WIRELESS AD-HOC NETWORKS FOR INDUSTRIAL AUTOMATION: CURRENT TRENDS AND FUTURE PROSPECTS

Mogens Mathiesen, Gilles Thonet, Niels Aakvaag

ABB Corporate Research
Bergerveien 12, 1375 Billingstad, Norway

Abstract: This paper provides an overview of recent advances in wireless communication technologies applied to industrial automation. Newly introduced communication concepts such as ad-hoc networks and wireless sensor/actuator networks now enable the deployment of extremely decentralised control architectures. Both open-loop and closed-loop applications are part of the roadmap, although data gathering and monitoring applications are expected to spread first. In addition to increased flexibility and facilitated operations, these new communication technologies have significant cost saving potential. Standardisation efforts led by international bodies such as the IEEE should propel prototyping and deployment activities in various industries. *Copyright © 2005 IFAC*

Keywords: Networks, Telecommunication, Telematics, Data Transmission, Connectivity, Self-organizing Systems, Decentralised Systems, Decentralised Control, Open-loop Control, Closed-loop Control

1. A NEW COMMUNICATION PARADIGM

Everyday life is invariably associated with using various network infrastructures – whether this is a local office network, a fieldbus for interconnecting plant equipment, or the cellular telephony network. The rapid diffusion of wireless communication technology has not changed this landscape much. Mobility and connection to inaccessible sites are now possible, but the need for some type of fixed infrastructure persists. It usually takes the form of base stations that organize communications over predefined geographical area in a master/slave fashion. In most cases, careful design and planning is necessary, which makes network deployment a complex and time-consuming task.

1.1 Historical Perspective

Two main trends put the traditional model of infrastructure-based networks into question. The first is based on recent uncertainties in the telecommunications business, following the challenged deployment of heavy and pervasive third-generation cellular networks. In addition to soaring installation and usage costs, these networks are increasingly perceived by the public as environment-unfriendly and health-hazardous (whether this is true or not). A number of players are calling for a more pragmatic and cost-effective approach, where users can switch between the almost ubiquitous cellular network and local wireless clusters (e.g. hot spots), depending on the surrounding environment and their instantaneous needs.

In parallel, a second trend finds its roots in military research. In the 1970s, US defence projects worked at enabling soldier-to-soldier communications in hostile environments. So-called packet radio networks were the first attempt to get rid of the fixed infrastructure through self-organisation of network nodes. Successive breakthroughs in hardware miniaturisation have now made it possible to deploy millimetre-scale sensing devices that spontaneously form a communication network. The University of California at Berkeley's Smart Dust project is a widely advertised instantiation of this trend (Kahn, *et al.*, 2000).

1.2 The Quest for Self-Organisation

The outcome of these trends is a new paradigm that has produced several terminologies. Although the term ad-hoc network is often used, other names are frequently encountered: mesh network, self-organised wireless network, or even parasitic network. Wireless sensor(/actuator) network is also widely used when large-scale sensing (and actuating) is the primary purpose.

Ad-hoc networks typically consist of a set of mobile nodes that freely join or leave the network with minimal administration overhead. Nodes that are within transmission range communicate directly with each other, whilst communication over longer distances uses intermediate nodes as relays in a multihop fashion. Network operation is said to be self-organised but also self-healing: should a transmission path fail, alternative paths are automatically established to reroute data and maintain network connectivity.

Fig. 1 shows an example of an industrial ad-hoc network. The normal routing path between station 1 and device 4 is represented by a plain line. If any part of this route fails, data can for example be routed via the dotted path instead.

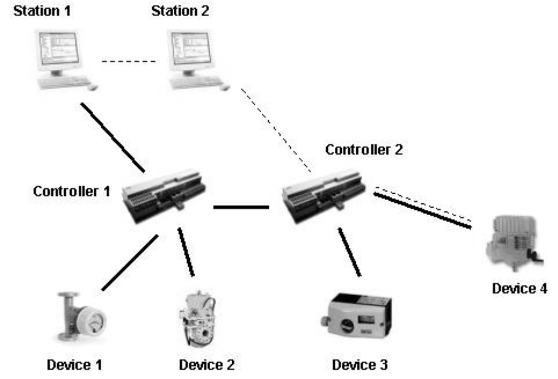

Fig. 1. Example of an industrial ad-hoc network.

1.3 From Relief to Plant Floor

Applications of such a networking concept have been unveiled in many different areas. Besides military communications, relief operations are a typical setting where communication capability is required quickly and 'on-the-fly' while infrastructure is generally damaged or unavailable. Car-based communications for vehicle cooperation (e.g. passing assistance, accident notification, navigation enhancement) is another field attracting significant research interest. Ad-hoc networks can also improve today's cellular operations by forming hybrid networks that increase their reach or achieve a better traffic balancing.

Industrial premises are fervent consumers of communications, with fieldbuses transporting information across manufacturing or process installations. Ad-hoc networks have a strong cost saving potential in these scenarios due to easier network planning, faster deployment, and lower maintenance. Looking ahead, this type of networking promises to support extremely decentralised automation architectures in which sensing, actuating, and control functions are freely allocated across the whole plant.

1.4 Structure of the Paper

The purpose of this article is to provide a comprehensive introduction to the use of ad-hoc networks in industrial automation environments. Section 2 describes the technology landscape of today's ad-hoc networks, with an emphasis on existing standards. Since the paper also aims at pinpointing and discussing promising application scenarios, Sections 3 and 4 are devoted, respectively, to open-loop control and closed-loop control use cases. The separation between open- and closed-loop control may seem arbitrary at first glance but it is fundamentally justified by important differences in underlying communications requirements. These differences clearly militate in favour of distinct product development roadmaps for the two types of control applications. The last section concludes the paper by underlining some hurdles that still need to be cleared, as well as some recommendations for starting prototyping activities.

