ABSTRACT

Wireless sensing systems are increasingly used both in more conventional applications and mainly in situations requiring some of their specific capabilities. Most measuring systems advising or requiring a huge number of sensors and sensing nodes that cover a more or less large area are possible to implement only if organized as centrally managed wireless networks of stand-alone nodes. Each node is provided with processing capabilities and incorporates the hardware and software required for data acquisition, data processing and data transmission to the network central unit. Such measuring systems are labelled wireless sensor networks (WSNs) and in the article the authors give an overview of the state of the art, the problems to overcome and the future trends of WSNs.

RESUMO

Os sistemas sem fios de sensores são cada vez mais utilizados quer em aplicações convencionais, quer, principalmente, em situações que requerem algumas das suas capacidades específicas. A maior parte dos sistemas de medição que aconselham ou requerem o uso de um elevado número de sensores e de pontos de medida cobrindo uma área mais ou menos grande são possíveis de implementar apenas se organizados como redes sem fios controladas centralmente de nós autónomos. Tais sistemas de medição são designados por redes sem fios de sensores (WSNs) e no presente artigo os autores fazem uma revisão do estado da arte, dos problemas a ultrapassar e das tendências futuras das WSNs.

1. Introduction

Sensor networks can be either wired or wireless. Sensor networks are intimately related to smart sensor. The “intelligence” of a smart sensor is the important and often fundamental asset allowing it to constitute a node of a network.

Wired sensor networks are mainly found in industrial environments. In such cases, the intelligence of each node is usually less important.

Wireless sensor networks started to be implemented during the 1990s namely for environment, engineering, agriculture and ecology applications. Security problems, mainly after the 11th September 2001 and the fight against terrorism and illegal activities are currently boosting the development of wireless sensor network.

1.1 Basics aspects of the communication between nodes

The communication between network nodes can be simplex, half duplex, or full duplex.

Simplex systems communicate in one direction only. Citizen Band (CB) and other radio formats are normally half duplex—meaning they can talk and listen, but not simultaneously. In this case, some indication is usually required to let the other party know it can talk. RS-232 is a half-duplex data bus.

Devices that can talk and listen at the same time are full-duplex devices. Many modern devices can simulate full-duplex performance by switching between transmit and receive fast enough.

According to the form the signal enters the hardware medium, the communication can be either analogue or digital. In analogue systems, the modulation technique is continuously variable (e.g., voice). Digital systems use an analogue-to-digital converter to digitize the signal and send a data packet that uses 1s and 0s to represent the analogue value. Digital transmissions offer such advantages as reduced fading, reduced noise, and increased throughput.

According to band the signal occupies, networks are said to be baseband or broadband. If the signal containing information is placed directly on the physical medium, the channel is called baseband (e.g. Standard Ethernet). If the signal is placed on a carrier (modulation), the channel is broadband (e.g. majority of wireless (radio) buses). Because many carriers can be placed on the same medium at different frequencies, a given hardware channel can carry many logical channels.

The interaction between network nodes and the host may be made using one of the following solutions: master-slave, peer-to-peer and broadcast.

In master-slave protocols, one node gives the commands and another node or collection of nodes executes them. The host is usually the master, and the nodes are usually slaves. This protocol allows tight traffic control because no node is allowed to speak unless requested by the master, and no
communication is allowed between slaves except through the master.

In a peer-to-peer network, all nodes are equal. A node can be a master one moment and then be reconfigured at another time. Peer-to-peer configurations offer the greatest flexibility, but they are the most difficult to control. Any node can communicate directly with any other node.

Broadcast networks are much like master-slave configurations, but the master can send commands to more than one slave at a time. Many industrial protocols (e.g., IEEE-1451) are based on master-slave (with broadcast) protocols. Wireless systems can be implemented in any of these protocols.

The final basic aspect revised here has to do with the time a node owns a transmission channel: circuit switched or packet switched networks.

In circuit-switched networks a circuit is established between the sender and the receiver for instance by sending an address and remains connected until the sender or receiver hung up.

Packet-switched networks route digital packets of information as they travel along different paths throughout the network. Each packet contains routing information so that the receiver can reassemble the packets into a complete message when they arrive. Complexity is high, but the potential for flexibility and improved channel use is also high. The Internet and World Wide Web are based on packet-switched networks.

