera linked to a laptop computer was used as the receiver. However due to the slow speed of the camera data were sent at extremely low data rates but with commercial high speed camera data rates in excess of 1 Kbps would be possible.

5.4 CCR mote

The CCR mote [44] was designed at UC Berkeley by Seth Hollar and Farrah Santoso. The mote was equipped with a temperature sensor and uses a corner cube reflector (CCR) module to allow passive laser communication. MEMS technology was used to construct the CCR. In order to communicate first of all an interrogator must project a diverged laser beam in the general direction of the motes. This beam contains commands to be executed by the motes. The motes receive this signal and by modulating and reflecting the beam back to the interrogator the mote can send back data if the command requires it to return data. The communication range is a function of the laser beams intensity.

5.5 Mini mote

The Mini mote [44] was designed by Seth Hollar and Christina Adela at UC Berkeley. The mote was a smaller version of the RF mote and has an Atmel AT90S2313 processor and an on-board temperature sensor. The Mini mote was cheaper to produce than the RF mote due to its smaller size and simpler circuit design. It could communicate via a radio link at 10 Kbps over a distance of 20 m depending on conditions.

5.6 weC mote

The weC mote [44] was designed by Seth Hollar and James McLurkin at UC Berkeley. The weC mote was an improved version of the Mini mote which had a number of additions and a slightly larger size. On-board it had temperature and light sensors as well as an integrated PCB antenna to improve the motes communication performance. The weC mote had a CPU clock rate of 4 MHz and was capable of being reprogrammed remotely over the radio through the sensor network it was part of. This allowed it to be adapted to carry out different tasks from the one it was originally programmed to do without the mote having to be collected from the field. The weC mote also used the TinyOS operating system.

5.7 MICA mote

The MICA mote [45] was a 2G commercial mote module (now obsolete) that was manufactured by Crossbow in the United States. It was mainly used for research and development of low power wireless sensor networks. The MICA mote platform was built around the Atmel Atmega 103L processor which was capable of running at 4 MHz. The MICA mote had 128 Kbytes of flash memory, a 512 kbyte serial flash, 4 Kbytes of SRAM and a 4 Kbyte EEPROM. TinyOS was used to control the mote and its sensors (Table 4).

The mote was able to communicate with the sensor network via a radio transceiver which used the RFM

Table 4: The MICA mote family [49]

Mote hardware platform		MICAz	MICA2	MICA2DOT	MICA
Models (as of August 2004)		MPR2400	MPR400/410/420	MPR500/510/520	MPR300/310
MCU	Chip	ATMega128L			ATMega103L
	Type	7.37 MHz, 8 bit		4 MHz, 8 bit	4 MHz, 8 bit
	Program memory (kB)	128			
	SRAM (kB)	4			
Sensor board	Type	51 pin		18 pin	51 pin
interface	10-Bit ADC	7.0 V to 3 V input		6.0 V to 3 V input	7.0 V to 3 V input
	UART	2		1	2
	Other interfaces	DIO, 12C		DIO	DIO, 12C
RF transceiver	Chip	CC2420	CC1000		TR1000
(radio)	Radio frequency (MHz)	2400	315/433/915		433/915
	Max. data rate (kbits/s)	250	38.4		40
	Antenna connector	MMCX		PCB solder hole	
Flash data	Chip	AT45DB014B			
logger memory	Connection type	SPI			
	Size (kB)	512			
Default power	Type	AA, 2x		Coin (CR2354)	AA, 2x
source	Typical capacity (mA-h)	2000		560	2000
	3.3 V booster	N/A			✓

Fig. 7 *A MICA2 Mote*

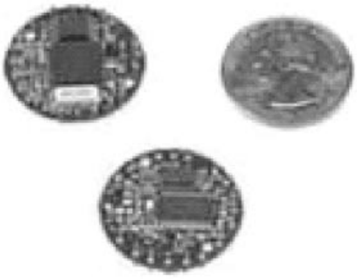

Fig. 8 *A MICA2DOT Mote*

TR1000 chipset, operated on the 916 or 433 MHz ISM bands and could carry data at 40 Kbps over distances of up to 100 feet.

Power was provided by two AA batteries and the device had a battery life of roughly 1 year depending on the application (very low duty cycle assumed). Sensor boards could be attached via a surface mount 51 pin connector that supported analogue input, I2C, SPI, UART and a multiplexed address/data bus. Sensors are available for light, temperature, sound, humidity, pressure, acceleration and magnetic fields. Users can add their own sensors using a prototyping board.

5.8 MICA2 mote

The Mica2 mote [46] is a 3G commercial mote. Like the Mica mote it is produced by Crossbow and used mainly for research and development. The Mica2 mote has the same processor and memory as the MICA mote but the radio transceiver uses the Chipcon CC1000 chipset and operates on either the 433 MHz band or the 868/916 MHz ISM bands with a data rate of 38.4 Kbps and a maximum outdoor range of 500 feet. The CC1000 accepts data from the processor byte by byte whereas the TR1000 accepted data bit by bit. Thus the processor on the MICA2 is freed from having to convert data to a bit stream for transmission (Fig. 7).

Like the MICA mote the MICA2 uses TinyOS in order to control the mote and its attached sensors. The MICA2 also allows every mote to function as a router and supports remote reprogramming over the sensor network. The MICA2 accepts the same sensor boards as the MICA.

5.9 MICA2Dot mote

The MICA2Dot mote [47] is a coin sized mote that is very similar to the MICA2. The mote has the same processor, memory and Chipcon CC1000 as the MICA2 mote and so has the same radio communication capabilities. The MICA2Dot mote operates using a 3 V coin cell battery and has reduced input/output capabilities (Fig. 8). The mote has a temperature sensor and LED on board as well as a ring of 18 solder-less expansion pins to enable extra sensor boards to be added. A range of boards are available with a subset of the sensor capabilities of the MICA and MICA2.

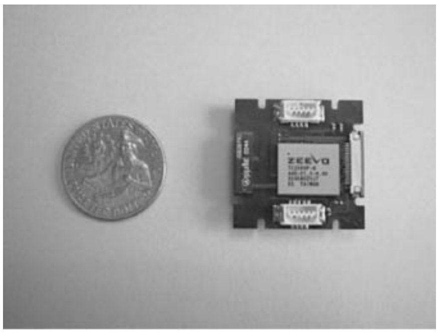

Fig. 9 *An Intel MOTE*

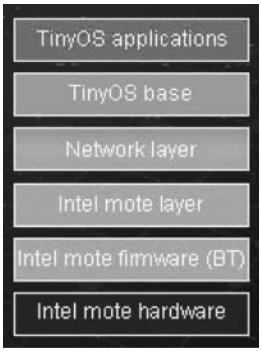

Fig. 10 *The Intel MOTE software stack*

5.10 MICAz

The MICAz mote [48] is identical to the MICA2 mote except that the radio transceiver uses the Chipcon CC2420 IEEE 802.15.4 (Zigbee) compliant chipset. This will allow the MICAz to communicate with equipment from other manufacturers. TinyOS implements basic communication but to date, there is no full implementation of the Bluetooth communications stack.

5.11 Intel mote

The aim of Intel's Deep Networking research project [50] was to develop a mote with more CPU power, digital signal processing, a more reliable wireless radio and better security features. The modular design of the original Berkeley motes was maintained whilst Intel worked on improving battery life and reducing costs (Fig. 9). The team is striving to design an ultra low-power mote that is about two orders of magnitude below the operational power of traditional low-power platforms (such as Intel XScale® based designs). This ultra low-power mote will require smart wireless communication capabilities to achieve a battery life of 6 months to 1 year using an operational duty cycle of 1% or less.

The Intel mote consists of a powerful ARM processor, SRAM and flash memory. Communication with other motes is via Bluetooth technology with the platform supporting alternative radio technologies as add on modules (Fig. 10). Optional sensor boards and an optional power regulator are also available. The goal is to find a cost-efficient way of integrating all the devices that are part of the Intel Mote platform: the CPU core, analog and digital radio components, and Flash and SRAM memory, as well as some of the sensors, which may be MEMS based. Ultimately, the goal is to integrate all of these features into a single system on a chip (SoC) or system in a package (SiP).

