Annales Academiae Paedagogicae Cracoviensis

Folia 52 Studia Technica II (2008)

Lubomír Smutný[1], Kazimierz Jaracz[2]

Industrial wireless local area networks with smart sensor nodes

The article deals with the present state in the development of wireless sensor networks – (nodes), trends and new challenges in this interesting area. The highest priority of this smart instrumentation is the best operating ability of sensor nodes with suitable protocol communication (for instance Zig Bee). New types of smart sensor nodes with wireless connection bring some advantages and also disadvantages. There are problems with communication protocols, interaction between different nodes, and the main problem is the power supply of the sensor instrumentation nodes. The present applications have the principle of homogenous nets and they include for instance smart sensors of temperature, moisture, pressure, water quality etc.

Some experience with wireless sensors, Bluetooth and Zig Bee nodes on communication with PIC microcomputer will be presented; interesting possibilities of further development will be shown.

The problem is investigated in the framework of the grant project Czech Science Foundation GAČR 101/07/1345.

Introduction

The rapid development and emergence of smart sensors even intelligent instrumentation and field network technologies have made the networking of smart transducers (sensors and actuators) a very economical and attractive solution for a broad ran-

[1] VŠB –Technical University of Ostrava, Department of Control Systems & Instrumentation, e-mail: lubomir.smutny@vsb.cz, URL: http://www.352.vsb.cz

[2] Pedagogical University of Cracow, Institute of Technology e-mail: jaracz@ap.krakow.pl

ge of measurement and control applications. It is clear that a variety of networks must exist to solve specific problems. However, it seems that industry is at a crossroads and this predicament has imposed unnecessary economic burden on both transducer end users and vendors to support the variety of networks.

This condition has also impeded the widespread adoption of these technologies, despite common willingness to build and use them. Wireless systems for industry have mostly used cellular-phone-style radio links, using point-to-point or point-to-multipoint transmission. In contrast, wireless mesh networks are multihop systems in which devices assist each other in transmitting packets through the network, especially in adverse conditions. You can drop these ad hoc networks into place with minimal preparation, and they provide a reliable, flexible system that can be extended to thousands of devices. The wireless mesh network topology developed at MIT (USA) for industrial control and sensing is a point-to-point-to-point, or peer-to-peer, system called an ad hoc, multihop network. A node can send and receive messages, and in a mesh network, a node also functions as a router and can relay messages for its neighbours. Through the relaying process, a packet of wireless data will find its way to its destination, passing through intermediate nodes with reliable communication links (see Fig. 2) [5], [3].

With the above background on the sensor, computer, cluster and communication technologies that enable wireless smart sensor networks, we are now in position to survey the existing and planned wireless networks of smart sensors. Since this in an emergent subject, it is first necessary to develop criteria according to which to compare such networks. That is done in the next paragraphs. Then a compilation of such networks follows [1].

Wireless smart sensor networks

Any network is sufficiently complex, so that many factors are needed to describe it. This is even more so for sensor networks, since smart sensors are themselves complex engineering constructs. However, there are some features of sensor networks that are of primary interest. These include the number of sensor locations.

The number of individual sensors obviously depends on the number at each location, possibly in micro-sensor clusters, as well as the number of locations. The area over which the sensors are deployed and networked is also of major interest. The basic goals of a smart sensor network generally depend upon the application, but the following tasks are common to many networks.

1. Determine the value of a given parameter at a given location: in an environmental network, the temperature, atmospheric pressure, amount of sunlight, and the relative humidity at a number of locations may need to be known. This example shows that a given sensor node may be connected to a number of different types of sensors, each with a different sampling rate and range of allowed values.

2. Detect the occurrence of events of interest and estimate parameters of the detected event(s): in the traffic sensor network, it may be necessary to detect a vehicle moving through an intersection and estimate its speed and direction.
3. Classify a detected object: is a vehicle in a traffic sensor network a car, a mini-van, a light truck, a bus, etc.
4. Track an object: in a military sensor network, track an enemy tank as it moves through the network.