2. TECHNOLOGICAL OVERVIEW

During the short history of wireless ad-hoc networking, several vendors have developed proprietary solutions to leverage the capabilities promised by it and to solve the problems associated with its deployment. Companies such as Ember, Millennial, CrossBow, and Dust all offer solutions that enable ad-hoc wireless connectivity between small, energy-efficient devices.

There are however two major issues associated with the proprietary approaches that have led to the development of different wireless standards:

1. The first one is coupled with the vision of cross-device connectivity. If devices are to communicate with each other regardless of type or function, they must do so on a common platform where core functionality ensures cross-platform interoperability.

2. Second, it is crucial for manufacturers of products relying on ad-hoc wireless connectivity that the technological foundation on which they base their products (i.e. chips and radios) is replaceable. This means that if a third-party provider goes out of business, it is still possible

to find replacements that comply with the same specifications.

Therefore, many technology providers and market leaders are now adopting wireless standards. The ones (existing or emerging) relevant for industrial settings are discussed in the next subsections.

2.1 Bluetooth

Bluetooth is the result of an Ericsson initiative launched in 1994 to study low-power communication between mobile phones and accessories. The Bluetooth Special Interest Group (SIG) (www.bluetooth.org) was subsequently formed in 1998 by Ericsson, IBM, Intel, Nokia, and Toshiba, and now includes over 2000 member companies. Its purpose is to further develop, publish, and promote the standard and to administer its qualification program.

With the growing hype around wireless personal area networks (WPANs), Bluetooth supporters tried to profile it as a generic short-range ad-hoc networking technology. Large portions of its specifications are now part of the standard IEEE 802.15.1 (IEEE Std. 802.15.1, 2002). This effort, however, has lost some momentum, due to both fierce competition and inherent limitations of Bluetooth. Furthermore, Ericsson recently announced that it will discontinue its design and development of new Bluetooth products for the semiconductor industry, adding uncertainties to the future of the technology.

Technical Overview. Bluetooth operates in the 2.4 GHz license-free band using a frequency hopping spread spectrum (FHSS) approach. The frequency range 2'400-2'483.5 MHz is divided into 79 separate channels and a pseudo-random hopping scheme is used at a nominal rate of 1'600 hops per second. The main advantage of frequency hopping is increased resilience to adverse radio interference. It also aids in preventing eavesdropping, though it is only necessary to capture one transmission packet to synchronize with the communication.

Bluetooth gives a very high quality of service (QoS). It guarantees a low latency for active nodes but wake-up for sleeping nodes is about three seconds. It is therefore well suited for scenarios where a high quality of service is required and where power is readily available, for example communication between wireless headsets and mobile telephones.

Bluetooth networks consist of one master node and up to seven slave nodes connected via a star topology to the master in a so-called piconet (Fig. 2). The master assigns unique addresses to all its slaves, and establishes a physical data connection in case of data transfer. Bluetooth nodes have the ability to belong to more than one network and form so-called scatternets (Fig. 3).

Technology Roadmap. A three-year plan including enhancements to performance, security, power consumption, and usability has recently been released by the Bluetooth SIG. The following advancements are being introduced:

1. *Performance and Power Consumption* – Bluetooth 2.0 + EDR (Enhanced Data Rate) allows up to 3 Mbps gross data rate while at the same time reducing power consumption.

2. *QoS, Security, and Power Consumption* – In 2005 the Bluetooth SIG will test and release a new version further enhancing the usability of multi-device scenarios, providing better privacy protection through longer alphanumeric PINs, as well as improving QoS via traffic prioritisation. The possibility of connecting up to 255 slaves to a master and additional power consumption decreases will make Bluetooth better suited to sensor network requirements.

3. *Multicast, Security, and Performance* – Increased range to 100 m while keeping low power, multicast functionality, and privacy enhancements is on the agenda for 2006.

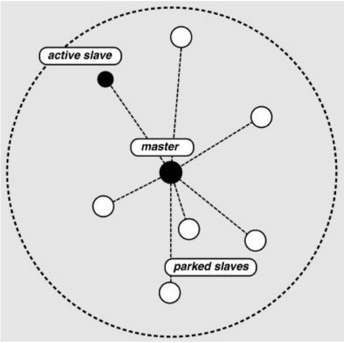

Fig. 2. Bluetooth piconet (source: Bluetooth SIG).

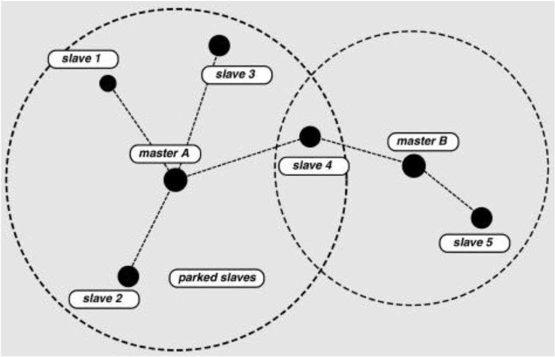

Fig. 3. Bluetooth scatternet (source: Bluetooth SIG).

Suitability for Industrial Automation. Bluetooth has some properties that limit its use in industrial environments:

1. Although it targets low-cost and low-power applications, its power consumption is high proportional to the achieved transmission range, and it does not compare favourably with standards like ZigBee (described in Section 2.3).

2. Piconets may only contain up to seven slave nodes in addition to the master.

3. Its master/slave architecture allows for no more than one hop between two master nodes after they have formed a scatternet.

4. Sleeping nodes display very long wake-up times of typically three seconds, which makes power optimisation a tough challenge.

For these reasons Bluetooth is not well-suited for ad-hoc networking in industrial environments. The enhancements described above will address many of these issues, but it may then be too late to regain the edge that competing technologies have on it. The likely future scenario for Bluetooth is simple cable replacement applications, and this is also what it was originally designed for.

