Wireless Technology in Industrial Networks

ANDREAS WILLIG, MEMBER, IEEE, KIRSTEN MATHEUS, MEMBER, IEEE, AND
ADAM WOLISZ, SENIOR MEMBER, IEEE

Invited Paper

With the success of wireless technologies in consumer electronics, standard wireless technologies are envisioned for the deployment in industrial environments as well. Industrial applications involving mobile subsystems or just the desire to save cabling make wireless technologies attractive. Nevertheless, these applications often have stringent requirements on reliability and timing. In wired environments, timing and reliability are well catered for by fieldbus systems (which are a mature technology designed to enable communication between digital controllers and the sensors and actuators interfacing to a physical process). When wireless links are included, reliability and timing requirements are significantly more difficult to meet, due to the adverse properties of the radio channels.

In this paper, we thus discuss some key issues coming up in wireless fieldbus and wireless industrial communication systems: 1) fundamental problems like achieving timely and reliable transmission despite channel errors; 2) the usage of existing wireless technologies for this specific field of applications; and 3) the creation of hybrid systems in which wireless stations are included into existing wired systems.

Keywords*—*Bluetooth (BT), fieldbus systems, hybrid systems, IEEE 802.11, IEEE 802.15.4, real-time communications, wireless technologies.

I. Introduction

The true convenience of being able to connect devices without the use of wires has lead to the unprecedented success of wireless technologies in the consumer goods industry. Based on this success, applications using these technologies are beginning to appear in various other settings as well. In an industrial or factory floor setting, for example, the benefits of using wireless technologies are manifold. First of all, the cost and time needed for the installation and maintenance of the large number of cables normally required in such an environment can be substantially reduced, thus making plant setup and reconfiguration more easy. This is especially important in harsh environments where chemicals, vibrations, or moving parts exist that could potentially damage any sort of cabling. In terms of plant flexibility, stationary systems can be wirelessly coupled to any mobile subsystems or mobile robots that may exist in order to achieve a connectivity that would otherwise be impossible. Furthermore, the task of temporarily accessing any of the machinery in the plant for diagnostic or programming purposes can be greatly simplified by the use of these wireless technologies.

Along with the simplification of accessing machinery, many industrial applications exist that could benefit from the use of wireless technologies. The localization and tracking of unfinished parts, the coordination of autonomous transport vehicles and mobile robots [1]–[3], as well as applications involving distributed control are all areas in which wireless technologies could be used in an industrial environment.

Many of these industrial applications are served by fieldbus systems [4]–[8] like PROFIBUS [9], [10], WorldFIP [11], [12] or CAN [13], [14], which are wired. Fieldbus systems have been specifically designed for solving automation or control tasks that rely on the interconnection of digital controllers with other digital controllers as well as sensors and/or actuators (including their underlying physical processes). The primary goal of these systems is to provide real-time communication services that are both predictable and reliable, i.e., make certain guarantees on eventual delivery of packets and delivery times. Some important characteristics of fieldbus traffic are: 1) presence of cyclic (i.e., recurring) or even periodic traffic (bounded jitter between subsequent packets required), subject to deadlines; 2) presence of important acyclic packets like alarms, which need to be reliably transmitted with bounded latencies; and 3) most packets are short, on the order of a few bytes. The protocol architecture of most fieldbus systems covers only the physical layer, the data link layer including the medium access control (MAC) sublayer, and the application layer of the OSI reference model.

Manuscript received March 25, 2004; revised March 11, 2005.

A. Willig is with the Hasso-Plattner-Institute, University of Potsdam, Potsdam 14482, Germany (e-mail: awillig@ieee.org).

K. Matheus is with CARMEQ GmbH, Berlin 10587, Germany (e-mail: kirsten.matheus@carmeq.com).

A. Wolisz is with the Telecommunication Networks Group (TKN), Technical University Berlin, Berlin 10587, Germany (e-mail: awo@ieee.org).

Digital Object Identifier 10.1109/JPROC.2005.849717

The obvious benefits of wireless transmission have led to a number of solutions. These solutions range from voice-oriented, large-scale cellular networks such as UMTS, to data-oriented solutions like wireless LANs (WLANs), wireless personal area networks (WPANs) and wireless sensor networks. WLAN systems, like the IEEE 802.11 family of standards [15]–[17], are designed to provide users with high data rates (tens of megabits per second) over ranges of tens to hundreds of meters. These parameters provide the user with untethered access to Ethernet, for example. WPAN systems, such as Bluetooth (BT) [18], [19] and IEEE 802.15.4 [20], [21] have been designed for connecting devices wirelessly while taking energy efficiency into account. They support medium data rates in the order of hundreds of kilobits per second to a few megabits per second and have ranges on the order of a few meters. Many vendors offer equipment compliant to these standards.

Running fieldbus-based applications with wireless technologies can be especially challenging. Since wireless channels are prone to possible transmission errors caused by either channel outages (which occur when the received signal strength drops below a critical threshold) and/or interference, the real-time and reliability requirements are more likely to be jeopardized than they would be over a wired channel. This is one of the key issues to be resolved in *wireless fieldbus systems*, or in general in the usage of wireless technologies in industrial applications, and the focus of this paper.

The goal of this paper is to give an overview of the problems and issues that arise when considering the use of standardized wireless technologies like IEEE 802.11, BT, or IEEE 802.15.4 in a fieldbus-controlled industrial network. The discussion of this topic takes the following structure. Section II considers the adverse effect that transmission errors and other properties of the wireless channel have on the timing and reliability of packet transmissions, irrespective of the specific wireless technology used. These effects can be (partially) compensated for by either designing robust and loss-tolerant applications/control algorithms or by trying to improve the channel quality when designing a wireless fieldbus protocol. We focus on taking the latter approach. Section III introduces the widely used wireless technologies of interest for use by fieldbus systems in industrial environments: BT [18], [19], IEEE 802.15.4 [20], [21], and IEEE 802.11 [15]. Given that users will most likely not want to simply throw out their functioning wired fieldbus installations in favor of wireless ones, Section IV discusses how wireless stations can be *integrated* into wired fieldbuses to create *hybrid wired/wireless fieldbus systems*. Conclusions are provided in Section V.

Besides the issues discussed in this paper, there are further issues to consider in wireless fieldbus systems. Two important ones are the following.

- *Security*: The wireless medium is an open medium and without countermeasures, it is easy for an attacker to eavesdrop, to insert malicious packets, or to simply jam the medium, this way challenging reliable and timely transmission. On the other hand, ensuring security goals like confidentiality or accountability was not the main focus in the design of many fieldbus systems [22], [23]. The recent trend to connect fieldbuses to the Internet by means of gateways has led to research toward securing the gateway [22], [24], but it is also required to protect a fieldbus against attacks from the inside, for example, by employing proper encryption and authentication schemes.
- *Energy supply and low power operation*: In some fieldbus systems, the same cable can be used for communication purposes as well as to supply a station with energy. If the cabling were to be dropped completely, alternative ways to supply stations with energy would have to be found. Some options are wireless energy transmission [25], [26], energy-scavenging methods [27], or using batteries. For battery-driven stations, energy is a scarce resource and should be used economically. Replacing batteries may be infeasible or can lead to machine downtimes. Several mechanisms to conserve energy in protocols and applications have been developed in the context of wireless (sensor) networks [28]–[30]. In the design of fieldbus protocols, however, the main concern was real-time communications, not energy efficiency. There are efforts to combine both targets [31].

Wireless fieldbus systems and wireless industrial networks have created interest in both academia and industry. The first publications date back to 1988 [32]. One of the earliest projects, the European Union OLCHFA project, started in June 1992 with the goal to provide wireless spread-spectrum transmission for the WorldFIP (formerly just FIP) fieldbus [33], [34]. Today, several companies and consortia are active, for example, the *wireless industrial networking alliance* (WINA).[1]

II. Fundamental Problems of Real-Time and Fieldbus Communication

This section introduces some of the fundamental properties of wireless transmission media, without referring to any wireless technology in particular (this is done in the following Section III). Given that there are a number of mature and commercially available (wired) fieldbus systems, the question is whether there are major difficulties when using them with wireless media. Some examples discussed in this section show that some protocols do indeed have difficulties. One particularly important problem is channel errors; channel errors can cause packets to miss their deadlines, for instance. Accordingly, not only are the consequences of errors of interest, but also the mechanisms that allow one to deal with them. Some of these mechanisms, which have been proposed specifically for fieldbus systems, will be discussed.