In Fig. 1 we can see smart sensor block structure for multiple value measurement in the industrial environment (pressure, moisture, temperature, etc.) with communication in ILAN or WILAN.

In Fig. 2 we can see Wireless Mesh Network; multiple nodes cooperate to relay a message to its destination. The mesh topology enhances the overall reliability of the network, which is particularly important when operating in harsh industrial environments.

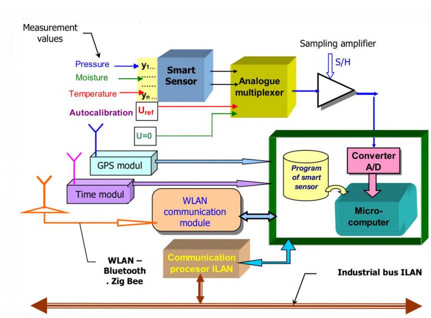


Fig. 1. Smart sensor block structure for multiple value measurement in ILAN or WLAN

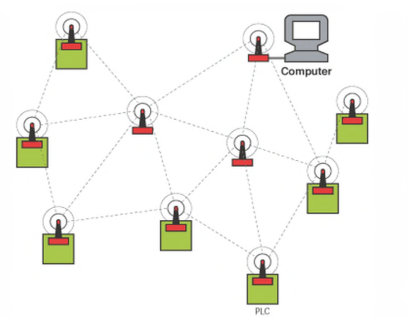


Fig. 2. Wireless Mesh Network with multiple cooperating nodes of smart sensors

WILAN topology nets Zig Bee

Like the Internet and other peer-to-peer router-based networks, a mesh network offers multiple redundant communication paths throughout the network. If one link fails for any reason (including the introduction of strong RF interference), the network automatically routes messages through alternate paths. In a mesh network, you can shorten the distance between nodes, which significantly increases the link quality. If you reduce the distance by two, the resulting signal is at least four times more powerful at the receiver. This makes links more reliable without increasing transmitter power in individual nodes. In a mesh network, you can extend the reach, add redundancy, and improve the general reliability of the network simply by adding more nodes [1].

The standard defines several WILAN topology types: peer-to-peer, star, cluster tree and mesh. In accordance with a network structure, different types of devices are developed. There are Reduced Functionality Devices (only as the end node – with sensors or actuators) and Full Functionality Devices (network routers and coordinators, network interfaces). Zig Bee utilizes the ISM communication band (Industrial, Scientific and Medical frequencies). It uses DSSS - Direct Sequence Spread Spectrum method with 27 channels to communicate with other Zig Bee devices. One channel is used at frequency of 868 MHz in Europe and with the transfer rate 20 kb/s. In America, Zig Bee uses 10 channels at the frequency of 915 MHz with the transfer rate 40 kb/s (band gap is 2 MHz). Worldwide frequency 2,4 GHz is used for 16 channels with the transfer rate 250 kb/s (with 5 MHz band gap) [8].

The employed access method is CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). The device (node) checks if the channel is clear (no other node is transmitting at the time). If the channel is not clear, the node waits for a randomly chosen period of time, and then checks again to see if the channel is clear. If the channel is clear, then the Request-to-send packet is sent. Second node (receiver) then sends Clear-to-send packet. The transceiver replies with data packet and waits for acknowledgement packet. Other devices (after receiver's CTS packet) wait for a period of time. Security of Zig Bee network is provided by Advanced Encryption Standard. Access control and others can be used, too [2].

Table 1 shows a comparison of three wireless standards in main technical and application areas as a transfer rate, range, frequency, bandwidth, consumption transmission, battery life, etc.

