On the Use of Wireless Networks at Low Level of Factory Automation Systems

Francesco De Pellegrini, Daniele Miorandi, Stefano Vitturi, and Andrea Zanella

***Abstract*—Wireless communication systems are rapidly becoming a viable solution for employment at the lowest level of factory automation systems, usually referred to as either "device" or "field" level, where the requested performance may be rather critical in terms of both transmission time and reliability. In this paper, we deal with the use of wireless networks at the device level. Specifically, after an analysis of the communication requirements, we introduce a general profile of a wireless fieldbus. Both the physical and data link layers are taken directly from existing wireless local area networks and wireless personal area networks standards, whereas the application layer is derived from the most popular wired fieldbuses. We discuss implementation issues related to two models of application layer protocols and present performance results obtained through numerical simulations. We also address some important aspects related to data security and power consumption.**

***Index Terms*—Factory automation systems, protocols, real-time applications, wireless local area networks (WLANs).**

I. Introduction

In the last decade, the adoption of communication networks at all levels of factory automation systems has experienced an impressive growth. In particular, at the lowest level, commonly referred to as either device or field level in the computer integrated manufacturing (CIM) model [1], fieldbuses have been extensively employed to connect controllers to sensors/actuators. Due to the typical operations performed at this level, the performance required to a fieldbus in terms of communication times may be rather critical. In particular, two major issues have to be considered: periodicity and real-time [2].

Periodicity is concerned with the ability of performing operations (for example, reading/writing of variables) at regular intervals; *real-time* refers to the maximum allowable time in which urgent communication tasks (typically the notification of alarms) have to take place.

Traditionally, fieldbuses have wired architectures, but recently, wireless communication systems have become an attractive solution also for employments at the device level. This has been allowed by the improvement of some performance figures of wireless networks such as the increased transmission speed and the improved reliability. Moreover, also the ongoing cost reduction of the radio network components represents an important incentive.

The adoption of wireless links overcomes some limits of wired fieldbuses, related to the connection of mobile equipment and the need for cabling, which in some cases may be expensive and/or difficult to deploy. However, the further benefits that may be envisaged are even more significant: for example, *ad hoc* networks may increase the flexibility in the production systems since they operate in a fully distributed way and are capable of self-(re)configuring after failure events. Indeed, sensor networks, which represent an important field of application of *ad hoc* networks are envisaged to be profitably used in industrial environments [3].

The use of wireless networks at the device level of factory automation systems is influenced by some factors that have to be carefully analyzed. First of all, both the radio transmission systems and the protocols employed have to be accurately selected in order to satisfy the specific requirements. Such a consideration is even more important since these networks are planned to be installed in hostile environments, where several types of noise may cause transmission errors. Second, also the power consumption of the radio components has to be carefully considered.

The remainder of this paper is organized as follows. Section II highlights the requirements of industrial communication systems at the device level and points out the communication profile of a possible wireless fieldbus. Section III analyzes some available wireless communication standards that could be employed at the device level. Section IV presents some considerations on the possible employment of *ad hoc* networks for industrial applications. Section V analyzes the security aspects of the transmitted data. Section VI deals with power consumption issues. Section VII gives an overview of the scientific work related to the use of wireless networks in factory automation systems. Section VIII describes how a wireless fieldbus could be implemented. Details on the protocols used are given, together with some performance figures obtained through numerical simulations. Section IX contains final remarks.

II. Background: Communications at the Device Level

The communications that take place at the device level involve controller devices, typically personal computers (PCs) or programmable logic controllers (PLCs), and sensors/actuators. In most cases, the amount of data exchanged is limited, but the timing constraints may be very tight, so that the required transmission speeds are of the order of some Mbit/s.

Manuscript received May 20, 2005; revised January 16, 2006.

F. De Pellegrini and D. Miorandi are with the CREATE-NET, 38100 Trento, Italy (e-mail: francesco.depellegrini@create-net.org; daniele.miorandi@create-net.org).

S. Vitturi is with the Italian National Council of Research, IEIIT-CNR, 35131 Padova, Italy, and is also with the Department of Information Engineering, University of Padova, 35131 Padova, Italy (e-mail: vitturi@dei.unipd.it).

A. Zanella is with the Department of Information Engineering, University of Padova, 35131 Padova, Italy (e-mail: andrea.zanella@dei.unipd.it).

Digital Object Identifier 10.1109/TII.2006.872960

Depending on the chosen network, different physical configurations may be used. Anyway, in many applications, the covered distances are limited to few tens of meters.

Since a network (either wired or wireless) employed at the device level replaces the point-to-point connections between controller and sensors/actuators, the most important requirement it has to satisfy is, in general, the dependability. More in detail, the network has to ensure that the quality of the communication has to be comparable with that of the replaced point-to-point connections.

As stated in [2], most of the traffic is represented by "identified data" (e.g., process variables, set points, and so on) that have to be transmitted periodically with (possibly) different periods. Typical values for the periodicity may range from hundreds of microseconds to hundreds of milliseconds. The transmitted values may be used, for example, by the algorithms of control loops that are implemented via the network. Since in several applications the periodicity of the data corresponds to the sampling time of the control loops, it is required that the update period of the variables is not influenced by jitter. In general, however, the maximum allowable jitter depends on the application.

Also the presence of aperiodic traffic has to be considered at the device level, since it is usually generated by the occurrence of unpredictable events such as those associated to alarm situations. In these cases, it is necessary that the notification of the events arrives within a specified deadline to the controller, which has to undertake appropriate response actions.

A. *Wireless Fieldbus*

With the term *wireless fieldbus*, in this paper, we mean a wireless communication network suitable to be used at the device level of factory automation systems.

Regarding the radio transmission system (physical layer), it is expected that some of the currently available standards for both wireless local area networks (WLANs) and wireless personal area networks (WPANs) can be employed for the wireless fieldbus, since both their transmission rates and covered distances are compatible with the considered application requirements.

As concerns higher layer protocols, some solutions considered in the past years for the data link layer of wired fieldbuses were derived from already existing standards. It is the case of both Profibus [4], whose data link layer is a modified version of the well-known IEEE 802.4 token bus standard [5], and Controller Area Network (CAN) [6], which was originally developed for automotive applications. Conversely, the data link layer of some other networks, such as, for example, WorldFIP [7], ControlNet [8], and the IEC fieldbus [9], were designed from scratch.

A similar situation is encountered at the application layer. Some of the currently available protocols are based on the manufacturing message specification (MMS) [10], which has been, for a long time, the only standardized application layer protocol for industrial communications. Examples are WorldFIP, the first version of Profibus, whose application layer protocol is named Fieldbus Message Specification (FMS), and the CAN application layer (CAL), which is part of the CANopen specification [11]. Some other protocols, instead, have been explicitly developed. We can mention Interbus [12], the IEC fieldbus, and DeviceNet [13].

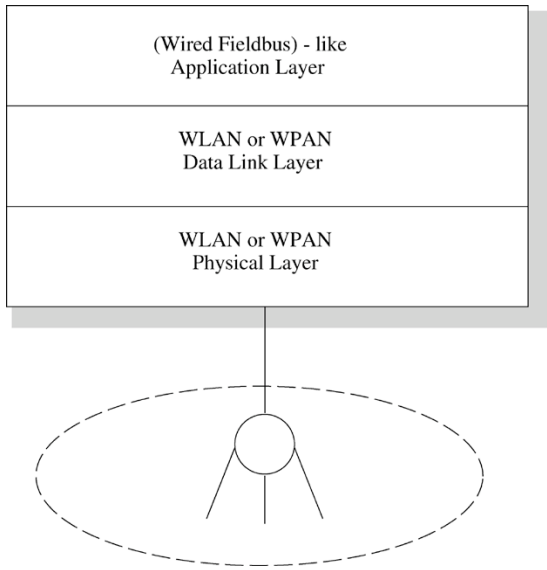

Fig. 1. Communication profile of the wireless fieldbus.

The issues related to protocol selection arise again in the design of wireless fieldbuses.

At the data link layer, the most convenient solution seems to be the use of the already available protocols for both WLANs and WPANs, provided that they are able to cope with the device level communication requirements.

At the application layer, the reuse of protocols already defined for the wired fieldbuses is highly desirable. This choice is indeed reasonable, since these protocols have demonstrated their effectiveness in the wired applications. Moreover, the implementation efforts would be limited to the interface with the data link layer.

Summarizing, the communication profile we propose for a wireless fieldbus is shown in Fig. 1. It comprises both the physical and data link layers taken directly from already available WLANs or WPANs, whereas the application layer may be obtained from those of wired fieldbuses adequately modified to adapt to the new data link layer.

The described profile does not agree completely with [14] and [15], where the use of the IEEE 802.11 MAC (one of those we will consider in the following) is not recommended, due to the potentially long access delay that may be observed in case of heavy contention. Nevertheless, both the above papers refer to the implementation of a complete industrial wireless network. However, the actual network configurations at the device level are based, in most cases, on an active device (the controller) that handles a set of passive devices (the sensors/actuators). As a consequence, since the access to the network is regulated by the controller, most of the conflicts may be avoided. Moreover, the MAC protocols proposed in [14] and [15] imply the modification and/or replacement of the original IEEE 802.11 MAC. Such a solution is difficult to implement since it requires to act directly on the firmware of the chipsets used for radio transmission.

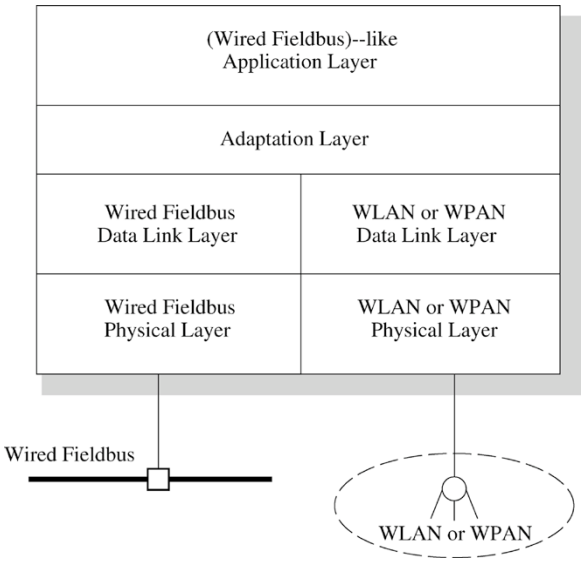

Fig. 2. Communication profile of a bridging station.

