SENSOR NETWORKS FOR INDUSTRIAL APPLICATIONS

A. Flammini, P. Ferrari, D. Marioli, E. Sisinni, A. Taroni
University of Brescia - Department of Electronics for the Automation
Via Branze 38 - 25123 Brescia – alessandra.flammini@ing.unibs.it
Tel: +39 030 3715627 – Fax: +39 030 380014
Web: www.ing.unibs.it/~wsnlab

Abstract

Industrial applications are moving from centralized architectures towards distributed ones, thanks to cost effectiveness, better flexibility, scalability, reliability and diagnostic functionalities. The use of sensors in industrial communications improves overall plant performance since sensor information can be used by several equipments and shared on the Web. A communication system suitable for computers and PLCs, that exchanges a large amount of data with soft real-time constrains, can be hardly adapted to sensors, especially to simple and low-cost ones. In fact, these devices typically require a cyclic, isochronous and hard real-time exchange of few data. For this reason, specific fieldbuses have been widely used to realize industrial sensor networks, while high-level industrial communication systems take advantage of Ethernet/Internet and, more recently, wireless technologies. In these years, Ethernet-based solutions that meet real-time operation requirements, called Real-Time Ethernet, are replacing traditional fieldbuses and research activities in real-time wireless sensor networking are growing.

In this paper, following an overview of the state-of-art of real-time sensor networks for industrial applications, problems and possible approaches to solve them are presented, with particular reference to methods and instrumentation for performance measurement.

I. INTRODUCTION

Sensor networks

Traditionally, sensors output is furnished by simple electronic circuits that provide a standard analog interface (e.g. 0-5V, 4-20mA, and so on). Thanks to availability of low cost microcontrollers, a new generation of sensors, normally called "smart sensors", is growing [1]. They provide improvements in terms of linearity, signal-to-noise ratio and diagnostic features; in many cases, network connectivity is also supported. Unfortunately there is not an unique communication standard for sensor networking. In fact, to support computer connectivity there is no choice; Ethernet [2], together with Internet protocols, is the universally recognized solution. On the contrary, sensor networking requires very simple and low-cost protocols to be supported by a 8-bit low cost microcontroller and several incompatible solutions are competing each other for market leadership in a particular application. Sensor networking, in fact, is the objective of many application fields: military, agriculture, environment monitoring, home automation, health and welfare, automotive, industrial applications. Each field has its own requirements: for instance, health and welfare need sensor compactness and wireless [3], while low cost is imperative for automotive and home automation [4]. More generally, a sensor network is evaluated with respect to some characteristics as: transmission range, that could be greatly affected by the physical mean; compactness; mobility, that implies wireless sensors with autonomous power source [5]; cost; performance, that is roughly represented by bit rate but that could depend on general timing requirements, like latency and jitter; least but not last robustness, that is safety and security [6].

The industrial scenario

As regards sensor networks for most of industrial applications, sensor compactness and mobility are not critical requirements. In fact sensors are usually placed in a fixed place and power supply availability is practically everywhere. On the contrary, robustness is a key factor, as strong electromagnetic power sources (welders, smelting furnaces, motors and so on) [7] can sensibly affect transmission quality. In addition, it is very important to transfer information within a small, fixed and known time and therefore performance is a crucial point.

The best way to respect deadline in information transfer is a centralized architecture; sensors are read when needed and event reaction time, that is the delay between an input event and the related output actuation, is minimal and well-known. Even in this employment, smart sensors offer several advantages; in fact, the term smart transducer is widely used to define a transducer whose output is something more than raw measurement data. A formal definition can be found in the standard IEEE 1451.2 [8]: "a Smart Transducer provides functions beyond those necessary for generating a correct representation of a sensed or controlled quantity. This functionality typically simplifies the integration of the transducer into applications in a networked environment". A sensor is smart if it can be managed regardless peculiarities due to its vendor or the adopted interfacing protocol. Transducers become PLUG & PLAY eliminating errors due to manual configuration and data entering: they can be installed, upgraded, replaced or moved with minimum effort. A smart transducer implements a general model for data, control, timing, configuration and calibration and it contains a standardized Transducer Electronic Data Sheets (TEDS) with manufacture-related data.

The simplified block diagram of such a device is given in Figure 1. The key aspect is the network capability; analog point-to-point interfaces (e.g. 4-20mA, 0-10V…) can be substituted by a single, low cost, and reliable digital field area network; this is the first step towards a real distributed system. Advantages of distributed architectures are countless, including increased flexibility, improved performances, cost reduction due to cabling diminution, easiness of installation and maintenance.

1-4244-1245-5/07/$25.00 ©2007 IEEE

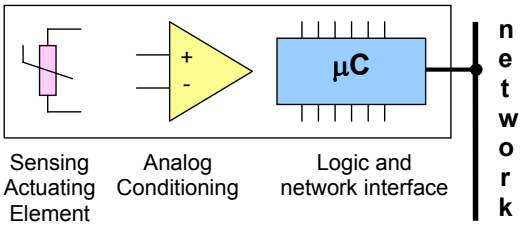

Figure 1: Smart transducer block diagram.

Unfortunately, distributed architectures imply transmission delays that could heavily affect performance. For the sake of clarity, an example is analyzed.

If we suppose a simple distributed architecture, as depicted in Figure 2, then a simple program as "if A>B then immediately actuate C", that properly works in a centralized architecture, could present some problems.

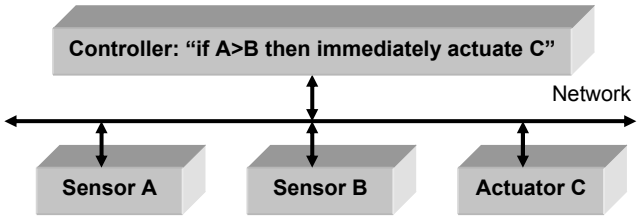

Figure 2: Distributed architecture.

In fact, A and B quantities could be sampled in different instants, that is $A=A(t_0)$ and $B=B(t_1)$ and therefore can be hardly compared. Even if we suppose $t_0 \approx t_1$, it could be difficult to exactly estimate the transmission time $t_{d,A}$ and $t_{d,B}$ of A and B to controller; typically they can be approximated by known limits ($T_{min} < t_{d,A} \neq t_{d,B} < T_{max}$). Even if we suppose that elaboration starts as soon as sensor messages arrive and the actuator actuates C as soon the controller message arrives, elaboration takes time t_{elab} and the controller message takes time $t_{d,act}$ to reach the actuator. Consequently there is a delay time T_d that, if we neglect sampling and actuating time, is equal to $T_d = \max(t_{d,A}, t_{d,B}) + t_{elab} + t_{d,C}$. T_d could be significant and variable, because $t_{d,A}$, $t_{d,B}$ and $t_{d,C}$ could depend on network traffic. This simple example shows how performance of a distributed architecture could be affected by network and application behavior; in fact the above T_d expression is simplified due to strong hypothesis we have done.

In addition, terms usage in industrial communications could be quite confusing, as expressions like "real-time" or "determinism" are often misused. According to International Electrotechnical Commission (IEC) [9], real-time is the ability of a system to provide a required result in a bounded time, that is maximum latency is "a priori" known. Consequently, a real-time communication system is able to transfer data in real-time. In some cases it is used a distinction between "soft real-time", with a statistical real-time behavior, and "hard real-time", where the maximum latency shall be respected in all cases, as in the IEC 61784-2 definition. Determinism is related to the ability to set an imposed and invariable latency, that is the required result is provided in a fixed, known and repeatable time. However, it is often used in substitution of hard real-time, that is a less stringent constrain. Isochrony refers to the ability to be strictly repetitive in time; an isochronous communication system imposes that each data transfer takes action in a strictly cyclic way with a very low jitter, where jitter is intended as the difference between the maximum and the minimum value of cycle time.

Some industrial applications, as packaging, manufacturing, wood machining or plastic extrusion, require high performance systems to achieve a cost reduction [10]. Data exchange must be fast, reliable and deterministic, that is latency times must be in the order of hundreds of microseconds to correctly close control loops between twin drives, while jitter times must be one order of magnitude lower.

In our example, traffic between controller and transducers can be organized in a cyclic way, as shown in Figure 3, i.e. the controller periodically (every cycle time) exchanges information organized in time slots with field devices.

If the chosen physical and medium layers ensure the respect of time slot bounds, then communication is real-time, deterministic and isochronous, that is frames are sent with a constant inter-arrival time. However, the system behavior, characterized by time T_d, could show a considerable jitter, because time between event (A>B) and reaction (C actuated) depends on sensor sampling time and, more generally, on synchronization among nodes application tasks.

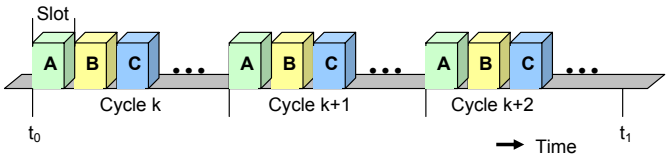

Figure 3: Cyclic traffic exchange.

For this reason, industrial communication protocols often provide some synchronization services, as input/output synchronization commands (e.g. global read, global write) or application synchronization utilities in order to achieve determinism. In fact, if all the nodes share a common sense of time (i.e. they have synchronized clocks) and the isochronous scheme of Figure 3 is adopted, then determinism could be reached simply modifying the system program into:

- sample A and B at time t_0 (i.e. the start of the cycle k)
- if $A(t_0)>B(t_0)$ then actuate C at time t_1

where time interval between t_0 and t_1 must be greater than three times the cycle time, supposing the elaboration is synchronized with the start of the $(k+1)^{th}$ cycle and the elaboration time is less than the cycle time in order to deliver message to C in $(k+2)^{th}$ cycle.