Standard IEEE (trade mark)	802.15.1 Bluetooth	802.15.4 ZigBee	802.11b Wi-Fi
Transfer rate	1 Mb/s	20/40/250 Kb/s	11/54 Mb/s
Range (m)	20 (class 2), 100+ (class 1)	20 – 75, 100+ (with amplifier)	100+
Frequency	2,4 GHz	868/915 MHz, 2,4 GHz	2,4 GHz
Band width (kb/s)	1000 - 3000	20 - 250	11000
Elements	7	255/65 K+	32
Battery life (days)	1 - 7	100 -1000+	0,1 - 5
Consumption transmission (mA)	45 (class 2) <150 (class 1)	30	300
Wobble spectrum method	FHSS*	DSSS**	DSSS
System resources	250 KB+	4-32 KB	1 MB+
Main advantages	Price, comfort	Consumption, price,	Flexibility, speed
Main mode of application	Cable substitution	Monitoring, control	Web, video,

** FHSS (Frequency Hopping Spread Spectrum), ** DSSS (Direct Sequence Spread Spectrum),*

Table 1. Basic Wireless Networks properties

Reliability, adaptability, and scalability are the most important attributes of a wireless network for industrial control and sensing applications. Point-to-point networks can provide reliability, but they don't scale to handle more than one pair of end points. Point-to-multipoint networks can handle more end points, but their reliability is determined by the placement of the access point and end points.

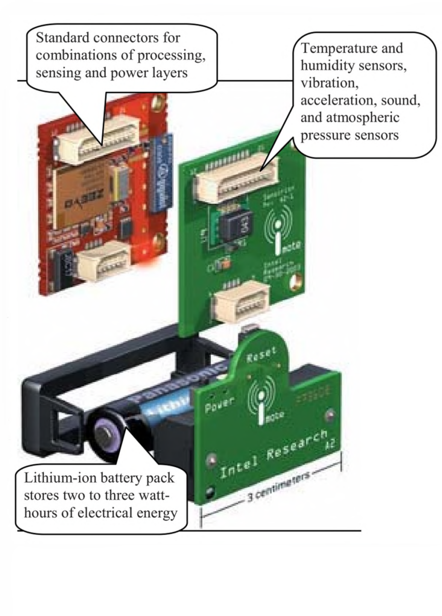
If environmental conditions result in poor reliability, it's difficult or impossible to adapt a point-to-multipoint network to increase reliability. By contrast, mesh networks are inherently reliable, adapt easily to environmental or architectural constraints, and can scale to handle thousands of end points

Examples and experience with smart instrumentation

An interesting application for wireless, multihop, mesh networks is the diagnostic monitoring of devices. This monitoring can occur outside the normal control loop, and wireless communications notify the system user of any abnormal operation of the device (see Fig. 2). In this control loop, an additional signal is extracted and analyzed during normal operation of the sensor. The signal is monitored for abnormalities without affecting the sensor's operation. If an abnormal signal or trend is observed, an alert is triggered [4].

The advantage of using a wireless link for onboard monitoring and notification is that the link is independent of the control loop. By using a wireless, multihop mesh network, data can be routed dynamically to similar wireless devices. Surrounding devices can respond to an alert from a failing device, even while the maintenance personnel are being notified. Another benefit of wireless networks is that maintenance personnel can directly access the diagnostic output of the sensor without running wires. This can eliminate a huge task in the case of a level sensor in a large storage tank, or a temperature probe at the top of a stack at a chemical refinery (see Fig. 3 and Fig. 4).

The network is self-configuring, all devices can transmit from their original position, and they don't have to be moved. A weak signal or dead zone can be fixed simply by dropping a repeater node into place. The network error rate is low and can be further reduced if occasional re-transmits are allowed [3]. Industrial systems can now benefit from a wireless format that satisfies the multiple conflicting demands of redundancy, distributed communications, flexibility, and reliability. Furthermore, self-configuring, self-healing networks are inherently less expensive to install and maintain as radios and microprocessors become cheaper. A significant barrier to low-cost connectivity has been removed [7]. The onboard processor offers other ways to save power. Communicating one bit of data through the radio transceiver costs as much energy as executing roughly 1,000 processor instructions. The "mote" can conserve power by storing and aggregating sensor readings, rather than sending them out immediately.