Intel Mote software is based on Tiny OS. The software stack includes an Intel Mote-specific layer with Bluetooth support and platform device drivers, as well as a network layer for topology establishment and single/multi-hop routing. The software will also incorporate security features, including authentication and encryption in the near future.

5.12 Energy scavenging

The size and efficiency of smartdust power sources will see great advances over the next few years, thanks to the huge commercial drive from a number of markets such as mobile phones, laptops and PDAs. Hydrogen fuel cell technology is set to replace lithium-ion batteries in mobile phones in the near future and MEMS fuel cells are in development that will increase the achievable power density even further. Smartdust will incorporate these micro-fuel cells, extending their lifetime by an order of magnitude.

Today, Smartdust devices using passive optical communications are able to operate using around 20 μW of power [51]. In contrast communication using RF transmission requires several mW. The best energy density achievable using modern batteries is around 1 J/mm^3—this equates to a best-case of 14 h operation of today's mote using a cubic mm battery. Micro fuel-cells are predicted to store around 10 J/mm^3, giving a 140 h mote lifetime using today's available hardware. It is reasonable to assume that advances in sensor, communication and processing design will reduce the average power requirements for Smartdust motes; an RF device that uses 1 mW, or a 10 μW optical device, will be possible and energy densities of 20 J/mm^3 will result from advances in fuel cells. However this still only provides 560 h or 23 days of continuous operation in the best case. It is therefore likely that Smartdust motes of the future will require some means of gathering and storing energy from their surroundings. This may be in the form of advanced solar cells [52], vibration powered dynamos [53] or efficient thermal devices [54].

In direct sunlight during the daytime, approximately 100 mW/cm^2 of power falls on the Earth's surface. If 100% of this power can be utilised and stored for operation during night-time, it is easily enough to power Smartdust using a 5 mm^2 solar collector. Unfortunately, the requirements are much more restrictive than this. At the moment, the maximum achievable efficiency of solar cells is 30%, but the power available from the sun falls dramatically on cloudy days, indoors or in shady places. The Smartdust of the future will incorporate solar energy collection as one means of acquiring power, but will augment this with further energy scavenging from vibrations or thermal gradients.

Extracting energy from vibrations involves using a small mass to induce a voltage either through a capacitive, inductive or piezoelectric effect. Using a 0.5 cm^3 mass, power outputs of 250 μW have been achieved [55]. However, the amount of power generated by these schemes is dependent on the size of the mass used; making it difficult to extract large amounts of power as devices become smaller and smaller. Also, this power source is highly dependent on the location of the individual Smartdust motes and operates most effectively only when the resonant frequency of the vibrating mass can be tuned to the local vibrations present in the mote's environment. As an alternative, thermal gradients are an attractive source of power because they exist in a wide variety of locations—such as between a lake and the air above it, near machinery or the human body or around vegetation. Experimental devices have been constructed that output 15 μW cm^3 and it is predicted that as much as 30 μW cm^3 is achievable [56].

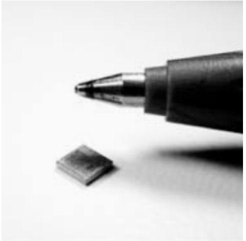

Fig. 11 *A Spec MOTE*

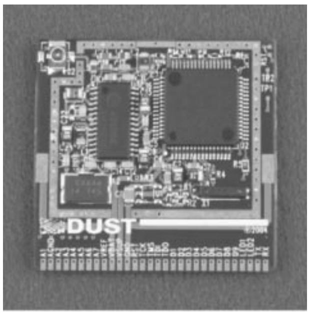

Fig. 12 *Prototype Smartdust*

Power scavenging from other sources is also envisaged, such as artificial photosynthesis [57], power from the human body [58] and intelligent scavenging in which devices are capable of drawing power from a range of sources. It is likely that as advances in other areas reduce the burden on Smartdust power supplies, drawing energy from a number of environmental sources and making informed decisions on the use of this energy will enable motes to remain active indefinitely.

5.13 Future trajectory

Spec [59] was developed by a team of researchers at UC Berkeley and is approximately 2 mm by 2.5 mm in size. Spec is a fully working single chip mote which has a RISC core and 3 Kbytes of memory. Spec uses radio communication on the 902.4 MHz band. In tests Spec has been shown to communicate over 40 ft indoors with a data rate of 19.2 Kbps (Fig. 11).

Dust Networks Inc. was founded in 2002 by a team including Kris Pister, a professor at the University of California, Berkeley, and the originator of the Smartdust concept. The company was founded to exploit the research results emerging from Berkeley with the aim of developing Smartdust, extremely small MOTES. Since then, the company has developed a wireless mesh networking system for sensing and control applications. Their products are similar in size to the MICA2DOT (Fig. 12). The M1010 MOTE also uses a similar radio to the MICA2DOT while the M2020 MOTE uses a Zigbee chipset, similar to the MICAz.

The development of ever-smaller and more capable smartdust will continue. Devices as small as a finger nail are already being produced in laboratories. Commercialisation of this technology is likely due to the enormous number of potential applications. It is difficult to distinguish between RFID and smartdust and any distinction is likely to disappear within 5 years. As

RFID becomes cheaper, smartdust will take advantage of the production processes to deliver what are effectively high-end RFID tags. Miniaturisation of the technology may be considered inevitable; it is driven by the same technologies as the semiconductor industry. Laser-based communications are far more energy efficient than current omni-directional radio. The key challenges still to be overcome if smartdust is to become a reality in IIS are high-gain, active directional antennae and energy scavenging.

6 Software for data collection

6.1 Overview

Applications which are distributed over traditional computer networks often consist of distinct programs, one per computer, which communicate using message passing mechanisms provided by their operating system. In such applications, communication is explicit. While this approach is manageable in networks of a few tens or hundreds of computers, it becomes unmanageable where thousands of computers are concerned. Wireless sensor networks are envisaged which may incorporate many thousands of sensor nodes. Links between nodes are unreliable and the nodes themselves may fail. Explicit programming of communication in these networks is at best difficult and at the same time undesirable. In a wireless sensor network, it is the information about the environment at a specific location which is of concern. The physical address of the node which can sense the environment at that location is unimportant and should ideally be hidden from the application. The application programmer would like to be able to ask question of the environment such as ‘what is the air temperature and humidity in the city’. What is needed is a software layer in the network which can translate such a query into a pattern of communication designed to obtain the desired information. This layer will abstract away the physical topology and hence tolerate unreliable communication links and failing nodes. The application programmer can then consider the environment as a database of real-world information to be queried like any other database.

6.2 TinyDB

There are several commercial and public domain software systems which aim to provide this abstraction of an environmental database. Once such system called TinyDB [60] was specifically developed to run on TinyOS, the operating system executed by the MOTES described in preceding sections of this document. TinyDB is a query processing system for the extraction of environmental information from a distributed network of sensor nodes. TinyDB relieves the application programmer from the necessity to write code. Instead, it provides an SQL-like (structured query language) interface to the network which incorporates the type of information to be sensed, the area(s) to be sensed and the time interval between samples. TinyDB handles the complexity of routing the queries to nodes in the area to be sensed and routing the resultant replies back to the requester. This semantic energy-efficient routing copes with changes in network topology and disappearing nodes as well as incremental expansion or contraction of the network. TinyDB supports concurrent queries, so for example, temperature could be sampled in one area at a given rate while at the same time, humidity could be sampled in a different area at a different rate.

Queries in TinyDB, as in SQL, consist of a SELECT-FROM-WHERE-GROUPBY clause supporting selection, join, projection and aggregation. The semantics of SELECT, FROM, WHERE and GROUP BY clauses are as in SQL. The FROM clause may refer to both the sensors table as well as stored tables. A typical TinyDB query is shown below.

```
SELECT roomno, AVG(light)
FROM sensors
GROUP BY roomno
HAVING AVG(light) >l
EPOCH DURATION 5 min
```

The query is designed to generate a snapshot of occupied rooms in a building every 5 min. A room is deemed to be occupied if the lights have been turned on —a realistic situation where lighting is automatically turned on whenever movement is detected within a room. TinyDB automatically interrogates all the sensors in a given room and calculates the average light level. One difference between this TinyDB query and a typical SQL query is that this single query will produce multiple responses—in this case, every 5 min forever. Nodes in TinyDB run a simple time synchronization protocol to agree on a global time base that allows them to start and end each epoch at the same time.