[1] See www.wina.org

A. Important Properties of Wireless Channels and Transceivers

1) Path Loss: The signal strength of a radio signal decreases with the distance between a transmitter and a receiver. This decrease is known as *path loss*. The magnitude of the path loss depends on several parameters, including the antenna technology, the frequencies used, and the environmental conditions that are present. An often-used approximation of path loss is the log-distance model. In this model, the received signal strength P_r at a distance d behaves as $P_r(d) \sim P_t \cdot (d_0/d)^\gamma$ for distances d larger than a reference distance d_0 and a radiated signal strength P_t. The reference distance depends on the antenna technology. The so-called *path-loss exponent* γ typically assumes values between two (free-space path loss) and six [35, Ch. 4], depending on the environment. In factory environments, path loss exponents between two and three have been observed [35, Table 4.2], [36], but sometimes values smaller than two can occur as well [37].

2) Half-Duplex Operation of Transceivers: Wireless transceivers are not able to transmit and receive simultaneously on the same channel because their own signals would drown all signals from any other stations. Because of this fact, most wireless transceivers are half-duplex. They inhibit simultaneous transmit and receive operations while allowing the same circuity to be shared, thus reducing the transceiver complexity. The primary disadvantage of this approach is the time loss experienced from explicit receive–transmit turnovers.

3) Physical Layer Overheads: To let the receiver of a packet acquire carrier-/bit-synchronization despite a noisy channel, most wireless systems use extra *training sequences* of well-known symbols. When the training sequence occurs at the beginning of a packet, it is called a *preamble*. For example, the IEEE 802.11 physical layer with direct sequence spread spectrum (DSSS) requires preambles of 128-μs length [15], transmitted with every packet.

Such physical layer overheads tend to be much smaller on wired transmission media.

4) Channel Errors: A wireless transmitter propagates waveforms into multiple spatial directions at the same time. These waveforms can be subject to reflections, diffraction, or scattering [35]. As a result, multiple copies of the same waveform can reach the receiver after following different paths with different relative lengths and different travel times (time dispersion). A common measure for such time dispersion is the *rms delay spread* (root mean square), or simply delay spread for short.[2] The time dispersion has two important consequences:

- With *small-scale or multipath fading* [35, Ch. 5], multiple copies can interfere constructively or destructively at the receiver. If a station (transmitter/receiver) or parts of the environment are allowed to move, the composite signal at the receiver alternates between constructive and destructive interference, leading to comparably fast fluctuations in received signal strength (*time variance*). In the case of destructive interference, the channel is often said to be in a *deep fade*, and many errors occur during the decoding of channel symbols. When the duration of a deep fade spans several consecutive channel symbols, symbol/bit errors will begin to appear in *bursts*.
- *Intersymbol interference (ISI)*: When the time dispersion is large, it can happen that waveforms belonging to different symbols overlap at the receiver. In the case of such ISI, particular effort is necessary to reconstruct the original symbol.

There are further distortions to wireless waveforms, including cochannel interference and adjacent channel interference from colocated wireless communication systems, thermal and man-made noise, as well as Doppler shifts [35], [38], [39]. In industrial environments, significant noise as well as distortion of transceiver circuitry can also be created by strong motors, static frequency changers, electrical discharge devices, and more. Measurements of some key wireless channel characteristics in industrial environments [36], [37], [40]–[44] have shown that the delay spread can reach values larger than 200 ns. Modulation schemes with symbol rates of several megabauds might then be subject to severe ISI.

These phenomena translate into bit errors and packet losses, with possible delays if packets need to be retransmitted. Packet losses occur when, for example, the receiver of a packet fails to acquire carrier synchronization or bit synchronization, whereas bit errors refer to errors caused by flipped bits after synchronization has already been successfully achieved [45]. The error characteristics shown by the wireless channel depend on the propagation environment, the chosen modulation scheme, the transmit power, the frequency in use, as well as many other parameters. In general, however, systems tend to show time-variable and sometimes quite high error rates.

The following description gives an example of how severe such a situation might be. Measurements in an industrial environment with an IEEE 802.11b-compliant chipset have shown that short-term bit error rates in the order of $10^{-4} \ldots 10^{-2}$ can be reached for a 2-Mb/s quaternary phase shift keying (QPSK) modulation [45]. Additionally, there are minute-long periods where packet loss rates of at least 10% (and sometimes up to 80%) have been observed. Also, bit errors and packet losses are "bursty", i.e., they occur in clusters with error-free periods ("runs") between the clusters. Naturally, these results are particular for the specific chipset and environment, but similar trends have also been observed in other wireless measurement studies [46]–[49].

B. Some Consequences of Channel Properties

1) Consistency Problems: When a system uses the producer–distributor–consumer communication model, like the WorldFIP [11], [12] fieldbus does, communication is based

[2] The rms delay spread is obtained from the channel impulse response by measuring the excess delays and received signal strengths of the second and subsequent received pulses relative to the time instant where the receiver gets the first pulse. The rms delay spread is the standard deviation of the weighted (by signal strengths) excess delays.

on unacknowledged broadcasts of data identifiers (by the distributor), to which the station possessing the identified data item (the *producer*) broadcasts its actual value.[3] All *consumers* interested in this data can copy the received value into an internal link-layer buffer for their applications. To achieve *spatial consistency* among a set of k consumers, it is required that *each* of these k consumers receive the data value. Spatial consistency is required, for example, when k distinct controllers work on the same physical process. Failure to reach spatial consistency might lead to inconsistent control decisions among the controllers. Such spatial inconsistency could occur, for example, if packets happen to be lost.

As an example, assume that the wireless channel is such that for every transmitter–receiver pair a packet is corrupted independently with a certain probability p. When the producer has received the identifier and broadcasts the data value, reaching spatial consistency requires that *all* k consumers receive the data packet, which happens with probability $(1-p)^k$. As a numerical example: with $p = 0.2$ spatial consistency between $k = 4$ consumers is reached with only ≈41% probability.

Another often-found requirement is *relative temporal consistency*. Consider, for example, a set of k sensors sampling a physical process. To achieve relative temporal consistency, all the sensors must sample the process within the same prespecified time window. Some fieldbus systems, such as the PROFIBUS DP [9], [10], use a broadcast-based approach to promote this kind of consistency. A controller broadcasts a special control packet called FREEZE, which causes sensors to sample their environment immediately and to buffer this value for later retrieval. Under the same assumptions as above, reaching relative temporal consistency among k sensors happens only with probability $(1-p)^k$.

2) Problems for Token-Passing Protocols: Fieldbus systems like the PROFIBUS [9], [10] rely on distributed token passing in order to circulate the right to initiate transmissions between a number of controllers (called master stations in PROFIBUS). The master stations are arranged in a *logical ring* on top of a broadcast medium. It is shown in [50] and [51] for PROFIBUS and in [52] for the similar IEEE 802.4 token bus [53] that repeated losses of token packets are a severe problem for the stability of the logical ring (*ring stability*). When a trial to pass the token from x to y fails, x is required to run the next trial *immediately*. In case of bursty channels, however, it might well happen that the channel between x and y is currently in a deep fade and will stay there for some time. This deep fade could potentially render all successive trials for passing the token useless, causing y to become lost from the ring. A master station y which has been lost from the ring has no transmit opportunities until it has been explicitly reincluded by another master. This reinclusion can take multiple token circulations, and packets arriving at master station y in the meantime will incur any corresponding delays. These delay problems are much less pronounced when nonbursty channels having the same average packet error rate are considered. Token passing protocols thus serve as an example for the fact that it is often not only the raw presence of bit errors that is important, but also the characteristics (bursty versus nonbursty) of the errors as well.

Another problem with token-passing protocols is that the station passing a token and its successor in the logical ring must be in mutual range. This stipulation cannot always be guaranteed when stations are mobile. The fieldbus protocols based on token passing have no provisions to deal with mobility, and appropriate mechanisms have to be added [54].

3) Problems for Carrier-Sense Multiple Access (CSMA)-Based Protocols: Fieldbus systems like CAN [13], [14] use CSMA-based protocols where collisions are possible. In general, CSMA-based protocols [55] work in a distributed fashion, where a station A wishing to transmit first needs to sense the transmission medium. If the medium is determined to be idle, the station starts to transmit. The many CSMA variants that exist differ in what happens when sensing the medium busy. In the option chosen for the CAN fieldbus, a station A wishing to transmit waits for the end of the ongoing transmission and starts its own packet immediately after it. Since another station B might do so as well, collisions can occur. The (wired) CAN protocol is based on a deterministic mechanism to *resolve* this contention. This mechanism is difficult to use for wireless media. It relies on a station's ability to transmit and receive simultaneously on the same channel, which is impossible with half-duplex wireless transceivers.[4]

Receivers need a minimum received signal strength in order to successfully decode packets or determine that another station is currently transmitting (carrier sensing). Due to path loss, the minimal signal strength required is not reached once the distance between transmitter and receiver becomes too large. Accordingly, carrier-sensing operations may fail, giving rise to the *hidden terminal problem* [58], from which all CSMA-based protocols suffer. Consider three stations A, B, and C, arranged such that A and C cannot sense each other's transmissions, but station B can receive signals from both A and C (Fig. 1). Station A currently transmits a packet to B. Station C wants to do the same, performs carrier sensing, and finds an idle channel because it is out of A's range. As a consequence, station C starts transmitting as well, and both A and C's packets collide at B.