1.2 Sensor Network Topologies

Wired and wireless sensor networks include but are not limited to the following topologies:

**Point-to-Point Networks**

Point-to-point networks, as the one depicted in figure 1, are theoretically the most reliable because there is only one single point of failure in the topology—the host itself.

![Figure 1 – Point-to-point network](image)

Digitization occurs in the host, where a single clock can be used to time stamp the analogue signals from multiple sensors. Improvement of the system can be achieved by adding redundant hosts, but wiring two hosts can be a problem. In wired networks, each sensor node requires a separate twisted shielded-pair wire connection. The cost is high, configuration management is difficult, and nearly all the information processing is done by the host. Some networks provide frequency-modulated (FM) signals on the wires to carry multiple sensor readings on separate FM channels. Some standards (e.g., the HART bus) support multiplexing of digital signals on the existing analogue wiring in older plants. These architectures blur the distinction between point-to-point and multi-drop networks.

The first wireless networks were simple radio-frequency (RF) implementations of this topology. These networks used RF modems to convert the RS-232 signal to a radio signal and back again. Interference and multi-path propagation effects caused significant degradation in factory environments. Complete wireless local area networks (WLANs) were implemented using this technique. These were successful in the office environment but not as well in factories. Remote data acquisition systems with this topology were implemented by using a data concentrator in the field to feed the data to a radio transmitter for transmission to the hosts, where the signals were demultiplexed into the original sensor signals.

**Multi-drop Networks**

In multi-drop networks, like the one depicted in figure 2, each node puts its information onto a common medium, which requires careful attention to protocols in hardware and software. Single-wire connection is less expensive but leads to potential single-point failure. Redundant connections mitigate this potential problem. Once the industry began the migration to multi-drop buses, problems associated with digitization began to emerge. With the distributed intelligence required to implement a multi-drop network, synchronization of clocks became a critical issue in some applications. This remains an important design parameter for any distributed digital system. Carrier sense multiple access with collision detection (CSMA/CD) protocol used in the Ethernet is a nondeterministic protocol for some real-time industrial applications, but Ethernet is perhaps the best compromise between cost and performance.

![Figure 2 – Multi-drop network](image)
Wireless systems use the same types of protocols to implement multi-drop topologies, simulating hard-wired connections with RF links.

**Web Networks**

In a web topology (figure 3) all nodes are potentially connected to all other nodes. Connectivity among a large collection of nodes gets complex because all nodes must have a connection to all other nodes. Some connections can be eliminated by using repeaters and routers to make virtual connections. The World Wide Web is a good example of this topology.

Web solutions may require impracticable to implement wiring connections unless one uses wiring that is already in place (e.g. telephone network, paying sometimes the price of low speed).

![Figure 3 – Web network](image)

Smart sensor nodes may cooperate to form a temporary configuration that provides sufficient capacity to replace the host. Self-hosting networks then become self-configuring and finally perhaps even self-aware.

In a wireless web network, individual nodes can be constantly connected (physically) with many other nodes in the network. The instant configuration of the network (routing) becomes software dependent. More common nowadays is data transmission from a node to another or to the host (or vice-versa) by relaying or repeating it through nodes that form the shortest available route (nodes operating correctly). This means that each node must be able of determining that route (self-organizing network). The assigned input and output channels dictate to each node which signals are meant for its own use and which should be passed on to the next node. The routing is one of the things that make web architectures more complicated to implement than the others. How the network responds to the reconfiguration when the nodes are mobile (e.g. mobile ad hoc networking, i.e. networks that spread across a geographical area has a severe impact on performance and reliability of the network (e.g. harsh environments, where connections can change quickly as the RF environment changes).

2. **Wireless Sensor Networks (WSN)**

Wireless sensor networks are computer networks consisting of spatially distributed autonomous sensors. Each sensor module (node) in a sensor network consists of sensors, data converters, a small microcontroller, radio transceiver or other wireless communications device, power management circuitry and battery.

In WSNs are involved issues from several different scientific and technical domains. In the following paragraphs only some of them are addressed.

2.2 **WSN Standards**

WSNs have been implemented according to one of the following standards: IEEE 802.11, ZigBee, Bluetooth, Wibree, and 6lowpan.

