

White Paper



Wireless Sensor Networks

Author	Tim Baugé
Date	17/09/09
Reference	NET090901
Issue	1

Abstract

Real world sensing is undergoing a revolution. Advances in computing platform miniaturisation, low-power radio and autonomic networking have enabled networked sensor systems that are more easily deployed and cost effective than ever before. Fine granularity real-time physical world sensing is a critical enabler for new products and services in a range of commercial and government sectors. This white paper provides a business and technology overview of Wireless Sensor Networks, a disruptive technology set to impact both business and personal applications, drawn from TRT (UK)'s longstanding involvement in this field. TRT (UK) has built up expertise in design and implementation of wireless sensor network protocols, with unique contributions in security and integration into wider business networks.

Keywords

Wireless sensor networks; sensors; telecommunication standards; protocols; environmental factors; intelligent sensors; monitoring; intelligent networks; white papers; information technology

Thales

Thales is a leading international electronics and systems group, addressing Aerospace and Space, Defence and Security markets worldwide. The Group's civil and military businesses develop in parallel and share a common base of technologies to serve a single objective: the security of people, property and nations. Thales's leading-edge technology is supported by 22,500 R&D engineers who offer a capability unmatched in Europe to develop and deploy field-proven mission-critical information systems. The Group builds its growth on its unique multidomestic strategy based on trusted partnerships with national customers and market players, while leveraging its global expertise to support local technology and industrial development. Thales employs 68,000 people in 50 countries with 2008 revenues of £10.2 billion.

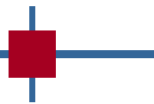
Thales Research and Technology (UK) Limited

Thales UK's Reading-based research & technology facility is the UK arm of the Thales corporate research centre. Its activities focus on providing solutions: Security and Communication Systems, Galileo and Position-Based Systems, and Enhanced Digital Environments. These are based on the key technologies of IP Networks and Network Security, Wireless Communications, Sensors and Signal Processing, and Navigation and Positioning. The facility offers a wide range of consultancy and development services to European Government Agencies and to industry throughout the world.

Thales Research and Technology (UK) Limited
Worton Drive, Worton Grange
Reading, Berkshire, RG2 0SB, UK

Company Registration No. 774298

e-mail: scs.trtuk@thalesgroup.com



Overview

Until recently a smart device was one which could provide added value through its embedded computing capability. Today we have higher expectations, and a smart device also needs to communicate and collaborate, preferably wirelessly. Phrases such as “Machine to Machine Communication”, “Cooperating Objects”, “Internet or Web of Things” capture different aspects of this revolution, which brings about a shift in how individual devices participate in business processes, defence and homeland security applications, or people’s professional and private lives. A key technology which underpins these concepts is Wireless Sensor Networks (WSN). These are small embedded sensing platforms with computing and communication capabilities, which combine low cost, flexible and fast deployment, resilient self management and embedded intelligence for cooperatively delivered value added services.

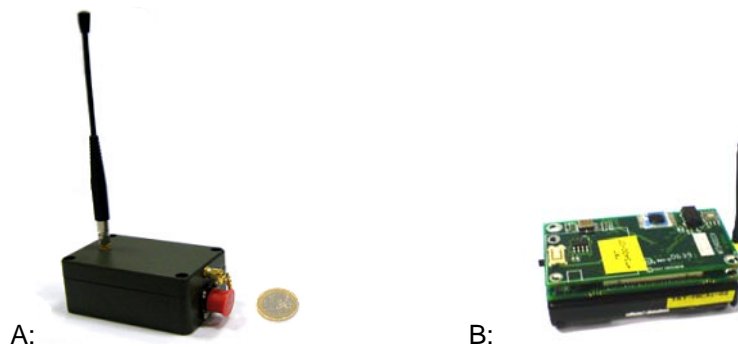


Figure 1 Small embedded sensing platforms with computing and communication capabilities. (A: Thales S-ULP, B: CrossBow MicaZ)

As a major growth technology, WSN research and development budgets are forecast to rise to \$1.3 billion in 2012 as growing technology adoption fuels demand for advanced capability¹. Revenue from devices alone is expected to exceed \$12 billion by 2013². A very wide breadth of industrial and personal applications stand to be impacted by WSN technologies as collaborating objects become pervasive. Thales has been involved in the early developments of WSNs over the last few years, focussing on both system wide and specific aspects of the technology. In particular, TRT (UK) has experience of design and implementation of practical deployments, with a specific focus on security for both access to, and operation of, sensor networks, in stand alone deployments and integration into wider business networks. This White Paper describes this disruptive technology from a business and technology perspective.