TinyDB also supports event-based queries so that a query response is delivered when some external event occurs.

```
ON EVENT bird-detect (loc):
SELECT AVG (light), AVG (temp), event.loc
FROM sensors AS s
WHERE dist (s.loc, event.loc) <10 m
SAMPLE INTERVAL 2 s for 30 s
```

The query samples and averages local light and temperature readings at 2 s intervals for a period of 30 s after a bird is detected within 10 m. Again, a single query produces multiple responses but for a finite time. This approach allows the system to be dormant until some external conditions occur, instead of continually polling or blocking on an iterator waiting for some data to arrive. Since most microprocessors include external interrupt lines that can wake a sleeping device to begin processing, events can provide significant reductions in power consumption, shown in Figure 13.

Both the above example queries periodically return sensed information to the node which issued the query (Fig. 13). In some applications this mode of operation is required. However, it may be more power-efficient to have each node store sensed values locally until they are requested by a TinyDB query. Where very large networks are deployed, there will be insufficient bandwidth to extract raw sensor information through a single AP for processing. Instead, information will be processed locally and only meta-information or alarms will be extracted.

```
CREATE
STORAGE POINT recentlight SIZE 8
AS (SELECT nodeid, light FROM sensors
SAMPLE PERIOD 10 s)
```

This query causes each node to sample light levels each 10 s and store the eight most recent samples in an array. A further TinyDB query may subsequently be issued to retrieve and process the data.

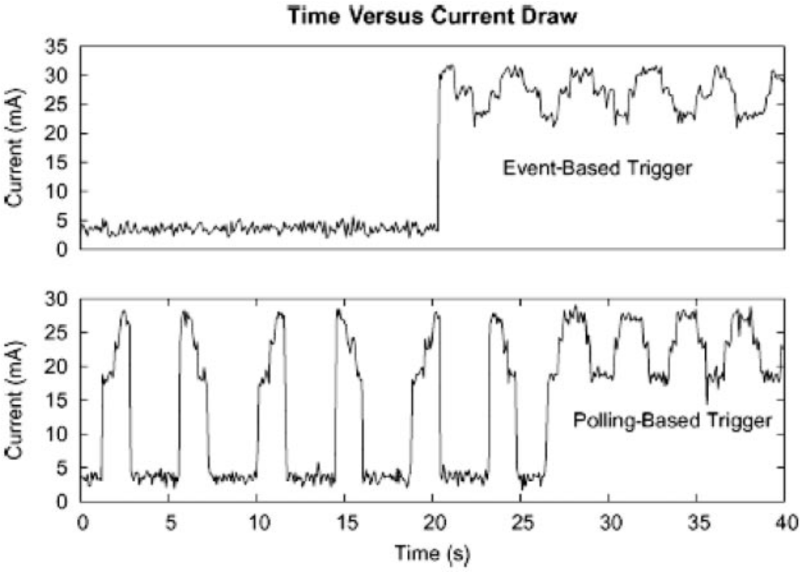

Fig. 13 *External interrupt driven query versus polling driven query*

```
SELECT COUNT(*)
FROM sensors AS s, recentLight AS rl
WHERE rl.nodeid = s.nodeid
AND s.light < rl.light
SAMPLE PERIOD 10 s
```

This TinyDB query outputs a stream of counts indicating the number of recent light readings (from zero to eight samples in the past) that were brighter than the current reading.

6.3 Future trajectory

The ability of application programmers to ignore network topology and focus on the information sensed will become a necessity as networks of thousands of sensors are deployed. One thread of research is aimed at extending IPs (TCP/IP) to wireless sensor networks [61] to produce an *Internet of Things* which has the advantage that applications written for the Internet can be seamlessly transferred to a wireless sensor network, albeit with performance implications. An alternative thread of research is concerned with the implementation of a *browsing reality* paradigm [62] where information on the real world is gathered by issuing a query, as with a conventional database, which has the advantage that information can be filtered, aggregated and presented in a way which suits the recipient. *The Internet of Things* may be viewed as a conservative node-centric approach while *browsing reality* may be viewed as a more radical information-centric approach. Any future IIS is likely to take advantage of both approaches. Node-centric is appropriate when it is the identity of the node which is important; such as PDAs carried by people and vehicle on-board units. Information-centric is appropriate when it is the information and its location which is important; such as ubiquitous pollution monitoring in urban environments.

7 Novel fabrication techniques

7.1 Surface mount

Surface mount has largely taken over from printed circuit boards containing conventional components as the preferred method of producing wireless sensor devices (Fig. 14). Current MOTES use surface-mount techniques. The advantages are that size of the device can be reduced without major changes in system design, as long as the component IC manufacturers offer a surface mount option for their ICs.

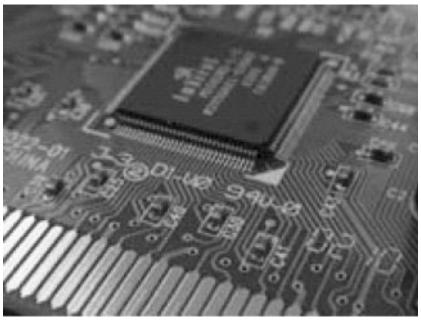

Fig. 14 *Surface mount packaging*

7.2 System in package

SiP takes the next logical integration step from surface mount by merging all of the electronic requirements of a functional system into one IC package. SiPs are small in physical size and incorporate [63] the following:

- flip chip, wirebond or other interconnect directly into the chip,
- passive components surface mounted discrete components,
- passive components embedded into or manufactured on the substrate material,
- more than one IC chip die, and
- other components such as housings, lids, RF shields, connectors, antennas, batteries, etc.

SiP has a parallel in SoC technology (Fig. 15). SoC is limited by what can be achieved within one wafer process. SiP is not limited by the constraint of a common wafer process, so that IC chips, each optimally suited for its function by both design and wafer fab process, can be easily combined together in one package (for example a CMOS digital IC with a GaAs HBT RF IC).

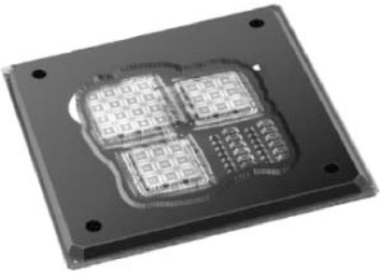

Fig. 15 *System-in-package*

There are several reasons why there is a market demand for SiP solutions:

- Size: The size of subsystem can be reduced by integrating multiple ICs and other components in an SiP
- Time to market: It is faster to combine ICs in an SiP than it is to implement SoC at the IC level. It is also faster to make changes to the system at the SiP level than to change the entire mask set of an SoC solution.
- Complexity: SiP solutions reduce the complexity of the motherboard by moving the routing complexity to the package substrate. This often results in reduced layer count in the motherboard and simplifies product design.
- Performance: CPU to memory data speeds are enhanced by combining the chips close to one another in the SiP and power is reduced by minimizing line lengths (and hence capacitive loads) between ICs in an SiP.
- Radio: for RF & Wireless SiPs the package is a part of the circuit and the package design and material selection can have a great impact on whether the RF circuit functions as intended.
- Flexibility: fully integrated SiP solutions enable system designers to implement additional functions, such as Bluetooth or camera modules, into a wireless sensor node with minimal design effort.
- Lower system cost: an optimized SiP solution usually results in an overall system cost reduction compared to discrete IC packages.
- Heterogeneity: SiP enables the system designer to mix and match IC technology in order to optimize the performance of each functional block.

7.3 System on Chip

SoC is a technology which allows very large complex systems to be produced on a single silicon substrate. The integration side of SoC design starts with partitioning of the system around the primarily pre-existing, blocklevel functions and identifying the new or differentiating functions needed. System-On-a-Chip design requires *system expertise* in order to maximise the effect of translating system functionality to a single-chip implementation.