Several solutions, such as the busy tone solutions [58], have been suggested for solving the hidden terminal problem. The most widely used approach today, however,

[3] In the producer–distributor–consumer communication model, *data* is identified instead of stations. A second common communication model used in fieldbuses is the master–slave scheme, as implemented, for example, in PROFIBUS [9]. In this scheme communication happens between addressable stations. The master needs to know the address of the station (slave) possessing a data item. It directs a request to the slave, and the slave has to respond to this immediately. Slaves do not initiate transmissions by their own.

[4] The ultimate goal of CAN's contention resolution procedure is to ensure that the station with the highest priority packet wins contention. Such a feature is implementable on wireless channels, but different mechanisms have to be used (for example, [56], [57]). An additional problem to be solved is that of hidden terminal situations: how to make sure that two stations out of mutual range agree on which one has the highest priority packet?

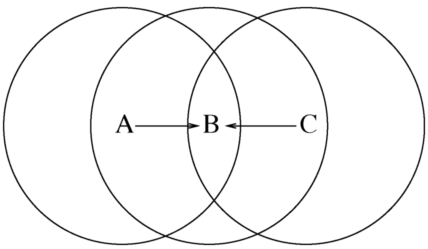

Fig. 1. Example scenario for hidden terminal problem; circles indicate transmission/sensing range.

is the RTS/CTS handshake adopted by the IEEE 802.11 standard [15]. In this scheme, station A starts its packet exchange with B using a short control packet called request-to-send (RTS). Station B answers with a clear-to-send (CTS) packet. Only upon receiving the RTS does station A continue with sending the data packet. Any other station receiving an RTS or CTS packet not destined for it must remain quiet for the time indicated in the RTS/CTS packets in order to avoid distortion of ongoing packet exchanges.

The problem with the RTS/CTS handshake in the context of fieldbus systems is that the majority of all packets are very small. Most packets are on the order of a few bytes, and data packets themselves are thus only slightly larger than RTS or CTS packets. Hence, the RTS/CTS handshake creates *significant* overhead. Sometimes it may be possible to avoid hidden terminal situations (and the RTS/CTS handshake) by careful reconsideration of the placement of stations. Another approach is to simply not use RTS/CTS and take the risk of having hidden terminal situations, while reducing its probability by cutting down the time needed to transmit a packet, but doing so requires an increase in the bitrate. This approach is feasible under certain conditions. Industrial applications often require only moderate bitrates in the order of hundreds of kilobits per second or a few megabits per second (CAN has 1 Mb/s as maximum rate). Current wireless technologies, however, offer bitrates in the order of tens of megabits per second (see Section III). Depending on the amount of physical layer overhead (for example, preambles) introduced in wireless technologies, multiple wireless packets can be transmitted in the time needed to transmit one packet on a wired fieldbus.

C. Mechanisms to Deal With Channel Errors

Even when problems like hidden terminal situations either do not occur at all or can be somehow circumvented, the problems created by channel errors remain. Many mechanisms have been developed in the past to make data transmission over wireless channels more robust against the multitude of possible impairments. It depends on the fieldbus system and communication model which of these mechanisms are applicable.

Fieldbus systems working according to the producer–distributor–consumer model make extensive use of broadcasting. There are no retransmissions, and, in general, the transmitter has no way to verify that deadlines are met. Techniques where no feedback from the receiver to the transmitter is given, are known as *open-loop techniques*. One useful approach is the forward error correction (FEC) coding [59]. In FEC schemes, the transmitter adds redundant bits to the packet which allow the receiver to correct bit errors if there are not too many of them. The ratio of user bits to the overall number of bits after encoding (user bits plus overhead bits) is called the *code rate*. Roughly, the smaller the code rate, the higher the overhead and the better the error correction capabilities. The rate of uncorrectable bit errors depends on the channel bit error rate and the distribution of errors. One example is provided by BT (see Section III-A). The interference created in situations where multiple piconets overlap leads to “almost binary” channels. Such a channel alternates between excellent and very bad states. During excellent states, the overhead of FEC is not needed, while at the same time the FEC may not be strong enough to correct all errors in the bad state and the FEC overhead is not useful.

There are many other options for increasing robustness that do not require feedback (open-loop mechanisms). Take for example: 1) using multipath- and interference-resistant modulation schemes such as orthogonal frequency division multiplexing (OFDM) [60] or spread spectrum modulation [61], [62]; 2) transmitting a packet not only once but multiple times; or 3) optimizing unit placement and the number of infrastructure equipment required [such as access points (APs)] [63], [64].

Some fieldbus systems, such as PROFIBUS, use retransmissions, and can give a transmitter some control of whether deadlines are met or not. Protocols where the transmitter receives feedback from the receiver and performs retransmissions when necessary, are commonly called automatic repeat request (ARQ) protocols [65]. Because of the receiver giving feedback, they can also be classified as *closed-loop techniques*. Retransmissions are useful when stringent reliability requirements have to be met that cannot be reached by open-loop techniques alone (example: important alarm packets). Furthermore, in contrast to open-loop FEC coding, ARQ protocols produce overhead only when it is needed to combat errors. During good channel periods, there are no retransmissions and the overhead of ARQ protocols is minimal. The available number of retransmissions, however, is naturally bounded by packet deadlines. All the time the transmitter spends for retransmitting one packet is taken away from the deadlines of other packets waiting to transmit. The quest in protocol design is, therefore, to find a good scheme that improves the delivery reliability within a given deadline.

In the following section, we discuss selected open-loop and closed-loop protocol mechanisms. These mechanisms have been proposed in the context of wireless fieldbus systems and wireless real-time communications.

1) Exploiting Spatial Diversity: As has been explained, due to multipath fading, the received signal strength is likely to change between receivers at different locations. Consider two receivers r and s, which are the same distance away from a transmitter. If r and s are relatively close to each other, the probability that r and s experience a deep fade *at the same time* is higher than if their distance is larger than the so-called *coherence distance*.[5] The channel behavior is thus space dependent, and this *spatial diversity* can be exploited in a number of ways.

Receive diversity is an open-loop technique [66] where the receiver is equipped with multiple antennas. The spacing of these antennas should take the anticipated coherence distance into account. When the signal received by one antenna is in a deep fade, it can happen that the signal is good enough for proper reception at another antenna if the antenna distance is large enough. The receiver is able to switch between the antennas and can, for example, choose the one giving the strongest signal.

In *transmit diversity* schemes, the transmitter uses multiple antennas. There are transmit diversity schemes working on the level of individual channel symbols (for example, [67]). When commercially available wireless network adapters are to be used, transmit diversity schemes working on the level of whole packets become more interesting.

In the closed-loop scheme discussed in [68], the transmitter switches transmit antennas only in the case of packet retransmissions. The first trial of a packet transmission is on antenna one, the first retransmission on antenna two, the second retransmission on antenna three and so forth, in a round-robin fashion. This approach is based on the assumption that, for bursty channel errors, it is better to switch to a spatially different channel than to retransmit over the same channel and possibly encounter the same error burst as the one hitting the original packet.

Sometimes, for reasons of cost or small form factors, it is not possible to equip stations with multiple antennas. One alternative approach to achieve spatial diversity in the transmission process is to let *other* stations help with retransmissions of packets [50]. When station A fails to transmit a packet to station C, another station B might have picked up the packet and perform the retransmission on behalf of A. To avoid the required coordination between different possible helpers $B_1, B_2, \ldots$, the role of B might be confined to a dedicated station. Such schemes provide a kind of *cooperative diversity* [69].

The approaches to exploit spatial diversity in retransmissions have been shown to be effective in reducing the probability of deadlines being missed [50], [68]. They work best, however, when the spatial channels are independent/uncorrelated. This is a reasonable assumption to make, when multipath fading is the dominant source of channel errors. When the receiving node is placed close to an interference source, however, switching transmit antennas would most likely not be helpful because all spatial channels would be affected.