Obviously, if the sensor network does not imply actions to take in real-time, but is only used to collect data from sensors, the only need is to "accurately" reconstruct the temporal sequence of data (data timestamping), because time accuracy/resolution affects data value accuracy/resolution.

This can be achieved by a timestamping mechanism in every node and a good synchronization among nodes.

In conclusions, due to hard constrains in terms of performance, robustness and cost, sensor networks for industrial applications, usually called fieldbuses, are often "tailored" solutions. Fieldbuses are used in most of industrial plants to digitally link subsystems and to transfer few data in real-time. They are typically characterized by a cyclic behavior, synchronization utilities, a quite low data rate (Mbit/s), good efficiency (number of data bit with respect to transmitted bit), a good transmission range (100m), low cost and a special attention to safety [11,12,13,14]. They are similar to proprietary technologies; they reach satisfactory performances but proposals of different vendors typically can not coexist. There are several open standards with pros and cons describing these networks; for instance, DeviceNet or PROFIBUS [15] are quite simple and can be easily integrated in low-cost microcontrollers, reducing the need for external components (e.g. some 8-bit Freescale or Microchip microcontrollers provide a CANbus 2.0B interface).

Nowadays, fieldbuses support the most of sensor networks in industrial applications, although many industrial fields [16], with few, simple and close sensors, still adopt traditional centralized architectures.

II. FROM FIELDBUS TO ETHERNET AND RTE

As high level communication systems adopt solutions based on TCP/IP [17], as for instance OPC (Ole for Process Control [18]), fieldbuses can be hardly integrated [19]. In addition, fieldbuses are often poor as regard diagnostic and self-configuring tools. Ethernet is the most common used physical layer of widespread TCP/IP-based solutions and it is widely used in industrial plants at PLC (Programmable Logic Controller) and SCADA (Supervisory Control And Data Acquisition) level, where it is called "Industrial Ethernet" [20]. The idea to use it even at the field level took place in the last years thanks to the more efficient switch-based architecture, to the increased transmission rate and to the availability of low-cost devices [21]. Ethernet seems unsuitable for real-time applications because the a priori estimation of the maximum transmission time of a data packet is impossible [22]. This is mainly due to the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) for the Medium Access Control (MAC) and to unpredictable delays introduced by switches, that depends on network topology, traffic conditions, switch technology ("Store&Forward", "Cut-Through", [23]), and so on. An important incentive to the diffusion of Ethernet in industrial plants comes from IEC61784-1 [15], that describes and acknowledges some commercial solutions of industrial Ethernet that in some cases could be used down to sensor level, as HSE (Fieldbus Foundation for Ethernet), Ethernet/IP, PROFINET. These protocols does not guarantee performance suitable for most of real-time control applications, therefore other solutions are emerging, called Real-Time Ethernet (RTE), as Powerlink [24], PROFINET IO [25], EtherCAT [26], MODBUS-RTPS [27] and so on, including dedicated solutions [28]. These technologies allow more powerful performances if compared to traditional fieldbuses, taking advantage from the high performance of Ethernet (e.g. 100Mbit/s or more instead of typical 1-10Mbit/s of high-performance fieldbuses).

Real-Time Ethernet (RTE) is defined by IEC61784-2 as the ISO/IEC 8802-3-based network that includes real-time communication [2]. RTE solve the non-determinism problem of Ethernet modifying media access rules by means of software protocols (e.g. master-slave protocols based on Time Division Multiple Access -TDMA-) or thanks to ad hoc switches or network interfaces. There is not a universally acknowledged single RTE protocol and the above cited solutions differ on the way they achieve determinism.

Synchronization among nodes, that is all the nodes follow a common clock (master clock), takes a very important role in RTE. Synchronization methods can vary from simple proprietary protocols [29], as broadcast triggering messages, to the use of standard solutions, as Network Time Protocol (NTP) or Precision Time Protocol (PTP) described in standard IEEE1588 [30,31]. At the present, standard IEEE1588 seems the most promising synchronization method because it is independent from technology and it allows full-software realizations but, in that case, it strictly depends on the application level. In addition, in industrial plants, star topologies are considered unsuitable, so if many switches are cascaded [32], propagation delay of a frame is asymmetric and IEEE1588 could yield to considerable estimation errors. Hardware-software solutions can be used in order to increase performance of IEEE1588 achieving an accurate timestamping of frames; by this way a synchronization in the order of 100 ns can be reach, but RTE protocols are not supported [33]. Besides IEEE1588-based approaches, new ideas have been proposed to synchronize nodes. For instance a suitable use of GPS (Global Positioning System) to obtain a Universal Coordinated Time (UTC) reference is described in [34].

Another common aim of an RTE network is to be compatible with TCP/IP traffic. In fact, industrial communications should support at the same time, on the same media, a fast (isochronous) real-time data exchange and, if an event occurs (alarm or diagnostic or configuration activity for a certain node), complex and acyclic communication. Some research activities have been carried out to quantify RTE performance reduction as a function of bandwidth dedicated to TCP/IP traffic [35], but methodologies for the test environment setup, like load generation and profile, are rather rough [36,37].

As an example of an RTE, PROFINET IO is briefly described [38]. PROFINET IO performance is described with the class number: RT_Class 1 (RT, Real-Time) is used in systems requiring cycle time down to tenth of milliseconds; RT_Class 2 (also called IRTflex, Isochronous Real-Time with Flexible network topology) and RT_Class 3 (also called IRTtop) are used with applications requiring isochrony and cycle time shorter than 1 ms. The PROFINET concept is to support on the same media hard real-time traffic, soft real-time traffic and non real-time traffic as TCP/IP. PROFINET IO defines IO-Controllers (i.e intelligent devices which carry out automation tasks), IO-Devices (i.e. field devices like sensors, actuators, IO module etc.) and IO-Supervisors for configuration and diagnosis purposes.

PROFINET IO data exchange is based on a highly repeatable cycle as described in IEC61158-5-10 [39] and illustrated in Figure 4. A synchronization message (sync frame) signals the cycle start. Several phases can be recognized in a cycle:

- RED phase: during this phase, only RT_Class 3 messages are sent on a time scheduled basis through "a priori" defined path. This means that all PROFINET IO RT_Class 3 devices know when, and on which physical port, they are allowed to talk or listen to.
- ORANGE phase: only RT_Class 2 frames are sent in this phase. Also RT_Class 2 has a time base schedule but the physical path is not defined.
- GREEN phase: this phase is composed of Ethernet message managed using the Ethernet priorities (IEEE 802.1Q). GREEN phase communication is used by: RT_Class 2 devices with extra frame to send; RT_Class 1 (RT) devices which are not synchronized each other; all the rest of the IP based communication (TCP, UDP). It should be noted that, as a result, RT_Class 1 frames may suffer from low but unpredictable delay.
- YELLOW phase: this is a transition phase used for the same type of traffic of the GREEN phase. During this period, only frames which can be completely transferred within the end of the YELLOW phase are transmitted.

A relevant portion of the cycle (in the GREEN phase) is left for non real-time communication (NRT) such as TCP or UDP. Such traffic has low priority tags and very variable delays. Indeed, IP traffic is used for big data transfers, and the only important thing is the bandwidth. In PROFINET IO, NRT phase occupies at least the 40% of the total bandwidth.

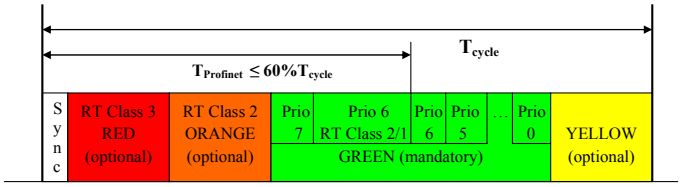

Figure 4: PROFINET IO cycle.

No collisions, no delays can happen within RT_Class 3 since the scheduling sequence in each cycle is "a priori" known and always identical. The engineering (network configuration) tool calculates the trip for every frame of a cycle and downloads the schedule in the network infrastructure. This means that the network infrastructure must be PROFINET IO compliant; in fact special switches must be used, that thanks to a powerful ASIC [40], forward RT_Class 3 frames looking only at the time schedule, without MAC address check. On the contrary, RT_Class 2 frames are forwarded using MAC addresses, as usual. In case traffic bursts, RT_Class 2 frames can be buffered and delayed to the next GREEN phase. RT_Class 2 exhibits a jitter higher than RT_Class 3. Normally these PROFINET IO compliant switches are integrated directly into RT_Class 3 nodes; the introduction of a normal switch (i.e. a "Store&Forward" [23] switch) could seriously affect overall performance.

III. METRICS AND INSTRUMENTS FOR RTE

RTE networks are an example of emerging technology where scientific research and industrial interest converge. RTE networks are a new topic and recently some workshops are appearing [41,42,43]. Besides a lack of widespread knowledge, a general absence of measurement methods and instruments characterizes RTE-based applications.