The chip production technology for SoC is no different from that used for conventional ICs. The difference lies in the design tools. Virtual IC designs become the building blocks of the SoC design and the tools must support design at the macro-level. Tools range from the circuit-design type which allow simulation of the SoC to co-design tools which allow the designer to move the boundaries between what is considered to be software and what is implemented in hardware.

Fig. 16 *An RFID printer*

7.4 RFID printing

Smart labels refer to labels with embedded ultra-thin RFID tags. Tags for smart labels in the 13.56 MHz, 900 MHz and 2.45 GHz frequency ranges are readily available. Many leading semiconductor manufacturers, including Philips Semiconductor and Texas Instruments, produce a wide variety of RFID chips. Smart labels are called ‘smart’ because of the flexible capabilities provided by the silicon chip embedded in the transponder. The transponder, in most cases, can be programmed and reprogrammed in the field, so the same label can be reused to serve multiple needs in a given application (Fig. 16). Hence, the label is no longer static like a bar code label, but rather is dynamic in its performance capability when equipped with RFID.

Smart label printers function as traditional thermal models when creating bar codes, graphics and human-readable text. However, they also have RFID encoders and readers embedded inside. Before the label is printed, the RFID data are encoded on the. Following encoding, the tag is read to ensure data accuracy. The label is then fed forward for printing.

7.5 3D printing

Three-dimensional (3D) printing functions by building parts in layers. From a computer (CAD) model of the desired part, a slicing algorithm draws detailed information for every layer. Each layer begins with a thin distribution of powder spread over the surface of a powder bed. Using a technology similar to ink-jet printing, a binder material selectively joins particles where the object is to be formed (Fig. 17). A piston that supports the powder bed and the part-in-progress lowers so that the next powder layer can be spread and selectively joined. This layer-by-layer process repeats until the part is completed. Following a heat treatment, unbound powder is removed, leaving the fabricated part [64].

3D printing technology is aimed at the production of mechanical parts rather than electronics but may have a use in the fabrication of sensors and actuators.

7.6 Future trajectory

The semiconductor industry continues to improve on materials and production processes. They predict [65, 66] that by 2018, processor speeds will increase to 50 GHz; power consumption will be reduced. However, as feature-size drops below 20 nm (around 2009), new physical effects come into play. The industry is aware of this potential roadblock to Moore’s Law:

> ‘The characterization of critical material properties at the nanometer scale ... is very limited and

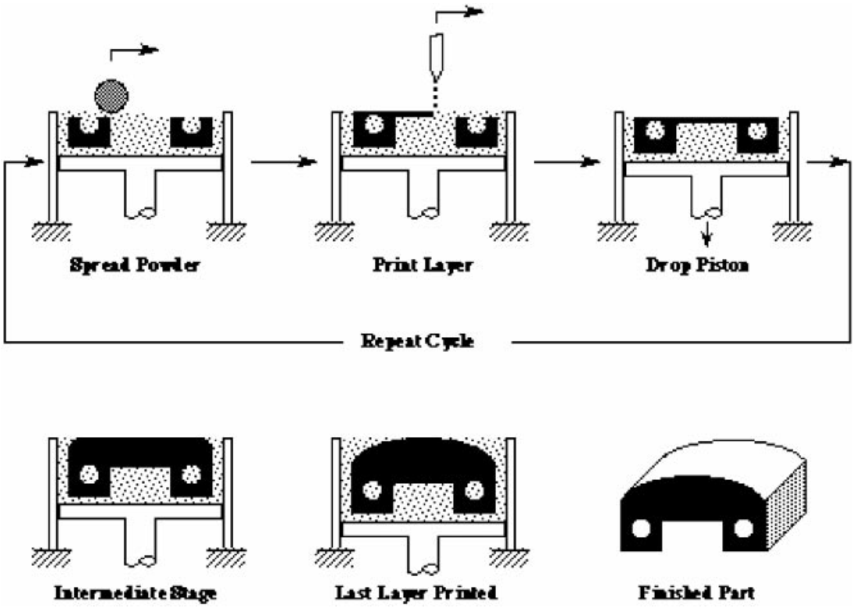

Fig. 17 *3D printing*

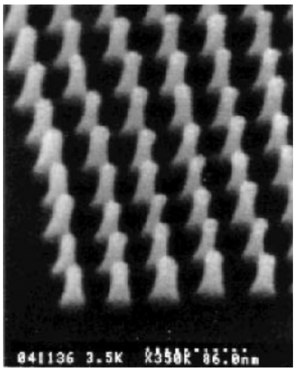

Fig. 18 *Nanoimprint Lithography*

> may hinder our ability to improve materials properties' [66].

It is clear to the industry that new processes and materials are required if progress is to be maintained. Revolutionary approaches to fabrication may lead to smart materials in which the computing is truly embedded. Materials will themselves be systems, sensing their environment, computing a response and actuating that response.

One approach to nano-scale fabrication is that of nanoimprint lithography [67]. The tools used to mass-produce silicon microchips are far too *blunt* for nanofabrication, and specialized lab methods are far too expensive and time-consuming to be practical (Fig. 18). A mechanism just slightly more sophisticated than a printing press could be the answer. By stamping a hard mould into a soft material, researchers have faithfully imprinted features smaller than 10 nm across. By flashing the solid with a powerful laser, the surface was melted just long enough to press in the mould and imprint the desired features. The investors of this technology claim that it is a viable alternative to the processes currently used by the semiconductor industry.

Printed polymer electronics using organic semiconductor materials is a potential route to very large-scale production of low cost wireless sensor devices [68]. Costs would be reduced to such levels that the devices would be considered disposable (as anti-theft RFID tags are today). Devices could be incorporated into everyday objects to deliver Weiser's vision [1]. Electrically conducting polymers are relatively new but they have already been used to prototype simple, flexible RFID tags (Fig. 19).

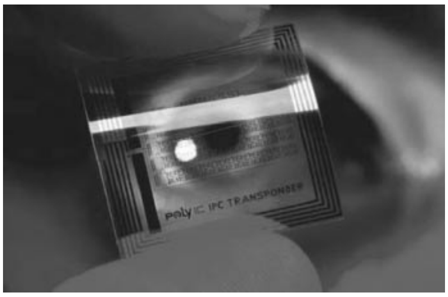

Fig. 19 *Printed polymer electronics*

8 Sensors

8.1 Overview

Current wireless sensor networks employ conventional technologies to interact with their environment. Often the wireless component is a single point-to-point link to a base station which merely replaces a single cable with radio [43]. Transducers are relatively large and will not scale as network nodes become Smartdust. New sensors will be required to operate on the atomic scale and such sensors will have to communicate with each other over vast areas using multi-hop routing algorithms.

8.2 Standards

Many companies are developing various wireless communication interfaces and protocols for sensors. An openly defined wireless transducer communication standard, which can accommodate various existing wireless technologies, will reduce risk for users, transducer manufacturers and system integrators. It will enhance the acceptance of the wireless technology for transducers connectivity. A family of standards IEEE 1451 is under development by the IEEE wireless sensor working group [69]. The standards will define protocols