2) Hybrid ARQ Schemes: In hybrid ARQ schemes, retransmissions and error-correction coding (FEC) can be combined in different ways [70]. In the simple type-I hybrid ARQ, all packets are FEC encoded and always use the same code. When the receiver cannot correct all bit errors, it drops the packet and requests a retransmission (up to a maximum number of trials per packet). In type-II hybrid ARQ, the receiver does not simply drop erroneous packets but seeks to use the information contained in these erroneous copies to help in the decoding of further retransmissions. A simple example of a type-II ARQ scheme is bit-by-bit majority voting: once the receiver has received at least three erroneous versions of the same packet, it can guess what the received packet should be by subsequently applying a majority voting procedure to all bits from previous trials. In [71], this method is varied by including the deadline and desired delivery probability (see also [72]) in the choice of the actual coding schemes. Majority voting is the last resort when no correct copy has been received before the deadline. Other schemes are discussed, for example, in [73] and [74].

A deadline-aware type-II ARQ scheme ("deadline-dependent coding") is presented in [75]. The transmitter maps the deadline for a packet and its desired delivery probability to one of several FEC coding methods, creating a number of overhead bits for the data. On the occasion that a retransmission must occur, the transmitter does not repeat the user data but rather sends more of the overhead bits. Such an approach is called *incremental redundancy*.

In the strategy presented in [76], the coding method is chosen based on how far away the deadline is. The closer the deadline comes, the stronger the chosen coding method (requiring more overhead bits) becomes. This approach includes, as a "special" coding method, the decision to defer a retransmission for a while. Such a postponing may avoid situations where energy and bandwidth are wasted when transmitting a packet during a deep fade on a bursty channel.

Instead of changing the coding method that is used, the transmitter can also adapt the modulation scheme (see [77] with a joint consideration for deadlines and energy consumption) or increase the transmit power as the deadline comes closer.

3) An Application Layer Mechanism: Sometimes it may not be possible for the lower layers to correct all channel errors. For important asynchronous events, like alarms, this restriction is intolerable, For periodic data sampling of a slowly varying, continuous process, one can simply accept occasional losses or try to *conceal* them. One can, for example, replace missing samples at the receiver by an *estimated* value. In [78], a scheme is proposed where the receiver estimates missing values on the basis of Kalman filters. It is demonstrated that by this technique certain signal classes need only 5 out of 100 samples to be able to reconstruct the original signal with good quality, and can be applied at the application layer.

D. Discussion

The wireless channel is a difficult environment. Some of the existing fieldbus protocols face serious degradations in their achievable deadlines when dealing with bursty channels (compare the token-passing example from Section II-B2). Other protocols, on the other hand, are not directly implementable at all. One example is the method used in

[5] This *coherence distance* depends, among other parameters, on the antenna type and the propagation environment [35, Sec. 5.8.5], [66]. When multipath components can arrive from every direction, for example, a spacing between half a wavelength and a full wavelength is sufficient to achieve diversity gains (compare [66]).

the CSMA-based CAN protocol for resolving contention between stations.

The wireless channel should influence the design of industrial applications. The fault assumptions, for example, are different in wireless channels than in wired channels [72]. It is likely that errors occur more often on wireless channels than on wired ones. Transmission errors on wireless channels, however, tend to be transient (deep fades end at some time and the channel becomes good again), whereas errors on wired channels are often of permanent nature, due to faulty cables, connectors, or other hardware components.

Note that for some applications the rate of residual errors (*after* applying any countermeasures) has to be kept at extremely low levels. "Fly-by-wireless" systems in aircrafts, for example, might require residual error rates of 10^{-19} [72]. New protocol mechanisms or the combination of existing protocol mechanisms are needed to achieve such low levels of residual error rates. Even if these levels become achievable, it will likely require a tremendous amount of design effort. To reduce this effort, it is helpful to relax the requirements posed to the communication system. This can be achieved, for example, by designing industrial applications that can tolerate a certain percentage of packet losses or deadline misses. This line of research is pursued in the area of networked control systems [79]–[81].

III. Review of Wireless Technologies for Industrial Automation

For the various reasons listed at the beginning of the introduction, wireless technologies might be of advantage in industrial environments. Due to the general tendency toward standardization and the fact that cheap, commercial-of-the-shelf (COTS) wireless technologies are available, it seems only logical to investigate these for their suitability in industrial deployment. Of particular interest for industrial environments are technologies that do not require any sort of frequency licensing. These technologies include the WPAN technologies such as IEEE 802.15.1/BT and IEEE 802.15.4/ZigBee as well as the WLAN technologies from the IEEE 802.11 family.

Despite the advantages a single wireless network might offer on the factory floor, it will be often required to run multiple WLAN/WPAN networks in parallel in different or overlapping regions of the plant. Because of this fact, the coexistence of multiple networks of either the same or varying types needs to be investigated. We consider how certain communication patterns typical to those of fieldbus systems can be implemented within such overlapping networks.

A. BT Technology/IEEE 802.15.1

BT was originally designed as a cable replacement technology aimed at providing effortless wireless connectivity for consumer devices in an *ad hoc* fashion [82]–[86]. In order to allow for deployment almost worldwide, the BT Special Interest Group (SIG) placed the technology in the unlicensed industrial, scientific, and medical (ISM) band at 2.4 GHz. By designing a comparably straightforward system, the designers of BT intended for it to have widespread use.

BT networks are organized into "piconets" in which a "master" unit coordinates the traffic to and from up to seven active "slave" units. The master unit originates the request for a connection setup. Within a single piconet, the various slave units can only communicate with each other via the master. Nevertheless, every BT unit can be a member of up to four different piconets simultaneously (though it can be master in only one of them). A formation in which several piconets are interlinked in such a manner is called a scatternet. Up till now, the role of scatternets is still relatively limited. Some of the specific problems seen within scatternets are discussed in [87].

Piconet traffic is strictly organized into a time-division multiple access (TDMA)/duplex scheme [88]. In this scheme, the master is only allowed to start transmitting in odd-numbered time slots (each slot is 625 μs long), while slaves can only respond in even-numbered slots after having been polled by a master packet.

Because there is no coordination between different piconets, packet collisions may occur if two piconets are located near one another. To minimize this collision effect as well as to cope with the fact that frequencies used by other devices on the radio channel can vary significantly over the bandwidth of the 2.4-GHz ISM band, every piconet performs a rather fast frequency hopping (FH) scheme over 79 carries of 1-MHz bandwidth each. The maximum hopping frequency of this scheme is set at 1.6 kHz (corresponding to the slot length of 625 μs) and the hop sequence used by each individual piconet is derived from the unique address of its master using a specified algorithm. For each BT packet sent, a new frequency is chosen to send it over. In BT version 1.2, an adaptive FH scheme (AFH) has been introduced which allows for the exclusion of certain carriers once it has been noted that packet corruption occurs at that carrier's frequency. It must be noted, however, that AFH is used more as a means to improve the performance of a BT piconet in the presence of other nonhopping systems in the 2.4-GHz ISM band (see also Section III-D) than a way to improve the performance among coexisting BT piconets.

On the physical layer (PHY), data is Gaussian frequency shift keying (GFSK) modulated at 1 M/s and transmitted with a power of 0 dBm (1 mW). With such a transmit power, BT devices can expect to have up to a nominal range of about 10 m. BT can also be used with up to 20-dBm transmit power. Transmitting at such high power results in a larger range, but requires implementing power control to fulfill the sharing rules of the ISM band.

On the data link layer, a distinction is made between asynchronous connectionless (ACL) and synchronous connection-oriented (SCO) packets: ACL links secure reliable data transmission with an ARQ scheme that initiates the retransmission of a packet in case the evaluation of the included cyclic redundancy check (CRC) shows inconsistencies. Six different types of ACL packets exist and can occupy either one, three, or five BT time slots, depending on which type is being used. Three of the ACL packet types include uncoded payloads, while the other three have payloads that are protected by rate-2/3 (code rate) FEC that uses a shortened Hamming block code of length 15 or 10 without any interleaving. The uncoded ACL-packet types are knowns as DH1, DH2, and DH3, while the three coded ones are known as DM1, DM3, and DM5. Using packets of type DH5 for data and DH1 for acknowledgment gives the maximum possible (unidirectional) throughput for BT at 723 kb/s.