Particularly, a complete set of suitable parameters to characterize an RTE-based application is not defined; moreover, even if a feature derived from the Information and Communication Technology (ICT) field seems adequate, measurement methodologies and test environments are often not available. For instance bandwidth and latency are well-known and widely used in Ethernet [44] and Internet [45] and they appear correct for RTE also. However, real bandwidth measurement is rather difficult, because it depends on data and on the state of linked nodes; actually, the peak value is often considered in the best case. As regard latency, it is usually measured in an empirical way thanks to instruments that measure the normally called "roundtrip delay", that is defined as the time interval between the transmission of special frames and the receipt of the related acknowledge [46]. The most famous method is the Ping command that is based on ICMP (Internet Control Message Protocol). Obviously, this method does not support the resolution required by RTE networks. The above cited IEC61784 suggests some performance indicators:

- delivery time: the time needed to convey application data from one node (source) to another node (destination).
- time synchronization accuracy: the maximum deviation between any two node clocks.
- non-time-based synchronization accuracy: the maximum jitter of the cyclic behavior of any two nodes when such cyclic behavior is established by means of periodical events over the network. For instance, this is the case of some RTE protocols that use a network message to signal the start of a cycle. In such protocols the sharing of a common clocks reference is not required.
- redundancy recovery time: "the maximum time from failure to become fully operational again in case of a single permanent failure".
- throughput RTE: the total amount of RTE application data (by octet length) on one link per second.
- non-RTE bandwidth: "the percentage of bandwidth, which can be used for non RTE communication on one link". The total link bandwidth shall also be specified, since they are related to each other.

Furthermore, several other indicators can be used [47,48]. For instance "Stack Traversal Time" is the time required by data to pass through the communication stack from top (application layer) to bottom (physical layer). "Event Reaction Time" is the time required by the system to acknowledge an external event (e.g input change) generating a response action. This time is very important in practical applications and it significantly depends on application level implementation. As the experimental evaluation of these

indicators is quite difficult on an industrial plant, the research activity is focused on provide simulation tools. Obviously network simulators like OPNET [49] or OMNET++ [50] do not natively support RTE protocols, therefore a great effort is spent to develop an effective model of an RTE node [51].

As regards measurement instrumentation, in the ICT field some instruments are used to associate a time reference to Ethernet frames: from the PC-based instruments like WireShark (formerly Ethereal), a well known network analyser software, [52, 53] with resolution in the order of 0.1 ms, to the high-performance network analyzers. The latter allows a time resolution in the order of tenths of nanoseconds that could be suitable for RTE networks; on the other hand, limits are the compactness, the cost and the robustness typically needed by industrial environments. As an example of new instruments designed for ICT, WAND group [54,55] of University of Waikato in New Zealand has developed a new instrument based on programmable logic devices that adds timestamps to every Ethernet packet. At present about 100 of these instruments, synchronized by GPS, are used all over the world to perform statistical analysis of Internet traffic.

As software-based instruments are not adequate and network analysers allow only a costly and localized measurement, often RTE performance characterization is done looking at input and output signals, for instance measuring the event reaction time with respect to external event and reaction.

In order to develop instruments tailored to RTE networks, a multi-probes approach must be considered taking advantage from recent developments in the FPGA technology and in the availability of network processors [56]. In fact, by means of a multi-probe architecture, it is possible to experimentally measure delay times (i.e. through a switch) and verify synchronization among nodes.

A new instrument

A new, low-cost, multi-probe instrument has been recently proposed [57]. General architecture is shown in Figure 5. The instrument can be viewed as a network of probes designed to simultaneously log Ethernet traffic in different links of a target RTE network. This "parallel" network, called measurement network, conveys data (logged by probes) toward a supervision equipment, called monitor station. Probes are requested to associate a reliable timestamp to every frame that transits on the Ethernet link they monitor. This results in a special probe architecture that enables RTE full-duplex logging together with strict time synchronization among probes.

Monitor station must store and elaborate all the incoming data, thus the only critical point is the system bandwidth, that is the ability to manage all the data without dropping frames. In fact, logged frames and timestamping related data must be transferred, resulting in quickly growing bandwidth requirements. Generally, if 100BaseT high-bandwidth RTE protocols are considered, the measurement network should work with 1000BaseT or more. In the realized implementation, a 1000BaseT measurement network has been used.

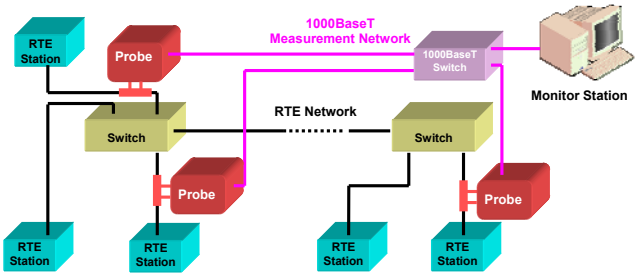

Figure 5: General architecture of the new multi-probe instrument.

One of the objectives during the development of the new instrument architecture was cost limitation. This led to have single-chip FPGA-based probes and a single Monitor Station implemented using a PC. Moreover, the monitor station can use open source user interface programs like the above cited WireShark. The probe local time is constantly synchronized with a reference clock despite local crystal oscillator variations (temperature, aging, etc). Synchronization Unit can operate using multiple synchronism sources: 1-PPS signal from an external source or IEEE1588 Sync Message coming from the measurement network. The local time is synthesized with an adder structure [58]. Briefly, an increment step is summed to the time register at every clock period of the local oscillator. Drift and offset can be compensated adjusting the increment step with a suitable control algorithm. The increment step is refreshed each time a synchronism event happens; it means 1 s with 1-PPS and 2 s with IEEE1588 PTP.

A two-probes prototype has been experimentally characterized comparing performance to a powerful single-probe network analyzer: Endace NinjaCapture 1500 [59]. The test network is the PROFINET IO Class 1 system shown in Figure 6.

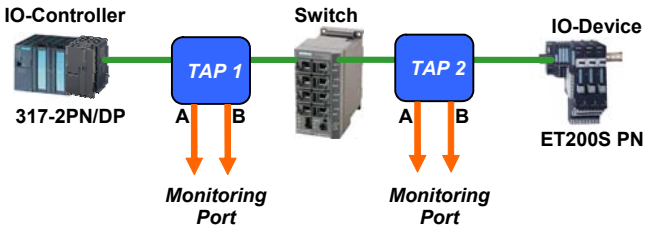

Figure 6: Experimental setup (PROFINET IO Class1 network).

Two Ethernet TAPs have been inserted in the network in order to capture traffic before and after the switch. A TAP can duplicate full-duplex traffic, so it has two monitoring ports (A and B) one for each direction. The metric to be compared is the experimental evaluation of the propagation delay of the switch.

Propagation delays can be measured in the following modes:

- Connecting an input of the Ninjacapture to the monitoring output A of TAP 1 and the other to output A of TAP 2. Delay along a single direction can be measured, since NinjaCapture has two logging inputs. Delay in the reverse direction can be measured connecting the NinjaCapture to output B of the TAPs.
- Using a single probe of the proposed instrument that has two input ports. Port 1 must be connected to the monitoring output A of TAP 1 and Port 2 to output A of TAP 2. As in the previous case, two separate measurements are needed to characterize the two traffic directions.
- Using two probes of the proposed instrument. Now the instrument has four logging inputs. The two inputs of Probe 1 are connected to outputs A and B of TAP 1; inputs of Probe 2 are connected to outputs A and B of TAP 2. A single acquisition campaign is sufficient for estimation of switch behavior in both traffic directions.

The measure of the propagation delay of this "Store&Forward" switch has been carried out with 64-byte long frames. Measurements results have been reported in Table 1. Generally, they are comparable even if the conditions are different. In particular, the proposed instrument can reduce measurement times, since a single setup is enough, and the user can save money since it is cheaper than NinjaCapture.

Table 1: Switch propagation delay.
(IOC: IO controller, IOD: IO device).

	Direction	Switch propagation delay (ns)		
		Ave.	Std. dev.	Max.
Ninja Capture	IOC → IOD	12 363	1670	15 567
	IOD → IOC	12 483	1650	15 572
Single probe	IOC → IOD	12 404	1653	15 563
	IOD → IOC	12 496	1658	15 592
Two probes	IOC → IOD	12 381	1693	15 601
	IOD → IOC	12 460	1679	15 576

IV. THE WIRELESS OPPORTUNITY

As previously stated, traditional networking offers many advantages but requires cables to interconnect devices. This leads to high installation and maintenance costs, e.g. due to low scalability and high failure rate of connectors. For this reason, wireless technologies gained an enormous success in the consumer goods industry in the last few years. In addition, the adoption of wireless solutions at the sensor level offers other advantages as continuous, high resolution, ubiquitous sensing, provides support for mobility, adds redundancy and takes advantage of MEMS technology.

In particular, besides high power consumptions, high area coverage and high cost solution such as the well known and mature mobile phone technologies (GSM, GPRS and UMTS just o cite few of them), two standards have monopolized the market of the Local/Personal Area Networks: IEEE802.11 [60] and IEEE802.15.1 [61]. The former is the wireless counterpart of the Ethernet standard and implements lower levels of WiFi [62], while the latter constitutes lower levels of the proprietary Bluetooth (BT) [63] solution. The main attractive of both of them is that they do not require any sort of frequency licensing because operate in the ISM (Industrial, Scientific and Medical) radio frequency region. However, WiFi and BT have been designed to address requirements of office/personal communication, and cannot efficiently be used to realize Wireless Sensor Networks (WSNs), as better explained in next sections.

Obviously, advantages due to the absence of cables could be usefully exploited in several fields and many efforts have been done in this direction. For example, in the past, novel trends [64] have emerged in the agricultural sector converged in the so called "precision agriculture", that concentrates on providing the means for observing, assessing and controlling agricultural practices. In this way, it would be possible to detect parasites on the field and automatically choose the right type and amount of insecticide. Another field where wireless technologies have been widely used is "environmental monitoring"; just to mention some applications, it is possible to monitor air quality in real-time by means of unattended stations or collect data in places that discourages human presence. Another interesting application is in the field of "smart structures", that comprises home and building automation; in this case, a wireless sensor and actuator network is integrated within a building to improve living conditions and reduce overall energy consumption. Also "medical and health care" are fields where WSNs have been successfully employed; e.g. it is possible to ensure patients continuous monitoring without limiting their mobility.