Conversely, the implementation of the wireless fieldbus communication profile shown in Fig. 1 only requires the adaptation of the application layer of a fieldbus to the data link layer of the radio system. As we will show in the rest of this paper, such an approach requires only software modifications.

B. Hybrid Networks

In several applications, we might not be interested in a wireless fieldbus but rather in a wireless extension of a wired fieldbus: the resulting configuration is a hybrid network.

The employment of hybrid networks has been extensively discussed in [16], where the use of coupling devices to connect different network segments is analyzed. Three types of coupling devices may be identified, on the basis of the protocol layer at which they operate. *Repeaters* work at the physical layer, *bridges* are employed at the data link layer, and *gateways* operate at the application layer. The architecture of the wireless fieldbus we propose is particularly suitable to implement extensions of wired networks. In this case, the unique active device acts as a bridge and is equipped with both wired and wireless interfaces. The communication profile of the bridging (active) station is shown in Fig. 2. As can be seen, an adaptation layer has to be introduced between the data link and the application layers. The adaptation layer has the task of mapping the requests coming from the application to the corresponding data link layer and vice versa. Such an architecture is particularly advantageous since a unique application layer protocol is used in both the wired and wireless domains. Thus, the user applications need not be aware of the type of network to which they are connected.

As stated in [16], coupling devices introduce additional transmission delays that have to be taken into consideration, especially when working at the device level. In particular, for the configuration we consider, two different delays have to be mentioned:

1) the forwarding delay, introduced by the bridging station on the frames coming from one segment that have to be forwarded to the other;
2) the queueing delay, which may occur when the segments use different transmission speeds and/or different data formats.

Although these delays may be predicted with sufficient precision, they have to be carefully taken into account, since they may lead to undesired effects. For example, if we consider two network segments working at different transmission speeds, then simultaneous operations induced by a trigger message issued by the active station may not occur: in fact, trivially, the message is received at different instants on the two segments.

Finally, it is worth mentioning that, since Ethernet [17] networks are beginning to be employed at the device level, it is likely that, in the near future, many hybrid networks will use Ethernet in the wired domain.

III. Wireless Communication Standards

In this section, we give a short description of some wireless communication systems, either already available or under standardization, that could be profitably employed to realize a wireless fieldbus.

A) Bluetooth Radio System: Bluetooth [18], [19] is a radio interface initially designed as cable replacement in the interconnection of portable, battery-driven electronic devices. The extreme versatility, low-cost, and low-power characteristics of this technology, however, have rapidly enlarged the range of possible applications to more challenging scenarios. Recently, Bluetooth has also been adopted in some industrial processes. For instance, Bluetooth is being deployed by the major delivery companies, to send package-tracking data to small receiving terminals located in sorting centers and hubs. Also, Bluetooth is used to communicate with sensor devices that monitor, for instance, critical water pumping stations, or it is being installed in commercial vehicles for driver communications, hands-free calling, and data capture [20]. Furthermore, Bluetooth devices purposely designed for deployment in industrial environments are being commercialized [21].

The Bluetooth system operates in the license-free industrial-scientific-medical (ISM) frequency band, available in most countries of the world from 2400 to 2483.5 MHz. In order to limit the interference from and toward other devices operating in the ISM band, Bluetooth makes use of a frequency-hopping spread spectrum (FHSS) modulation scheme: the 80-MHz frequency spectrum is divided into 79 channels, 1-MHz wide each, that are visited in a pseudo-random fashion, on the basis of a specific frequency-hopping sequence. The nominal hop rate is 1600 hops/s, corresponding to a slot duration of $T_{slot} = 625\ \mu$s. The communication services toward the upper layers are provided by the logical link control and adaptation protocol (L2CAP).

The minimal Bluetooth configuration is called *piconet*. Connections in each piconet are based on a star-shaped logical topology, where the central unit acts as master, while the other units play the role of slaves. The number of slave units that can actively participate to the piconet operations is limited to seven. Channel access is ruled by a basic polling mechanism that

allows slaves to transmit only upon receiving a data packet (or an explicit POLL packet) by the master. Therefore, full-duplex communication is obtained on a time-division-duplex (TDD) fashion.

Both synchronous connection-oriented (SCO) link and asynchronous connectionless (ACL) links are defined by the standard.

SCO links support symmetrical, circuit-switched, point-to-point connections typically used for voice. These links are defined on the channel by reserving two consecutive slots (forward and return slots) with a fixed period. Reservation is carried out by the master and slave when the link is set up.

ACL links support symmetrical or asymmetrical, packet-switched, point-to-multipoint connections, typically used for bursty data transmission. ACL links can use 1, 3, and 5 slots per data packet in order to increase the system capacity. The payload field of ACL packet types can be optionally protected by a 2/3 forward error control (FEC) code. Moreover, a mandatory automatic retransmission query (ARQ) mechanism at the baseband layer provides high reliability on ACL links by retransmitting each packet until a positive acknowledgment (ACK) is returned by the destination (or maximum number of retransmission attempts is reached).

A. IEEE 802.11

Regarding the MAC layer, the IEEE 802.11 standards represent the wireless counterparts of wired Ethernet networks and are today the *de-facto* standards for WLANs. Standards of the IEEE 802.11 family provide physical layer and the MAC layer recommendations, relying on existing standards for upper layer services. In particular, there exist several specifications for IEEE 802.11 operations, namely, 802.11a/b/g and e, with key differences at the physical layer. The access to wireless channels is ruled according to the same MAC layer, as described in [22] and [23]. The bandwidth occupied by IEEE 802.11 is free, settled around the (overcrowded) 2.4-GHz ISM band for devices following the 802.11b and g specifications and around the 5-GHz ISM band in the 802.11a specifications. The 802.11g and 802.11a are more recent standards adopting orthogonal frequency division multiplexing (OFDM) modulation and delivering up to 54 Mbit/s. The 802.11g standard is backward compatible with existing 11 Mbit/s 802.11b devices, which represent, presently, the most common wireless devices on the market.[1] Devices compatible with 802.11a/b/g standards present an adaptive modulation and coding (AMC) scheme, which updates dynamically the modulation format and coding rate to track time-varying channels. The AMC mechanism is not specified in the standard, and its implementation is left to manufacturers.

The MAC standardized in [23] defines two major communication modes, the point coordination function (PCF), which is a poll-based mechanism based on a base station, usually the access point of a WLAN, and the distributed coordination function (DCF), which is a pure *ad hoc* mode. In particular, the DCF communication mode is mandatory in any implementation compliant with [22] and [23]. The PCF mode is not mandatory, even though it lately received some attention for real-time multimedia applications, which are out of the scope of this paper. Thus, due to the ease of deployment of 802.11 in *ad hoc* mode, the DCF is the only communication mode currently implemented by IEEE 802.11 devices. Under the DCF mode, the medium access control (MAC) is based on the carrier sense multiple access (CSMA) mechanism, which requires nodes to sense the channel idle for a specific time interval before attempting any packet transmission. As a main difference with wired Ethernet, CSMA over a wireless channel is inherently half-duplex, meaning that a station can either transmit or receive, so that it cannot detect collisions occurring to transmitted packets. To this aim, the standard provides a collision avoidance (CA) mechanism: in case the channel is sensed busy, nodes defer their transmission attempts to a later time, on the basis of a backoff mechanism, as detailed in the standard. This transmission modality is referred to as *basic access*.

Even adopting the CA technique, collisions can still occur, since hidden nodes [24] may be present due to the finite covering radius of stations. This problem is mitigated through a reservation mode, based on the exchange of RTS and CTS packets. Finally, packet transmissions have to be acknowledged by the receiver to the transmitter. Notice that, for broadcast or multicast transmissions, a specific flag is used, meaning that an acknowledgment is not needed in return. Furthermore, during multicast/broadcast transmissions, the RTS/CTS exchange is not performed.

A particularly interesting standardization activity is that undertaken by the IEEE 802.11n task group. The enhancements proposed therein are based on the use of the multiple input, multiple output (MIMO) technique and orthogonal frequency division multiplexing (OFDM) to boost data throughput rates using two and four antennas arrays. This, coupled with the use of advanced coding schemes (e.g., low-density parity check codes) and of wider channels (up to 40 MHz), is expected to bring data rates well over 500 Mb/s.

B. IEEE 802.15

The standardization activity of the IEEE 802.15 working group is of particular interest for industrial applications. Originally started to include into the IEEE 802.x family the Bluetooth standard (issue now pursued by the 802.15.1 task group), it has seen two emerging directions for future evolution of the standard. On one hand, high rate WPANs (HR-WPANs) have been considered by the 802.15.3 task group for personal applications that need high rate and quality-of-service (QoS) constraints in order to accommodate multimedia applications. On the other hand, the 802.15.4 task group focused on low rate WPANs (LR-WPANs), which demands ultra-low power consumption and capacity of *ad hoc* communications.

HR-WPAN's (802.15.3): The high rate WPAN standard IEEE 802.15.3 [25] aims at providing wireless *ad hoc* connectivity among devices located in a limited coverage area (less than 10 m). The architecture is centralized (as in Bluetooth), and a device, called the piconet coordinator (PNC), controls access to the channel. A piconet can accommodate up to 256 nodes. The PNC periodically sends a beacon frame, which is used to set the timing allocation and to send management information. The

[1]Recently, 802.11g devices are replacing the 802.11b ones.

beacon acts as start delimiter of the superframe, which is composed of a part in which slaves can access the channel in a distributed way, employing a CSMA/CA protocol, and a channel time allocation period, during which access is granted on a time division multiple access (TDMA) basis (in order to provide hard QoS guarantees). Three types of services are provided: asynchronous connectionless (which makes use of the contention access period), and asynchronous and isochronous connection oriented, which exploit the channel time allocated period.[2] The devices operate in the unlicensed ISM band and are capable of transmitting at rates of 11/22/33/44/55 Mb/s, by using QPSK-TCM, DQPSK, and 16/32/64-QAM-TCM modulation schemes, respectively. Differently from what happens in a Bluetooth piconet, in a 802.15.3 piconet, traffic can flow directly from device to device in a peer-to-peer fashion, without the need of passing through the PNC. A dynamic channel selection scheme is encompassed to allow for the overlap in time and space of different piconets; the possibility of intrapiconet communications (by means of so-called "child" and/or "neighbor" piconets) is considered. Reservations for the allocated slots can be made in some particular slots, called open management channel time allocation (MCTA), during which access is obtained by means of a simple ALOHA mechanism. Security issues are addressed in the protocol, where the use of strong cryptography (by means of a 128-bit suite) is described.