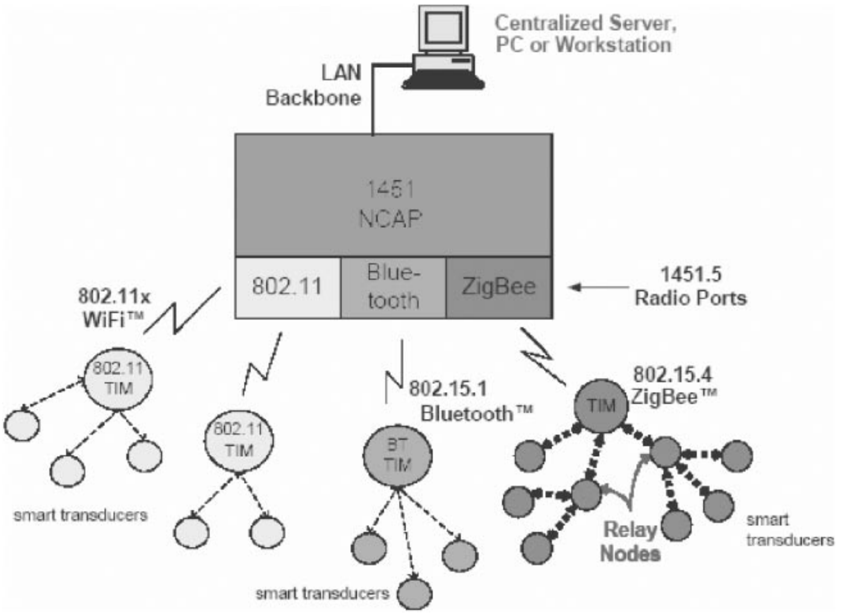

Fig. 20 *IEEE 1451.5 A smart transducer interface for sensors and actuators*

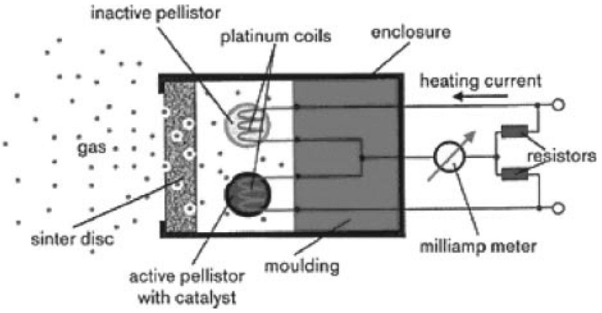

Fig. 21 *An electrochemical sensor [12]*

which are capable of running over a variety of physical layer protocols such as IEEE 802.11 WiFi, IEEE 802.15.1 Bluetooth and IEEE 802.15.4 Zigbee, as shown in Fig. 20.

8.3 Electrochemical sensors

Electrochemical sensors are the most popular sensing method for toxic gases and oxygen monitoring. They are not used for combustible gas monitoring.

The electrochemical sensor is a self-powered micro-fuel cell. The cell consists of a casing containing a gel or electrolyte and two active electrodes: the working electrode (anode) and the counter-electrode (cathode). The top of the casing has a membrane which can be permeated by the gas sample. Oxidization takes place at the anode and reduction at the cathode. A current is created as the positive ions flow to the cathode and the negative ions flow to the anode. Gases such as oxygen, nitrogen oxides and chlorine which are electrochemically reducible are sensed at the cathode while those which are electrochemically oxidizable such as carbon monoxide, nitrogen dioxide and hydrogen sulphide are sensed at the anode (Fig. 21).

Advantages: they can be specific to a particular gas or vapour. They are typically very accurate even at low ppm levels. Because they contain their own energy source, they do not impose a drain on the battery of the host node [16].

Disadvantages: they have a narrow temperature range. They have a short shelf life. They are subject to several interfering gases such as hydrogen. Sensor lifetime will be shortened in very dry and very hot areas.

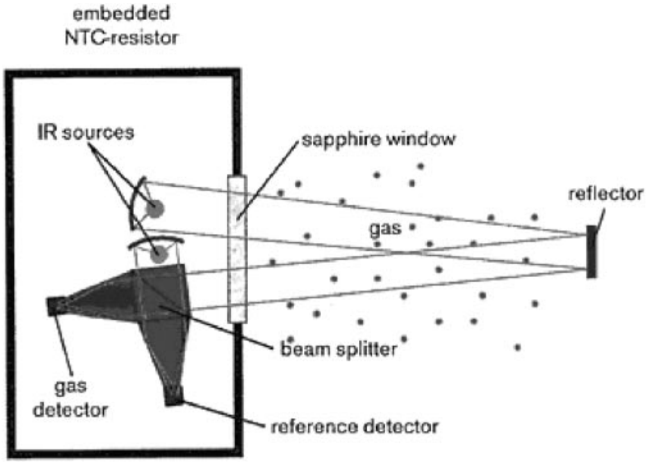

Fig. 22 *An infrared optical sensor [12]*

8.4 Optical sensors

Infrared gas sensors exploit the property that many gases absorb radiation in the 2–14 μm, infrared region of the spectrum showing features which may be regarded as *fingerprints* to identify the gases and enable their concentrations to be deduced. The sensor bodies contain an infrared source and infrared detectors inside a compact and combined gas cavity/optical cell. The detectors have infrared bandpass filters placed in front, which tune them to the specific gases to be sensed. When the specific gas enters the cavity it is registered as a change in detector signal. The magnitude of this change is related to the concentration of that gas via a simple exponential formula. Sensors are available to detect a variety of gases including methane, acetylene, ethylene, propane and carbon dioxide (Fig. 22).

Advantages: they can be made specific to a particular gas, they require less calibration than other sensors, there is no contact with the gas, no minimum level of oxygen is necessary and they are relatively maintenance free.

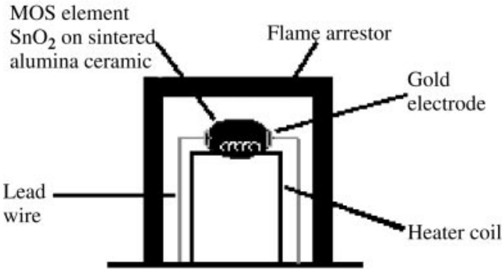

Fig. 23 *A semiconductor sensor*

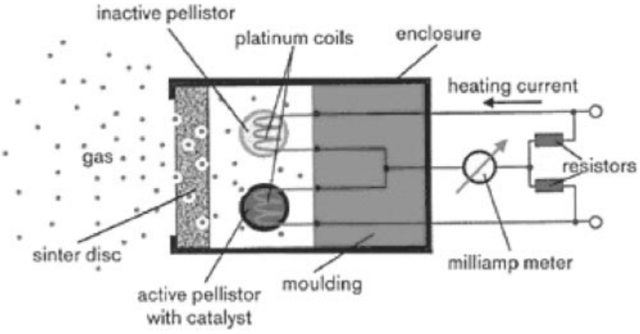

Fig. 24 *A pellistor sensor [12]*

Disadvantages: they cannot monitor all gases, they can be affected by humidity and water, they can be expensive and dust and dirt can coat the optics and impair response. Typical devices consume about 300 mW [16], largely due to the infra-red source, which makes them unsuitable for large-scale networks of battery-powered sensor nodes. Sensors can take up to 30 s to detect the presence of their target gas.

8.5 Semiconductor sensors

Semiconductor sensors are used for hydrogen sulfide (H_2S) gas measurements but as well as in certain combustible hydrocarbon (CHC) measuring applications. Semiconductor sensors are one of the best sensors for H_2S gas monitoring where sensitivity to low concentrations (ppm range) is required.

A semiconducting material is applied to a non-conducting substrate between two electrodes. The substrate is heated to a temperature such that the gas being monitored can cause a reversible change in the conductivity of the semiconducting material. Under zero gas conditions, Oxygen (O_2) molecules tie up free electrons in the semiconductor material by absorbing to its surface, thereby inhibiting electrical flow. As H_2S or CHC gas or vapour molecules are introduced, they replace the O_2, releasing the free electrons and decreasing the resistance between the electrodes. This change in resistance is measured electrically and is proportional to the concentration of the gas being measured (Fig. 23).

MOS sensors are *broad range* devices designed to respond to the widest possible range of toxic and combustible gases, including chlorinated solvent vapours and other contaminants difficult to detect by other means. This non-specificity can be advantageous in situations where unknown toxic gases may be present, and a simple go/no-go determination of the presence of toxic contaminants is sufficient

Advantages: small, mechanically rugged, ppm sensitive, inexpensive.

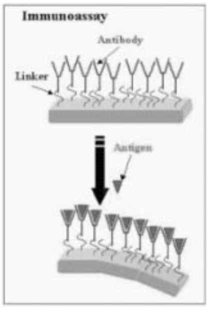

Fig. 25 *A microcantilever sensor*

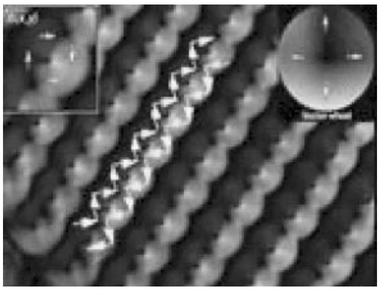

Fig. 26 *Semiconducting nanocrystals*

Disadvantages: sensitive to humidity, sensitive to temperature, non-specific to gases and vapours. The quality of sensors varies widely from manufacturer to manufacturer with substantial variations in performance often found from a single manufacturer.