Wireless Sensor Networks

As stated in previous section, wireless communications are an effective and reliable solution in home and office automations. Generally speaking, several medium can be exploited, including light and ultrasound, but considerations regarding data size, rates and area coverage make RF links more attractive. Many standards have been proposed to satisfy requirements of the consumer world, as proved by the IEEE802 subgroups that cope with these topics (refer to Figure 7), but the most interesting for WSN applications are probably those comprised in the IEEE802.15 [65] working group, whose effort focuses on the development of Personal Area Networks or short distance wireless networks (≈10 m).

In particular, here is defined the concept of Personal Operating Space, a spherical region that surrounds a wireless device with a radius of 10 m. Even if originally designed for portable and mobile computing devices such as PCs, Personal Digital Assistants (PDAs), cell phones, pagers, and consumer electronics, it may be successfully applied to WSNs. However, it must be underlined that large scale applications in the sensor networking area are yet in the development stage.

First of all, it is important to distinguish between the idea behind the WSN concept and implications related to an industrial scenario, better described further. From a general point of view, a WSN is made up of a large number of tiny

devices (sensors), which are densely deployed and collaborate to monitor and analyze a phenomenon of interest [64].

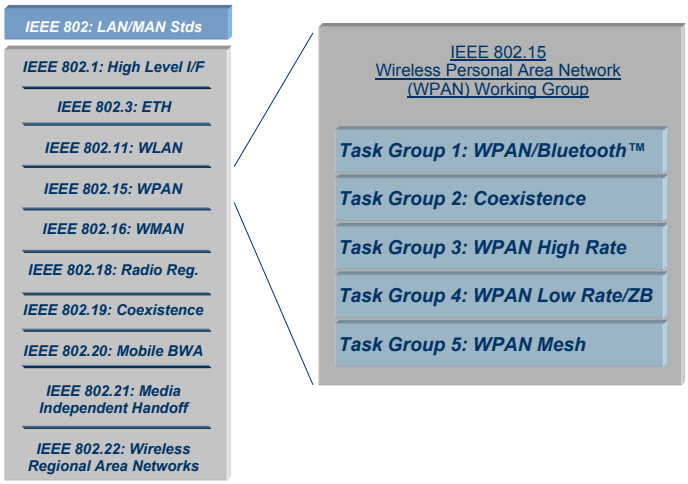

Figure 7: IEEE802 family wireless standards.

Due to cost and dimension constrains they have limited computational resources; power consumption must be as low as possible to ensure a true autonomous activity. In addition, sensors could be randomly positioned thus requiring localization and self-organizing capability. Besides issues considered in this paper, there are other questions that must be considered in a wireless system. In particular, security could be a key aspect; air is an open medium and it is easy for an attacker to malicious alter transmissions or make the link unreliable injecting jam sequences.

The block diagram of a wireless sensor node is represented in Figure 8.

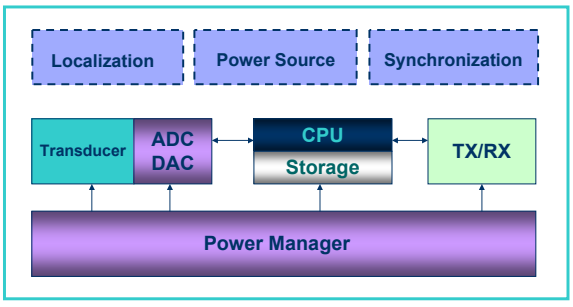

Figure 8: Wireless transducer block diagram.

As every smart sensor, a wireless transducer consists of three main parts: a sensing unit, a processing unit and a transceiver unit. In addition, a power manager is present to handle on board power sources, such as electrochemical batteries or more exotic power scavenging units. Moreover, most of the performed tasks require also the knowledge of positions and time, furnished by proper localization and synchronization units. Many researchers are currently engaged in the design of proprietary schemes that fulfil such requirements, each one with its pros and cons. However, according to authors the most promising solution is to adapt standard solutions, that are already available on the market and can exploit huge volume production and mature technologies, to the application under investigation.

In the following, aspects regarding power consumption, localization and communication architecture will be detailed, while in next section the industrial scenario will be considered.

Power consumption

Power consumption of a wireless sensor node can be divided into three different domains: sensing, processing and communicating. The first one is strictly related to the application and in most of cases can be neglected. As regards data processing, usually processor consumption during the active phase decreases by an order of magnitude or less if compared with that needed in the communication phase. As explained in [66], supposing a Rayleigh fading and a forth order loss law, the energy required to transmit 1KB over a distance of 100 m is approximately the same as that for executing 3 million of operations by a 100 MIPS/W processor. From another point of view, it is convenient to implement complex algorithms if this result in shorter data packets and/or in a more robust data link that requires less retransmissions. It is a well known results that consumption is proportional to the voltage supply (Vdd), and to the operating frequency (f), i.e. $P \propto Vdd,f$ [67]. This relationship suggests two strategies to lower consumption: dynamic scale voltage, i.e. reducing the supply voltage Vdd as low as possible, and changing the CPU clock frequency f according to the computational load (usually, microprocessor uses a low and a high frequency oscillator in the idle and active phase respectively). The most demanding unit is thus the transceiver. If we consider short range (≈10 m) systems operating in the GHz range with low radiation power (≈0 dBm), energy required to transmit is almost the same as that required in data reception. Obviously, devices spent most of their time doing nothing; this means that low duty cycle strategies, probably the most diffused solution in battery supplied nodes, can be applied. What really matters is the average current consumption $I_{cc,mean}$ of the wireless sensor. For this reason becomes fundamental evaluate not only the active power but also consumption in standby mode and start-up phase duration. If we consider a simple node that:

- wakes-up every T seconds (it depends on the Medium Access Protocol implemented),
- takes T_a [s] at I_a [A] to start-up and measure quantities (processing phase)
- takes T_{RF} [s] at I_{RF} [A] to transmit and receive (transceiver phase) information by means of the RF link
- requires I_{sleep} [A] in the standby phase

the $I_{cc,mean}$ can be computed as shown in equation (1):

$$I_{cc,mean} = \frac{I_a \cdot T_a + I_{RF} \cdot T_{RF} + I_{sleep} \cdot (T - T_a - T_{RF})}{T} \quad (1).$$

Designer can adapt T_a and T_{RF} (e.g. shortening the measuring phase or choosing a very simple protocol and/or a high

transfer rate) so that $I_{cc,mean}$ remains in the order of I_{sleep}, as shown in equations (2):

$$T_a, T_{RF} << T; \quad T_a \approx T \cdot \frac{I_{sleep}}{I_a}; \quad T_{RF} \approx T \cdot \frac{I_{sleep}}{T_{RF}} \quad (2).$$

Electrochemical batteries are probably the most economic and versatile small power sources. Neglecting the power unit self consumption, battery life L (hours), defined as the time elapsed to fall below a voltage threshold (cut-off voltage), can be roughly computed as follows:

$$L = \frac{\eta \cdot C}{K_v \cdot I_{cc,mean}} \quad (3)$$

where C (Ah) is battery capacity, η is the power supply efficiency and K_v is the power supply output voltage gain. Batteries are usually divided into primary or not rechargeable cells and secondary cells; according to adopted electrolyte (NiCd, NiMH, LiION…), they offer nominal voltage in the order of 1.2 – 3.6V and capacity up to 3Ah for the AA format.

Localization

WSN are severely constrained for energy and cost of deployment and operation. Therefore, localization is usually performed employing the same radio transceiver which is also used for inter-nodes communication. If higher performances are needed it is possible to adopt other techniques as GPS, whose cost is justified only in some applications. The basic idea is to exploit the Radio Signal Strength Indicator (RSSI), a standard feature in most radios. Two approaches are commonly accepted in literature - RSSI-maps and Signal Propagation Models. Many RSSI-measurements at different locations form a so called RSSI-map which is stored on a node or on a base station [68,69,70]. A node that wants to estimate its position compares the measured RSSI-values with the entries in the RSSI-map. The position with the most equal entry is then chosen. Although the precision of this technique is relatively high, movements of objects or persons enforce a recreation of the map, which is very time consuming. As an alternative the Signal Propagation Models have been established [71,72]; RSSI is used to evaluate power attenuation and correlate it to the distance with respect to anchorage points. In fact, if PT is the transmit power, PL(d0) is path loss for a reference distance of d0, $\eta \in [2,4]$ is the path loss exponent and the random variation in the power measured at the antenna connector is expressed as a gaussian random variable of zero mean and σ^2 variance, $X\sigma = N(0,\sigma^2)$, it is well known that the relation (4) is valid:

$$RSSI(d) = PT - PL(do) - 10\eta Log\left(\frac{d}{do}\right) + X\sigma \quad (4)$$

All powers are in dBm and all distances are in meters. In this model obstructions like walls are not considered; otherwise an extra constant needs to be subtracted from equation (4) to account for the attenuation in them (the constant depends on the type and number of obstructions).