LR-WPAN's (802.15.4): An 802.15.4 LR-WPAN [26] is a simple communication network that allows wireless connectivity in applications with limited power and cost constraints and relaxed performance requirements. The main objectives of an LR-WPAN is to provide short-range wireless connections at an extremely low cost and a reasonable battery lifetime while maintaining a simple and easy-to-implement protocol. Data rates of 250, 40, and 20 kb/s are provided. The highest rate is obtained by means of an O-QPSK modulation scheme that works in the 2.4-GHz centered ISM band, whereas the lower rates are achieved employing BPSK and operating in the (unlicensed) 868/915-MHz band. Two different network architectures are encompassed by the standard, depending on the applications requirements: the star topology (similar to the Bluetooth piconet) or the peer-to-peer topology. In any case, a coordinating station is demanded to initiate, coordinate, and route communications on the network. Devices with partial capabilities, which cannot act as coordinators, are envisaged.

The LR-WPAN standard allows the optional use of a superframe structure, based on the use of beacon frames. The format of the superframe is defined by the coordinator and has the same structure of the 802.15.3 superframe. However, most applications are expected to work in the contention access modality only, where access to the shared medium is controlled by means of a distributed CSMA/CA scheme. Devices can periodically enter a sleep mode, in order to reduce the duty cycle and achieve battery savings. This mechanism defines a tradeoff between battery consumption and message latency. For battery-critical applications, very low duty cycles are expected to be employed.

[2]It is worth remarking that 802.15.3 appears of strong interest for industrial, as well as other time-critical applications, thanks to its ability to provide contention-free access to the channel. However, the technology is not mature yet, and therefore, implementation issues will not be considered in the following.

Most IEEE 802.15.4-compliant devices currently on the market are delivered under the ZigBee [27] label. Such devices are based on the IEEE 802.15.4 PHY and MAC protocol. Furthermore, they adopt proprietary network and application layers. The goal of the ZigBee alliance is to provide a standardized platform for application developers, able to offer more complex services than those encompassed by the 802.15.4 interface. The ZigBee network layer protocol provides network establishment, membership management, devices configuration, addressing, packet routing, and network-level security. The application layer makes use of a predefined set of application programming interfaces (APIs), in order to supply the users with the appropriate services. APIs are mapped onto the lower layer via an application support layer that also provides device discovery and binding functions.

UWB-Based Extensions: Physical-layer extensions based on ultrawideband (UWB) communications are envisaged for both IEEE 802.15.3/4. The IEEE 802.15.3a working task is working on a UWB-based PHY that should be able to provide data rates up to 1 Gb/s with a communication range of the order of 10 m. Two proposals (one based on DS-UWB and one based on MB-OFDM) are currently under evaluation; given the difficulty to converge to a compromise, industry alliances were formed to propose proprietary solutions based on the two options. At the same time, the IEEE 802.15.4a task group is proposing a UWB-based PHY (based on impulse radio-like techniques) able to provide data rates up to 10 Mb/s while attaining a communication range of the order of 100 m. The standard is likely going to be approved in early 2006.

IV. *Ad Hoc* Networks and Industrial Communications: A Perspective

Ad hoc networks rely on a fully-distributed architecture, providing a natural framework for distributed operations. Such architectures show some particularly desirable features, as follows.

- *Self-configuration*: *ad hoc* networks are able to self-configure, leading to a connected and stable topology. As a consequence, *ad hoc* networks are also able to self-recover from a stale situation, due to some devices breaking down or running out of battery (in some sense, they are inherently fault-tolerant self-healing systems). This feature enables also applications to mobile environments, where, for example, sensors can be embedded into moving robots. It is clear that the ability of self-(re)configuring represents an extremely interesting issue, providing these networks with a very high degree of flexibility.
- *Distributed operations*: in *ad hoc* networks, there is no central controller, so that all operations (access control to the radio medium, routing, etc.) are operated in a distributed fashion. Thus, applications may take advantage of this natural feature by working in a distributed fashion. However, distributed operations require coordination and cooperation between the various network entities, which have to perform local actions in order to achieve a global goal.

Probably the most interesting applications of *ad hoc* concepts to industrial communication systems are into the area of *sensor*

networks [3]. These networks are expected to be constituted by a massively large number of devices, equipped with a radio transceiver and a sensor (pressure, temperature, acceleration, humidity, mechanical stress level, lightning conditions, etc.). Such devices are expected to be extremely small, capable of low-power operations, and very cheap, so that a massive number of them can be used to perform distributed sensing. Nodes organize themselves into an *ad hoc* network, so that all the data sensed can be delivered to a special unit, called sink, that estimates the system state and performs the necessary operations. However, it has to be pointed out that sensor networks, due to their typical way of operation, are not a viable solution for applications with strict real-time requirements.

This form of sensor networks, which relies upon distributed sensing and central control, will probably evolve toward the so-called sensor-actor networks, where also the control is performed in a distributed fashion by active devices [28]. The main difference between purely sensor networks and sensor-actor networks is expected to be the capability of handling real-time critical operations, which could clearly enlarge the application scope of such networks.

In conclusion, even if for the time being networks based upon the *ad hoc* paradigm does not represent a viable choice for wireless industrial communication systems, it is undeniable that they represent a really promising research direction for the field.

V. Security of the Transmitted Data

An unavoidable remark on the use of wireless communication systems at the device level is owed, indeed, to security aspects, due to the simple fact that in the wireless domain, signals are not shielded by wired waveguides, as in the case of, for example, coaxial cables or optical fibers.

Many previous works described the problems of security in WLANs (see, for example, [29]–[31], and references therein).

As concerns industrial plants, we envisage two major security problems. First, there exists a *signal integrity* issue, meaning that strong interference, caused possibly by malicious users with a near RF device, may simply disconnect the entire network. Preserving the network connectivity, indeed, may be crucial for some industrial plants, where signal integrity and safety may coincide. This kind of security threat is even worse for Bluetooth and IEEE 802.11 systems, where interference can be obviously produced by other devices operating in the ISM band. The spread spectrum techniques implemented by the two standards, however, are usually able to alleviate the interference problem in most cases. Furthermore, the research community (e.g., IEEE 802.15 task group 2) is investigating sophisticated techniques to improve the channel agility of the radio interfaces, in order to dynamically avoid interference in the ISM band [32], [33].

The second aspect of security is related to the *authentication* problem: since the RF signals are usually hard to confine, unauthorized users should be prevented from accessing the WLAN and exploiting the connected resources. The IEEE 802.11 standard provides a native mechanism to enforce WLAN authentication, namely, the wired equivalent privacy (WEP), implemented at the MAC layer. From previous research work [29], the security level provided by WEP protocol has proven to be insufficient to some extent. Hence, a full suite to enhance authentication is being developed by the 802.11i committee and should shortly specify more effective methods to safeguard WLAN's security.

The current Bluetooth specification defines security at the link level only, leaving to the application developers the burden of selecting the most appropriate security mechanisms for their particular application [34]. In general, the security level provided by the Bluetooth standard shows some weaknesses that do not make it suitable for applications that transfer sensitive information. However, the Bluetooth's security seemed to be adequate for small *ad hoc* networks, as are expected to be deployed in the automated factory scenario envisioned here.

VI. Power Consumption Aspects

When dealing with radio interfaces, it is not possible to leave the energetic aspects out of consideration. The power drawn by wireless interfaces has a strong impact in the overall energy budget of battery-powered devices, as stated by some recent studies [35]–[37]. Improvements on the current batteries technology do not appear capable of solving the problem in the short period, although much research is currently ongoing on the subject [38]. As a consequence, the development of wireless interfaces faces a fast increase of the data rates, not followed by analogous improvements in the energy consumption, thus exacerbating consumption issues. This explains the ever-growing attention dedicated to power-saving strategies, which are investigated at several different levels of a radio system [39], [40]. A first classification of such strategies can be based on the time scale over which they operate. Thus, we can distinguish between short-time solutions, which pursue energy-saving by optimizing the physical interfaces and the MAC mechanisms, and long-time strategies, which involve the definition of low-power modes and energy-aware scheduling/routing algorithms. Usually, short-time techniques provide lower benefit in terms of energy, but they do not affect the throughput and delay on the radio link. On the other hand, long-time solutions can drastically reduce the energy consumption of the device to the expense of throughput and delay.

A. Energy Efficiency of the IEEE 802.11 Interface

Power consumption is a central issue for IEEE 802.11 devices, where all operations for packet transmission and reception, including carrier sensing and backoff delaying, imply not negligible energy costs. It is known from the literature [36], [37] that the energy cost to receive is close to the cost of transmission. Furthermore, the carrier sensing procedure implemented by IEEE 802.11 stations is inherently an energy-demanding process [36], [37], [41]. Also, a relevant amount of energy is spent during backoff period for discarding alien (non-destination) packets and for channel sensing as well. Long-time energy saving is pursued by the definition of a low-power *doze* mode, which can be entered by nodes in order to save energy. Nodes in doze mode suspend all their radio activities for most of the time, waking up on a periodic time interval, called *beacon interval*, to exchange information on possible pending traffic. The beacon interval is usually set to 100 ms but can be modified by a system call. For light loaded systems, the adoption of this low-power mode usually leads

to a drastic reduction of the energy consumption, but this is obtained to the detriment of the node response time. Node response time, in fact, turns out to increase, on average, by at least half of the wake-up period, with the consequent decay of both the performance indexes, which will be analyzed in Section VIII.

A statistical description of the energy spent by a IEEE 802.11 terminal and possible strategies for power saving can be found in [39], [42], [43], and references therein. Despite the high energy cost, IEEE 802.11 radio interface is becoming very popular and likely to last for a long time in commercial devices. With reference to factory automation systems, however, the low energy efficiency of current IEEE 802.11 technology makes its use recommendable only for applications relying on the power supply line while requiring a certain degree of mobility (moving platforms, robots).

B. Energy Efficiency of Bluetooth

Due to the system design, a Bluetooth device can hardly compete in terms of transmission speed with other existing radio technologies, like IEEE 802.11b. However, it is definitely competitive in terms of cost and energy consumption. The Bluetooth protocol, in fact, was designed to replace cables on the interconnection of battery-driven electronic devices, where energy saving is a key issue.