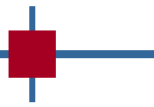
Leading application domains

WSNs have seen early adoption in a number of application spaces. In the defence sector, sensor networks fit naturally into the ISTAR³ space, increasing the timeliness, coverage and granularity of the operational picture. Applications such as force protection with unattended ground sensors formed into intelligent networks around forward operating bases are receiving much attention. Additionally military operations in urban environments are increasing the complexity of situation awareness, and calling for much finer detailed context information to be delivered by WSNs. Body area networks integrated with soldier communication systems are also a key application, as vital health functions can be monitored when soldiers enter hazardous areas.

¹ ON World Inc., Wireless Sensor Networks, January 2009

² Harbor Research, Pervasive Internet/M2M Forecast Report, February 2009

³ Intelligence, Surveillance, Target Acquisition, and Reconnaissance.



The homeland security sector has similar requirements, and there is much interest in WSNs for critical infrastructure monitoring (utilities, airports, etc), border protection, incident detection and crisis management. These applications have requirements for permanent, as well as ad hoc, deployments of sensing capability, which raises technology challenges for lifespan and security. In the civil sector, WSNs have excited interest from two classes of applications. Firstly body area networks have fuelled developments in telemedicine or wellbeing applications. The WSN involved are mainly body worn, but also interface with the surrounding infrastructure. The second broad class of applications is smart infrastructure, which includes markets such as the operational efficiency of smart grids and condition monitoring of high value assets.

Business drivers

To be disruptive, new technology needs compelling commercial or societal drivers to justify challenging the traditional approaches. A useful starting point for this White Paper therefore is to identify the business drivers which define the technology as disruptive.

Commercial benefits

The argument that the lifecycle costs for wireless communications are less than for wire-based communication is often cited as a leading commercial driver behind WSNs. While the cost comparison is a major factor, especially in retrofit applications or harsh environments, it would be limiting to reduce the benefits of WSNs to cost effective connectivity. The ability to sense, communicate and collaborate in real time, combined with the proliferation of capable devices turns context information into a pervasive commodity. This provides significant added value to a variety of applications, such as industrial business processes, as they can access a real-time and finely defined operational picture. The increased timeliness and granularity of available context information enables more intelligent applications and services to be deployed, making use of high or low level context to support the respective layers of decision making. Overall, by providing a real time interconnection between the physical and digital worlds, WSNs allow step changes in efficiency and effectiveness, as well as enabling new added value services across many business sectors.

Regulatory and societal pressures

Beyond the commercial benefits, WSNs are increasingly underpinning regulatory and societal demands. For example, the green agenda is pushing for greater environmental responsibility which requires an increase in monitoring capability. Ranging from large-scale environmental sensor networks, through building efficiency ratings, to process monitoring, there is an ongoing requirement to quantify impact. WSNs address these requirements in a flexible and cost effective manner.

Another key driver is the demand for operational accountability. While the ability to access real-time context information is essential to the management of dangerous environments or crisis situations, increased public scrutiny has fuelled the need for traceability and demonstrable accountability. By providing automated, integrated and time stamped context information, WSNs are able to deliver the required audit trails.

Technology overview

Having reviewed some of the main business drivers behind the technology, this section provides a brief overview of the technology.

Technology building blocks

WSNs are self-organising networks of small embedded devices called motes⁴ as shown in Figure 2. These are deployed in the environment being monitored, either placed individually or scattered with high enough density relative to their sensing and communication ranges to ensure good connectivity and sensing coverage.