However, experimental campaigns [73,74] pointed out that RSSI fluctuates for both intrinsic and extrinsic causes, such as:

- Transmitter variability: different transmitters behave differently even when they are configured exactly in the same way;
- Receiver variability: different receivers behave differently even when all environmental parameters are the same;
- Antenna orientation: different antennas have their own radiation patterns;
- Multi-path fading and shadowing in the RF channel: channel behaviour greatly depends on environmental characteristics;

As shown in [75], RSSI-based ranging and localization can be cheap and effective alternatives to the higher costs or complexity involved with other techniques such as GPS, but only when applied in the right environment. It has been shown that nodes must be elevated from the ground and free from obstructions; in addition, also transmission power, antenna orientation and node density greatly affects accuracy. Due to these very strict constraints, RSSI localization has limited applicability in unknown or changing environments, unless the system can be enabled to automatically adjust parameters such as signal strength and calibration coefficients.

As a concluding remark, localization is a hot topic in WSNs, especially when mobility is required, but it is still an expensive (computationally and monetary) task. Several researchers are involved in this field and a clear solution is not yet emerged.

Network communication architecture

A preliminary architecture classification of WSNs can be done distinguishing among infrastructure and ad-hoc networks [76], as shown in Figure 9.

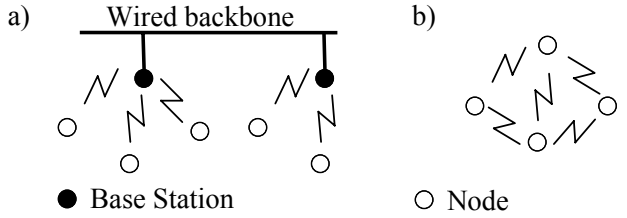

Figure 9: a) Infrastructure and b) ad-hoc WSN architecture.

Infrastructure. Wireless networks often extend, rather than replace, wired networks, and are referred to as infrastructure networks. A hierarchy of wide area and local area wired networks is used as the backbone network. The wired backbone connects to special switching nodes called Base Stations. Therefore, within infrastructure networks, wireless access to and from the wired host occurs in the last hop, between base stations and nodes that share the bandwidth of the wireless channel.

Ad hoc. Ad hoc networks, on the other hand, are multihop wireless networks in which a set of nodes cooperatively maintain network connectivity. This on-demand network architecture is completely un-tethered from physical wires. They are characterized by dynamic, unpredictable, random, multi-hop topologies with typically no infrastructure support. Mobile nodes must periodically exchange topology information which is used for routing updates.

Referring to the protocol stack, the traditional ISO/OSI model is modified as shown in Figure 10. The main difference is the presence of "vertical" planes whose aim is to manage power, localization and synchronization units shown in Figure 8.

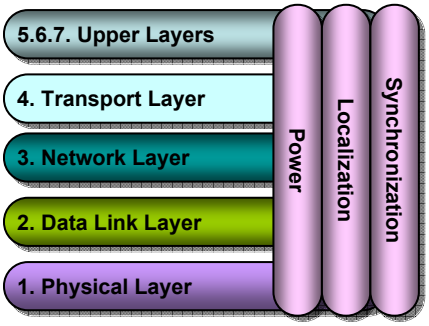

Figure 10: Wireless transducer block diagram.

The PHYsical (PHY) layer is responsible for frequency selection, modulation and data encryption. It is well known that long distance communications are not efficient in terms of power consumption and implementation complexity, suggesting the adoption of short range transceivers. In addition, this approach can overcome shadowing and path-loss effects if multi hop networks are implemented. Most diffused commercial available solutions implement spread spectrum modulation and offer data rates in the order of 0.1-1Mbps. The occupied band is the free ISM near the 2.4GHz portion of the spectrum. Power consumption is in the order of 10 mA for the transmitting/receiving phase down to less than 1 μA in the standby mode.

The Data-link Layer is responsible for multiplexing of data streams, data frame detection, Medium Access Control (MAC) and error control. Since the MAC controls the radio, it has a large impact on the overall energy consumption, and hence, the life time of a node. The air is a shared medium and it must be fairly assigned to nodes; the MAC decides when competing nodes may access the radio channel and tries to ensure that nodes don't interfere with each other's transmissions. The two major approaches are contention and schedule based one. The former allows collisions letting nodes to contend for the resource; the latter regulates accesses scheduling (usually there is a particular node or access point that broadcasts this information) when and for how long each controlled node can access the shared medium. Just to make an example, IEEE802.15.4 [77] implements Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) that belongs to contention methods, while IEEE802.15.1 adopts TDMA, a scheduling approach. The MAC layer operates on a local scale and lacks the global information to optimize network lifetime; it should ensure that energy it spends is proportional to the amount of traffic that it handles. Schedule-based protocols are the most efficient, at the cost of reduced flexibility; on the contrary, contention-based ones tend to collapse when the load approaches the channel capacity and wastes energy in idle listening, overhearing and protocol overheads. A rough classification can be done according to:

- the number of used RF channels;
- the degree of organization among nodes.
- the way a node is notified of an incoming packet;

It is not to possible to state what is the best solution, that must satisfy trade-offs dictated by the application [78]. Some considerations regarding the industrial environment are carried out in the next section.

The NetWorK Layer (NWK) routes the data supplied by the upper layers from the *source(s)* to the *sink(s)*. In a more formal way, sources are entities that provide data/measurements while sinks are those nodes where information is required. In single-hop architecture sources and sinks are directly interconnected by a radio link, while in multi-hop one nodes can forward information not intended for them. The topology architectures used in WSNs include star, mesh, and star-mesh hybrid topologies, as shown in Figure 11.

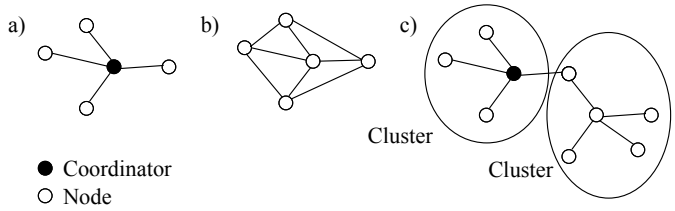

Figure 11: Network topologies: a)Star, b)Mesh, c)Hybrid.

The right topology depends on the amount and frequency of the data to be transmitted, transmission distance, battery life requirements, and the mobility and level of change in the sensor node. A star topology is a single-hop system in which a particular node, called coordinator, manages communications and all remaining nodes communicate only with it. It is a sort of master-slave structure where the coordinator acts also as a bridge towards other networks. It is a power efficient solution, that ensures a long network life even if a node collapses, but is able to handle a small number of nodes over a small area. Mesh topologies are multi-hopping systems in which all nodes are identical and communicate with each other, so that a coordinator or base station is not strictly needed. The multi-hop system allows for a much longer range than a star topology at the cost of higher power consumptions rate and higher latency. In fact, nodes have a high duty cycle since they need to "listen to" messages and network changes and latency is related to the number of "hops" between source and sink. Aim of a star-mesh hybrid architecture (also known as cluster tree) is to take advantage of the low power and simplicity of the star topology, as well as the extended range and self-healing nature of a mesh one. Nodes are organized in a star topology around routers or

repeaters which, in turn, organize themselves in a mesh network. However, latency may be a problem.

The Transport layer is usually implemented only if end-users access the WSN through the Internet. Upper layers are usually summed up in a generic application layer that makes the hardware and software of the lower layers transparent to the end-user.

Wireless Sensor Networks and the industrial scenario

Although WSNs are generally characterised by fast deployment and cost effectiveness, their applicability in industrial environments is yet in the development stage. The vast majority of conventional wireless protocols emphasise bit rate over versatility and reliability, which is unsuitable for industrial control and monitoring applications. For this reason, even if wireless is largely used at the Enterprise and Factory control level, applications at the field level are still in the deployment stage. For instance, Siemens [79] has just announced a wireless HMI (Human Machine Interface) module that relies over an extension of the IEEE802.11 they call IndustrialWLAN or IWLAN and that supports PROFINET protocol. The same manufacture offers other devices, as industrial access points and client nodes, that can be used as "cable replacement" of a PROFINET network. Even if IWLAN sensors are not yet announced, nodes may act as gateways towards standard fieldbuses as PROFIBUS.

An interesting survey has been conducted by the RUNES project, started in Sept. 2004 with the aim to expand and simplify networks of devices and embedded systems. The final conclusion reported in their first meeting [80] is that "Adoption of networked embedded systems (particularly wireless) is slower in the industrial sector than the rest of the sectors examined in this technology roadmapping exercise... While technologies are maturing, wireless should not be used for critical control applications. Monitoring in hazardous and inaccessible areas should be given priority in the short/medium term and in moving towards this some lessons can be learnt from successful telemetry deployments."

The basic goal of WSN is a reliable data delivery consuming minimum power. Traditionally, sensor networks data delivery is said to be [81]:

- time driven, when sensors communicate their data (continuously) at a pre-specified rate;
- event driven, when sensors report information only if an event of interest occurs;
- hybrid, when all approaches coexist.

Data Delivery Model of industrial communications is time driven for majority of operations (data collection), but, even if infrequent, events as alarms or network management issues must be detected/notified quickly. Real-time, i.e. the respect of temporal deadline, must be ensured with low and predictable delay of data transfer (typically, less than 10 ms); therefore synchronization among nodes must take place. As previously said, radio frequency links are disturbed particularly by too long transmission ranges or impenetrable walls and obstacles; therefore, methods for error detection or error correction are crucial. In addition, message lengths are mostly very short; therefore, data efficiency for short telegrams is a very important design guideline. The use of the time-triggered paradigm supports the protocol efficiency because the transmission of message parameters like sender identification, message length, message priority, etc... may be implicitly codified in the communication schedule.