SCO links, in contrast, support real-time traffic by reserving time slots at periodic intervals. Retransmissions are not allowed with these types of links, but in BT version 1.2/2.0, "extended" SCO links have been introduced where a limited number of retransmissions can be made. The three different types of SCO packets all have the same length and require a time of 366 μs for transmission. They typically transport 64 kb/s of continuous variable slope delta (CVSD)-encoded speech [89] and are differentiated by having either unproteced payloads, rate-2/3 FEC encoded payloads, or rate-1/3 FEC encoded payloads. These packet types are known as HV3, HV2, and HV1, respectively. The extended SCO link is very flexible, supporting various transmission rates. Lost SCO packets can be replaced by an erasure pattern.

Because of the short range of BT and the small number of slaves that are active at any given time, several independent BT piconets will most likely coexist on a factory floor. With the help of radio network simulations, BT–BT coexistence results have been presented in [90]–[92]. These simulations took traffic, spatial node distribution, fading models, as well as co- and adjacent channel effects into consideration. Some of the results of these simulations have also been verified in a radio network testbed [93], making them, therefore, more detailed than a purely theoretical approach.

The results have been obtained for an area of 10×20 m^2, assuming an average master–slave distance of 2 m. Even though a factory floor generally is significantly larger, it is reasonable to assume that the performance depends only on the node density and not on the absolute numbers of nodes or the area covered. The considered area of 10×20 m^2 supports either 30 simultaneous, 1/3 loaded SCO connections with an average packet loss rate of 1% or 100 (!) simultaneous WWW sessions (bursty traffic with an *average* data rate of 33.2 kb/s each) with a degradation of the aggregate throughput of only 5%. With 50 fully functional piconets in the area, a maximum aggregate throughput of 18 Mb/s can be expected when each individual piconet transmits at an average unidirectional data rate of 360 kb/s.

Furthermore, the results show that in the interference scenarios the provided FEC methods are unsuitable to handle the almost binary character of the transmission channel. When two overlapping piconets operate on different frequencies, the signal quality is good, but when they hop to the same frequency, packets can be destroyed beyond recognition. When using no coding method at all (as is the case with HV3, DH1, DH2, and DH3), the power consumed by the network as well as the overall load of the network is reduced. In order to obtain a good throughput and have low interference, it is disadvantageous to use short packet types. This fact is unfortunate because short packets are typically used in industrial applications. In fact, it is very hard to set up a scenario in which any other packet type yields a larger throughput than that of DH5 [92].

These results present a basis on which the suitability of using BT technology for specific applications in a specific industrial environment can be investigated.

Security is supported in BT by the specification of authentication and encryption.

The most recent development for BT is BT version 2.0 [94]. BT version 2.0 has enhanced data rates using $\pi/4$-DQPSK and 8DPSK modulation schemes in addition to the traditional GFSK modulation scheme. The transmission rate resulting from these enhancements is about three times faster than it was in previous versions of BT.

B. IEEE 802.15.4

The IEEE 802.15.4 standard [20] was finalized in October 2003 and specifies the characteristics of the physical layer and the MAC layer of a radio networking stack.[6] The goal of this standard was to create a very low cost, very low power, two-way wireless communication solution that meets the unique requirements of sensors and control devices [20], [21]. In contrast to BT and IEEE 802.11, IEEE 802.15.4 has been specifically developed for use with applications in which a static network exists that has many infrequently used devices that transmit only small data packets. Such applications are exactly what many industrial environments would require.

In order to encourage widespread deployment, IEEE 802.15.4 has been placed in unlicensed frequency bands. When using the 2.4-GHz ISM band, IEEE 802.15.4 systems can get the same sort of global deployment as BT and IEEE 802.11b/g systems. The IEEE 802.15.4 standard has also been specified for use in the 868-MHz ISM band in Europe and in the 915-MHz ISM band in North America. Within these bands, DSSS is used in order to comply with the respective sharing rules of each band as well as to allow for simple analog circuitry to be used. The maximum data rate of the DSSS is 250 kb/s in a single channel within the 2.4-GHz band. In total, the 2.4-GHz band accommodates 16 such channels. In the 868-MHz ISM band, one channel with a data rate of 20 kb/s is available, whereas in the 915-MHz band, ten channels of 40 kb/s each can be used. Because of various system parameters, especially the MAC protocol that is in use, the maximum user data rate will most likely be about half of its nominal value, or less. If upper layers detect a throughput degradation while using a specific channel within the used frequency band, IEEE 802.15.4 can scan the frequency band for a channel that promises better perfomance values and switch to that channel [95] (unless transmitting in the 868-MHz band).

[6] There is sometimes confusion between IEEE 802.15.4 and ZigBee. The ZigBee alliance (see http://www.zigbee.org) is a consortium driven by industry and research institutions. It finalized the ZigBee specification in December 2004 and describes higher layer protocols (networking, application) that operate *on top* of IEEE 802.15.4.

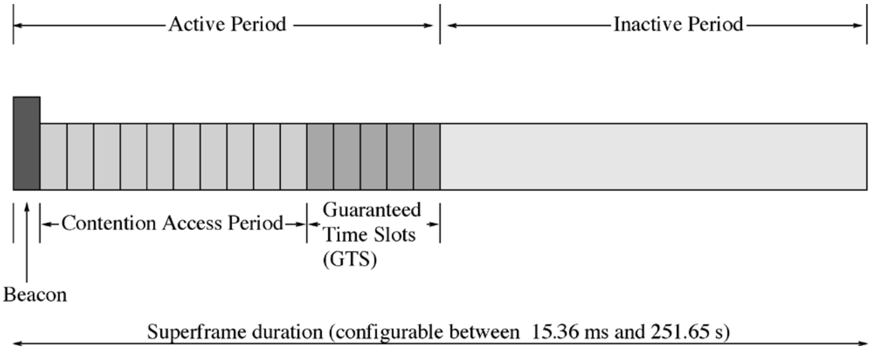
Active Period
Inactive Period
Contention Access Period
Guaranteed Time Slots (GTS)
Beacon
Superframe duration (configurable between 15.36 ms and 251.65 s)

Fig. 2. Superframe structure for IEEE 802.15.4 beaconed mode.

The IEEE 802.15.4 standard differentiates between two different kinds of devices. A *full-function device* (FFD) can become a network coordinator and can work with other FFDs in a peer-to-peer fashion. *Reduced-function devices* (RFD), on the other hand, are always associated with one of these FFDs and are limited to exchanging data with this device alone. Among RFDs there is no peer-to-peer communication possible. All devices have a 64-b address, but it is possible for RFDs to obtain a 16-b shorthand address from their coordinator FFD.

With respect to the MAC protocol used by the IEEE 802.15.4 standard, there are two different modes of operation. In *unbeaconed mode*, all stations use an unslotted CSMA variant. Here, a station initiating transmission of a packet does not perform carrier sensing immediately, but introduces a random waiting time, called a *backoff time*. Having such a backoff time facilitates the avoidance of collisions. In *beaconed mode* (see Fig. 2), the network coordinator imposes a *superframe structure*. The coordinator transmits beacons periodically, choosing one of a number of configurable periods between 15.36 ms and 251.65 s. The remaining superframe starts with the *contention-access period*, in which the RFDs access the medium according to a slotted CSMA-CA variant, which incurs more overhead than the unslotted variant. An optional contention free period is available, where the network coordinator allocates guaranteed time slots (GTSs) to individual RFDs for either uplink data or downlink data. In addition to these two modes of operation, an *inactive period* of operation exists. During this period, all nodes including the coordinator in the network are put to sleep in order to conserve energy.

Data packets are acknowledged and the protocol supports retransmissions, but there is no FEC coding. In the beaconed mode, the throughput is smaller than in the unbeaconed mode, in which no beacon frames exist and the unslotted CSMA variant has less overhead. Under the conditions investigated in [96], the maximum user data rate when running in the 2.4-GHz ISM band is 38 kb/s with one source, and up to 70 kbs when multiple sources are present. These observed data rates are, in fact, quite small.

Similar to BT, IEEE 802.15.4 uses low transmit power levels. In addition to this, IEEE 802.15.4 also uses very short symbol rates (up to 62.5 ksymbols/s), allowing the increased delay spread found in industrial plants not to cause a problem.

For security purposes, IEEE 802.15.4 provides authentication, encryption, and integrity service. The developer can choose between no security, an access control list, and a 32–128-b Advanced Encryption Standard (AES) encryption with authentication.