In order to meet this goal, the Bluetooth standard provides both short- and long-time mechanisms. For instance, at the baseband layer, receiving units stop reception and switch to a low-power mode as soon as they determine that the incoming packet is addressed to another unit or the signal strength is too low to guarantee a good reception (see [18, p. 124]). Hence, a Bluetooth unit not addressed by any valid packet stands active for no longer than 10% of the time while remaining in a low-power mode for the remaining 90% of the time [44].

Furthermore, Bluetooth provides three different low-power modes: *hold*, *sniff*, and *park*. The hold mode allows slave units to suspend their activity in a piconet (possibly entering a low-power mode) for a given period of time, previously agreed with the master. The sniff mode is a persistent version of the hold mode: slaves in sniff mode can be polled only during short time windows that are set up on a periodic base. Both the dimension and the period of the polling window are negotiated by exchange of sniff primitives between master and slave. The park mode, finally, resembles the low-power doze mode previously introduced for IEEE 802.11. Units give up their active member address and get a (longer) park-mode address. Parked units spend most of the time in doze mode and wake up periodically for keeping the synchronization with the piconet and checking for possible wake-up messages from the master. The three low-power modes tradeoff energy saving for response latency, thus permitting higher flexibility in the management of Bluetooth units.

VII. Related Work

Several significant contributions regarding the use of wireless networks for industrial applications have appeared in the literature during the last years. A complete and up-to-date overview of the current state of the art is given in [16], where the authors discuss some of the most critical aspects concerning the adoption of wireless technologies for industrial networks. In particular, they analyze the problem of achieving reliable transmission, using standard wireless systems, in presence of significant channel errors, typical of industrial environments. Moreover, considerable emphasis is devoted to the implementation and engineering of hybrid systems.

In [45], the R-FIELDBUS project [15], supported by the European Commission in the 5th FP, is described. The project is aimed at the implementation of a wireless fieldbus based on the architecture of Profibus DP. Besides device level communications, the R-FIELDBUS has been designed to offer also multimedia transmission, achieved trough the TCP/IP stack. Obviously, these two types of traffic have to be correctly handled in order to always ensure the highest priority to the real-time data. For such a reason, some specific communication modules need to be inserted between the two application layers (which generate the real-time and multimedia data, respectively) and the data link layer. An important result of the R-FIELDBUS project is the accurate investigation carried out on the available radio technologies. As a result, the IEEE 802.11b physical layer, using direct sequence spread spectrum (DSSS) modulation, was selected as the most suitable for industrial applications. Moreover, the adoption of the IEEE 802.11 MAC layer was not recommended because of the randomness possibly introduced in the packet delay. For such a reason, the R-FIELDBUS makes use of the Profibus data link layer.

In [46], a set of measurements on IEEE 802.11 wireless links in an industrial environment are described. The measurements, which have been performed using commercially available components, are concentrated on the physical layer in order to obtain a better knowledge of the bit-error patterns peculiar of these environments. The experience allowed to conclude that the behavior of the wireless links is characterized by the presence of both bit errors and packet losses, which are definitely time varying. As a consequence, the authors suggest an adaptive modification of the MAC protocol, in order to account for the time-varying channel conditions. The paper considers also some popular error models used to simulate the network performances, namely, the *independent model* and the *Gilbert/Elliot model*, as well as a *semi-Markov model*, comparing them with the actual error behavior of a factory environment. The analysis revealed that, although not completely in agreement with the measurements, the Gilbert/Elliot model may be considered a useful and realistic tool for simulating errors on a wireless link.

The paper [14] deals with a wireless implementation of Profibus. The author focuses the attention on the data link layer and proposes a set of polling-oriented MAC protocols for the wireless domain of an integrated (wired/wireless) Profibus network, in which the wireless segment is implemented via the IEEE 802.11 physical layer. In practice, a special station, named *base station/internetworking unit*, has to provide a virtual ring extension to the wired stations in such a way that they can "see" the wireless stations as if they were actually connected to the wired segment. The paper reports some numerical simulations aiming at evaluating the confirmation delays of high-priority messages (i.e., latency of alarms). The results obtained demonstrate that the proposed polling-based protocols

perform generally better than the original Profibus data link layer protocol, since the logical ring maintenance functions of this latter are heavily influenced by the occurrence of both packet losses and bit errors. It may be worth mentioning that the results in [14] could suggest reconsidering the choice made by the R-FIELDBUS that adopts the original Profibus data link layer protocol.

An interesting practical application is reported in [47]. Here the authors describe the realization of a protocol converter between Profibus FMS and IEEE 802.11, necessary to exchange data with some mobile unmanned container transporters in an automated container terminal. The converter is implemented through a PC equipped with the suitable interface boards for both types of networks. In order to avoid undesired delays caused by the random access on the wireless domain, a virtual polling algorithm has been developed. In practice, an ordered access to the wireless stations is implemented, and the station where the protocol converter is resident acts as a virtual master and polls repeatedly the wireless stations. The (fixed) duration of the polling cycle is determined by a parameter, manually set at the beginning of the operations, named virtual polling period. Another parameter that influences the system performance is the size of the buffers used to store the data to be transferred between the two networks in the protocol converter. The practical experience has demonstrated that both soft real-time and non real-time data may be effectively transmitted on the hybrid network.

The integration of wireless stations into the WorldFIP fieldbus is described in [48], where, again, an ordered access on the wireless side has been implemented by means of a TDMA technique.

Also a wireless extension of the MMS protocol has been considered (see [49] for details).

In [50], a proposal of a hybrid wired/wireless implementation of Profibus is presented. The authors preliminarily take into consideration the possibility of using repeaters to interconnect wired and wireless stations. However, such a solution is discarded since the necessary logical ring maintenance operations could lead to unsustainable delays. Then a network architecture, based on several segments with independent tokens, is considered. In such a case, special "Brouter Link Stations" are used to connect different segments (either wired or wireless). The authors analyze the behavior of the proposed network and evaluate the worst-case response times for high-priority messages (which are typically used to transfer data relevant to alarm situations).

Two of the authors of this paper have considered the use of Bluetooth to realize a wireless extension of Profibus DP [51] for configurations in which a limited set of devices is concentrated in a restricted area, since such a situation is typically encountered in industrial plants.

Further, a hybrid (wired/wireless) implementation of Profibus DP based on Ethernet and Bluetooth has also been proposed [52].

Finally, although not strictly related to the scope of this paper, the work reported in [53] describes an interesting technique of wireless network design for an IC factory based on a hierarchical genetic algorithm (HGA). Besides the description of the algorithm, the authors make some remarkable considerations about the use of WLANs in the automation systems of industrial plants.

VIII. Use of Wireless Networks at the Device Level of Factory Automation Systems

In this section, we give some examples of implementation of the wireless fieldbus using two widespread radio networks. In particular, we concentrate on IEEE 802.11 and Bluetooth.

While the results presented in this section do not cover the whole operating range of industrial applications, we believe that they represent a first, essential, step to verify the feasibility of a wireless fieldbus based on off-the-shelf available technologies and solutions.

We consider two models of application layer protocols, which are typical of the most popular fieldbuses.

The first one, referred to as *polling-oriented*, is based on the cyclic exchange of messages between a master device and several slaves. The most important fieldbus that exploits a protocol of this type is Profibus DP. A similar approach is adopted by Interbus.

The second application layer protocol, in the following referred to as *variable-oriented*, is based on the exchange of a set of identified variables with (possibly) different periodicity. Examples of fieldbuses using such a type of application layer are WorldFIP, the IEC fieldbus, and ControlNet.

For both the types of wireless networks considered, we will give details on how the above application layer protocols may be implemented. Indeed, we will concentrate on the techniques used for handling both cyclic and acyclic data that account for the periodicity and real-time properties, respectively. Moreover, the results of numerical simulations concerning some important performance indexes will be shown.

A. Application Layer Protocols Design Over IEEE 802.11

The IEEE 802.11, in agreement with the LAN's standardization, recommends the use of logical link control (LLC) [54] as interface toward the upper layers. Thus, both the application layer protocols we propose may be implemented making use of the LLC communication services.[3] They are of three types: connectionless acknowledged services, connection-oriented unacknowledged services, and connectionless unacknowledged services. All of them are supplied through service access points (SAPs).

Polling-Oriented Protocols Over IEEE 802.11: With these protocols, the cyclic data are exchanged by means of periodic queries issued by the master to the slaves. Each master request contains the output data for a specific slave that, in the response frame, encloses the input data. In such a way, the only possible periodicity value is determined by the frequency by which the slaves are polled.

In order to implement the aforementioned function, we propose the use of the acknowledged connectionless services of LLC, as shown in Fig. 3. We assume that the protocol makes

[3]The use of LLC reveals particularly advantageous in case of a hybrid network employing Ethernet for the wired domain. In such case indeed, the adaptation layer is no longer necessary, since both networks use the same LLC sub-layer.

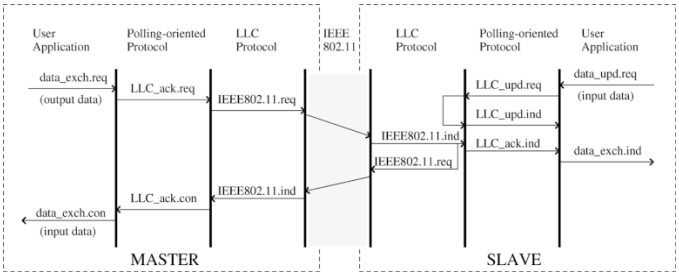

Fig. 3. IEEE 802.11 polling-oriented protocols: periodic exchange of data.

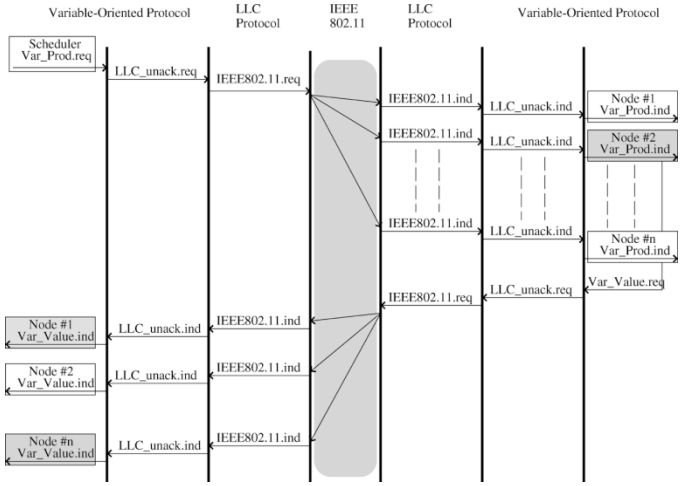

Fig. 4. IEEE 802.11 variable-oriented protocols: example of data exchange.

available the service *Data_Exch*. The exchange starts with a request issued by the master (primitive *Data_Exch.req*). As a consequence, a request of an LLC acknowledged service is sent, and the output data are encapsulated into an LLC frame passed to the IEEE 802.11 MAC. The slave, which is notified of the data arrival by an indication of the LLC service, responds with a frame containing the input data that had been previously prepared by means of the *Data_Upd* service (made available by the polling-oriented protocol) that, in turn, triggered the DL-REPLAY-UPDATE service of LLC, as shown by the primitives *LLC_upd.req* and *LLC_upd.con*.