For all these reasons, best solution seems to adopt small, reliable infrastructured star network that exploits time division as the medium access policy. In fact, typical radio link area allows to cover a machinery and several machineries may be interconnected by traditional wired fieldbuses; in addition, cellular topology allows frequency reuse. Most of the existing wireless systems/standards do not satisfy these requirements, since they all use event driven data delivery with contention based MAC protocols. Nevertheless, several efforts have been made to ensure the so called Quality of Service (QoS), i.e. the ability of a network to deliver predictable results, even in wireless. Just to make an example, the newly released IEEE 802.11e [82] amendment tries to overcome these flaws defining several improvements on the legacy MAC. In particular, the traditional contention based (CP according to the standard nomenclature) and contention free periods (CFP according to the standard nomenclature) have been replaced by an Hybrid Coordination Function (HCF) that preserves backward compatibility and satisfies QoS requirements. In the CP it is possible to define message priorities using a sort of slotted CSMA ruled by different Arbitrary InterFrame Space (AIFS); in the CFP the hybrid coordinator controls the access to the channel by polling the stations with QoS requirements. IEEE 802.11e amendment defines also new synchronization mechanism for the upper layers that dramatically improves the accuracy of the traditional Timing Synchronization Function.

In conclusion, proprietary tailor-made upper layers protocols are usually developed relying over new transceiver compliant with standard physical level; in this way portability and low cost is ensured without sacrificing performances. As the early adopters of these solutions it is possible to figure food processing, petrochemical and asset tracking (fast parcel operators) sectors, where monitoring tasks of slow dynamic quantities can be greatly simplified by cables replacement and new scenarios may be envisioned.

Such an implementation has been pursued by the ABB with its WISA (acronym of Wireless Interface to Sensors and Actuators) [83]. Nodes communication hardware is based on standard IEEE802.15.1 transceiver; the MAC layer in WISA adopts time division multiple access with frequency division duplex (TDMA/FDD), ensuring simultaneous transmission and reception of radio signals. The network level implements the star topology with up to 120 nodes per coordinator. Also a "wireless power supply" has been provided; simple nodes as proximities switches harvest energy by means of inductive coupling with a mains powered supply unit. The downlink, i.e. transmission from the coordinator to nodes, is always active in order to establish cycle and slot synchronization, to send acknowledgments and control data. On the contrary, the uplink, i.e. transmission from node to coordinator, is event driven, in order to lower power consumption. As stated by the manufacturer, for proximity switches that exchange a 1 byte-wide packet the typical latency between node and coordinator is in the order of 5 ms, with a maximum event rate of 5 Hz. In

the following section a brief description of available tools for WSNs planning is done. In particular, it must be underlined that fault assumptions are very different in wireless communication than in wired on. Even if transmission errors are more frequent than on wired links, they are bursty in nature. On the contrary, errors on wired channels are often of permanent nature due to connector or cable failures. However, as stated in RUNES report [80], "the industrial automation sector, in general, is characterized by conservatism. Companies do not want to take chances with large investments in new installations and require demonstration of practicality". For all these reasons, new tools must be developed, with particular attention to simulators that should allow to accurately predict the network behavior in a real scenario.

Available tools

In order to fully understand the complexity of designing wireless protocols that work in real life, it is necessary to model, simulate and also to implement and test on real world systems. Abreast of traditional instruments as spectrum analyzers, that are out of the scope of this digression, a plethora of simulators and "sniffers" appeared on the market in order to predict and verify the WSNs behavior.

Even if simulations at packet level are useful in verify protocols performance, designing an effective WSN involves extensive and accurate knowledge of the environment and radio behavior. In fact, assumptions made in most propagation model do not necessarily reflect the real-world conditions. Traditional mistakes can be summarized as follows:

- the world is flat,
- radio's transmission area is circular and all radios have equal range,
- if I can hear you, you can hear me,
- if I can hear you at all, I can hear you perfectly,
- signal strength is a simple function of distance.

Finite element simulation of the environment could overcome these limits but are time consuming and very difficult to implement. For all these reasons a new approach must be pursued.

In [84] it has been shown that traditional stochastic models fail in forecast parameters as packet error rate, especially when applied in industrial scenarios. In addition, classical tools do not consider node components as sensor hardware, batteries, CPU that must be correctly modeled to ensure an accurate estimation of network life. A survey on these topics is furnished by [85]. For all these reasons simulation of WSNs is still an open research field that must be flanked by experimental validations. This task can be partially accomplished by low cost instruments known as "sniffers".

These devices are realized using the same hardware of sensor nodes (i.e. they are low cost but purposely designed for a particular physical layer) and detect and capture wireless radio signal packets in the ambience presenting them in convenient graphic displays, furnishing an useful insight on what occur in air.

A case study

This section describes an application developed for plastic machinery [86]. The aim is to control the temperature along the hot barrel of extruders adopted in plastic machining. Specifications are a maximum of N=16 thermal probes (nodes) scanned with a cycle time of Tcycle=128ms [87]. The adopted transducer is a J type thermocouple; transmitted temperature is expressed with a resolution of 0.1°C over a typical range [0,400]°C. One of the advantages that justifies the adoption of a wireless link is the elimination of the expensive compensating cables used to connect the thermocouple with the electronic circuit.

A proprietary protocol stack, processed by a simple 8bit microcontroller, (HCS08GT60 from Freescale), has been developed to minimize the overhead, to reduce the datagram lengths and to achieve high efficiency decreasing computational effort. An IEEE802.15.4 compliant device has been chosen (formally MC13192 from Freescale). Concerning the MAC, TDMA has been adopted to guarantee the cycle time deadline of sensory data transmission and CSMA/CA for network management purposes. As regards the NWK topology, a star architecture has been adopted. In fact, nodes along the barrel are relatively close one from each other and no complex routing strategies are needed; therefore a small firmware footprint can be obtained. Several wireless subnets can coexist exploiting frequency diversity and each coordinator acts also as a MODBUS RTU slave. With regard to the application layer, it simply encapsulates sensor data within the protocol datagram. No particular attention has been devoted to security, since this is not a real problem in monitoring applications.

The network coordinator is mains powered and is always in the on-state. It periodically sends a BEACON packet that delimits the beginning of a new cycle. The first part of the cycle is devoted to network constitution (Join Period in Figure 12); it lasts 32ms.

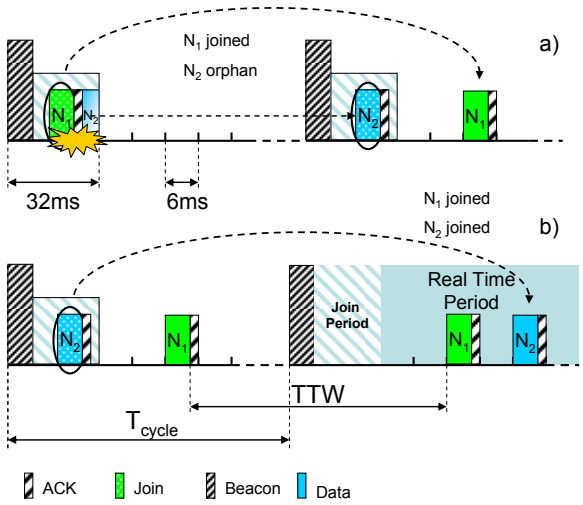

Figure 12: CSMA/CA and TDMA hybrid approach. a) N1 affiliation; b) N2 affiliation

A node that wants to join the network waits for the BEACON and sends a JOIN packet with a CSMA/CA

approach. If the coordinator accepts, it sends an ACK packet specifying the Network IDentifier (NID) and the node time slot, that corresponds to the Devide IDentifier (DID). Datagrams are shown in Figure 13.

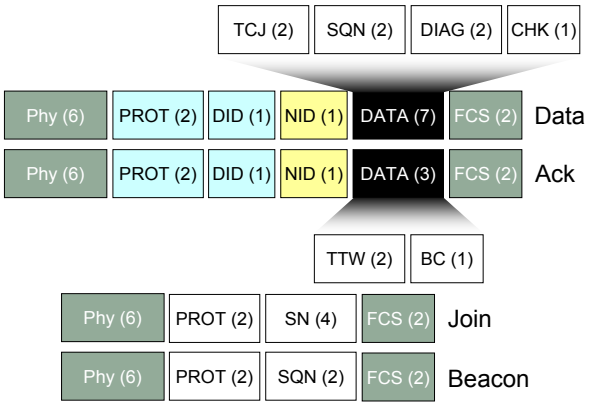

Figure 13: DATA and ACK datagrams; field lengths are in octets.

The PHY level header and the FCS: Frame Check Sequence fields are imposed by the IEEE802.15.4-PHY. The PROT field is used to distinguish the proposed protocol with respect to IEEE802.15.4 and specifies protocol version; SQN is a sequence number to allow for cycle traceability; SN is the node univocal identifier (factory set); the TTW (Time To Wake-up) indicates the amount of time that must elapse before next wake up and allows for time synchronization, as better explained in the following; BC is the Backup Channel adopted to improve reliability by means of channel diversity. The remaining part of the cycle (Real Time Period in Figure 12) is devoted to real-time data communication that occurs by means of TDMA; it lasts 96ms. Once a node is linked with the coordinator, it sleeps for most of the time in power saving mode and periodically (every Tcycle) wakes up and sends its data - DATA packet - to the coordinator that answers with the ACK packet. The application payload is made up of seven bytes; two bytes are reserved for the temperature information (TCJ), two bytes constitute a progressive sequence number (SQN), two bytes are for diagnostic and identification purposes (DIAG: node status, battery level, cold junction status…); finally, one checksum byte is computed to check data integrity (CHK) and ensure that frame belongs to this kind of network.