8.6 Pellistor sensors

The concept of the pellistor is based on the fact that the most foolproof way to determine whether a flammable gas is present in air is to test a sample by trying to burn it!

A catalytic combustion sensor (pellistor sensor) consists of a sensor element, and compensation element, made by a carrier on a coil of platinum wire with noble metal catalysts and sintering at high temperature as shown in Fig. 24. The sensor measures the rise in temperature (change in resistance) of a platinum wire coil due to the catalytic combustion of the gas on the surface of the catalyst.

This temperature rise is directly proportional to the concentration of the gas, and since the resistance of the wire also changes in proportion to the rise in temperature, the gas concentration can be measured by using a bridge circuit to measure the difference in potential between the sensor element (detector) and compensation element (compensator).

Although low-power Pellistor sensors are available [16], they typically consume more than 250 mW which makes them unsuitable for large-scale networks of battery-powered sensor nodes.

8.7 Future trajectory

Biosensors are chemical sensors which consist of a receptor (biocomponent), transducer (physical component) and a separator (membrane). Receptor interacts with the target and produces a measurable component. Transducer converts the component into a measurable signal (electrical or optical). The membrane links the receptor to the transducer while preventing contamination of the transducer [70].

A typical example of such a biosensor which can be built using current technology is a microcantilever. The device operates when a chemical (or biological) agent coating on one surface of the cantilever reacts with the target (to be sensed) chemical causing a small deflection. This deflection is detected and converted to an electrical signal using a piezo-resistive coating. Advances in nanoscale fabrication technology will allow arrays of micro-cantilevers to produce, each coated with a different agent, to generate a chemical profile of the environment.

The US is investing heavily in the development of biosensors for the healthcare, food and automotive industries [77]. Current and near-future markets for biosensors include the following:

- instant cholesterol and cardiac risk tests;
- faster, more accurate cancer diagnostics;
- automobile cabin air quality monitors;
- fuel cell vehicle safety monitors;
- quick tests for food pathogens such as *Escherichia coli*;
- CO sensors for home smoke detectors;
- auto emission testing analyzers;
- portable water pollution monitors;
- chemical and biological warfare agent detectors;
- blood alcohol breath analyzers.

Semiconducting nanocrystals (often called quantum dots or nanodots) are very small transistors that have unique optical properties only observed on the nanoscale—the addition or removal of an electron changes a dot's characteristics. By incorporating nanodots into sensors, it will be possible to recognize the presence of a single molecule of a substance. A sensor as sensitive as this is critical for detecting solids and liquids with low vapour pressure, such as high explosives and VX nerve agent. Researchers are also exploring the use of nanodots to detect biological agents, which may lead to the development of new ways to detect infectious diseases or anthrax spores, displacing today's state-of-the-art DNA detectors [16].

9 Acknowledgments

This report was commissioned by the Foresight Programme of the Office of Science and Innovation, Department of Trade and Industry to support its project on intelligent infrastructure systems. Any opinions expressed have emerged from reviewing existing futures work and are not those of the Office of Science and Innovation.

10 References

1 Weiser, M.: 'The computer for the 21st century', *Sci. Am.*, 1991, **265**, pp. 94–104

2 ITC: 'Guide to scanning technologies'. [Internet] (Intermec Technologies Corporation, 2003, 2nd edn). http://epsfiles.intermec.com/eps_files/eps_wp/GuideToScanningTech_wp_web.pdf, accessed May 2005

3 Williams, D.: 'The strategic implications of Wal-Mart's RFID mandate'. [Internet]. (Directions magazine, 2004). http://www.directionsmag.com/article.php?article_id = 629&trv = 1&PHPSESSID = 8c5fa2d7cf88e231a6b4343c6860bd4a, accessed May 2005

4 7595179 Stanford, V.: 'Pervasive computing goes the last hundred feet with RFID systems', *IEEE Pervasive Comput.*, 2003, **2**, (2), pp. 9–13. http://ieeexplore.ieee.org/iel5/7756/27106/01203746.pdf?isnumber = 27106&prod = JNL&arnumber = 1203746&arSt = + 9&ared = + 14&arAuthor = Stanford%2C + V, accessed May 2005

5 ITC: 'Supply chain RFID: how it works and why it pays'. [Internet] (Intermec Technologies Corporation, 2003). http://epsfiles.intermec.com/eps_files/eps_wp/SupplyChainRFID_wp_web.pdf, accessed May 2005

6 LaranRFID: 'A basic introduction to RFID technology and its use in the supply chain'. [Internet], (LaranRFID, revised edn). http://admin.laranrfid.com/media/files/WhitePaperRFID.pdf, accessed May 2005

7 Juels, A., and Pappu, R.: 'Squealing Euros: privacy protection in RFID-enabled banknotes'. [Internet] (2005). http://www.only4gurus.net/rsa/euro.pdf, accessed June 2005

8 ParcelCall: 'Deliverable 11: Final system concept'. Project IST-1999-10700. (2002)

9 RedPrarie: 'RFID: just the facts'. [Internet]. (RedPrarie, 2003). http://www.redprairie.com/uk/Knowledge%20Center/Documents.aspx?did = 30, accessed May 2005

10 CEPT UHF: 'Electromagnetic compatibility and radio spectrum matters (ERM); radio frequency identification equipment operating in the band 865 MHz to 868 MHz with power levels up to 2 W; part 1: technical requirements and methods of measurement'. [Internet] (2005). http://webapp.etsi.org/action%5CV/V20040903/en_30220801v010101v.pdf, accessed May 2005

11 Hightechaid: 'ISO/IEC 18000 - RFID air interface standards'. [Internet] (2005). http://www.hightechaid.com/standards/18000.htm, accessed May 2005

12 ISO 18000: 'Radio frequency identification for item management'. [Internet] (2005). http://www.iso.org/iso/en/CombinedQuery Result.CombinedQueryResult?queryString = 18000, accessed May 2005

13 EPCglobal: 'EPCglobal Inc'. [Internet] (2005). http://www.epcglobalinc.org/index.html, accessed May 2005

14 EPCglobal: 'The EPCglobal Network™'. [Internet] (2004). http://www.epcglobalinc.org/news/EPCglobal_Network_Overview_10072004.pdf, accessed May 2005

15 Strasburg, J., and Yi, M.: 'Benetton to track clothes by using tiny chips' [Internet]. (San Francisco Chronicle, 2003). http://seattlepi.nwsource.com/business/112912_clothingchip18.shtml, accessed May 2005

16 I-CODE: 'Smart label technology'. [Internet] (Philips Electronics, 2005). http://www.semiconductors.philips.com/markets/identification/products/icode/, accessed May 2005

17 Marks & Spencer: 'Background to Marks & Spencer's business trial of RFID in its clothing supply chain'. [Internet] (2005). http://www2.marksandspencer.com/thecompany/mediacentre/pressreleases/2005/com2005-02-18-00.shtml, accessed May 2005

18 Emigh, J.: 'RSA finds more flaws in RFID'. [Internet] (2005). http://www.eweek.com/article2/0%2C1759%2C1778694%2C00.asp, accessed May 2005

19 Bono, S. *et al.*: 'Security analysis of a cryptographically-enabled RFID device'. [Internet] (2005). http://www.rfidanalysis.org/DSTbreak.pdf, accessed May 2005

20 Speedpass: 'Life should be this easy'. [Internet]. (Exxon Mobil, 2004). http://www.speedpass.com/home.jsp, accessed May 2005

21 TI-RFid: 'Automotive applications'. [Internet]. (Texas Instruments, 2005). http://www.ti.com/rfid/docs/applications/auto/autoApp.shtml, accessed May 2005