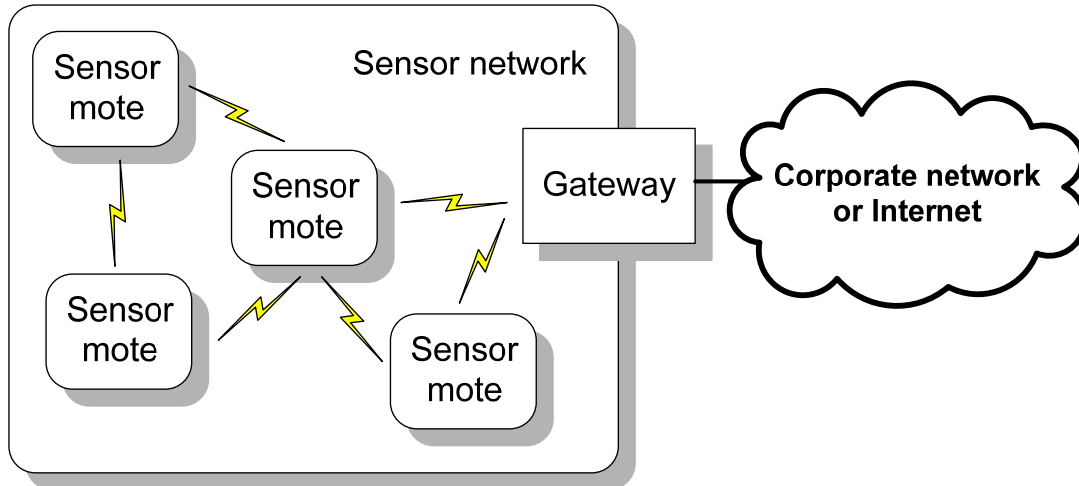


Figure 2: Wireless Sensor Network architecture

The self-organisation algorithms and protocols in the motes ensure that the devices form a network and carry out their monitoring tasks. These include sensing activities, but may also involve determining their location, exchanging sensing information, aggregating data, reasoning in a local or distributed manner, raising alarms, activating other sensors, etc. As the devices are generally constrained in terms of communication bandwidth, processing power and energy supply, optimal use of the resources is an important factor in designing the monitoring tasks. In order to communicate with the outside world, WSNs rely on gateways. These may be fixed or mobile, permanently or intermittently present, unique or multiple. They allow access to the monitoring services from a corporate network or the wider Internet. As a higher capability and availability platform, the gateway can also host management, processing and security functions for the WSN.

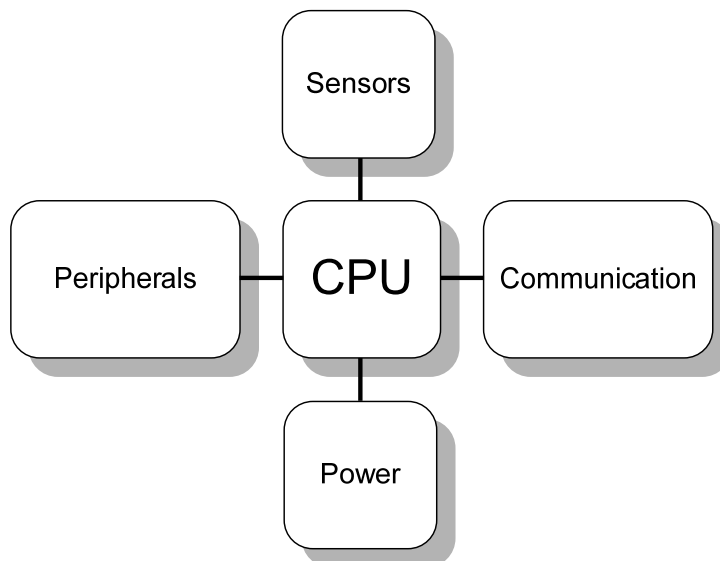
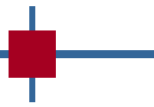


Figure 3: Sensor node architecture

⁴ "Mote: a particle of dust", from the Shorter Oxford English Dictionary.



The motes themselves can be modelled using the architecture shown in Figure 3. The “CPU” (Central Processing Unit) block is the overall controller of the device, linking all the other blocks together and providing the mote management functions as well as running the application. The “sensors” block contains the actual sensors attached to the mote. The “communication” block contains the communication capabilities of the device, which will typically be an IEEE802.15.4 radio or similar. This block handles the duty cycling of the radio to save power. The “peripherals” block contains all other optional functionality, for example GPS⁵ receiver, audible alarm, extended memory, etc.

Relevant standards

In order to achieve cost targets through mass production, as well as interoperability between manufacturer components, a number of standards have been established in this field. The leading ones are mentioned in this section, with a brief overview.

Various standards cover the radio and link layer technology, all operating in the 2.4GHz licence free band. The radio standard most often associated with WSNs is IEEE802.15.4⁶, also known as the Wireless Personal Area Network standard (WPAN). Typical implementations offer a range of up to 300m in open environments, and rates of up to 250 kilobits per second. Given the relatively low data rate, the medium access protocol can be implemented in software, and in practice many platforms rely on the mote’s operating system to provide it.

Other radio standards are also competing in this arena, two of which have enough momentum to warrant a mention here. The first is Bluetooth, which is producing a standard called Bluetooth Low Power⁷ (inheriting from Wibree and Bluetooth Ultra Low Power work). The standard is still under development, but the expected performance is 10m range for a 1 megabit per second rate. While Bluetooth has a full networking capability through the Scatternet topology, its adoption has mainly been through the single hop Piconet deployments, and the technology is particularly relevant for body area networks in healthcare applications. The second is low power WiFi implementations (IEEE802.11), which provide a similar range to WPAN but with a significantly higher bandwidth. Compatibility with the large amounts of existing WiFi infrastructure is a double-edged sword, as this also raises the interference problems which WPANs minimise by using a small frame size. However low power WiFi is an approach that is gaining in popularity.