C. IEEE 802.11 Technologies

IEEE 802.11 is composed of a number of specifications that primarily define the physical and MAC layers of WLAN systems [15]–[17], [44], [97]. Similar to other standards from the IEEE 802.x series, the IEEE 802.11 MAC suggest the IEEE 802.2 logical link control (LLC) [98] as a standard interface to higher layers. Since IEEE 802.11 is a WLAN standard, its key intentions are to provide high throughput and a continuous network connection. Because of the focus on COTS technologies for wireless connections in industrial deployments, only the most common variations and extensions of IEEE 802.11 systems will be discussed here. These variations and extensions include the general 802.11 MAC, IEEE 802.11a, IEEE 802.11b, and IEEE 802.11g for physical layers, as well as relevant extensions in respect to network planning and QoS.

The main parameters of IEEE 802.11 a/b/g are the following.

- *IEEE 802.11a* [16] is placed in 5-GHz bands that are license exempt in Europe (5.15–5.35 GHz and 5.47–5.725 GHz) and unlicensed in the United States (UNII bands, 5.15–5.35 GHz and 5.725–5.825 GHz). Over the whole spectrum, this allows for 21 systems to be running in parallel in Europe and eight in the United States [99]. The IEEE 802.11a physical layer (PHY) is based on the multicarrier system orthogonal frequency-division multiplexing (OFDM) [60]. Seven modes are defined, ranging from BPSK modulation with rate-1/2 FEC and a 6-Mb/s data rate to 64-QAM modulation with rate-3/4 FEC and a 54-Mb/s data rate. The maximum user-visible rates depend on the packet sizes transmitted. In the 54-Mb/s mode, the transmission of Ethernet packets that are 1500 B long results in a maximum user rate of about 30 Mb/s, while sending packets with user payloads of just 60 B results in a throughput of 2.6 Mb/s [100]. The latter throughput value is the one of interest for industrial applications, as small packet sizes are dominant in fieldbus networks.

- *IEEE 802.11b* [17] is a high-rate extension to the original IEEE 802.11 DSSS mode and thus uses the 2.4-GHz ISM band. Although in principle either 11 or 13 different center frequencies can be used for the DSSS (depending on whether you are in the United States or in Europe), only three systems can actually operate in parallel. In addition to supporting the 1- and 2-Mb/s modulation rates of the basic IEEE 802.11 system, the payload of the IEEE 802.11b PHY allows for modulation with 5.5- and 11-Mb/s complementary code keying (CCK). The maximum user data rates are 7.11 Mb/s in the case of Ethernet packets and 0.75 Mb/s in the case of packets with user payloads of 60 B in length.
- *IEEE 802.11g* is an extension to the IEEE 802.11b specification and is consequently also placed in the 2.4-GHz band. It supports four different physical layers of which two are mandatory: the PHY that is identical to IEEE 802.11b and an OFDM PHY that uses the same modulation and coding combinations as IEEE 802.11a. Because of the different frequency band, the maximum user transmit rates are about 26 Mb/s for Ethernet packets and about 2 Mb/s for packets with user payloads of 60 B when using the 54-Mb/s modulation scheme.

It can be seen that when transmitting packets that contain small payloads (as is the case for most fieldbus systems), throughput values are significantly reduced. This reduction is due to the comparably large overhead of IEEE 802.11 packets and the different parameters present in the CSMA protocol [100]. In contrast to BT or IEEE 802.15.4, IEEE 802.11 has been specifically optimized to transmit large data files, therefore showing a suboptimal performance when the majority of data is made up of short control packets. Note that throughput values can decrease even more when additionally using higher layer protocols. Measurements for the throughput of TCP/IP traffic in Ethernet packets for the IEEE 802.11b specification, for example, have returned results of a 5-Mb/s maximum throughput [101], [102]. IEEE 802.11 employs immediate MAC-layer acknowledgment and retransmissions. These acknowledgment packets do not have to actually contend for the channel; instead, they have a reserved time slot that is only used upon the reception of a correctly received packet.

In principle, it is possible to have IEEE 802.11 ad hoc networks that consist solely of mobile stations (MSs). It is more likely, however, that IEEE 802.11 will be used in an infrastructure mode, whereby an AP relays all communications between stations and other networks. To organize the traffic on the radio link, the IEEE 802.11 MAC provides two coordination functions. The first of these coordination functions, the *distributed coordination function* (DCF), is mandatory and requires that all stations compete for the channel according to a CSMA-CA protocol. When the carrier-sense mechanism determines the channel to be free, a station may start to transmit. If the channel is sensed busy, the station awaits the end of the ongoing transmission, where the channel becomes idle again. At this instant, a random backoff timer is started. If the channel becomes busy before the timer expired, the timer freezes and restarts once the channel is idle again. If the timer expires and no other station has started transmission in the meantime, the station starts transmission. The contention window from which the backoff values are chosen increases exponentially after each failed trial to transmit a packet.

The basic CSMA-CA method can be enhanced with an optional RTS/CTS handshake to avoid hidden terminal situations. The user can control whether or not this handshake is used by configuring a threshold for frame sizes. If a frame size exceeds this threshold, then RTS/CTS will be used; otherwise, it will not. The second coordination function, *point coordination function* (PCF) [15], is not mandatory and is designed to provide time-bounded services by means of subdividing time into (variable-length) superframes which in turn are subdivided into a *contention-free period* (CFP) and a *contention period* (CP). Within the CFP, a polling scheme is used, while access is regulated according to the DCF during the CP. The use of PCF is not very widespread[7] and it has a reputation of being slightly inefficient [103], [104].

The IEEE 802.11 WLAN DCF was designed for "best effort" traffic like file transvers that is neither time critical nor periodic. The PCF has difficulties to provide periodic services due to superframe stretching (i.e., jitter in the start times of superframes) and foreshortened CFP's [103]. For better support of timing-sensitive transmissions, there is an ongoing activity—IEEE 802.11e—that extends the basic MAC protocol [105]–[107]. In IEEE 802.11e, the enhanced DCF (EDCF) is designed as an improvement over the DCF. The EDCF allows to assign different basic contention window durations according to the priority of a data packet, thus providing stochastic service differentiation (data packets with shorter basic contention windows are more probable to obtain channel access than those with longer ones). The PCF is improved upon with the introduction of the *hybrid coordination function* (HCF) that is not based directly on polling, but by which the hybrid coordinator assigns time slots to stations on an explicit basis. The stations can use these time slots as needed, but are restrained to the given time window. With this restriction, the possibility to achieve periodicity is significantly improved.

Because of the existence of (metal) obstacles and the comparably large transmit power of 20 dBm, the delay spread of a factory floor has to be looked at if IEEE 802.11 is to be used there. While the delay spread in homes and offices is assumed to be <50 and <100 ns respectively, it takes on values of 200–300 ns in a factory floor setting (the delay spread is much less severe in BT due to its much smaller transmit power and range). In the case of IEEE 802.11b, a conventional RAKE receiver supports (only) about 60-ns

[7] The PCF is more complex to implement than the DCF and the authors know of no implementation that supports it.

delay spread in 11 Mb/s mode and 200 ns in 5.5 Mb/s mode [108]. Nevertheless, more receiver algorithms with suitable robustness have recently come into existence [109], [110]. In case of IEEE 802.11a or g, the situation is better. Because of the guard interval between channel symbols inherent in the OFDM technology, delay spreads of several hundred nanoseconds can be supported easily without paying attention to the receiver algorithms implemented [108].

When considering the overall network performance and not just the individual link performance (the interference performance is discussed in Section III-D), the number of publications presenting well-founded results is limited. The existing ones, however, show that capacity is indeed an issue. The authors in [111] and [112] discuss how the aggregate throughput in a single network decreases with the number of users, due to either hidden or exposed terminal problems[8] or due to additional RTS/CTS overhead. With only ten stations [111] or a hidden node probability of 5% [112], the system throughput is approximately halved (!) in the case of 1500-B payloads (the smaller packet sizes typical in fieldbuses are even less efficient).

When installing IEEE 802.11a in a cellular fashion, the situation can be simplified. First of all, there is more bandwidth available in the 5-GHz band than in the 2.4 ISM band. Secondly, a decentralized channel selection algorithm has been standardized for IEEE 802.11a in IEEE 802.11h [99], organizing a number of spatially overlapping networks to choose nonoverlapping frequency bands. The most relevant parameter for WLAN frequency planning is the number of mobile terminals that have to be served. From this parameter, the optimum number of APs and distance between APs can be determined.

For security, IEEE 802.11 WLAN's support several authentication processes which are listed in the specification (none are mandatory).

D. Coexistence of Wireless Technologies

In the future, it will be standard for multiple wireless technologies to be used in a single environment. This is generally not a problem unless the technologies are placed in the same frequency band. As the previous sections indicated, the 2.4-GHz band hosts BT, IEEE 802.15.4, IEEE 802.11b, and possibly other systems. It is thus necessary to investigate the performance of coexisting networks and to introduce methods for reducing mutual disturbances between them.