2.2.1 **IEEE 802.11 (IEEE Std 802.11 (ISO/IEC 8802-11: 1999))**

IEEE 802.11 standards focus on the bottom two levels the ISO model, the physical layer and link layer. LAN applications, network operating systems, protocols, including TCP/IP and Novell NetWare, run on an 802.11-compliant WLAN as they run over Ethernet. The 802.11 family currently includes six over-the-air modulation techniques that all use the same protocol. The most popular techniques are those defined by the b, a, and g amendments to the original standard; security was originally included and was later enhanced via the 802.11i amendment. The standard accepts several media access methods (e.g. Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)), types of modulation, carrier and sub-carrier frequencies. IEEE 802.11b and 802.11g standards use the 2.40 GHz band. Because of this choice of frequency band, 802.11b and 802.11g equipment can incur interference from cordless telephones, Bluetooth devices, and other appliances using this same band. The 802.11a standard uses the 5 GHz band, and is therefore not affected by products operating on the 2.4 GHz band.

The 802.11 family define a Wireless Local Area Network [WLAN].

The 802.11 wireless LAN standards provide a number of channels within each frequency band and a number of data rates. Frequency-Hopping Spread Spectrum [FHSS], or direct sequence Spread Spectrum [DSSS] are specified.

IEEE 802.11 specifies a LAN with a minimum of two stations. IEEE 802.11a [Wi-Fi] transmits at a frequency of 5 GHz with data rates of 54 Mbps using Orthogonal Frequency Division Multiplexing [OFDM]. IEEE 802.11b [Wi-Fi] transmits at a frequency of 2.4 GHz with data rates of 11 Mbps using direct sequence spread spectrum modulation [DSSS]. IEEE 802.11g transmits at a frequency of 2.4 GHz with data rates of 54Mbps {OFDM, DSSS}. IEEE 802.11b and 802.11g are compatible so devices can coexist in the same network. 802.11h transmits at a frequency of 5GHz with data rates of 100Mbps.
2.2.2 ZIGBEE

ZigBee is the name of a specification for a set of high level communication protocols using small, low-power digital radios based on the IEEE 802.15.4 standard for wireless personal area networks (WPANs). ZigBee operates in the industrial, scientific and medical (ISM) radio bands; 868 MHz in Europe, 915 MHz in the USA and 2.4 GHz in most jurisdictions worldwide. The technology is intended to be simpler and cheaper than other WPANs such as Bluetooth. The most capable ZigBee node type is said to require only about 10% of the software of a typical Bluetooth or Wireless Internet node, while the simplest nodes are about 2%. However, actual code sizes are much higher, closer to 50% of Bluetooth code size.

ZigBee protocols are intended for use in embedded applications requiring low data rates and low power consumption.

There are three different types of ZigBee device: (a) ZigBee coordinator (ZC): the most capable device, the coordinator forms the root of the network tree and might bridge to other networks. There is exactly one ZigBee coordinator in each network. It is able to store information about the network, including acting as the repository for security keys; (b) ZigBee Router (ZR): routers can act as an intermediate router, passing data from other devices; (c) ZigBee End Device (ZED): contains just enough functionality to talk to its parent node (either the coordinator or a router) and cannot relay data from other devices. The current profiles derived from the ZigBee protocols support beacon and non-beacon enabled networks. In non-beacon enabled networks (those whose beacon order is 15), an unslotted CSMA/CA channel access mechanism is used. In this type of network, ZigBee Routers typically have their receivers continuously active, requiring a more robust power supply. However, this allows for heterogeneous networks in which some devices receive continuously, while others only transmit when an external stimulus is detected. In beacon enabled networks, the ZigBee Routers transmit periodic beacons to confirm their presence to other network nodes. Nodes may sleep between beacons, thus lowering their duty cycle and extending their battery life. The minima beacon intervals are 15.36 ms at 250 kbit/s, 24 ms at 40 kbit/s and 48 ms at 20 kbit/s. Low duty cycle operation with long beacon intervals requires precise timing which can conflict with the need for low product cost.