Obviously, in a distributed time-triggered system, a synchronized timebase is a crucial requirement to enable a reliable system behaviour. First requirement is not to overlap two successive 6 ms-wide slots. This condition may be complicated by very low performance clock that microcontrollers use in power save mode. The so called "rate synchronization" has been chosen, i.e. all nodes measure the same time interval lengths. The coordinator detects the time of arrival of each packet sent by nodes and computes the next Time To Wakeup [ms] TTW based on its internal clock. The TTW and Tcycle values should coincide, but relative drift between coordinator and node clocks makes them different. A simple P(roportional) I(ntegral) controller has been implemented to correct the "error" between them. As asserted before, nodes wait for an ACK packet; if this packet gets lost, i.e. a timeout condition is reached, a single retransmission occurs, signalled in DIAG field. No ACK is sent to stay within the time slot duration thus avoiding collisions.

Measurements on the field showed that the average current of the RF section is $I_{RF,AVG}$=0.5mA while other circuitries (micorocontroller and sensor conditioning) require $I_{OTHER,AVG}$=0.8mA. It means that if no retransmissions occur the node life is about 2 months if a power source of 2.3Ah is employed (two alkaline AA batteries).

In order to evaluate performances in a real application, some additional measurements have been conducted in a factory building. Four wireless thermocouples were installed on a plastic injection moulding machine. In particular, there was no direct line-of-sight between some thermocouple nodes and the coordinator. Traffic "on the air" was sniffed for an hour. Figure 14 reports a histogram showing the frequency distribution of lost packets. The horizontal axis represents the number of consecutive lost packets (lack of information interval), while the vertical one represents the percentage of the number of occurrences with respect to the overall cycle number NCYCLE=28125; in particular, the maximum number of consecutive lost packets is equal to 7, and occurs only one time.

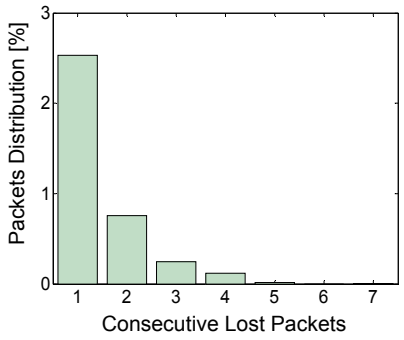

Figure 14: QoS of the wireless thermocouples network.

V. CONCLUSIONS

In this paper an overview of technologies available for sensor networking in industrial applications has been presented. The state of the art has been summerized describing opportunities and limits as applied to "real world" case studies.

Fieldbuses gained more and more success in the last few years thanks to their advantages in terms of scalability and easiness of installation and thanks to their ability to furnish tailored answers to industrial field requirements. The actual frontier is the convergence towards an unified standard solution, that seems to be the adoption of the so called Real Time Ethernet.

On the other side, advancements in communications ICs are making wireless an attractive alternative, at least in some monitoring applications. Besides lower cost, due to the absence of cabling, main advantages are flexibility and redundancy, just to cite few of them.

VI. References

1. G. Smith and M. Bowen, Consideration for the utilization of smart sensors, Sensor and Actuators A 46-47 (1995) 521-524.
2. ISO/IEC 8802-3, Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications.
3. H.S. Ng, M.L. Sim, C.M. Tan, C.C. Wong, Wireless technologies for telemedicine, BT Technology Journal (Kluwer Academic Publishers) Volume: 24, Issue: 2, April, 2006, pp. 130-137.
4. Gabriel, C.; Horia, H., Integrating sensor devices in a LIN bus network, 26th International Spring Seminar on Electronics Technology: Integrated Management of Electronic Materials Production, 2003, 8-11 May 2003 Page(s): 150 – 153.
5. S.P. Beeby, M.J. Tudor and N.M. White, Energy harvesting vibration sources for microsystems applications, Meas. Sci. Technol. 17 No 12 (December 2006) R175-R195.
6. Luk, M., Mezzour, G., Perrig, A., and Gligor, V. 2007. MiniSec: a secure sensor network communication architecture. In Proceedings of the 6th international Conference on information Processing in Sensor Networks (Cambridge, Massachusetts, USA, April 25 - 27, 2007). IPSN '07. ACM Press, New York, NY, pp. 479-488.
7. Jeffrey I., Gilmore C., Siemens G., LoVetri J., Hardware invariant protocol disruptive interference for 100BaseTX Ethernet communications, Electromagnetic Compatibility, IEEE Transactions on , Volume: 46 , Issue: 3 , Aug. 2004, Pages:412 – 422
8. Institute of Electrical and Electronics Engineers , "IEEE Standard for a Smart Transducer Interface for Sensors and Actuators – Transducer to Microprocessor Communication Protocols and Transducer Electronic Data Sheet (TEDS) Formats", IEEE Std. 1451.2 – 1997, 1997.
9. IEC 61784-2(Ed. 1.0), Industrial communication networks – Profiles – Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3, to be published at the end of 2007.
10. J.-P. Thomesse, "Fieldbus technology in industrial automation", Proceedings of the IEEE, Vol. 93, Issue 6, pp:1073 – 1101, June 2005.
11. G. Cena and L. Durante and A. Valenzano, Standard Field bus networks for industrial application, Computers Standards & Interfaces 17 (1995), Pages:155-167
12. Cavalieri, S.; di Stefano, A.; Mirabella, O., Impact of fieldbus on communication in robotic systems, Robotics and Automation, IEEE Transactions on , Volume: 13 , Issue: 1 , Feb. 1997 Pages:30 - 48
13. Cena, G.; Valenzano, A.; FastCAN: a high-performance enhanced CAN-like network, Industrial Electronics, IEEE Transactions on, Volume 47, Issue 4, Aug. 2000 Page(s):951 - 963
14. Tovar, E.; Vasques, F.; Real-time fieldbus communications using Profibus networks, Industrial Electronics, IEEE Transactions on, Volume 46, Issue 6, Dec. 1999 Page(s):1241 – 1251
15. IEC 61784-1(Ed.2.0), Industrial communication networks – Profiles – Part 1: Fieldbus profiles.
16. S.M. Savaresi, The role of real-time communication for distributed or centralized architectures in vehicle dynamics control systems, Proc. of IEEE WFCS2006, Torino, June 2006. pp 67-72.
17. Specifications available on line : http://www.ietf.org/rfc/rfc793.txt.
18. Holley, D.W., Understanding and using OPC maintenance and reliability applications, Computing & Control Engineering Journal , Volume: 15 , Issue: 1 , Feb.-March 2004, Pages:28-31
19. Garcia J., Palomo F.R., Luque A., Aracil C. et al., Reconfigurable distributed network control system for industrial plant automation, Industrial Electronics, IEEE Transactions on , Volume: 51 , Issue: 6 , Dec. 2004 , Pages:1168 – 1180
20. http://ethernet.industrial-networking.com/articles/technical.asp
21. Flammini A., Ferrari P., Sisinni E., Marioli D., Taroni A. (2002). Sensor Interfaces: from field-bus to Ethernet and Internet. Sensors and Actuators A-Physical. Vol. 101/1-2, pp. 194-202
22. M. Bertoluzzo, G. Buja, S. Vitturi, "Ethernet Networks for Factory Automation", IEEE IES Newsletter, Vol- 50, No. 4, 2003, pp. 5-10
23. P. Kermani, L. Kleinrock, A Tradeoff Study of Switching Systems in Computer Communication Networks, IEEE Trans. on Computers, Vol. C-29, n. 12, Dec 1980.
24. http://www.ethernet-powerlink.org
25. http://www.profibus.com
26. http://www.ethercat.org
27. http://www.modbus-ida.org
28. P. Ferrari, A. Flammini, D. Marioli, S. Rosa, A. Taroni, C. Cattaneo, C. Manduca, GDNET: a Specific Approach to Distributed Input/Output Synchronization for Plastic Machinery, Proc. of IEEE WFCS2006, Torino, June 2006. pp 1206-1213.
29. Loeser, J.; Haertig, H., Low-latency hard real-time communication over switched Ethernet, Real-Time Systems, 2004. ECRTS 2004. Proceedings. 16th Euromicro Conference on , 30 June-2 July 2004, pp. 13-22
30. IEEE 1588:2002, Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems
31. Eidson, J.C.; Kang Lee; Sharing a common sense of time, Instrumentation & Measurement Magazine, IEEE, Volume 6, Issue 1, March 2003 Page(s):26 - 32
32. Jasperneite J., Shehab K., Weber K., Enhancements to the time synchronization standard IEEE-1588 for a system of cascaded bridges, IEEE International Workshop on Factory Communication Systems 2004, Sept. 2004, Pages:239 – 244