As far as the acyclic data are concerned, they may be handled in different ways. We propose the following three specific techniques.

1) The first technique, which in the following will be referred to as *late*, specifies that the slaves signal the presence of acyclic data by setting a flag in the cyclic data packet. The master, at the end of the current polling cycle, queries those slaves that required the acyclic services. This technique, which is analogous to that of Profibus DP, is based on the traditional assumption that slaves are passive devices that cannot access autonomously the network.
2) The second technique, named *current*, allows a slave, when polled, to send directly acyclic data to the master. In practice, the slave replaces the cyclic data with the acyclic ones. The master recognizes acyclic data (for example, by means of a special code written by the slave in the LLC SAPs) and undertakes the appropriate actions. Using this procedure, when a slave transmits acyclic information, the input data of that slave are not updated for one polling cycle. Nevertheless, such a solution is of ease implementation and has the advantage of reducing both the jitter and the acyclic data latency.
3) The third technique, called *immediate*, exploits the decentralized nature of the IEEE 802.11 MAC protocol and hence the capability of the devices to autonomously access the network. In this case, a slave station, when acyclic data are generated, immediately tries to send them to the master. Clearly, in this case, collisions with the cyclic traffic may take place, and we rely on the ability of the MAC to resolve the contention for accessing the channel.

The three techniques described above may be implemented effectively by using both types of connectionless LLC services. However, since this type of data may derive from critical events, they have to be correctly received. For such a reason, we decide to use the acknowledged connectionless services of LLC.

Variable-Oriented Protocols Over IEEE 802.11: These protocols rely on a producer/consumer model that allows the exchange of a set of identified variables over the network. The technique makes possible to select, for each variable, a specific rate of production, realizing in such a way a cyclic exchange with different periodicity. A "scheduler" device (the equivalent of the bus arbitrator in WorldFIP) is responsible for issuing the production requests with the specified periodicity. The application layer supplies the user applications with a set of services necessary to access the identified variables for reading, writing, and handling operations.

Since the producer/consumer technique implies that a produced variable has to be made available to all the network nodes (instead of sending it to a specific destination), the most suitable LLC services for implementing the exchange of cyclic data are the unacknowledged connectionless services. An example of data exchange implemented with the variable-oriented protocol is shown in Fig. 4. As can be seen, the production request issued by the scheduler with the service *Var_Prod* (made available by the protocol) is mapped on an LLC service that causes the broadcasting of an IEEE 802.11 PDU to the network nodes. As a result, only the actual producer of the variable (node 2 in the example) transmits the requested value using the service *Var_Value* (supplied by the variable-oriented protocol). Then the produced variable is acquired by all the consumers (nodes 1 and n in the example).

Acyclic data may be handled in two different ways that resemble both the *late* and *immediate* techniques discussed for the *polling-based* protocol. More in detail, with the late technique, a station, during the production of a variable, may signal the presence of acyclic data it needs to transmit. The actual transmission of such data may take place in the time intervals between subsequent scheduled operations. The procedure is handled by the scheduler that, as soon as possible, grants the station that made the request of acyclic data transmission with the right to access the network. Even in this case, in order to ensure that acyclic messages arrive correctly at destination, we implement them by means of LLC

confirmed services. Such a technique, which is employed by both WorldFIP and the IEC fieldbus, requires that there is enough time between periodic operations to accommodate the possible acyclic activities. Contrarily, the transmission of acyclic data could be delayed by the scheduler.

Such a problem may be overcome with the immediate technique: in this case, the stations try to transmit the acyclic data at the time of their actual occurrence, since they can autonomously access the transmission medium.

With both the above techniques, in principle, the overlapping between cyclic and acyclic operations cannot be avoided. This means that, while the network is processing an acyclic data request by a device, it could be necessary to issue a new cyclic request. Such a situation may be encountered since the possible retransmissions of IEEE 802.11 frames carrying acyclic data prolong the duration of the acyclic data services. As a consequence, data related to the cyclic traffic can get lost, due to collisions with acyclic data, since they were broadcasted, and hence cannot be retransmitted. Thus, the overall effect of such collisions may be the sporadic missing of a cyclic update of some variables that, in most cases, will not cause serious problems to the system performance. On the other hand, acyclic operations are highly likely to be successfully performed.

B. Application Layer Protocols Design Over Bluetooth

The protocols we propose for Bluetooth are designed with a network working on a restricted geographic area and with a limited number of devices in mind. For such a reason, our analysis will be limited to a basic piconet configuration.

Due to the specific operation of a piconet (the "integrated" polling performed by the Bluetooth master on the slaves), the implementation of a variable-oriented protocol over Bluetooth is not advisable. Indeed, the producer/consumer technique is based on the use of broadcast messages that may contain either the variable production requests or the values of the variables. Unfortunately, the realization of such a technique in Bluetooth would require very high delays, since the master has to send in sequence the same message to each slave, employing necessarily one polling cycle.[4] Moreover, the slaves would have to elaborate the requests, and the responses could arrive not before another polling cycle.

As a consequence, we decided to propose only a polling-oriented protocol over Bluetooth.

Similarly to the IEEE 802.11 design, the cyclic data are exchanged by means of periodic queries issued by the master to the slaves.[5] The L2CAP of Bluetooth offers two connection-oriented services that are suitable to implement such a function, namely, DataWrite and DataRead. Fig. 5 shows an example of implementation of data exchange (similarly to the equivalent protocol over IEEE 802.11, we assume that both

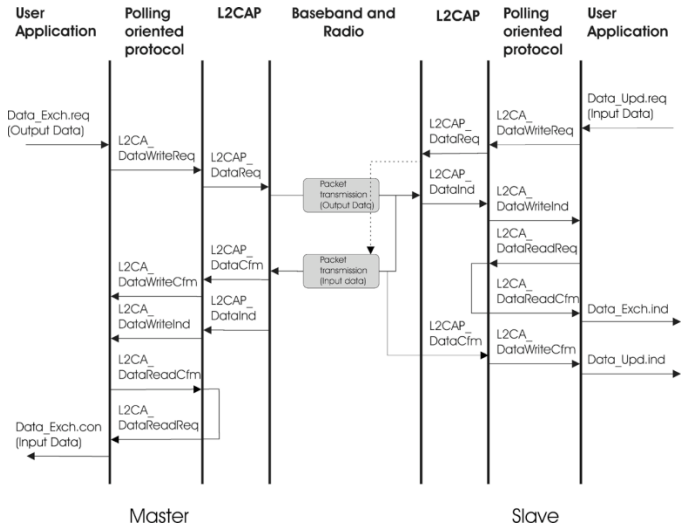

Fig. 5. Bluetooth polling-oriented protocols: periodic exchange of data.

the services *Data_Exch* and *Data_Upd* are available). The procedure begins with a request from the master (primitive *Data_Exch.req*), carrying the output data, toward a selected slave. The primitive is mapped onto a write request to the L2CAP layer (*L2CA_DataWriteReq*), which in turn triggers the BT master to poll the specified BT slave (*L2CAP_DataReq*). This latter is notified of the arrival of the data with the primitive *L2CAP_DataInd*. The slave uses the DataRead service to acquire the data (with the primitives *L2CA_DataReadReq* and *L2CA_DataReadCfm*). At the same time, the slave sends the input data to the master. This is realized in the immediate response of the BT slave (i.e., in the return packet it sends to the BT master), since the input data were previously prepared by means of the primitives *Data_Upd.req*, *L2CA_DataWriteReq*, and *L2CAP_DataReq*, respectively.

The acyclic data, in principle, could be handled with both the late and current techniques already described for IEEE 802.11 (the third one, immediate, is not applicable since the BT slaves cannot access autonomously the transmission medium). However, the late technique could lead to significant delays in both the cyclic and acyclic data transmissions. In fact, when a slave signals the presence of acyclic data, the master, at the end of the current cycle, has to stop the polling of the slaves and to issue a specific reading request. Such a procedure may take some Bluetooth polling cycles, since the request has first to be interpreted by the slave and then the acyclic data have to be made available. For such a reason, the polling-oriented protocol implemented on Bluetooth will use only the current technique to read acyclic data.

C. Numerical Results

In order to verify the performance of the proposed protocol stacks and check whether they are able to verify the tight timing requirements typical of the communication at the device level, we implemented the protocol models we proposed and run extensive simulations with ns2 [55]. To keep the focus on the performance of typical industrial application layers over wireless networks, we concentrated on a pure wireless system. The study

[4]An alternative solution could be represented by the implementation of a purpose-oriented scheduler, which cannot in any case be done by using off-the-shelves Bluetooth transceivers.

[5]The master of the polling-oriented protocol and the Bluetooth master are, physically, the same device. However, their functions are different. In order to avoid confusion, in the following, we will use the notation "BT master" when referring to the Bluetooth master. The same applies for the slaves.

of the (possible) performance degradation induced by the inclusion of a wired segment (resulting thus in a hybrid configuration) is left to future studies.

Let us define the update period T_u as the period with which the data to/from a device are updated. In polling-oriented protocols, it corresponds to the time interval between two successive successful delivery of a message with cyclic data from a slave to the master. In variable-oriented protocols, it consists of the time interval between the reception, by the intended destination devices, of a variable requested by the scheduler. We will focus on the first two stochastic moments of the update time, taken as representative performance measure for the ability of the network to process data at a high speed and with limited jitter (note also that the outage probability for the update time, defined as the probability that the update time exceeds a given threshold, can then be estimated by means of the classical Chebyshev's bound [56]). In principle, the update time should be a deterministic value; however, in the protocol stacks we are proposing, randomness is induced by the presence of channel losses (for all the configurations under study), by the randomness inherently present in the medium access strategy (for 802.11-based protocols) and by the possible presence of alarm messages (for the late and immediate techniques in 802.11-based polling-oriented protocols).