2.2 WLAN

Wireless Local Area Network (WLAN) is the generic name for the IEEE 802.11 suite of standards. It is primarily divided into three sub-standards, namely a, b, and g, completed by a set of additional specifications for enhanced security, improved performance, etc. WLAN is infrastructure-based, meaning that each device connects as a client to fixed access points (APs). Once connected, a device communicates using TCP/IP with other devices.

WLAN is intended to replace wired Ethernet connections. The Wi-Fi Alliance (www.wi-fi.org) is a non-profit international organisation formed in 1999 to certify WLAN product interoperability. It currently has over 200 member companies worldwide and more than 1500 products have so far received the Wi-Fi certification. Typical usage patterns are mobile Internet connections in office or community-like local networks.

Technical Overview. The three main sub standards offer distinct features:

1. **802.11b** is the most widely used of the WLAN standards. It operates in the 2.4 GHz band, ensures a range of about 100 m, and offers data rates of up to 11 Mbps (IEEE Std 802.11b, 1999).

2. **802.11a** is less popular since it operates in the 5 GHz band, thus providing a lower range but at an increased data rate of up to 54 Mbps. Extensions of this standard offering up to 108 Mbps are also available (IEEE Std 802.11a, 1999).

3. **802.11g** is the newest standard of the family and combines advantages from the other two, i.e. staying in the 2.4 GHz band while communicating at up to 54 Mbps. It is backward-compatible with 802.11b (IEEE Std. 802.11g, 2003).

Although these standards are still infrastructure based, they also include an ad-hoc mode that allows for one-hop transmissions between APs and mobile devices.

WLAN is unfortunately infamous for its security breaches. This is mainly due to a problem with the Wireless Encryption Protocol (WEP). As described in Fluhrer *et al.* (2001) the WEP key can be cracked after sniffing a large amount of wireless data. To overcome this problem 802.11g makes use of a new security standard entitled Wi-Fi Protected Access (WPA), which is much stronger than WEP.

Technology Roadmap. The following developments are of particular interest to WLAN-based ad-hoc networking:

1. **802.11n** defines a substandard for over 200-Mbps data rates in WLAN environments. Several groups of large industry players have emerged with separate, distinct proposals that are more advantageous to their planned products. Ratification is however unlikely to happen before the end of 2005 or even late in 2006 given the number of contending proposals (over 60).

2. **802.11s** aims at enabling mesh connectivity in the 802.11 family. This substandard will deliver multihop communication between up to 32 APs, making an ad-hoc infrastructure possible for WLAN.

Suitability for Industrial Automation. WLAN is an excellent alternative for Ethernet cable replacement or mobile office-like applications. Readily available off-the-shelf products and decreasing prices make it ideal for high-speed wireless backbones and field technician-like applications. Due to higher power requirements it is however not suitable for communication between small autonomous industrial devices. Also, actual latency and interference sensitivity with other 2.4-GHz equipment makes WLAN a potentially delicate solution for real-time requirements.

Extensions such as 802.11n and 802.11s will eventually bring along improved performance and multihopping capability, making them initiatives to closely monitor in the short future.

2.3 ZigBee

ZigBee is a new international standard for network connectivity based on the IEEE 802.15.4 specification (IEEE Std. 802.15.4, 2003). It focuses on interoperability between units within the areas of home automation, building automation, industrial monitoring and control, and computer peripherals. The ZigBee Alliance (www.zigbee.org) is in charge of further development, standardisation, and worldwide marketing. Promoters are Ember, Freescale, Honeywell, Invensys, Mitsubishi Electric, Motorola, Philips, and Samsung. ABB is a member of the alliance.

ZigBee specifically addresses the energy usage issue to the extent that a device can run for many years on the same inexpensive batteries. This is achieved by having a very low duty cycle in addition to not requiring close synchronisation.

Technical Overview. Since ZigBee relies on the IEEE 802.15.4 physical layer it operates in various unlicensed bands worldwide: 2.4 GHz (global), 915 MHz (Americas), and 868 MHz (Europe). Raw data rates of 250 kbps can be achieved at 2.4 GHz (16 channels), 40 kbps at 915 MHz (10 channels), and 20 kbps at 868 MHz (1 channel). Transmission range is in the region from 10 to 100 m, depending on power output and environmental characteristics.

The IEEE 802.15.4 physical (PHY) layer is based on direct sequence spread spectrum (DSSS) and includes receiver energy detection, link quality indication, and clear channel assessment. Both contention-based and contention-free channel access methods are supported with a maximum packet size of 128 bytes. Also employed are 64-bit IEEE and 16-bit short addressing, supporting over 65.000 nodes per network. The IEEE 802.15.4 medium access control (MAC) layer provides network association and disassociation, has an optional super-frame structure with beacons for time synchronisation, and a guaranteed time slot mechanism for high priority communications. The channel access method is carrier sense medium access with collision avoidance (CSMA/CA).

ZigBee defines the network, security, and application framework profile layers for an IEEE 802.15.4-based system. The network layer supports three networking topologies: star, mesh, and cluster tree as shown in Fig. 4. Star networks provide for very long battery life operation, whereas mesh networks enable high levels of reliability and scalability through multihop transmissions. Cluster-tree networks utilize a hybrid star/mesh topology that combines the benefits of both for high levels of reliability and support for battery-powered nodes.

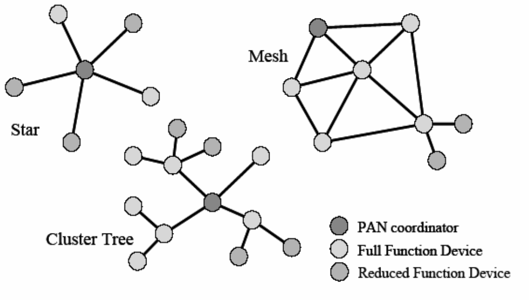

Fig. 4. ZigBee network topologies (source: ZigBee Alliance).