33. Weibel H., Dreher A., High Precision Clock Synchronization with IEEE1588, Industrial Automation Asia, Oct/Nov 2004, Pages: 32-37
34. Loy D. Horauer M., Schmid U., Schossmaier K., Specification and Implementation of the Universal TimeCoordinated Synchronization Unit (UTCSU), Real-Time Systems, Volume: 12, Issue: 3, May, 1997, pp. 295-327
35. He J. Yang Z., Fan Z. et al., Modeling two-windows TCP behavior in differentiated services networks, Computer Communications Volume: 27, Issue: 18, December 1, 2004, pp. 1840-1850
36. Ferrari P., Flammini A., Marioli D., Taroni A., Experimental evaluation of PROFINET performance, Proc. of WFCS 04 - International Workshop on Factory Communication SystemsVienna, Austria, Sep. 22-24, 2004, pp. 331-334.
37. Robinson B., Liberatore V., On the impact of Bursty Cross-Traffic on Distributed Real-Time Process Control, Proc. of WFCS04 - International Workshop on Factory Communication SystemsVienna, Austria, Sep. 22-24, 2004, pp. 147-152.
38. J. Jasperneite, J. Feld, "PROFINET: An Integration Platform for heterogeneous Industrial Communication Systems", Proc of 10th IEEE ETFA2005, Sept. 2005, Catania, Italy.
39. Digital data communications for measurement and control - Fieldbus for use in industrial control systems - Part 5-10: Application layer service definition. To be published at the end of 2007
40. ERTEC400 Reference Manual, Siemens, http://www.automation.siemens.com.
41. http://wfcs2006.ieiit.cnr.it/
42. http://www.csem.ch/events/RTN06/RTN06.html
43. http://www.action-m.com/etfa2006/
44. Tobagi, F.A.; Dalgic, I., Performance evaluation of 10Base-T and 100Base-T Ethernets carrying multimedia traffic, Selected Areas in Communications, IEEE Journal on , Volume: 14 , Issue: 7 , Sept. 1996, Pages:1436 - 1454
45. Zhang L. Zhiyong C. , Interlayer Jitter Index for the Transmission of Layered Video Stream over the Internet, Real-Time Imaging Volume: 8, Issue: 2, April, 2002, pp. 127-136
46. L. Liang, Z. Sun, D. He, New parameters and metrics for multiparty communications, Next Generation Internet Networks, 2005, 18-20 April 2005, 396 – 403
47. S. Soucek; T. Sauter, "Quality of service concerns in IP-based control systems", IEEE Trans. on Industrial Electronics, Vol 51, Issue 6, pp. 1249-1258, Dec 2004
48. G. Marsal, B.Denis, J. M. Faure, G. Frey, "Evaluation of Response Time in Ethernet-based Automation Systems", Proc. of 11th IEEE ETFA2006, Sept. 2006, Prague CZ, CF-001848
49. OPNET Modeler, OPNET Technologies. http://www.opnet.com.
50. OMNET++ Community site, http://www.omnetpp.org
51. P. Ferrari, A. Flammini, D. Marioli, A. Taroni, F. Venturini "Experimental Analysis to Estimate Jitter in PROFINET IO Class 1 Networks", Proc. of 11th IEEE ETFA2006, Sept. 2006, Prague CZ, CF-002151.
52. http://www.wireshark.org/
53. Ansari, S.; Rajeev, S.G.; Chandrashekar, H.S., Packet sniffing: a brief introduction, Potentials, IEEE , Volume: 21 , Issue: 5 , Dec. 2002-Jan. 2003 Pages:17 - 19
54. Micheel J., Graham I., Donnelly S., Precision Timestamping of Network Packets, Proceedings of the ACM SIGCOMM Internet Measurement Workshop, San Francisco, California, USA, November 2001
55. Cleary J., Graham I., et al., High precision traffic measurement, Communications Magazine, IEEE, Volume: 40 , Issue: 3 , March 2002, Pages:167 - 173
56. Chakraborty, S.; Künzli, S.; Thiele, L.; Herkersdorf, A.; Sagmeister, P., Performance evaluation of network processor architectures: combining simulation with analytical estimation, Computer Networks, Volume: 41, Issue: 5, April 5, 2003, pp. 641-665
57. A. Depari, P. Ferrari, A. Flammini, D. Marioli. A. Taroni, "Multi-probe measurement instrument for real-time ethernet networks", Proc. of IEEE WFCS2006, pp. 313-320, June 2006.
58. K. Schossmaier, U. Schmid, M. Horauer, D. Loy, "Specification and Implementation of the Universal Time Coordinated Synchronization Unit (UTCSU)", Journal of Real-Time Systems, No. 3, Vol. 12, pp. 295, May 1997
59. Endace Ninjabox Analyser www.endace.com
60. IEEE Standard for Information technology - Telecommunications and information exchange between systems, Local and metropolitan area networks, Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications
61. IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements. Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs)
62. WiFi Alliance web site: http://www.wi-fi.org/
63. Bluetooth Special Interest Group web site: http://www.bluetooth.com

64 Akyildiz, I.F.; Su, W.; Sankarasubramaniam, Y.; Cayirci, E., Wireless sensor networks: a survey, Computer Networks, Volume: 38, Issue: 4, March 15, 2002, pp. 393-422

65 IEEE 802.15 Working Group for WPAN web site: http://www.ieee802.org/15/

66 Pottie, G.J.; Kaiser, W.J.; "Wireless Integrated Network Sensors" COMMUNICATIONS OF THE ACM, May 2000, Vol. 43, No. 5, Pp. 51-58

67 Sinha, A.; Chandrakasan, A.; Dynamic power management in wireless sensor networks, IEEE Design & Test of Computers, Volume 18, Issue 2, March-April 2001 Page(s):62 – 74

68 Alippi, C., Mottarella, A., Vanini, G.; A RF map-based localization algorithm for indoor environments, Proceedings of IEEE Symposium on International Circuits and Systems 2005 ISCAS 2005. Publication Date:

23-26 May 2005, Page(s): 652-655 Vol. 1, ISBN: 0-7803-8834-8

69 J. Hightower, R. Want, G. Borriello, SpotON: An indoor 3D location sensing technology based on RF signal strength, UW CSE 2000-02-02, University of Washington, Seattle (2000).

70 M. Rodriguez, J. P. Pece, and C. J. Escudero, In-building location using Bluetooth, in Proceedings of the International Workshop on Wireless Ad Hoc Networks, 23-26 May 2005 NY, available on line: http://www.ctr.kcl.ac.uk/IWWAN2005/papers/65.pdf.

71 E. Elnahraway, X. Li, and R. P. Martin, The limits of localization using RSS, In Proceedings of the 2nd International Conference On Embedded Networked Sensor Systems, Baltimore, MD, USA, 2004.

72 N. Patwari, A. O. Hero, Using Proximity and Quantized RSS for Sensor Localization in Wireless Networks, in Proceedings of the 2nd International ACM Workshop on Wireless Sensor Networks and Applications (WSNA), San Diego, CA, Sept. 19, 2003.

73 D. Lymberopoulos, Q. Lindsey, A. Savvides, An Empirical Analysis of Radio Signal Strength Variability in IEEE 802.15.4 Networks using Monopole Antennas, in ENALAB Technical Report 050501, 2005 – available on line: www.eng.yale.edu/enalab/publications/rssi_paper.pdf.

74 A.Flammini; D. Marioli; G. Mazzoleni; E. Sisinni; A. Taroni; Received Signal Strength Characterization for Wireless Sensor Networking, in Proceedings of the IEEE Instrumentation and Measurement Technology Conference, 2006. IMTC 2006. April 2006 Page(s):207-211

75 Whitehouse K., Karlof C., Culler D., "A Practical Evaluation of Radio Signal Strength for Ranging-based Localization". ACM SIGMOBILE Mobile Computing and Communications Review archive, SPECIAL ISSUE: Special issue on localization, Volume 11 , Issue 1 (January 2007), Pages: 41 - 52

76 K- Römer, F. Mattern, The Design Space of Wireless Sensor Networks. IEEE Wireless Communications, Vol. 11, No. 6, pp. 54-61, December 2004

77 IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements. Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs).

78 Demirkol, I.; Ersoy, C.; Alagoz, F., MAC protocols for wireless sensor networks: a survey, IEEE Communications Magazine, Volume 44, Issue 4, April 2006 Page(s): 115 - 121

79 http://www.automation.siemens.com:80/ …hmi/html_76/microsites/simatic-mobile-panel-277- …iwlan.htm

80 Sixth Framework Programme, Priority 2, "Information Society Technologies", Project Name: Reconfigurable Ubiquitous Networked Embedded Systems, Public deliverable D8.1.2 Proceedings of the RUNES Industry Forum. Available on line: http://www.ist-runes.org/public_deliverables.html

81 D. Chen and P. K. Varshney, QoS Support in Wireless Sensor Networks: A Survey, Proc. of the 2004 International Conference on Wireless Networks (ICWN 2004), Las Vegas, Nevada, USA, June 21-24, 2004

82 IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements – IEEE802.11e

83 Dzung, D.; Apneseth, C.; Endresen, J.; Frey, J.-E.; Design and implementation of a real-time wireless sensor/actuator communication system, 10th IEEE Conference on Emerging Technologies and Factory Automation, 2005. ETFA 2005. Volume 2, 19-22 Sept. 2005 Page(s):10 pp.

84. Willig, A.; Kubisch, M.; Hoene, C.; Wolisz, A.; Measurements of a wireless link in an industrial environment using an IEEE 802.11-compliant physical layer, IEEE Transactions on Industrial Electronics, Volume 49, Issue 6, Dec. 2002 Page(s):1265 – 1282.

85 Egea-Lopez, E.; Vales-Alonso, J.; Martinez-Sala, A.; Pavon-Mario, P.; Garcia-Haro, J.;, Simulation scalability issues in wireless sensor networks, IEEE Communications Magazine, Volume 44, Issue 7, July 2006 Page(s):64 – 73.

86. Accepted for oral presentation at the IEEE International Symposium on Industrial Electronics ISIE07, June 4-7, 2007 Vigo (Spain).

87. Flammini, A.; Marioli, D.; Sisinni, E.; Taroni, A.; Pezzotti, M.; A wireless thermocouples network for temperature control in plastic machinery, IEEE International Workshop on Factory Communication Systems, WFCS2006, June 27, 2006 Page(s):219 – 222.