ZigBee devices are required to conform to the IEEE 802.15.4-2003 Low-Rate Wireless Personal Area Network (WPAN) standard. The standard specifies its lower protocol layers—the physical layer (PHY), and the medium access control (MAC) portion of the data link layer (DLL). This standard specifies operation in the unlicensed 2.4 GHz, 915 MHz and 868 MHz ISM bands. In the 2.4 GHz band there are 16 ZigBee channels, with each channel requiring 5 MHz of bandwidth. The radios use direct-sequence spread spectrum coding, which is managed by the digital stream into the modulator. BPSK is used in the 868 and 915 MHz bands, and orthogonal QPSK that transmits two bits per symbol is used in the 2.4 GHz band. The raw, over-the-air data rate is 250 kbit/s per channel in the 2.4 GHz band, 40 kbit/s per channel in the 915 MHz band, and 20 kbit/s in the 868 MHz band. Transmission range is between 10 and 75 meters heavily dependent on the particular environment. The maximum output power of the radios is generally 0 dBm (1 mW). The basic channel access mode specified by IEEE 802.15.4-2003 is "carrier sense, multiple access/collision avoidance" (CSMA/CA), i.e. a node briefly check to see that no one is talking before it starts. There are three notable exceptions to the use of CSMA: beacons are sent on a fixed timing schedule, and do not use CSMA; message acknowledgements also do not use CSMA; devices in Beacon Oriented networks that have low latency real-time requirements may also use Guaranteed Time Slots (GTS) which by definition do not use CSMA.

The software is designed to be easy to develop on small, cheap microprocessors. The radio design used by ZigBee has been carefully optimized for low cost in large scale production. Even though the radios themselves are cheap, the ZigBee Qualification Process involves a full validation of the requirements of the physical layer. ZigBee radios have very tight engineering constraints: they are both power and bandwidth constrained.

2.2.3 BLUETOOTH

Bluetooth is a short-range wireless communications technology intended to replace the cables connecting portable and/or fixed devices while maintaining high levels of security. The key features of Bluetooth technology are robustness, low power, and low cost. Bluetooth enabled electronic devices connect and communicate wirelessly through short-range, ad hoc networks known as piconets. Each device can simultaneously communicate with up to seven other devices within a single piconet. Each device can also belong to several piconets simultaneously. Piconets are established dynamically and automatically as Bluetooth enabled devices enter and leave radio proximity.

Bluetooth simultaneously handles both data and voice transmissions (e.g. hands-free headset for voice calls, and synchronizing PDA, laptop, and mobile phone applications). It also operates in the unlicensed industrial, scientific and medical (ISM) band at 2.4 to 2.485 GHz, using a spread spectrum, frequency hopping, full-duplex signal at a nominal rate of 1600 hops/sec.

Bluetooth technology’s adaptive frequency hopping (AFH) capability was designed to reduce interference between wireless technologies sharing the 2.4 GHz spectrum.

The range of Bluetooth devices depends on the class. Table 1 summarizes the situation.
Table 1: Bluetooth range

<table>
<thead>
<tr>
<th>Class</th>
<th>Maximum Permitted Power (mW dBm)</th>
<th>Range (approximate)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class 1</td>
<td>100 mW (20 dBm)</td>
<td>~100 meters</td>
</tr>
<tr>
<td>Class 2</td>
<td>2.5 mW (4 dBm)</td>
<td>~10 meters</td>
</tr>
<tr>
<td>Class 3</td>
<td>1 mW (0 dBm)</td>
<td>~1 meter</td>
</tr>
</tbody>
</table>

2.2.4 WIBREE

Wibree is a digital radio technology (Nokia 2006) intended to become an open standard of wireless communications, designed for ultra low power consumption (button cell batteries), within a short range (10 meters) based around low-cost transceiver microchips in each device. Wibree is designed to work side-by-side with and complement Bluetooth. It operates in 2.4 GHz ISM band with physical layer bit rate of 1 Mbps. The main applications include devices such as wrist watches, wireless keyboards, toys and sports sensors where low power-consumption is a key design requirement. Wibree should be up to ten times more efficient than Bluetooth. The reported output power is around -6 dBm.