ZigBee security is based on access control lists, packet freshness timers and 128-bit encryption. As described by Sastry and Wagner (2004) such an approach is considered a sound step forward for embedded security, although some pitfalls must be dealt with at implementation stage.

Suitability for Industrial Automation. ZigBee has been developed especially for ad-hoc networking applications involving low duty cycles and low data rates. Applications that require the ability to quickly attach information, detach, and go to deep sleep are well suited, resulting in low power consumption and extended battery life. Primary industrial targets include energy-critical sensors and small autonomous devices. Envisioned tasks are for instance meter reading, field instrument communication, or simple intermittent control duties (e.g. switching lights on and off).

2.4 Ultra Wideband Communications

Ultra wideband (UWB) is a recent communication technology, though its technical roots can be traced back to the 1960s in relation to radar transmissions. Most of the early work was performed under classified US Government programs. Since 1994, however, much research has been carried out without classification restrictions and led to an accelerated progress in UWB technology.

As of now UWB is not standardised and different vendors are developing their own proprietary solutions. Some of them (e.g. Freescale's XS110) have already been released and have become battling candidates for a future standard. The IEEE 802.15.3a specification is in that respect a strong candidate for UWB-based WPANs.

Technical Overview. UWB technology is loosely defined as any wireless transmission scheme that occupies a bandwidth of more than 25% of a centre frequency, or wider than 1.5 GHz (Yang and Giannakis, 2004). In principle, the bandwidth of UWB signals spreads from near DC to several GHz. UWB communications differ from traditional radio-frequency (RF) technologies in that, instead of using a narrowband frequency carrier to transmit data, it sends energy pulses across a large spectrum of frequencies (typically 3 to 10 GHz). Being a carrier-less technique, it does not require costly and energy-consuming RF components like filters and oscillators.

In Fig. 5 the principal difference between narrowband and UWB techniques is seen. Narrow band techniques are exemplified here as operating at a base frequency of 2.4 GHz. All the standards discussed so far in this section operate at least partly at this frequency. Transmissions occur within a narrow frequency band where a considerable amount of energy is used to achieve the required range.

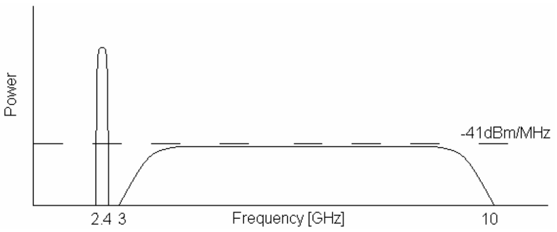

Fig. 5. Spectral comparison between UWB and some narrowband systems.

UWB on the other hand operates differently. Instead of concentrating all power at a limited base frequency, it distributes the power evenly over a wide frequency range spanning from 3 to 10 GHz. Due to the emitted spectral power never exceeding -41dBm/MHz, the signal becomes allowable according to the US Federal Communications Commission (FCC) regulations, even though it operates at licensed frequencies. The limited power that is expended limits the range to about 10 meters.

UWB has several potential advantages: high data rate, robustness against fading given its ultra-wide spectrum, good emitted power control, and possibility of high-precision localisation. These features make UWB an attractive alternative to narrowband communications, especially in interference-prone or bandwidth-demanding industrial environments.

Not much has been written about UWB security, but vendors such as Pulse Link claim that a higher level can be expected compared to narrowband techniques. Since the pulse sequencing technology makes the signals difficult to distinguish from regular RF noise, and since communications occur in picosecond bursts, data sniffing is supposedly harder to achieve.

Suitability for Industrial Automation. Due to the short range of UWB and current FCC rules, initial uses are restricted to automotive collision and information systems, consumer electronics (e.g. wireless music and video), medical imaging, and ground- or wall-penetrating communications. Its potential for industrial automation looks promising but still needs to be assessed.

2.5 Comparison

Comparisons between the different current wireless standards are shown in Fig. 6 and in Table 1. Due to the standards addressing different applications, they are usually not direct competitors.

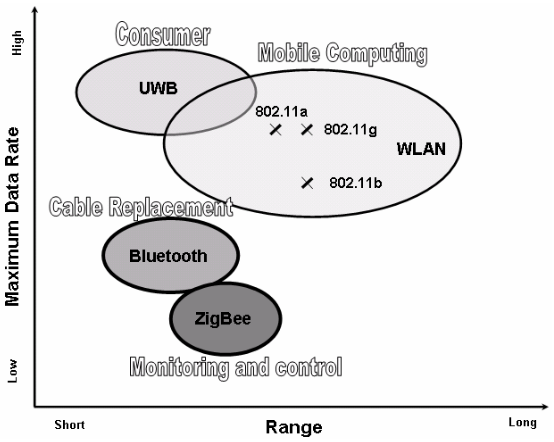

Fig. 6. Comparison between current wireless standards.

Only ZigBee has been especially designed for ad-hoc networking using a large number of nodes. It is also the standard most useful in an industrial monitoring and control setting. On the other hand, some industrial applications such as the mobile maintenance scenario described Section 3.1 require higher data rates and therefore justify the use of a standard like WLAN.

UWB may become a relevant industrial contender if the standardisation and regulation panoramas brighten, and if mesh functionality is further developed.

2.6 Business Model

In order to assess the real cost potential of wireless ad-hoc networking, a very simple business model is established based on the following scenario.