CSMA is, in principle, a mechanism for improving the coexistence of multiple communication systems that use the same frequency band. In fact, the goal of the carrier-sensing operation is to avoid interfering with ongoing transmissions. It depends, however, on the actual implementation of the carrier-sensing mechanism whether transmissions of *other* types of wireless networks can be detected or not. In the IEEE 802.15.4 standard, for example, the user can choose between different carrier-sensing modes [20, Sec. 6.7.9]. In one of these modes, the carrier-sense circuitry indicates a busy medium when the received signal *energy* is above some threshold. It does not matter if the received signal comes from another IEEE 802.15.4 station, an IEEE 802.11 station, or any other device radiating in the same frequency band. In one of the other carrier-sensing modes, it is required that the received signal be decoded properly, i.e., use the right modulation scheme. In this mode, an IEEE 802.15.4 station can only detect ongoing transmissions from other IEEE 802.15.4 stations and not from, say, an IEEE 802.11 station.

The interference between BT and IEEE 802.11b has been investigated extensively [101], [102], [113]–[117]. In [118], it was found that IEEE 802.11b requires a carrier-to-interference ratio (CIR) of about 10 dB to cope with a (narrow-band) interference in its (wide) passband. Nevertheless, with IEEE 802.11a becoming more widely spread (especially in industrial environments) and the use of AFH for BT version 1.2, the interference situation is becoming much more relaxed. At least this is the case for frequency static systems like IEEE 802.11. An IEEE 802.11 system transmits on a fixed set of BT channels. When multiple AFH-enabled BT systems operate in parallel with an IEEE 802.11 network, all of the BT systems stop using any of the channels occupied by the IEEE 802.11 network. The BT systems now have to share the remaining channels. Since there are fewer available channels than in the case without an IEEE 802.11 network, the BT systems create more interference to each other.

Along with the introduction of AFH, another coexistence improvement has been made to BT. In BT version 1.0/1.1, the BT reverse link packet that contained the acknowledgment was transmitted on a different frequency than that of the forward link packet. In doing so, the loss probability in the case of a static interferer was increased because the reverse link might hop into the interfered band even if the forward link transmission was successful. With the BT version 1.2 AFH, forward and reverse link packets are now transmitted on the same frequency, and such a situation will not occur anymore.

If a BT system and an IEEE 802.11b system are so close together that the 20-dB higher transmition power of IEEE 802.11b blocks the BT receivers from receiving (when antennas are less than 20–30 cm apart), then only methods such as a joint scheduler can help to enable a fair coexistence [102].

Since IEEE 802.15.4 and IEEE 802.11b are frequency static and can be manually or automatically made to use different frequency bands, the authors of [95] have concluded that IEEE 802.15.4 will have little or no impact on IEEE 802.11b as long as some frequency management is deployed. Additionally, typical IEEE 802.15.4 applications are expected to have a low *duty cycle* between 0.1% and 1% (meaning that stations will transmit nothing for 99.9% or 99% of their time, respectively). Stations operating in this duty cycle range do not create significant interference to other networks.

E. Comparison of Wireless Systems

In the last few sections, we examined three different systems. All three systems have been designed for use in

[8] The hidden terminal problem has been discussed in Section II-B3. In the exposed terminal problem, station A wants to transmit a packet to station C. Station A senses an interferer B and refrains from transmission, even when B's signals do not reach C. A possible transmission is thus suppressed.

Table 1
Comparison of BT, IEEE 802.15.4, and IEEE 802.11 Technologies

	Bluetooth/IEEE 802.15.1	IEEE 802.15.4	IEEE 802.11a/b/g
Range	10 (50-100m)	10m	50-100m
Throughput max.	723 Kbit/s	≤ 125 Kbit/s	30.6 Mbit/s (Ethernet), 2.6 Mbit/s (60 bytes payload)
Power consumption	low	very low	medium
Periodic data	yes (depending on polling algorithm)	yes	DCF: no; PCF: yes (with some jitter); HCF: yes
Retransmissions	yes	yes	yes
FEC	available	no	no

different scenarios, thus offering various advantages and disadvantages over one another depending on their use. The 802.11 systems are suitable for transmitting large amounts of data. IEEE 802.15.4 is suitable when communication is infrequent, small packet sizes are used, and power consumption is an issue. BT fills the gap between these two by being able to transmit at medium data rates with a lower power consumption than IEEE 802.11 (see also Table 1).

Although all three systems can be used on the factory floor, none of them will be able to run at their nominal performance levels because of the adverse radio conditions that will be present. These conditions, such as frequency-selective fading or interference, are especially prevalent if the system is placed in the 2.4-GHz ISM band.

Note that the effects of Doppler shifts caused by mobility have not been considered. The velocity of moving entities on the factory floor is expected to be too small to matter (not more than 20 km/h; see [40], based on a user survey). Seamless connectivity of moving entities might require hand-over algorithms. While for IEEE 802.11 roaming is specified in IEEE 802.11f (though with some performance limits [119]), it is not covered in the specifications of BT and IEEE 802.15.4 (though not impossible to realize).

F. Implementation of Fieldbus Services

When wireless fieldbus systems are to be implemented with one of the COTS technologies discussed in this section, the fieldbus services and communication models have to be mapped to the services and interfaces offered by these systems. We discuss mapping approaches for two of these technologies: IEEE 802.11 with DCF, and BT.

1) IEEE 802.11 DCF: Even with problems like channel errors or hidden terminal situations taken aside, the IEEE 802.11 DCF lacks predictability due to its stochastic access mechanism with random backoff times and station contention.

One can eliminate contention by using a contention-free access mechanism such as polling[9] or token-passing *on top* of the IEEE 802.11 DCF. In the case of polling, for example, this can mean that a station starts to use the DCF access mechanism only after receiving a poll packet. It is important to consider whether the fieldbus packets should be embedded into unicast IEEE 802.11 packets or into broadcast IEEE 802.11 packets:

- In the case of broadcast packets, there is no RTS/CTS handshake, there are no ACK frames, and no MAC layer retransmissions are performed. Accordingly, the transmission of responses or the initiation of retransmissions have to be implemented in higher layers. From the perspective of the MAC layer, request and response packets are equivalent in the sense that the MAC entity has to contend for the channel in the same way for both types of packets. This contention includes the carrier-sensing operation. As a result, in the 802.11 DCF case, an acknowledgment or response packet might be delayed by interference or traffic from colocated systems, causing the round-trip time to become randomized. In fieldbus systems such as PROFIBUS [9], [10], on the other hand, response or acknowledgment packets are sent immediately, and no carrier sensing is required. In this type of system, the round-trip time is predictable.
- In the case of unicast packets, the RTS/CTS handshake can be switched off. All stations, however, generate ACK frames automatically and the MAC layer performs retransmissions. These ACK frames are not always useful. The PROFIBUS offers a mechanism, for example, where the responder can place answer data directly into its MAC layer acknowledgment packet. This answer data is fetched from a link-layer buffer, and it becomes the responsibility of the higher layers to write appropriate data to this buffer. Such an immediate acknowledgment carrying data is not possible in IEEE 802.11, however, since the ACK frames are always empty. To emulate this behavior, the responder must issue a separate data packet for the response data. The overall transaction thus includes two extra ACK packets.

The way in which the producer–distributor–consumer communication model ([120]; see also Section II-B1) can be implemented using the IEEE 802.11 DCF and the IEEE 802.2 Logical Link Control (LLC) [98] protocol is investigated in [121]. The LLC is a common link-layer protocol for the IEEE 802.x technologies.[10] An additional producer–consumer protocol (PCP) uses the services of the LLC to implement the producer–distributor–consumer mechanism. To query a data item, the distributor's PCP entity first

[9] The "standard" solution for polling with IEEE 802.11, PCF, has not found widespread deployment. When only DCF equipment is available, polling must be implemented separately.

[10] Together, the LLC and the different IEEE 802.x technologies cover the data link layer and the physical layer of the OSI reference model. The IEEE 802.x technologies provide the physical layer and the MAC sublayer, whereas the LLC provides the upper parts of the data link layer. It is composed of mechanisms for error control, connection management, as well as others.

broadcasts a packet containing the unique identifier of the data item. To achieve this broadcasting, the distributor PCP entity requests the unacknowledged connectionless service of the LLC. The LLC, in turn, maps this service request to an IEEE 802.11 MAC-layer broadcast and the packet is sent. When the MAC entity of any station y receives this packet, it passes it on to its own LLC entity, and then on to its PCP entity. If station y happens to be the producer, it gets the value of the data item. To send this data item, station y then invokes the unacknowledged connectionless LLC service, eventually resulting in a MAC layer broadcast. Any station receiving the data packet passes it on to its LLC entity and then on to its local PCP entity. A station not interested in this data item drops it.