The alarm latency, [6] denoted by D is defined as the time encompassed between the generation, by a device, of an alarm message and its successful transmission to the intended destination by means of the acyclic data services. In order to keep the notation simple, we consider that all the devices have the same features (symmetrical scenario) and generate alarms according to a Poisson process of intensity $\lambda = 0.1\ \mathrm{s}^{-1}$ (which is equivalent to the occurrence of one alarm every 100 ms on average). Various different performance metrics may be considered to describe the behavior of D. In particular, we may refer to its mean/minimum/maximum values or to the outage probability. In the proposed simulations, we decided to focus on the mean alarm value of the alarm latency, since such a choice seems more coherent with the scope of this paper (indeed, we do not look for a complete characterization of a wireless fieldbus system, but rather, we are aimed at studying the feasibility of the proposed protocols). For the same reason, all messages, regardless of whether they carry data variables or alarms, are assumed to have a size of 10 bytes, which represents an indicative order of magnitude of the amount of data typically exchanged between controller and sensors/actuators at low levels of factory automation systems. Of course, specific applications may deal with (even significant) different amounts of data, and a complete study would require to evaluate the performance metrics as a function of the variable size.

As far as the underlying radio channel is concerned, we considered two different channel models: one for Bluetooth-based networks and another one for IEEE 802.11-based networks. Starting from the latter, we based our simulations on the Gilbert/Elliott model described in [46], where some models are proposed and compared with the results obtained from a real testbed. As done also in [14], we used the parameters estimated from the Trace 24 of the *factorial* measurements in [46] and modified the packet error rate (PER) in the BAD state, in order to achieve an average PER ranging from 10^{-2} to 10^{-1} (in [46], the measured average PER is 0.1099). Further, in our simulations, we assumed that the AMC mechanism does not react to channel losses by enforcing more robust modulation/coding schemes. Such an assumption is, to a certain extent, compelled by the lack of traces of *joint bit rates and packet errors* for real 802.11a/b/g devices in an industrial environment, which would be needed to run more precise simulations. However, it is interesting to point out that our approach provides an approximate worst-case behavior: indeed, given the considerable overhead introduced by the IEEE 802.11 MAC, retransmitting at lower bit rates is usually more advantageous than repeating transmissions by means of the exponential backoff mechanism encompassed by the standard. For Bluetooth, we considered a simple memoryless channel model. Indeed, the frequency hopping scheme encompassed by the standard at the physical layer is considered to be able to hide the time correlation between the channel conditions encountered by subsequent packets. This configures a classical block-fading channel (formulas for computing the PER in Rice, Rayleigh, m-Nakagami, and AWGN channels are reported in [57]).

We start by considering variable-oriented protocols running over IEEE 802.11. According to the discussion in the previous section, we implemented the immediate technique only, which was shown to provide better performance and a higher flexibility to the protocol designers.

We consider a cycle in which seven variables were produced with a periodicity of 10 ms each. Also in this case, it may be observed that these values might not necessarily represent a significant benchmark. However, as explained above, they allow for a preliminary study of the protocol. Moreover, as it will be shown later on that such a choice permits a straightforward comparison with the polling-oriented protocols implemented for IEEE 802.11 and Bluetooth.

In order to use the same configuration of the polling-oriented protocol, we supposed that the network comprises $N = 7$ devices (plus the scheduler), each of them producing one variable. In Fig. 6, we reported the mean update time (in terms of the 95% confidence interval) versus the average PER. It can be seen that the update time is not particularly sensitive to the mean PER, and the randomness introduced by the channel behavior does not impact much on the performance (due to lack of space, we did not report the update time jitter, whose behavior can nonetheless be inferred from Fig. 6). The mean alarm latency is reported in Fig. 7. It is worth noting that the response time in presence of alarms is extremely short, remaining below the value of 1 ms. We can then conclude that, with the adoption of the immediate technique, the proposed protocol is able to handle extremely time-critical events. It may also be observed that, since the alarm latencies are very short, likely, the load introduced by the periodic traffic has no relevant effects. However, in order to better circumstantiate such an observation, more accurate simulations should be performed aimed at verifying the actual influence of the periodic traffic.

Next, we considered polling-oriented protocols over IEEE 802.11. We studied the performance of the three techniques

[6] In this section, we focus on the most critical type of acyclic data: those deriving from the generation of alarms.

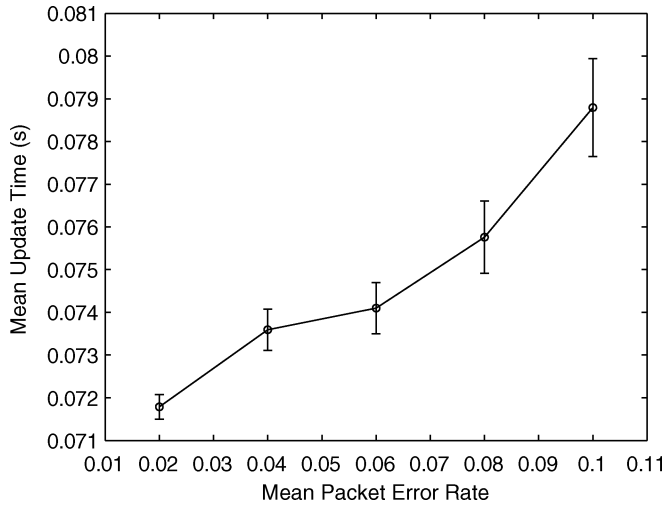

Fig. 6. Variable-oriented protocols over IEEE 802.11: mean update time versus average PER, $N = 7$, $\lambda = 0.1$, 95% confidence interval.

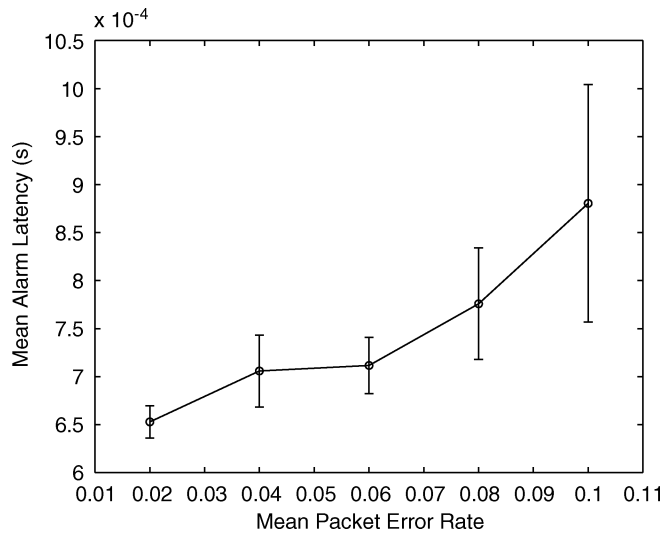

Fig. 7. Variable-oriented protocols over IEEE 802.11: mean alarm latency versus average PER, $N = 7$, $\lambda = 0.1$, 95% confidence interval.

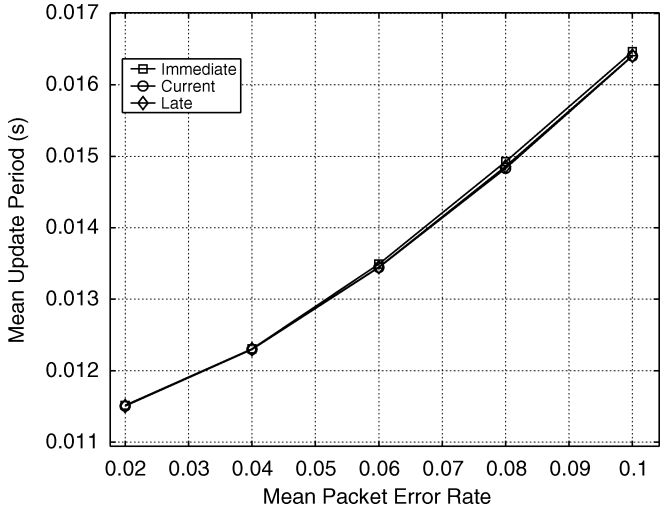

Fig. 8. Polling-oriented protocols over IEEE 802.11: mean update time versus average PER, $N = 7$, $\lambda = 0.1$.

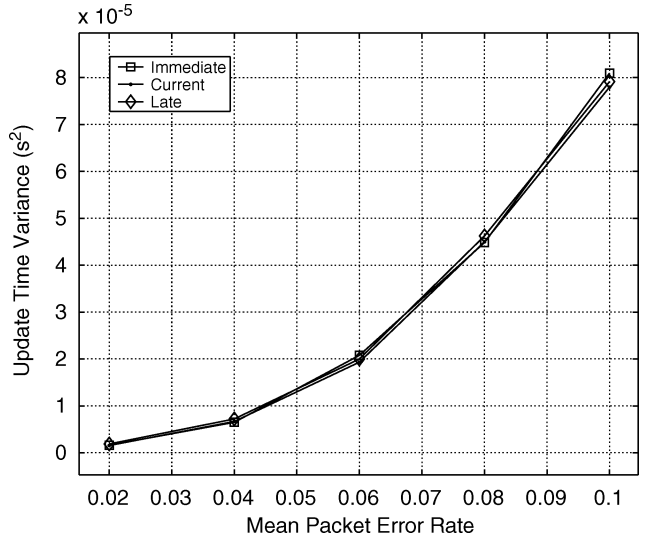

Fig. 9. Polling-oriented protocols over IEEE 802.11: update time variance versus average PER, $N = 7$, $\lambda = 0.1$.

we presented in the previous section to handle alarm messages, evaluating them in terms of the three metrics of interest previously described. In Fig. 8, we plotted the results for the mean update time versus the average packet rate for a network comprising one master and $N = 7$ slaves, where we set $\lambda = 0.1\ \mathrm{s}^{-1}$. As it may be seen, all techniques perform similarly and, more important, with results that are well within the timing constraints of most industrial applications. Results for the update time variance are reported in Fig. 9, where it may be seen that the three techniques perform similarly. Such a result was not *a priori* expectable, since the immediate technique may, in principle, generate collisions, which cause an increase of the update time jitter and hence a greater value of the variance. On the other hand, a big gap between the immediate technique and the other two more conservative ones does appear when we consider the alarm latency, as it may be seen in Fig. 10. In such figure, indeed we see that the immediate algorithm, whose functioning relies on the distributed nature of the IEEE 802.11 MAC protocol, clearly outperforms the other techniques, giving stable results of a few milliseconds, a value that is comparable with those of the most performing (wired) fieldbuses [58]. As done also for variable-oriented protocols, we can thus conclude that the immediate technique is suitable to handle time-critical events and represents an interesting option for protocol designers. Of course, in order to completely characterize the behavior of such a technique, more extensive simulations and practical implementations would be required, which are out of the scope of this paper.