A process automation environment with 200 devices to be connected by either a traditional wired fieldbus or one of the wireless technologies presented above is assumed. Man-hour cost is set at $50. Maintenance costs are assumed to be the same for all solutions. This is obviously a simplification since in practice a wired infrastructure will require more time-consuming maintenance. System integration costs are supposed to be comparable and therefore excluded from the comparison. This is reasonably close to truth, at least for the wireless solutions.

The following technology alternatives are compared to each other: wired solution, Bluetooth, WLAN, and ZigBee (UWB is excluded from this discussion due to still uncertain technical features and costs).

Wired Fieldbus. The cost of wiring is approximately $350 per device to connect to the existing fieldbus infrastructure, including components and installation work, totalling $70.000.

Table 1 Comparison between current wireless standards

Parameter	**Bluetooth**	**WLAN IEEE 802.11a/b/g**	**ZigBee**	**Ultra Wideband**
Range	10 m	100 m	30-100 m	10 m
Associated Standard	IEEE 802.15.1	IEEE 802.11a/b/g	IEEE 802.15.4	IEEE 802.15.3a
Frequency Bands	2.4 GHz	2.4 GHz or 5 GHz	868 MHz, 915 MHz, 2.4 GHz	3.1-10.6 GHz
Physical Layer	FHSS	DSSS or OFDM	DSSS	UWB SS
Maximal Gross Data Rate	1 Mbps	5.5/11/54 Mbps (depending on substandard)	20/40/250 kbps (depending on channel)	50-480+ Mbps
Average RF Power	1/2.5/100 mW (depending on range)	40-800 mW (depending on substandard)	200-500 µW (depending on duty cycle)	20-40 mW
Battery Life	1-7 days	0.5-5 days	100-1'000+ days	30 days
Maximal Range	10-100 m	20-100 m	30-100 m	10-15 m
Network Topology	Star, piconet, scatternet	Star	Star, mesh, cluster-tree	Depending on future standard
Maximal Number of Nodes	7 slaves in a piconet	32 APs	65'000	Depending on future standard
Node Acquisition Time	3 s	2 s	30 ms	
Node Wake-up Time	3 s	1 s	15 ms	
Node Cost	$15	$20	$10	$10 (estimated)
Infrastructure Cost	$400 per master	$100 per AP	$100 per AP	
System Resources	250+ kB	1+ MB	4-20 kB	
Security Provisions	40-bit RC4	128-bit RC4	128-bit AES	Inherent security advantages
Expected Main Use	Cable replacement	Wireless Ethernet, mobile office	Monitoring and control, autonomous devices	Short-range high-speed applications

AP	= Access Point
DSSS	= Direct Sequence Spread Spectrum
FHSS	= Frequency Hopping Spread Spectrum
OFDM	= Orthogonal Frequency Division Multiplexing
SS	= Spread Spectrum

Bluetooth. From Table 1 a node cost of $15 is assumed, which includes the radio module, an additional microcontroller, and passive components. Mounting cost is said to take an hour per device, at $50. All end nodes need to be Bluetooth slaves controlled by an AP (or master). As there are maximum seven slaves per AP, a best-case estimate is that 30 APs are required, with a unit price of about $400. Each AP needs a wired Ethernet connection, adding about $100 in cabling cost per AP, and an additional $50 for mounting work. Finally, there is some additional AP configuration work to be done (e.g., DHCP setup, pairing of master with slaves, etc.), representing approximately three hours or $150 per AP. Total cost sums to about $34.000.

WLAN. Nodes include radio chip, microcontroller, and passive components, and are estimated to cost $20 each. This value, taken from Table 1, includes some additional cost for a customised protocol solution that would be required to cope with low latency needs. Mounting cost per node is approximately $50. As there is no limit to the number of nodes associated to a single AP, fewer will be needed than for Bluetooth. The actual number will depend on the physical spread of the devices, so for the sake of this example ten APs are assumed. Unit cost is approximately $100, with the same AP cabling and mounting costs as for Bluetooth. Finally, WLAN APs are easier to set up than Bluetooth APs, as there is no need for the same type of pairing. Still, some added work to ensure for instance access rights to the AP must be expected. This is assumed to represent a two-hour job, giving an additional $100 per AP. Grand total for WLAN is estimated at $17.500.

ZigBee. Here also, each node includes radio chip, microcontroller, and passive components. Node cost is approximately $10 (although this value is expected to quickly drop). Mounting cost is assumed at $50. Only one AP is required to connect to the wired infrastructure, the rest of the wireless network being ad-hoc and multihop. Unit price is around $100, which is negligible since only one is needed. The network being self-configuring, no cost is associated with configuration. Total cost for ZigBee is therefore approximately $12.000.

Table 2 summarizes the installation cost estimations. Assumptions are sometimes restrictive, and additional costs (such as qualification programs for getting a formal label from the respective standardisation bodies) should be taken into account. Further, a lifetime analysis including maintenance costs is necessary for a complete evaluation. This simple example nevertheless indicates that due to its inherent mesh nature, ZigBee is profiling itself as a serious contender for cost-effective wireless industrial sensor networking.

Table 2 Total network installation cost of various solutions

Wired Fieldbus	**Bluetooth**	**WLAN**	**ZigBee**
$70’000	$34’000	$17’500	$12’000

3. OPEN-LOOP APPLICATIONS

Open-loop applications are characterised by having wireless links only for data gathering purposes. There is no wireless connection in the feedback loop of the control system. This can be implemented in a number of ways, for example as shown in Fig. 7.

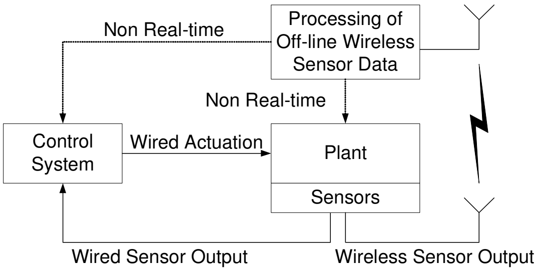

Fig. 7. Wireless open-loop systems.