22 Lipton, E.: 'Bowing to critics, U.S. to alter design of electronic passports'. [Internet], (New York Times, 2005). http://www.nytimes.com/2005/04/27/politics/27passport.html?ex = 1272254400&en = 2c60e9474291cebd&ei = 5090&partner = rssuserland&emc = rss&YOUR_REG_SYSTEM_SUCKS_NYT, accessed May 2005

23 3GPP: 'Universal mobile telecommunications system (UMTS); quality of service (QoS) concept and architecture'. [Internet], 3GPP TS 23.107 version 6.2.0 Release 6. (2004). http://www.3gpp.org/ftp/Specs/html-info/23107.htm, accessed May 2005

24 6792088 Ohmori, S., Yamao, Y., and Nakajima, N.: 'The future generations of mobile communications based on broadband access technologies', *IEEE Commun. Mag.*, 2000, **38**, (12), pp. 134–142. http://ieeexplore.ieee.org/iel5/35/19207/00888267.pdf?isnumber = 19207&prod = JNL&arnumber = 888267&arSt = + 134&ared = + 142&arAuthor = Ohmori%2C + S.%3B + Yamao%2C + Y.%3B + Nakajima%2C + N, accessed May 2005

25 FRAMES: 'Future radio wideband multiple access systems'. [Internet], ACTS Project AC090 (2005). http://www.cordis.lu/infowin/acts/rus/projects/frames/index.html, accessed May 2005

26 RAINBOW: 'Radio access independent broadband on wireless'. [Internet], ACTS Project AC015. (2005). http://www.cordis.lu/infowin/acts/rus/projects/ac015.htm, accessed May 2005

27 MEMO: 'Multimedia environment for mobiles'. [Internet], ACTS Project AC054. (2005). http://www.cordis.lu/infowin/acts/rus/projects/ac054.htm, accessed May 2005

28 DRIVE: 'Dynamic radio for ip services in a vehicular environment'. IST Project IST-1999-12515. (2005). http://www.ist-drive.org, accessed May 2005

29 OverDRIVE: ‘Spectrum-efficient uni and multicast services over dynamic multi-radio networks in vehicular environments’. [Internet], IST Project IST-2001-35125. (2005). http://www.comnets.rwth-aachen.de/~o_drive/index.html, accessed May 2005

30 WINE: ‘Wireless internet networks’. [Internet], IST Project IST-1999-10028. (2005). http://www.vtt.fi/ele/projects/wine, accessed May 2005

31 MOBY DICK: ‘Mobility and differentiated services in a future IP network’. [Internet], IST Project IST-2000-25394. (2005). http://www.ist-mobydick.org, accessed May 2005

32 SHAMAN: ‘Secure heterogeneous access for mobile applications and networks’. [Internet], IST Project IST-2000-25350 (2005). http://www.ist-shaman.org, accessed May 2005

33 MIND: ‘Mobile IP based network developments’. [Internet], IST Project IST-2000-28584. (2005). http://www.cordis.lu/ist/ka4/mobile/proclu/p/ist_ended_projects.htm, accessed May 2005

34 7443948 Salkintzis, A.K., Fors, C., and Pazhyannur, R.: ‘WLAN-GPRS integration for next generation mobile data networks’, *IEEE Wirel. Commun.*, 2002, **9**, (5), pp. 112–124. http://ieeexplore.ieee.org/iel5/7742/22372/01043861.pdf?isnumber = 22372&prod = JNL&arnumber = 1043861&arSt = + 112&ared = + 124&arAuthor = Salkintzis%2C + A.K.%3B + Fors%2C + C.%3B + Pazhyannur%2C + R., accessed May 2005

35 7950579 Hui, S.K. and Yeung, K.H.: ‘Challenges in the migration to 4G mobile systems’, *IEEE Commun. Mag.*, 2003, **41**, (12), pp. 54–59. http://ieeexplore.ieee.org/iel5/35/28028/01252799.pdf?isnumber = 28028&prod = JNL&arnumber = 1252799&arSt = + 54&ared = + 59&arAuthor = Suk + Yu + Hui%3B + Kai + Hau + Yeung, accessed May 2005

36 7130449 Kellerer, W. et al.: ‘(Auto) mobile communication in a heterogeneous and converged world’, *IEEE Pers. Commun.*, (2001), **8**, (6), pp. 41–47. http://ieeexplore.ieee.org/iel5/98/20958/00972167.pdf?isnumber = 20958&prod = JNL&arnumber = 972167&arSt = 41&ared = 47&arAuthor = Kellerer%2C + W.%3B + Bettstetter%2C + C.%3B + Schwingenschlogl%2C + C.%3B + Sties%2C + P, accessed May 2005

37 7187268 Avagnina, D. *et al.*: ‘Wireless networks based on high-altitude platforms for the provision of integrated navigation/communication services’, *IEEE Commun. Mag.*, 2002, **40**, (2), pp. 119–125. http://ieeexplore.ieee.org/iel5/35/21205/00983918.pdf?isnumber = 21205&prod = JNL&arnumber = 983918&arSt = 119&ared = 125&arAuthor = Avagnina%2C + D.%3B + Dovis%2C + F.%3B + Ghiglione%2C + A.%3B + Mulassano%2C + P, accessed May 2005

38 IETF MANET: ‘Internet engineering task force MANET working group’. [Internet] (2005). http://www.ietf.org/html.charters/manet-charter.html, accessed May 2005

39 7668616 Mohapatra, P., Li, J., and Gui, C.: ‘QoS in mobile ad hoc networks’, *IEEE Wirel. Commun.*, 2003, **10**, (3), pp. 44–52. http://ieeexplore.ieee.org/iel5/7742/27210/01209595.pdf?isnumber = 27210&prod = JNL&arnumber = 1209595&arSt = + 44&ared = + 52&arAuthor = Mohapatra%2C + P.%3B + Jian + Li%3B + Chao + Gui, accessed May 2005

40 PACE: ‘Protocols for adhoc collaborative environments’. [Internet] (2005) http://www.cs.ncl.ac.uk/research/projects/detail.php?id = 191, accessed June 2005

41 Culler, D.E. and Hong, W.: ‘Wireless sensor networks’, *Commun. ACM*, 2004, **47**, (6), pp. 30–33. http://delivery.acm.org/10.1145/1000000/990703/p30-culler.pdf?key1 = 990703&key2 = 0432626111&coll = portal&dl = ACM&CFID = 45247078&CFTOKEN = 36720041, accessed May 2005

42 Craig, W.C.: ‘Zigbee: wireless control that simply works’. [Internet] (ZMD AG, 2004). http://www.zigbee.org/en/resources/#WhitePapers, accessed May 2005

43 Microstrain: ‘Microminiature sensors’. [Internet] (2005). http://www.microstrain.com/wireless-sensors.aspx, accessed May 2005

44 Hollar, S.E.: ‘COTS dust’. [Internet]. (2001), http://www-bsac.eecs.berkeley.edu/archive/users/hollar-seth/macro_motes/macromotes.html, accessed May 2005

45 MICA: ‘MPR300/MPR310 MICA Mote’. [Internet] (2005). http://www.xbow.com/Products/productsdetails.aspx?sid = 71, accessed May 2005

46 MICA2: ‘MICA2 series (MPR4x0)’. [Internet] (2005). http://www.xbow.com/Products/productsdetails.aspx?sid = 72, accessed May 2005

47 MICA2DOT: ‘MICA2DOT series (MPR5x0)’. [Internet] (2005). http://www.xbow.com/Products/productsdetails.aspx?sid = 73, accessed May 2005

48 MICAz: ‘MICAz ZigBee Series (MPR2400)’. [Internet] (2005). http://www.xbow.com/Products/productsdetails.aspx?sid = 101, accessed May 2005

49 MPR: ‘MPR/MIB User’s Manual’. [Internet] (2005). http://www.xbow.com/Support/Support_pdf_files/MPR-MIB_Series_Users_Manual.pdf, accessed May 2005

50 Intel Mote: ‘Intel Mote project in sensor networks and RFID’. [Internet] (2005). http://www.intel.com/research/exploratory/motes.htm, accessed May 2005