Given the ubiquity of the Internet Protocol (IP) in modern communications, there is a growing interest in using it in sensor networks. As the expected bandwidth in these networks cannot support the overhead of IP, stateless compression techniques have been devised in the Internet Engineering Task Force (IETF), with IPv6 over Low power WPAN (6LoWPAN)⁸. The resulting overhead is appropriate for WPAN technology, but requires a node to compress / decompress, as well as fragment, due to packet size restrictions.

The standards described so far provide generic networking capability, limited to the lower layers of the networking stack. A number of significant standards have emerged which cover higher

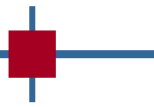
⁵ Global Positioning System

⁶ www.ieee802.org/15/pub/TG4.html

⁷

www.bluetooth.com/Bluetooth/Products/More_about_emBluetoothem_low_energy_technology.htm

⁸ www.ietf.org/html.charters/6lowpan-charter.html



layers, offering applications a managed network interface. ZigBee⁹ is built on top of IEEE802.15.4, and adds networking, transport and application profile layers. The standard has gone through a number of iterations (the latest general release being ZigBee Pro in 2007). Standard compliance comes at two levels, either as ZigBee compliant platforms, which adhere to the networking specification only, or as ZigBee certified products, which additionally conform to an application profile. These profiles can be either public and well known allowing interoperability of devices, or proprietary. The alliance maintains a standard components register from which public profiles can be specified.

While industrial automation is included in the scope of ZigBee, a different set of standards have emerged from industries that wish to transparently use their existing communication standards over WSNs. WirelessHART¹⁰ is one of the most mature, integrating the HART protocol with wireless bearers. Specifically designed to meet existing performance requirements from the industry, the technology is well adapted but less versatile than the more generic offerings. ISA100.11a¹¹, a recent standard (first release in April 2009) aims to be more general and caters for the wireless transport of many fieldbus technologies.

Related technologies

WSNs also depend on advances in other technology fields. Energy scavenging and storage remains one of the main challenges for sensor motes, as most applications cannot support the labour and environmental impact of changing batteries, even infrequently. Devices must generally be able to survive for their operational lifetime on the battery they are deployed with. Energy efficient components and designs are also required to improve for the next generation of devices. Sensor technology is another area that is adapting to the new requirements, as MEMS (Microelectromechanical systems) sensors and smart system integration (system on a chip, etc) are more energy efficient.

Two adjacent technologies should also be noted here. RFIDs (radio frequency identifier), which pioneered the “Internet of Things” concept, is a distinct technology whose purpose is to identify and track real world objects. RFID enables a convergence of real world and business processes in retail, asset tracking, supply chain, etc. Finally information management deserves a mention here as a major technology field that provides the means of making sense of the vast amounts of information which WSNs will inevitably produce. By integrating some data processing into the sensor motes themselves, a first level of information management can be pushed into the network.

Conclusions

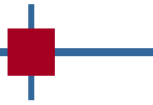
In this White Paper we have presented an overview of the current state of the art in Wireless Sensor Networks, the business drivers underpinning this area, key technical concepts and relevant standards. As a major disruptive technology, WSNs are poised to change the business and personal expectations of interactions between the digital and real worlds. Electronic tools and applications are increasingly expected to operate on fine grained and real-time information about the physical environment. Systems and solutions across a wide range of applications are now exploiting this new opportunity for higher added value sensing at lower overall cost.

The Networks Group at TRT (UK) has extensive experience and is able to assist in the design and analysis of sensor networks with capability in consultancy, simulation and prototyping.

⁹ www.zigbee.org

¹⁰ www.hartcomm2.org/hart_protocol/wireless_hart/wireless_hart_main.html

¹¹ www.isa.org



THE INFORMATION IN THIS DOCUMENT IS SUPPLIED "AS IS" WITHOUT ANY EXPRESS OR IMPLIED WARRANTY WITH RESPECT TO THE ACCURACY, COMPLETENESS, OR USEFULNESS OF ITS INFORMATION AND IN PARTICULAR WITHOUT ANY WARRANTY AS TO FITNESS OF SUCH INFORMATION FOR THE INTENDED PURPOSE.

THALES NOR ANY PERSON ACTING ON ITS BEHALF:-

- A) MAKES ANY WARRANTY OR REPRESENTATION, EXPRESS OR IMPLIED, THAT THE USE OF THE INFORMATION IN THIS DOCUMENT MAY NOT INFRINGE THIRD PARTY RIGHTS;
- OR
- B) ASSUMES ANY LIABILITIES, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE) OR OTHERWISE, WITH RESPECT TO THE USE OF, OR FOR DAMAGES RESULTING FROM THE USE OF ANY INFORMATION IN THIS DOCUMENT.

NO RIGHT OR LICENCE IS GRANTED TO THE RECIPIENT IN RELATION TO ANY INFORMATION IN THIS DOCUMENT.