Finally, we tested the polling-oriented protocol over Bluetooth networks. In such case, we reported results for the mean update time and the mean alarm latency for a fully loaded piconet, with $N = 7$ slaves with an alarm generation rate $\lambda = 0.1\ \mathrm{s}^{-1}$. Results are depicted in Figs. 11 and 12, respectively, together with the analytical curves obtained in [51]. We note

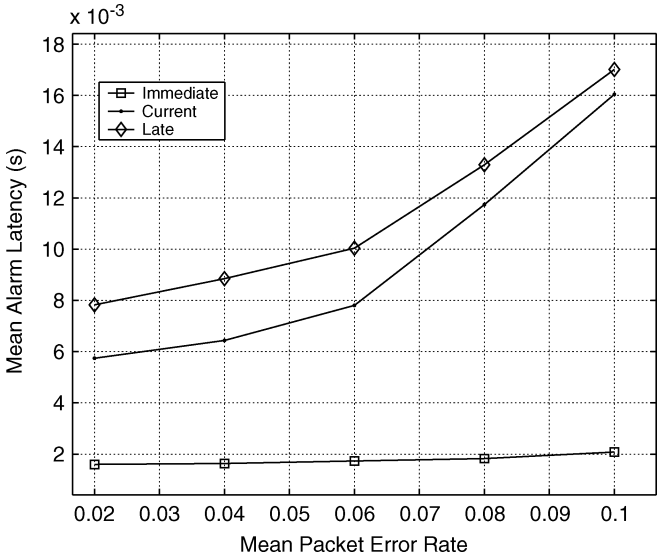

Fig. 10. Polling-oriented protocols over IEEE 802.11: mean alarm latency versus average PER, $N = 7, \lambda = 0.1$.

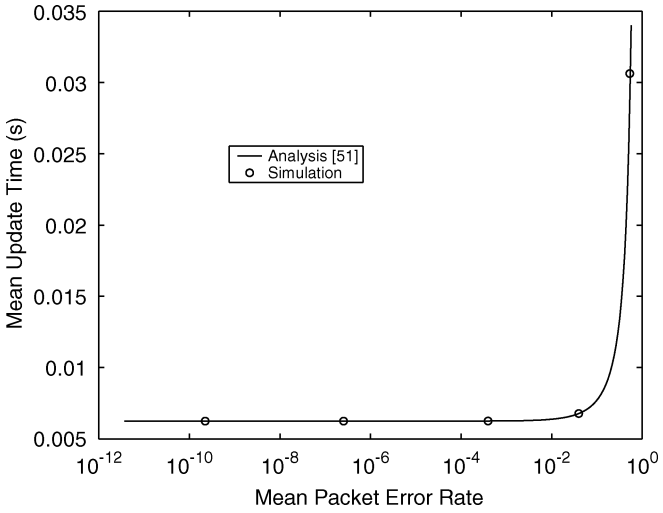

Fig. 11. Polling-oriented protocols over Bluetooth: mean update time versus average PER, $N = 7, \lambda = 0.1$.

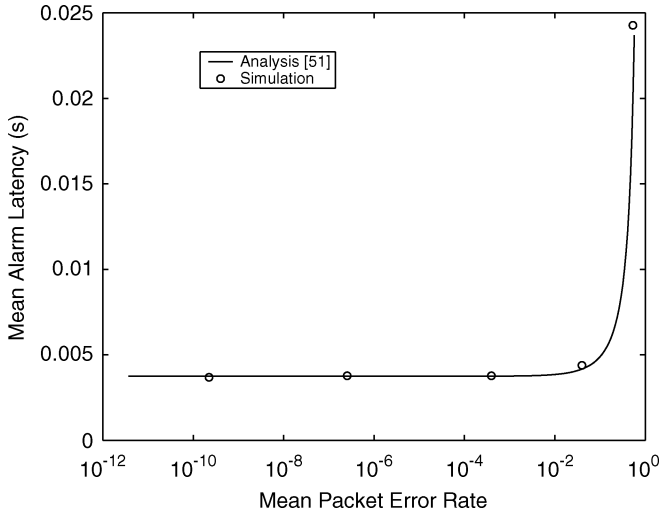

Fig. 12. Polling-oriented protocols over Bluetooth: mean alarm latency versus average PER, $N = 7, \lambda = 0.1$.

also in this case that, for an average PER up to $5 \cdot 10^{-2}$, performances are still reasonably good, enabling the application of such solution to a wide spectrum of industrial applications. Even if the performance indexes are not directly comparable to those of IEEE 802.11-based solutions, we may anyway conclude that such implementation may represent an interesting choice for networks with not too tight timing requirements but that may benefit from the reduced power consumption provided by the Bluetooth radio interface.

IX. Conclusion

In this paper, we focused on the use of wireless communication systems at the device level of factory automation systems.

We started discussing the features and requirements of the device level industrial communication, and we selected IEEE 802.11 and Bluetooth as possible candidates for the lowest layers of a wireless fieldbus. Then we proposed two models of application layer protocols and showed how they could be implemented over the chosen wireless technologies. Numerical simulations provided evidence of the feasibility of the proposed protocol stacks, able to present performance figures not far from those of wired fieldbuses.

Although the obtained results are encouraging, several aspects need to be further investigated. Besides issues related to the wireless technologies, such as security and power consumption, key problems are relevant to both protocols definition and implementation. At present, indeed, no standards are available for data link and application layer protocols of wireless industrial communication systems. Further, no standardization actions are presently undertaken by the competent bodies. Thus, there is the concrete risk of assisting, in the near future, to a proliferation of proprietary products.

In perspective, two research directions appear particularly appealing. The first one concerns the effective implementation of a wireless fieldbus based on the IEEE 802.15 standard, which presents very desirable features in terms of contention-free access to the channel and very low power consumption. The second one regards networks based on the *ad hoc* paradigm. In this case, the attention is focused on the employment of sensor networks and sensor-actor networks aiming at performing real-time distributed operations.

Acknowledgment

The authors would like to thank H. Zhang for the clarifications provided on the ongoing standardization activities within the IEEE 802.15 working group. The authors also would like to thank the anonymous reviewers who contributed to improve the quality of this paper.

References

[1] T. J. Williams, *A Reference Model for Computer Integrated Manufacturing: A Description From the Viewpoint of Industrial Automation*. Research Triangle Park, NC: Instrum. Soc. Amer., 1989.

[2] J. P. Thomesse, "Fieldbuses and interoperability," *Control Eng. Practice*, vol. 7, no. 1, pp. 81–94, 1998.

[3] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," *Comput. Netw.*, vol. 38, no. 4, pp. 393–422, Mar. 2002.

[4] *Profibus Standard: Translation of the German National Standard DIN 19245 Parts 1 and 2*, DIN 19245, Profibus Nutzerorganization e.V. Std, 1991.

[5] *IEEE Standard 802.4, Information Processing Systems—Local Area Network—Part 4: Token Passing Bus Access Method and Physical Layer Specification*, IEEE Std. 802.4, Aug. 1990.

[6] *Road Vehicles—Interchange of Digital Information—Controller area Network for High-Speed Communication, ISO IS 11898*, ISO IS 11898, International Standard Organization, Std., Nov. 1993.

[7] IEC 61158-3,4: Digital Data Communications for Measurement and Control—Fieldbus for Use in Industrial Control Systems—Parts 3 and 4: Application Layer Service Definition and Protocol Specification, Communication Model Type 3, International Electrotechnical Commission Std., Jan. 2000.

[8] *ControlNet Specifications*, , ControlNet International Std., Mar. 1998.

[9] *IEC 61158-3,4: Digital Data Communications for Measurement and Control—Fieldbus for Use in Industrial Control Systems—Parts 3 and 4: Application Layer Service Definition and Protocol Specification, Communication Model Type 1*, IEC 61158-3,4, International Electrotechnical Commission Std., Jan. 2000.

[10] *Manufacturing Message Specification Parts 1 and 2, ISO IS 9506*, ISO IS 9506, International Standard Organization Std., 1990.

[11] *CANopen Application Layer and Communication Profile, Version 4.01*, CiA/DS301, International Users and Manufacturers Group e.V. Std., Jun. 2000, CAN In Automation.

[12] *IEC 61158-3,4: Digital Data Communications for Measurement and Control—Fieldbus for Use in Industrial Control Systems—Parts 3 and 4: Application Layer Service Definition and Protocol Specification, Communication Model Type 8*, IEC 61158-3,4, International Electrotechnical Commission Std., Jan. 2000.

[13] *EN50325-2: Industrial Communication Subsystem Based on ISO 11898 (CAN) for Controller-Device Interface -Part 2: DeviceNet*, EN50325-2, European Committee for Electrotechnical Standardization, Std., Jun. 2000.

[14] A. Willig, "Polling-based MAC protocols for improving real-time performance in a wireless network," *IEEE Trans. Ind. Electron.*, vol. 50, no. 4, pp. 806–817, Aug. 2003.

[15] R-fieldbus [Online]. Available: http://www.rfieldbus.de.

[16] A. Willig, K. Matheus, and A. Wolisz, "Wireless technologies in industrial networks," *Proc. IEEE*, vol. 93, no. 6, pp. 1130–1150, Jun. 2005.

[17] *IEEE 802.3 Standard: Carrier Sense Multiple Access With Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications*, 802.3, IEEE Std., Oct. 2000.

[18] *"Specification of Bluetooth System,"* ver. 1.1, Feb. 22, 2001.

[19] J. Haartsen, "Bluetooth toward ubiquitous wireless connectivity," *Revue HF, Soc. Belge Ing. Telecommun. Electron*, pp. 8–16, 2000.

[20] Bluetooth Wireless—Efficient Business [Online]. Available: http://www.bluetooth.com/business/.

[21] Bluetooth Wireless—Consumer Products [Online]. Available: http://www.bluetooth.com/products/.