51 Atwood, B., Warneke, B., and Pister, K.S.J.: ‘Preliminary circuits for smartdust’. Proc. Southwest Symposium on Mixed Signal Devices, Arizona, USA, February 2000, pp. 87–92. http://www-bsac.eecs.berkeley.edu/archive/users/warneke-brett/pubs/SSMSD2000.pdf, accessed June 2005

52 6621495 Goetzberger, A. and Hebling, C.: ‘Photovoltaic materials, past, present, future’, *Sol. Energy Mater. Sol. Cells*, 2000, **62**, (1), pp. 1–19. http://industries.bnet.com/whitepaper.aspx?&kw = photovoltaic&dtid = 1&docid = 123441, accessed June 2005

53 James, E.P. et al.: ‘An investigation of self-powered systems for condition monitoring applications’, *Sens. Actuators A*, (2004), 110 (1–3), pp. 171–176. http://www.sciencedirect.com/science/article/B6THG-4BBHC8H-J/2/a537ceddd9f90ab6c3fb65f759402229, accessed June 2005

54 6046748 Stordeur, M., and Stark, I.: ‘Low power thermoelectric generator—self-sufficient energy supply for micro systems’. Proc. 16th Int. Conf. Thermoelectrics, pp. 575–577

55 8068903 Roundy, S., Wright, P., and Rabaey, J.: ‘A study of low level vibrations as a power source for wireless sensor nodes’, *Comput. Commun.*, 2003, **26**, (11), pp. 1131–1144. http://www.sciencedirect.com/science?_ob = MImg&_imagekey = B6TYP-47CWTY0-1-2R&_cdi = 5624&_user = 3821961&_orig = browse&_coverDate = 07%2F01%2F2003&_sk = 999739988&view = c&wchp = dGLbVlb-zSkWb&md5 = fb6a2a680d75493a12ab48d6d2d974d6&ie = /sdarticle.pdf, accessed June 2005

56 8001088 Roundy, S. et al.: ‘Power sources for wireless networks’, Proc. 1st European Workshop on Wireless Sensor Networks (EWSN ’04), Berlin, Germany, January 2004, pp. 19–21. http://www.eureka.gme.usherb.ca/memslab/docs/PowerReview-2.pdf, accessed June 2005

57 Sun, L.: ‘Towards artificial photosynthesis: ruthenium-manganese chemistry for energy production’, *Chem. Soc. Rev.*, 2001, **30**, (1), pp. 36–49

58 Starner, T., and Paradiso, J.A.: ‘Human generated power for mobile electronics’, in ‘Low Power Electronics Design’, (CRC Press, 2004), pp. 1–35. http://www.media.mit.edu/resenv/pubs/books/Starner-Paradiso-CRC.1.452.pdf, accessed June 2005

59 Yang, S.: ‘Researchers create wireless sensor chip the size of glitter’. [Internet]. (2003) http://www.berkeley.edu/news/media/releases/2003/06/04_sensor.shtml, accessed May 2005

60 8532158 Madden, S., Franklin, M.J., Hellerstein, J.M., and Hong, W.: ‘TinyDB: an acquisitional query processing system for sensor networks’, *ACM Trans. Database Syst.*, 2005, **30**, (1), pp. 122–173. http://delivery.acm.org/10.1145/1070000/1061322/p122-madden.pdf?key1 = 1061322&key2 = 2914439111&coll = GUIDE&dl = GUIDE&CFID = 47916502&CFTOKEN = 58608250, accessed June 2005

61 μIP: ‘The uIP Embedded TCP/IP stack’. [Internet] (2005). http://www.sics.se/~adam/uip/index.html, accessed June 2005

62 Nagel, D.J.: ‘Wireless sensor systems and networks: technologies, applications, implications and impacts’. [Internet] (2004) http://www.csis.org/tech/biotech/wireless.pdf, accessed June 2005

63 Scanlan, C.M., and Karim, N.: ‘System-in-package technology, application and trends’. [Internet]. (Amkor Technology, 2004). http://www.amkor.com/products/notes_papers/SiP_TECHNOLOGY_APPLICATION_AND_TRENDS_Paper.PDF, accessed May 2005

64 3D Printing: ‘Three dimensional printing’. [Internet] (Massachusetts Institute of Technology, 2005). http://www.mit.edu/~tdp/whatis3dp.html, accessed June 2005

65 ITRS: ‘International technology roadmap for semiconductors 2003 edition executive summary’. [Internet] (2003). http://public.itrs.net/Files/2003ITRS/ExecSum2003.pdf, accessed June 2005

66 ITRS: ‘International technology roadmap for semiconductors 2004 update: overview and summaries’. [Internet] (2004). http://www.itrs.net/Common/2004Update/2004_00_Overview.pdf, accessed June 2005

67 OFT: ‘10 Emerging technologies that will change the world: nanoimprint lithography’. [Internet], (Office of Force Transformation, 2003). http://www.oft.osd.mil/library/library_files/article_10_emerging_0203.doc, accessed June 2005

68 Clemens, W. and Mildner, W.: ‘Printed electronics with integrated polymer circuits’. [Internet] (2004). http://www.packagingdigest.com/Whitepaper_0407.pdf, accessed June 2005

69 IEEE 1451.5: ‘Draft standard for a smart transducer interface for sensors and actuators’. [Internet] (2005). http://grouper.ieee.org/groups/1451/5/, accessed June 2005

70 Walsh, M.: ‘Nano and MEMS technologies for chemical biosensors—program overview’. [Internet]. (National Institute of Standards and Technology, 2003). http://www.atp.nist.gov/atp/focus/98wp-nan.htm, accessed May 2005

71 Alivisatos, P.: 'The use of nanocrystals in biological detection', *Nat. Biotechnol.*, 2004, **22**, (1), pp. 47–52. http://www.nature.com/nbt/journal/v22/n1/pdf/nbt927.pdf, accessed June 2005

72 E2V EC420: 'Electrochemical sensor for carbon monoxide'. [Internet] (2005). http://e2vtechnologies.com/datasheets/pellistors,_infrared_and_electrochemical/ec420.pdf, accessed June 2005

73 E2V IR600: 'Miniature infrared gas sensors for hazardous areas'. [Internet] (2005). http://e2vtechnologies.com/datasheets/pellistors,_infrared_and_electrochemical/ir600_series.pdf, accessed June 2005

74 E2V VQ32: 'VQ32 combustible gas detector elements'. [Internet], (2005). http://e2vtechnologies.com/datasheets/pellistors,_infrared_and_electrochemical/vq32.pdf, accessed 22 June 2005

75 EYES: 'Deliverable 1.1: system architecture specification'. [Internet] Project IST-2001-34734 (2002). http://www.eyes.eu.org/publications/d1.1.pdf, accessed May 2005

76 Hill, H.: 'Spec takes the next step toward the vision of true smartdust'. [Internet] (2005). http://www.cs.berkeley.edu/~jhill/spec/index.htm, accessed May 2005

77 M1010: 'SmartMesh M1010 MOTE'. [Internet] (2005). http://www.dust-inc.com/PDF/M1010_Mote.pdf, accessed May 2005

78 M2020: 'SmartMesh M2020 MOTE'. [Internet] (2005). http://www.dust-inc.com/PDF/M2020_Mote.pdf, accessed May 2005

79 8192155 Perrig, A., Stankovic, J., and Wagner, D.: 'Security in wireless sensor networks', *Commun. ACM*, 2004, **47**, (6), pp. 53–57. http://delivery.acm.org/10.1145/1000000/990707/p53-perrig.pdf?key1=990707&key2=1103626111&coll=portal&dl=ACM&CFID=45247078&CFTOKEN=36720041, accessed May 2005

80 Sensors Online: 'Planning and designing gas detection systems'. [Internet] (2002). http://www.sensorsmag.com/articles/0102/34/index.htm, accessed June 2005

81 8239262 Shi, E., and Perrig, A.: 'Designing secure sensor networks', *IEEE Wirel. Commun.*, 2004, **11**, (6), pp. 38–43. http://ieeexplore.ieee.org/iel5/7742/29957/01368895.pdf?isnumber=29957&prod=JNL&arnumber=1368895&arSt=+38&ared=+43&arAuthor=Shi%2C+E.%3B+Perrig%2C+A, accessed May 2005