A real plant is controlled via a number of actuators. The operation of the plant gives rise to some measurable output that is sensed. These values are in turn fed back to the control system for processing. The wireless links are associated with processing or operations that are not part of the classical feedback path of the control system. They may convey all sensor values, or only a chosen subset back to the off-line processing unit. Processing of off-line data is typically non real-time and is used to deduce some additional information subsequently fed either to the control system or embedded directly into the actual plant.

Examples include mobile maintenance, process control, ad-hoc benchmarking, redundancy, and mobility. These are outlined in more detail below. For each of them there is a different set of requirements regarding bandwidth, power consumption, response time, etc. Common to all the scenarios described below is that they have a fixed wired infrastructure that handles normal operation of the plant.

3.1 Mobile Maintenance

In a process control environment, service personnel frequently needs to communicate with field devices, either for test, calibration, or fault tracking. Traditionally, staff connects to the device with a cable and perform the appropriate physical maintenance. Adding wireless capabilities to field assets greatly enhances plant operations. First, the actual connection to the device is no longer physical. Thus the operator has easier access to those that are difficult to reach. Second, by being in radio contact with the devices it is easy to provide the user with location-sensitive information, i.e. the browser interface may be limited to devices in physical proximity and data can be aggregated and presented according to both functionality and locality. Data obtained in this way will typically be uploaded onto some field terminal for later off-line processing or storage (Fig. 8).

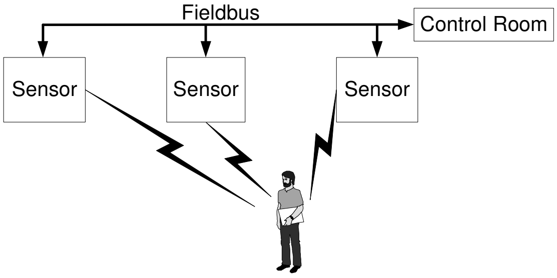

Fig. 8. Mobile maintenance.

Bandwidth requirements may be considerable if historical or maintenance data is transferred over the air interface. However, there will be no restriction on latency and very relaxed power constraints, making this an ideal application for wireless ad-hoc networks.

3.2 Process Control

Another application of considerable interest is getting access to field instruments that are not typically connected and whose data do not necessarily constitute an integral part of the main control loop. One example is historical and real-time temperature data from within rotating machinery. This is a location that is difficult to access with wired equipment. Data transfer rates are typically low and, being off-line, have relaxed latency requirements.

A related application is the interfacing of new devices to legacy systems. The process industry has an enormous installed base of sensors and field instruments. Any company aiming at wireless applications in this environment needs to address the issue of interfacing to proprietary legacy equipment. This constitutes both a potential hurdle and a new opportunity. Obstacles are due to both the type of sensor and to the conservative nature of the business. Assuming the latter can be overcome there is a potential in adding low-latency, non-critical sensors to the existing infrastructure. In order to do this, it is necessary to construct a new device serving as a bridge between the self-organizing nodes in the wireless network and the wired network. This bridge needs to be able to interface to a number of sensor devices and present a unified interface to the existing fieldbus.

A schematic representation of using ad-hoc wireless networking in a process control environment is shown in Fig. 9.

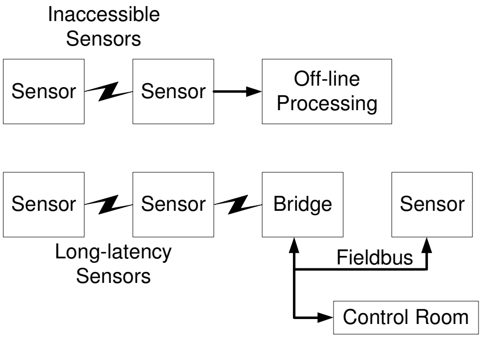

Fig. 9. Process control.

The set of requirements will obviously vary greatly depending on configuration and sensor type.

3.3 Ad-hoc Benchmarking

A fascinating new topic in process control is ad-hoc benchmarking (Fig. 10). The scenario is the following: the operation of a plant is suspected to be suboptimal. Removable sensors are placed at central locations in the process. Once in place, they establish an ad-hoc wireless network and route their measured values to some aggregation point for off-line processing. The beauty of this approach is that the system is easy to install, self-configures, and can be reused in different locations.

Once a new and optimised control strategy has been developed, it may be implemented into the central controller or into individual pieces of equipment.

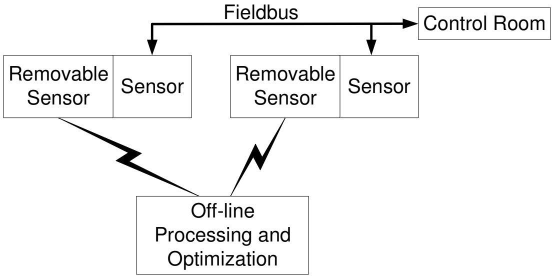

Fig. 10. Ad-hoc benchmarking.

3.4 Redundancy

Systems that demand high levels of safety are frequently required to have built-in redundancy in terms of sensing, communication, and processing. This requirement is typically encountered in the oil and gas industry, both onshore and offshore, where explosive substances are handled and operational malfunction can cause disastrous effects. During primary system failure, the secondary network will have to take over the transfer of process data. This scenario is illustrated in Fig. 11.

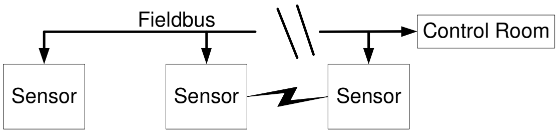

Fig. 11. Redundancy.