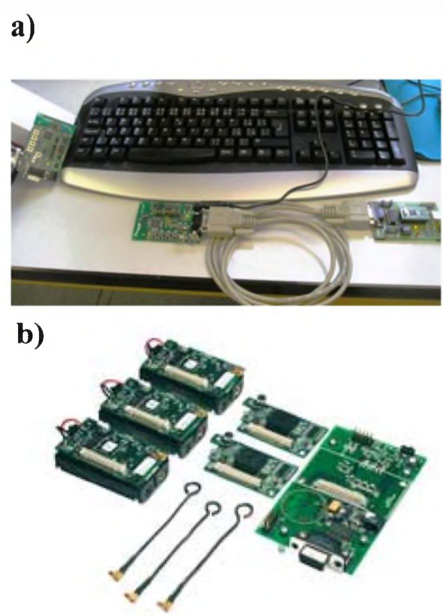


Fig. 3. A prototype iMote for sensing, processing and communication tasks with WILAN

Fig. 4. a) Zig Bee demo kit for basic experimental tasks on DCSI laboratories
b) Mote Kit modules for lab experiments

The processor can also compress information before it is sent and can summarize the sensor logs with an average or the high and low values if the details are not crucial. Nodes may swap sensor data with one another, identify important observations and then send simplified descriptions out to the user [6].

There is no way of avoiding certain network-protocol conversations between nodes, but these messages can be held until there are sensor measurements to transmit and then stuffed into the same "envelopes" as those packets of data. Smart nodes combine processing and memory capabilities with sensors, wireless communications and a self-contained power supply. A drawing of a prototype iMote produced by Intel Research is presented in Fig. 3. The next figure shows the Zig Bee demo kit for basic experimental tasks and PDA Pocket LOOX with GPS module on the Department of Control Systems & Instrumentation laboratories of VŠB-TUO.

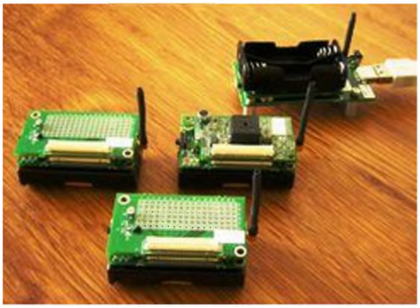


Fig. 5. Intelligent wireless sensor node system MOTE

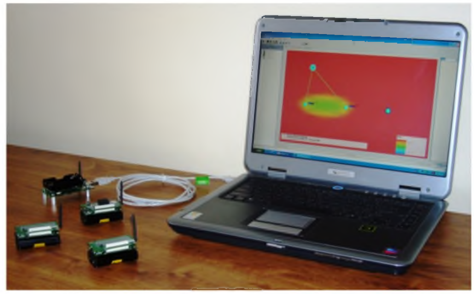


Fig. 6. Wireless sensor system MOTE – Basic Kit with program SCADA/ MMI support

MOTE-KIT400 is the basic experimental kit for basic task solution. It uses the 2nd generation of MICA2 and it is compatible with programme support Tiny OS. The kit contains all basic tools for development and testing of wireless nets prototypes (Properties of MOTE Basic kit: MICA2 processor/radio printed boards, 2 MTS300 sensors printed boards – light, temperature, sound, MIB510 programme board with serial interface, Mote-Test programme software, Frequency: 315MHz, 433MHz and 868/916MHz). These MOTE modules utilize a Tiny OS system as a programme support.

Tiny OS is an open-source operating system designed for wireless embedded sensor networks. It features a component-based architecture which enables rapid innovation and implementation while minimizing code size as required by the severe memory constraints inherent in sensor networks. Tiny OS component library includes network protocols, distributed services, sensor drivers, and data acquisition tools – all of which can be used as-is or be further refined for a custom application. Tiny OS event-driven execution model enables fine-grained power management, yet allows the scheduling flexibility that is required by the unpredictable nature of wireless communication and physical world interfaces.