2.2.5 6lowpan (IPv6 over Low power Wireless Personal Area Networks)

6lowpan is the name of the working group in the internet area of IETF. 6lowpan is the paragon that is aimed at allowing IPv6 packets to be sent to and received from personal area networks (PANs), more specifically over IEEE 802.15.4-standard based networks. IPv6 concerns data delivery for wired networks—the internet. Likewise, IEEE 802.15.4 devices provide sensing communication-ability in the wireless domain. Some applications are: wireless internet connectivity at lower data rates for devices with very limited form factor (e.g. automation and entertainment applications in home, office and factory environments).

2.3 Operating systems and programming languages

Operating systems for wireless sensor network nodes typically are less complex than general-purpose operating systems because of: (1) the special requirements of sensor network applications; (2) resource constraints in sensor network hardware platforms. Sensor network applications are usually not interactive in the same way as applications for PCs and thus the operating system does not need to include support for user interfaces; (3) constrains in memory and memory mapping hardware support make mechanisms such as virtual memory either unneeded or impossible to implement.

Operating systems specifically targeted at sensor networks do not have real-time support (they could, thow, because the hardware is not different from traditional embedded systems and it is therefore possible to use embedded operating systems such as eCos or uC/OS often designed with real-time properties).

TinyOS is perhaps the first operating system specifically designed for wireless sensor networks. It is based on an event-driven programming model instead of multithreading. TinyOS programs are composed into event handlers and tasks with run to completion-semantics. When an external event occurs, such as an incoming data packet or a sensor reading, TinyOS calls the appropriate event handler to handle the event. Event handlers can post tasks that are scheduled by the TinyOS kernel some time later.

Both the TinyOS system and programs written for TinyOS are written in a special programming language called nesC which is an extension to the C programming language. nesC is designed to detect race conditions between tasks and event handlers.

There are also operating systems that allow programming in C (e.g. Contiki, MANTIS, SOS).

Programming the sensor nodes is more difficult than programming normal computer systems. New programming models have been developed to cope with the resource constrained nature of these nodes: c@t (Computation at a point in space (@)Time ), DCL (Distributed Compositional Language), galsC, nesC, Protothreads, SNACK, SQTL.

2.4 Wireless Sensor Networks: present and future

2.4.1 Present

The literature and information on wireless sensor network applications, solutions and scientific and technological development is abundant (e.g. [1,2]. We mention here briefly only two frameworks for WSN implementation: internet and MICA mote based WSNs.

Internet based wireless sensor networks

Internet hardware and software are a good substrate for WSNs implementation [3,4]. Internet TCP/IP is compatible with several solutions available at the physical, data link, network, transport, and application layers of the OSI model, which simplifies WSN design and operation. The topologies and management of the network are flexible. Applications with different requirements can be accommodated. In [5] solutions for an application concerning air quality monitoring using web sensors are presented and discussed.

MICA motes

Motes are typically designed in stackable layers. The core of a mote is a small, low-cost, low-power computer. The computer monitors one or more sensors and connects to the outside world with a radio link. For power saving, motes are about 99 percent of
the time in a standby mode. Several times each second, the device flicks on its radio to check for incoming messages, but if there are none, the radio is shut off within milliseconds. Similarly, the sensors usually take their readings only once every few minutes. Data is transmitted only when the memory is full.

Motes operating system TinyOS forces mote programs to shut down except when certain events that warrant action occur. The operating system is also highly modular. If a program needs only certain functions from TinyOS, the nonessential parts of the operating system are automatically removed from the mote. This modular approach ensures that the program code fills as little memory as possible, leaving more room for sensor data. Modules also enhance the robustness of the devices by limiting how the distinct parts of the software interact.

MICA motes are available to the general public through a company called Crossbow. These motes come in two form factors: rectangular, measuring 2.25 x 1.25 by 0.25 inches (5.7 x 3.18 x .64 centimetres), it is sized to fit on top of two AA batteries that provide it with power; circular, measuring 1.0 by 0.25 inches (2.5 x .64 centimetres), it is sized to fit on top of a 3 volt button cell battery.

The MICA mote uses an Atmel ATmega 128L processor running at 4 megahertz. The 128L is an 8-bit microcontroller that has 128 kilobytes of onboard flash memory to store the mote's program. It consumes only 8 mA when it is running, and only 15 µA in sleep mode, which allows a MICA mote to run for more than a year with two AA batteries. A typical AA battery can produce about 1,000 mA-hours. At 8 mA, the ATmega would operate for about 120 hours if it operated constantly. However, the programmer will typically write his/her code so that the CPU is asleep much of the time, allowing it to extend battery life considerably. For example, the mote might sleep for 10 seconds, wake up and check status for a few microseconds, and then go back to sleep.