Contrary to the other applications, the wireless network will here transport vital data. However, transmission is only done as a last resort, in case of cable breakage or other equipment failure. Whether this constitutes an improvement in safety is a matter of probability. In a number of cases it is likely to provide an increased safety level since it utilizes a completely different infrastructure, thus minimizing the risk of failure affecting the backup system.

Bandwidth and latency of the primary system may well be stringent. It can therefore be necessary to implement device fallback algorithms, where the system backs off to a less demanding set of requirements once a primary system malfunction has been detected. The wireless ad-hoc network needs to be operative at all times, sending dummy "I'm alive" packets to inform the management system that the backup is functional.

3.5 Mobility

Mobility serves as the final example of open-loop applications well suited for wireless ad-hoc networks. Consider a processing plant with movable units placed on for example a conveyor belt. As units move about they cannot easily be connected to a fixed infrastructure. Nevertheless, mobile sensors can frequently measure physical parameters of interest to the overall performance of the plant. Fig. 12 shows a typical example of this scenario.

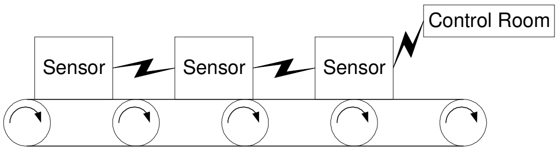

Fig. 12. Mobility.

One instantiation of this application is in the pulp and paper industry. Sensors are added to the drying process of the paper mass, measuring humidity and temperature along the chain. Data is gathered, possibly being relayed from sensor to sensor, as shown in Fig. 12, or sent to one or several stationary base stations connected to the fixed infrastructure. Measured values are then post-processed and used to tune the drying process.

Given the off-line processing, latency is not a central issue. However, this particular application requires a reasonably accurate time stamping of the data samples.

3.6 *Towards New Open-loop Applications*

From the above discussion it is clear that there is great potential for using wireless ad-hoc networks in industrial automation – whether the application is geared towards process or manufacturing operations. A number of user scenarios have been exposed and there are countless others. The various applications share some basic requirements or functionality, but also have their own particularities. In order to obtain an efficient implementation of an ad-hoc network in an open-loop environment, a thorough analysis of application requirements has to be conducted.

4. CLOSED-LOOP APPLICATIONS

Besides using wireless ad-hoc networks to gather industrial data or monitor plant assets, extending the reach to the control loop itself is the next step on the agenda. Distributed control with feedback loops closed over wireless links is an emerging research topic that is attracting growing attention.

Although technical hurdles still need to be cleared, closed-loop wireless control will be a natural element of future fully decentralised automation architectures. Actual deployment for complex control applications is however not expected for some years since proper communication and control techniques still need to be devised to fit the various industrial requirements. Most contributions to the field have to date been led by universities (Liu, and Goldsmith, 2003; Liu, and Goldsmith, 2004; Ploplys, *et al.*, 2004; Sinopoli, *et al.*, 2004).

Fig. 13 shows a very general closed-loop scenario in which both sensing and actuation are performed through wireless links. Note that actuators may be wired while keeping the wireless sensing loop.

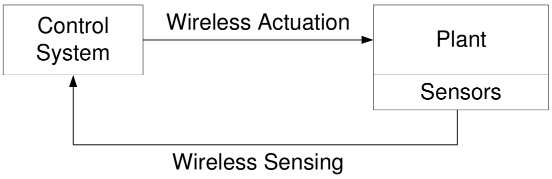

Fig. 13. Closed-loop wireless control system.

4.1 *Trading off Communication Parameters*

As discussed earlier, building a distributed control system over a wireless sensor(/actuator) network is not a straightforward task. To keep control systems running smoothly, data transmission over the industrial network should be timely, reliable, and accurate (Liu and Goldsmith, 2003). This becomes very challenging with wireless links since they introduce random delays and packet losses due to interference, signal attenuation, and multipath transmissions. In this setting, achieving closed-loop control over wireless links can be rephrased the following way: *Designing a decentralised wireless ad-hoc network that minimizes the impact of communication faults on the control system.*

Liu and Goldsmith (2003) claim that three communication parameters need particular attention from the control perspective:

1. **Data rate** – a high value means high temporal granularity.

2. **Latency** – a low value implies a faster response.

3. **Packet loss** – a small probability is associated with a reliable communication link.

However, since these are competing objectives, tradeoffs are required when designing the communication network. Liu and Goldsmith (2003) conclude that fundamental changes in the link layer design are required for wireless closed-loop control. Ideally, joint optimisation is the best approach, with both communication and control variables optimised at the same time.

4.2 *Process Control*

Wireless closed-loop control is ideally suited to improve the way processes are automated. In addition to functional advantages at cost or organisation levels (such as easier installation and plant reconfiguration), ad-hoc networks can also leverage their self-organised structure to facilitate existing operations.

Simple applications utilizing wireless sensor data directly in the controller are already appearing. For instance, Ember designed a mesh network to support the water treatment process (Tuck and Burgess, 2003). The goal of the network was to connect turbidity meters in the pipe gallery back to the control system. Reliability and ease of installation were the two driving forces. Since such an installation is very challenging from a radio communication point of view (with concrete walls and metal stairs), multihop transmissions facilitated end-to-end communications where traditional point-to-point wireless links would have required long and complicated network planning.

Similar sensing applications in other environments with high reliability needs are also feasible. For instance, the oil and gas industry is continuously calling for cost reductions since exploration becomes increasingly expensive. Savings in network maintenance, cabling cost and weight can bring significant advantages to offshore installations that may increase their lifetime. Large networks with complex sensing and actuating interactions with highly critical control systems will, as previously discussed, require robust and jointly optimised control and communication algorithms.

4.3 Production Lines

Manufacturing automation and production lines in particular can also greatly benefit from new wireless ad-hoc networking technologies. Closing control loops over wireless links to sensors and/or actuators is the natural evolution towards more distributed automation architectures.