Tiny OS has been ported to over a dozen platforms and numerous sensor boards. A wide community uses it in simulation to develop and test various algorithms and protocols. Over 500 research groups and companies are using Tiny OS on the Berkeley/Crossbow Motes. Numerous groups are actively contributing code to the source forge site and working together to establish standard, interoperable network services built from a base of direct experience and honed through competitive analysis in an open environment.

Conclusions

With the coming availability of low-cost, short-range radios, along with advances in wireless networking, it is expected that smart sensor networks will become commonly employed. Each node will have sufficient processing power to make a decision, and it will be able to broadcast this decision to other nodes in the cluster.

One opportunity for mesh networks is in distributed control systems. There's been a trend in recent years to place more intelligence throughout the control system. Distributed intelligence is naturally served by wireless multihop mesh networks. Reliability, adaptability, and scalability are the most important attributes of a wireless network for industrial control and sensing applications. Point-to-point networks can provide reliability, but they don't scale to handle more than one pair of end points. Point-to-multipoint networks can handle more end points, but their reliability is determined by the placement of the access point and end points.

The control of the wireless system is distributed throughout the network, allowing intelligent peers to communicate directly with other points in the network without having to be routed through a central control point. Sensor networks are made possible because of the commercial availability of small and high-performance sensors, inexpensive and facile micro-controllers, and multiple wireless communication options. Wireless communication options span the range from short-range Bluetooth or Zig Bee links through mid-range channels (Wi-Fi) to global satellite systems (WiMAX). Integration of wireless links with the Internet is increasingly common, so that even local systems of sensors and other instrumentation can be read out or controlled globally.

Examples of wireless sensor networks were surveyed and compared. Their scales range from a few to a few thousand sensor locations in regions as small as a building and as large as global. Some experience with wireless sensors, Bluetooth and Zig Bee nodes on communication with PIC microcomputers were presented and interesting possibilities of further development were shown.

The presented results have been supported and achieved in developing the research project Czech Science Foundation GAČR 101/07/1345.

References

[1] Bond A., *Looking forward to a wireless future. Control Engineering Europe*, 2005, Vol. 6, No. 6, pp. 52–54.

[2] Koumpis, K. – Hanna, L. – Andersson, M. – Johansson, M.: A review and roadmap of wireless industrial control. *The Industrial Wireless Book Email Newsletter*, GGH Mar-

keting Communications Ltd. Available <last actualization 03/2006) from http://wireless.industrial-networking.com/articles/articleprint.asp?id=913
[3] Poor, R. Wireless Mesh Networks. *WEB magazine Intelligent systems - Sensors*, 02/ 2003. Available <last actualization 03/2006).
[4] Sazonov, E., Janoyan, K., Jhac R. Wireless Intelligent Sensor Network for Autonomous Structural Health Monitoring. In *Smart Structures / NDE 2004*, San Diego (California, USA), 2004.
[5] Smutný, L. 2002A. Smart Instruments in Wireless LAN. *In Proceedings of International Workshop on Intelligent Mining Systems*. Fukuoka (Japan): KYUSHU University Fukuoka, April 2002, p. 85-90, ISBN 80-86111-90-3.
[6] Smutný, L. 2002B. To Be or Not to Be Wireless. In *Proceedings of the 5th International Scientific – Technical Conference Process Control 2002*. Pardubice : University of Pardubice, 9-12 June 2002, p. R245-1 to R245-6. ISBN 80-7194-452-1.
[7] Smutný L., Balšánek M., Wojciaszyk, P. 2006. Smart sensors on IWLAN– industrial wireless local area networks. In *Proceedings of the 7th International Scientific-Technical Conference „Process Control 2006"*. Kouty nad Desnou : University of Pardubice, 2006. pp. R191-1÷ 6. ISBN 80-7194-860-8.
[8] Zigbee Alliance 2004 [online], Zig Bee Overview. Available from http://www.zigbee.org/

Key words: wireless LAN, smart sensor, nodes, Zig Bee, Bluetooth,