MICA motes come with 512 kilobytes of flash memory to hold data. They also have a 10-bit A/D converter so that sensor data can be digitized.

Separate sensors on a daughter card can connect to the mote. Sensors available include temperature, acceleration, light, sound and magnetic.

The final component of a MICA mote is the radio. It has a range of several hundred feet and can transmit approximately 40,000 bits per second. When it is off, the radio consumes less than 1 µA. When receiving data, it consumes 10 mA. When transmitting, it consumes 25 mA.

**Future**

Applications requiring more measurements and more measuring points are or rather have been on demand. Important applications will require large or extremely large fixed or mobile networks (millions or billions of smart nodes!!!!). WSNs are the natural solution. However, several challenges at different levels have to be faced, namely (1) hardware: sensors and nodes size, power they can harvest or store, harsh environmental operating conditions, node failures, mobility of nodes, dynamic network topology, communication failures, and heterogeneity of nodes, large scale of deployment, unattended operation; (2) software: network programming, lifetime maximization, robustness and fault tolerance, self-configuration, security, mobility (when sensor nodes or base stations are moving), middleware, the design of middle-level primitives between the software and the hardware. Let us look in more detail some of the problems and challenges.

**Sensors**

Temperature, humidity, acceleration, and presence sensing is fairly easy to implement using small, low-power consumption devices. The measurement of other quantities using micro or nano-sensors must be developed to respond to some of the present and future needs.

**Power**

The current technologies already allow extended operation using small size low ampere-hour batteries. This is achieved with both low consumption components but mainly by keeping the nodes in stand-by as long as possible. However, some applications will surely require battery recharge. Sun, wind, vibration and bio energy are some of the possible solutions already under study.

**Network programming and re-programming**

Programming of a wireless network with many nodes is not easy, particular if it is a mobile ad-hoc one with millions of nodes. New solutions have to be found. We are aware that to replace the software on motes with updated versions, an idea based on the way viruses and worms are spread on the Internet has been tried. The new program is packaged in a special form and delivered to the root mote, which installs it and "infects" its neighbours with the package. The upgrade makes its way through the network like an epidemic, but it does so in a more controlled fashion that avoids redundant communications and adapts to the way that the motes are scattered in space.

**Security**

Because of the tight constraints on power use and processor speed, a sensor (or perceptive) network functions differently from the Internet and office LANs, where computers have individual names and addresses and most messages are sent from one machine to a specific recipient machine. In sensor networks, one node generally broadcasts messages to many, with the intended recipients identified by attributes such as their physical location or sensor value range. TinyDB is a software that makes a
perceptive network system function much like a database. A user can "query" all the smart nodes at once with a request. The request enters the network at its "root" node, which forwards copies to its neighbours and so on until all sensors have received the command. Motes that have nothing to answer may ignore the message; others may turn on their sensors if they have been sleeping; still others may run a series of calculations on the data logged in their memories, extract readings that meet the requested criteria, and pass that information back to the root mote for collection. All the user sees is a spreadsheet-like list of the relevant measurements and locations. Software running on a high-powered server could then perform a wider analysis of the trends to determine which machines require maintenance. This reprogramming model immediately suggests one of the harder problems in sensor network design: how to secure them against hackers, viruses and eavesdroppers. TinyOS has built-in algorithms that can authenticate the identity of motes. But for the system to work well, keys must be distributed to a large number of small nodes in reliable and uncomplicated ways. Malefactors can attack perceptive networks using strategies that are different from what is generally seen on the Internet. One promising way to defend the networks is to treat the effects of an attack as essentially another form of noisy sensor data, so the perceptive network as a whole will still function even if a small fraction of nodes has been compromised.

3. Conclusion

Wireless sensor networks are required for present and future applications and the overcome of some of their current limitations will foster new applications. The present technologies limit WSNs in hardware related aspects like sensed quantities, size of nodes, and nodes’ autonomy but it is at the software level that improvements and new solutions are more required. All these developments must produce very low-cost devices so that the cost of networks with a large number of nodes is not prohibitive.

REFERENCES