Mobility is typically not a critical issue for factories, and when it is, movement patterns are very often regular or corresponding to some form of prior scheduling. High transmission speed is usually not required since factory communications mostly carry small amounts of data, often limited to binary inputs/outputs. Multihop routing is thus usually an achievable task in these settings.

At the same time, reliability and energy conservation are two important factors for manufacturing automation. Recently, ABB, the global power and automation company, made significant progress in addressing these two issues for closed-loop control. The so-called Wireless Proximity Sensor (Apneseth, *et al.*, 2002) boasts a proprietary communication protocol that ensures reliable delivery of messages within the short time frames required by current programmable logic control (PLC) systems. Powering is achieved by inductive coupling to a secondary coil within the sensing unit. The self-contained energy supply completely eliminates the need for cables or battery replacement.

The ABB example features progresses directed towards fully wireless closed-loop control systems, but actual multihop, large-scale scenarios still require further research.

4.4 Towards Real Distributed Wireless Control

Distributed wireless operation between the controller and sensors/actuators is still in its infancy. Initiatives are starting to spread both in process control and discrete automation. These are usually characterised by being small-scale, single-hop, and with simple control functionality. In order to achieve complex control in a real closed-loop fashion, several research directions should be prioritised:

1. Reliable communication protocols able to route data across large-scale sensor and actuator networks.

2. Efficient power conservation schemes that fit energy-constrained environments.

3. Redesign of jointly optimised communication and control algorithms to guarantee a smooth migration towards fully wireless automation infrastructures.

The authors believe that the successful completion of these steps will open up new avenues for radically improved and cost-effective industrial automation.

5. CONCLUSIONS

This survey has introduced wireless ad-hoc networks and their applications in industrial automation. A technology overview has provided a progressive introduction to the main wireless communication standards contending in the industrial arena. ZigBee is the only one so far that has been especially designed for actual mesh networking, but emerging standards based on UWB technologies may end up being highly relevant for industrial automation as well. Bluetooth has lost momentum and does not appear well suited for ad-hoc networking needs, whereas WLAN mainly targets mobile office or field technician-like applications.

The paper has also made the distinction between open-loop and closed-loop applications, and presented some example scenarios. Due to the fact that open-loop applications deliver data that is less process-critical, these scenarios have already started to appear in industry. A quick rollout of closed-loop applications is not expected due to inherently complex reliability and performance issues. It is however likely that some of these scenarios will soon emerge in small or slow process environments. For faster and larger process scenarios, more research must be performed in order to optimize communication, control, and power consumption.

The authors believe that wireless ad-hoc networks have a huge potential for changing the face of industrial automation. Although hurdles are still to be cleared, many innovative companies around the world are already paving the way for fully decentralised, highly adaptive and cost-effective automation networks.

REFERENCES

Apneseth, C., D. Dzung, S. Kjesbu, G. Scheible and W. Zimmermann (2002). Wireless – Introducing Wireless Proximity Switches. *ABB Review*, **Vol. 4**, pp. 42–49, www.abb.com/technology.

Fluhrer S., I. Mantin, and A. Shamir (2001). Weaknesses in the Key Scheduling Algorithm of RC4. In: *Eighth Annual Workshop on Selected Areas in Cryptography*, Toronto, Canada.

Kahn, J.M., R.H. Katz and K.S.J. Pister (2000). Emerging Challenges: Mobile Networking for "Smart Dust". *Journal of Communications and Networks*, **Vol. 2**, No. 3, pp. 271–278.

Liu, X. and A.J. Goldsmith (2003). Wireless Communication Tradeoffs in Distributed Control. In: *Proc. of 42nd IEEE Conference on Decision and Control*, pp. 688–694, Maui, Hawaii.

Liu, X. and A.J. Goldsmith (2004). Wireless Medium Access Control in Networked Control Systems. In: *Proc. of American Control Conference*, Boston, USA.

Ploplys, N.J., P.A. Kawka and A.G. Alleyne (2004). Closed-Loop Control over Wireless Networks. *IEEE Control Systems Magazine*, **Vol. 6**, pp. 58–71.

Sastry, N. and D. Wagner (2004). Security Consideration for IEEE 802.15.4 Networks. In: *ACM Workshop on Wireless Security,* Philadelphia, USA.

Sinopoli, B., L. Schenato, M. Franceschetti, K. Poolla, M.I. Jordan and S. Sastry (2004). Kalman Filtering with Intermittent Observations. In: *IEEE Transactions on Automatic Control,* **Vol. 49**, No. 9, pp. 1453-1464.

Tuck, A. and C. Burgess (2003). Mesh Meets the Need – Wireless for Industrial Control. *ISA Technical Information and Communities*, www.isa.org.

Yang, L. and G.B. Giannakis (2004). Ultra-Wideband Communications: An Idea whose Time Has Come. In: *IEEE Signal Processing Magazine,* **Vol. 21**, No. 6, pp. 26-54.

IEEE Std 802.11a (1999). Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: High-speed Physical Layer in the 5 GHz Band. LAN/MAN Standards Committee of the IEEE Computer Society.

IEEE Std 802.11b (1999). Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: High-speed Physical Layer Extension in the 2.4 GHz Band. LAN/MAN Standards Committee of the IEEE Computer Society.

IEEE Std 802.11g (2003). Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications – Amendment 4: Further High Data Rate Extension in the 2.4 GHz Band. LAN/MAN Standards Committee of the IEEE Computer Society.

IEEE Std 802.15.1 (2002). Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs). LAN/MAN Standards Committee of the IEEE Computer Society.

IEEE Std 802.15.4 (2003). Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-rate Wireless Personal Area Networks (LR-WPANs). LAN/MAN Standards Committee of the IEEE Computer Society.