[22] *Supplement to 802.11-1999, Wireless LAN MAC and PHY Specifications: Higher Speed Physical Layer (PHY) Extension in the 2.4 GHz Band*, 802.11-1999, IEEE Std., Sep. 1999.

[23] IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std., Aug. 1999.

[24] M. Borgo, A. Zanella, P. Bisaglia, and S. Merlin, "Analysis of the hidden terminal effect in multi-rate IEEE 802.11b networks," in *Proc. IEEE WPMC*, 2004 [Online]. Available: http://www.dei.unipd.it/~zanella/.

[25] *IEEE Standard for Information Technology Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks—Part 15.1–15.4.*, , IEEE Std., Jan. 2003.

[26] *Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low—Rate Wireless Personal Area Networks (WPAN's)*, , IEEE Std., Sep. 2003.

[27] Zigbee alliance [Online]. Available: http://www.zigbee.org.

[28] I. F. Akyildiz and H. Kasimoglu, "Wireless sensor and actor networks: research challenges," *Ad Hoc Netw. J.*, vol. 2, no. 2, pp. 351–367, 2004.

[29] N. Borisov, I. Goldberg, and Wagner, "Intercepting mobile communications: The insecurity of 802.11," in *Proc. ACM MobiCom*, Rome, Italy, 2001.

[30] Y. Zhang, W. Lee, and Y. Huang, "Intrusion detection techniques for mobile wireless networks," *ACM Wireless Netw. J.*, vol. 9, no. 5, pp. 545–556, Sep. 2003.

[31] L. Zhou and Z. J. Haas, "Securing ad hoc networks," *IEEE Network*, vol. 13, no. 6, pp. 24–30, Nov.-Dec. 1999.

[32] C. Hodgdon, "Adaptive frequency hopping for reduced interference between Bluetooth and wireless LAN," Ericsson Technology Licensing, White Paper, May 2003 [Online]. Available: www.ericsson.com/bluetooth/files/whitepaper_on_afh_final.pdf.

[33] P. Popovski, H. Yomo, S. Guarracino, and R. Prasad, "Adaptive mitigation of self—interference in Bluetooth scatternets," in *Proceedings WPMC*, Abano Terme, Padova, Italy, Sep. 12–14, 2004, pp. 285–289.

[34] C. Gehrmann, Bluetooth Security Bluetooth SIG Security Expert Group, White Paper, Apr. 1, 2002.

[35] J. C. Chen, K. M. Sivalingam, and P. Agrawal, "Performance comparison of battery power consumption in wireless multiple access protocols," *Wireless Netw.*, vol. 5, pp. 445–460, 1999.

[36] L. M. Feeney and M. Nilsson, "Investigating the energy consumption of a wireless network interface in an ad hoc networking environment," in *Proc. IEEE INFOCOM*, 2001 [Online]. Available: http://www.citeseer.ist.psu.edu/feeney01investigating.html.

[37] M. Stemm and R. H. Katz, "Measuring and reducing energy consumption of network interfaces in hand-held devices," *IEICE Trans. Commun.*, vol. E80-B, no. 8, pp. 1125–1131, 1997.

[38] L. D. Paulson, "Will fuel cells replace batteries in mobile devices?," *IEEE Computer*, vol. 36, no. 11, pp. 10–12, Nov. 2003.

[39] Y.-C. Tseng, C.-S. Hsu, and T.-Y. Hsieh, "Power-saving protocols for IEEE 802.11—based multi-hop," in *Proc. IEEE INFOCOM*, New York, 2002.

[40] T. Simunic, H. Vikalo, P. Glynn, and G. D. Micheli, "Energy efficient design of portable wireless systems," in *Proc. Int. Symp. Low Power Electronics Design Archive*, Rapallo, Italy, 2000, vol. 49–54.

[41] H. Woesner, J.-P. Ebert, M. Schlager, and A. Wolisz, "Power saving mechanisms in emerging standards for wireless LANs: The MAC level perspective," *IEEE Pers. Commun.*, vol. 5, no. 3, pp. 40–48, Jun. 1998.

[42] A. Zanella and F. D. Pellegrini, "Mathematical analysis of IEEE 802.11 energy efficiency," in *Proc. IEEE WPMC*, 2004 [Online]. Available: http://www.dei.unipd.it/~depe/.

[43] R. Bruno, M. Conti, and E. Gregori, "Optimization of efficiency and energy consumption in p-persistent CSMA-based wireless LANs," *IEEE Trans. Mobile Comput.*, vol. 1, no. 1, pp. 10–31, Jan.-Mar. 2002.

[44] A. Zanella, D. Miorandi, and S. Pupolin, "Mathematical analysis of Bluetooth energy efficiency," in *Proc. WPMC*, Yokosuka, Kanagawa, Japan, Oct. 19–20, 2003, vol. 1, pp. 152–156.

[45] L. Rauchhaupt, "System and device architecture of a radio based fieldbus—the rfieldbus system," in *Proc. WFCS*, Vasteras, Sweden, 2002.

[46] A. Willig, M. Kubisch, C. Hoene, and A. Wolisz, "Measurements of a wireless link in an industrial environment using an IEEE 802.11-compliant physical layer," *IEEE Trans. Ind. Electron.*, vol. 49, no. 6, pp. 1265–1282, Dec. 2002.

[47] S. Lee, K. C. Lee, M. H. Lee, and F. Harashima, "Integration of mobile vehicles for automated material handling using Profibus and IEEE 802.11 networks," *IEEE Trans. Ind. Electron.*, vol. 49, no. 3, pp. 693–701, Jun. 2002.

[48] P. Morel and A. Croisier, "A wireless gateway for fieldbus," in *Proc. PIMRC*, 1995.

[49] P. Morel and J. D. Decotignie, "Integration of wireless mobile nodes in MAP/MMS," in *Proc. 13th IFAC Workshop Distributed Computer Control Systems*, 1995.

[50] L. Ferreira, M. Alves, and E. Tovar, "Hybrid wired/wireless profibus networks supported by bridges/routers," in *Proc. WFCS*, Vasteras, Sweden, 2002.

[51] D. Miorandi and S. Vitturi, "A wireless extension of Profibus DP based on the Bluetooth radio system," *Ad Hoc Netw. J.*, vol. 3, no. 4, pp. 479–494, 2004.

[52] ——, "Hybrid wired/wireless implementations of Profibus DP: A feasibility study based on Ethernet and Bluetooth," *Comput. Commun.*, vol. 27, no. 10, pp. 946–960.

[53] K. Tang, K. Mann, and S. Kwong, "Wireless communication network design in IC factory," *IEEE Trans. Ind. Electron.*, vol. 50, no. 4, pp. 452–459, Apr. 2001.

[54] *IEEE 802.2 Logical Link Control (With Amendments 3, 6 and 7)*, 802.2, IEEE Std., 1998.

[55] The Network Simulator—ns-2 [Online]. Available: http://www.isi.edu/nsnam/ns/.

[56] L. Kleinrock, *Queueing Systems*. New York: Wiley, 1975.

[57] D. Miorandi and A. Zanella, "Achievable rate regions for Bluetooth piconets in fading channels," in *Proc. IEEE VTC Spring Meeting*, Milan, Italy, 2004.

[58] S. Vitturi, "On the effects of the acyclic traffic on profibus dp networks," *Comput. Stand. Interfaces*, vol. 26, pp. 131–144, Mar. 2004.

Francesco De Pellegrini (M'01) was born on April 13, 1974 in Belluno, Italy. He received the Laurea degree in 2000 and the Ph.D. degree in 2004, both in telecommunication engineering, from the University of Padova, Padova, Italy.

His research interests are location detection in sensor networks, multirate systems, turn-prohibition routing, WLAN VoIP, and bio-inspired networking.

Dr. De Pellegrini serves as a reviewer for several international networking conferences, including IEEE PIMRC, LCN, CCNC, WCNC, and VTC.

Daniele Miorandi was born in Rovereto, Italy, in 1977. He received the Laurea degree (summa cum laude) in telecommunication engineering from the University of Padova, Padova, Italy, in 2001, with a thesis on spectral synthesis using finite state machines. He received the Ph.D. degree in communication engineering from the University of Padova in 2005, with a thesis entitled "Stochastic Modelling of Wireless Ad Hoc Networks."

In 2003–2004, he spent one year of his doctoral thesis visiting the MAESTRO project at INRIA Sophia Antipolis, France. In 2004, he had an appointment as "Incaricato di Ricerca" at IEIIT-CNR, Torino, Italy. Since January 2005, he has been a Postdoc Researcher at CREATE-NET, Trento, Italy. His research interests include design and analysis of bio-inspired communication paradigms for pervasive computing environments, analysis of TCP performance over wireless/satellite networks, scaling laws for large-scale information systems, protocols and architectures for wireless mesh networks, and real-time industrial communications over wireless links.

Stefano Vitturi received the Laurea degree in electronic engineering from the University of Padua, Padua, Italy, in 1984.

From 1985–1998, he has worked at the control and data acquisition system of RFX, a nuclear fusion experiment included in the Fusion Program of the European Community, located in Padova, Italy. Since 1986, he has been a Researcher with the Italian National Research Council (CNR). Currently, he is with the IEIIT-CNR, where institutional activities are electronics, information engineering, and telecommunications. During his work at RFX, he has been involved in research and applications on factory automation systems, communication protocols, local area networks, and programmable logic controllers. Since 1995, he has been involved in research activities on industrial communication systems; such activities concern the modelling of real-time communication networks (either wired or wireless), performance analysis, and implementation of devices conforming to the most popular communication protocols.

Andrea Zanella received the Laurea degree in computer engineering in 1998 and the Ph.D. degree in electronic and telecommunications engineering in 2002 from the University of Padova, Padova, Italy. His thesis was entitled "Analysis and Modeling of Wireless Data Networks."

He is an Assistant Professor with the Department of Information Engineering (DEI), University of Padova. Before that, he spent nine months as a Visiting Scholar at the Department of Computer Science, University of California, Los Angeles (UCLA), where he worked on wireless networks and wireless access to the Internet under the supervision of Prof. M. Gerla. His major research interest is in the field of wireless communication networks and distributed systems. He has been working on many different issues related to such topics, spanning from the definition of mathematical models for physical radio links to the design and analysis of mechanisms for improving the transmission of Internet protocols (mainly TCP) over lossy connections. Furthermore, a large part of his research activity has been focused on Bluetooth and WLAN internetworking.

Dr. Zanella is a Reviewer for several international conferences and IEEE journals in the ICT area.