Since this approach is based on IEEE 802.11 MAC layer broadcasts, the data production requests and the packets carrying the data items are not retransmitted. From the perspective of a consumer who is interested in updates of a particular data item, two things are necessary for a successful update: the producer must receive the production request, and the consumer must receive the broadcasted data item. The time between two updates of a data item at a consumer is called the *update time*. Even when the production requests have a perfectly constant spacing, channel errors will eventually turn this update time into a random variable.

In master–slave systems like PROFIBUS-DP, there is a master cyclically exchanging data with a number of slaves. Exchanging data means that the master can send data to the slave (for example, data that the slave should output to the physical environment) as well as receive input data from the slave. In addition, a slave might want to issue asynchronous alarm events (called diagnosis messages in PROFIBUS-DP) from time to time, in order to, for example, notify the master of unusual or dangerous conditions. If the slaves are set to be purely passive devices, they can only notify the master about this alarm whenever they are polled, by, for example, setting a special bit in the answer data packet.

Mechanisms to implement this behavior are considered in [122] for a monomaster scenario, using IEEE 802.11 DCF along with LLC. For cyclic polling of a slave, the master uses an acknowledged connectionless LLC service. In this service, the higher layers on a slave device can prepare answer data and place this into an LLC buffer. When the master sends its data packet, the LLC instance on the slave responds with the data stored in this buffer. The LLC data packets of both the master and the slave devices are mapped to IEEE 802.11 unicast packets. Since unicast packets are used, the MAC layer will send an ACK for every received data packet. As discussed above, the slave is not able to send the response data within the ACK frame, instead the whole channel access procedure must be invoked by the slave.

The handling of asynchronous alarm packets can be done in different ways. In [122], three methods are proposed.

- In the *late technique*, the master collects all alarm notifications during a cycle and handles them at the end of the cycle by separately polling each of the slaves in need.
- In the *current technique*, the slave *replaces* the cyclic answer data with the event data.
- In the *immediate technique*, the slave transmits the alarm packet by itself, without being polled. Since the standard DCF access procedure is used, the slave contends with ongoing cyclic exchanges.

Interesting performance metrics for such a system are the mean update time of a cyclically polled data item and the mean *alarm latency*. This alarm latency can be defined as the time between the occurence of an alarm at a slave and reception of the alarm packet at the master. For a simple channel error model that is loosing packets independently with a fixed probability p (varied between 0% and 10%), a fixed number of stations, and the assumption that at most one slave has an outstanding alarm at any time, it can be shown that all three techniques have similar mean update times. Also, the variance of the update times is close together. With respect to mean alarm latency, the "immediate" technique is much more advantageous than the "current" technique, which in turn is better than the "late" technique. The "immediate" technique is dangerous in alarm shower[11] situations, since not only do the alarms contend with the cyclic traffic, but they also contend with each other, causing collisions to be more likely to occur. These problems would be amplified in hidden terminal situations.

With respect to IEEE 802.11, it must be said that many proposals have been made to modify the physical and/or MAC layer to better support deterministic or stochastic real-time services [123]–[125]. Many of these proposals, however, necessitate modifications to existing networking equipment. While the upcoming IEEE 802.11e standard [105] offers promising features, further investigation is needed to fully exploit the possible mappings of fieldbus services to the features offered by this standard. One can only hope that 802.11e achieves better market penetration than PCF has.

2) BT: Due to its polling-based MAC approach, BT [19], [126], [127] can be an interesting candidate, when its inherent limitations (limited size of a piconet, moderate data rates) are acceptable. The usage of BT in industrial and fieldbus applications has been considered in a number of publications [128]–[131].

In [130], the implementation of the monomaster PROFIBUS-DP using the services offered by the BT L2CAP (LLC and Adaptation Protocol) is discussed. Both cyclic polling and delivery of alarm packets are supported. The L2CAP offers a feature similar to the acknowledged connectionless LLC service, by allowing the higher layers at a slave station to place a piece of data into an L2CAP buffer. When the slave is polled by the master (the poll packet can contain data), it answers in the very next time slot and includes the buffered response data in the answer packet. As opposed to IEEE 802.11 with DCF, the slaves' answer packet does not have to go through any channel access

[11] An exceptional situation in the physical process or in the operation of controllers leads to the generation of alarm messages. These messages may, as an aftereffect, lead to the generation of further alarm messages, and so on. Such a situation is called an alarm shower.

mechanism. The proposed implementation for delivery of alarm packets is similar to the "current" technique discussed above. The master polls all of its slaves in a cycle. When a poll packet fails, immediate retransmissions are performed. Two performance metrics are investigated for this: the mean alarm latency and the mean *cycle time*. Mean cycle time can be defined as the time between two successive polls of the same slave. Because of possible retransmissions, the actual cycle time is a random variable. For performance evaluation, it is assumed that the packet error rate between the master and a slave is constant. When all channels have the same packet error rate, both the average cycle time and the average alarm latency increase linearly with the number of slaves. When fixing the number of slaves, the average cycle time and alarm latency grow to infinity as the packet error rate increases.

In [131], hybrid configurations consisting of BT-based monomaster PROFIBUS-DP over the wireless medium, and either monomaster or multimaster Ethernet-based PROFIBUS-DP implementations on the wired medium are considered, and metrics such as cycle times and alarm delays are investigated. In [129], a cochannel interference model appropriate for multiple overlaid and unsynchronized piconets is developed and is used for deriving the packet error rate seen by one piconet. This error rate is used to derive probabilistic bounds on having a data/acknowledgment transaction miss a deadline.

IV. Hybrid Wired/Wireless Fieldbus Systems

In a hybrid wired/wireless fieldbus system, both *wired stations* (with transceivers being attached to a cable) and *wireless stations* (having wireless transceivers) should be able to communicate with each other.

In master–slave protocols, for example, a wired (wireless) master should be able to send a request to a wireless (wired) slave and get a response back. Often, there are legacy wired fieldbus systems running in a plant. The addition of wireless stations should not require any modifications to the protocols and applications running on these wired stations.

The wireless interconnection of wired stations by means of encapsulating bridges has been considered in [132]. The idea behind such an interconnection is to cut the cabling of a wired fieldbus system at some point and insert a wireless link between the two ends (cable replacement). This cable replacement is useful, for example, for placing a subset of a fully wired network on a mobile system, such as on a portal crane or a guided vehicle. Such approaches are not discussed further in this paper.

A *segment* is defined as a set of stations that are attached to a common medium, run the same protocols, agree on transmission parameters, and thus are able to directly communicate. A *wired segment* consists entirely of wired stations, while a *wireless segment* consists entirely of wireless stations. When two wireless segments overlap in space, they need to be separated by some means, for example, by the use of nonoverlapping frequencies.

Wired and wireless segments are coupled through the use of a single or multiple *coupling devices*. It is possible for these devices to work on different layers of the OSI reference model. The main classes of coupling devices in the realm of fieldbus systems are repeaters (working on the physical layer), bridges (working on the data link layer), and gateways (application level) [133]–[135].

For real-time communications, the delay introduced by these coupling devices is important. In repeaters and certain types of bridges, packets are forwarded from one segment to another with either no modifications to their contents or with only minor ones (for example, to translate between different addressing formats). Here, the *forwarding delay* can be defined as the time difference between the time instant at which the last bit of a packet is received on the input segment and the time instant at which the last bit of the packet was transmitted on the output segment. The forwarding delay depends on the type of the device and the actual implementation of the forwarding operation.

- In *cut-through forwarding*, the transmission of signals on the output segment can start before the packet has been fully received by the input segment.
- In *store-and-forward (S+F) forwarding*, the coupling device starts to generate signals at the output segment at some time after the whole packet has been received.

The origins and consequences of this forwarding delay are discussed in the following sections.

A. Cut-Through Forwarding

Cut-through forwarding is typically the mode of operation used by repeaters, but some types of bridges can also be made to work in this mode.

1) Origins of Forwarding Delay: Some of the factors which must be taken into consideration when designing cut-through devices include the following [136].

- The media can have different frame format requirements. In the IEEE 802.11 DSSS physical layer, for example, all frames are prepended with a 128-μs-long preamble and a 64-μs-long physical header, independent of any MAC protocol. In the PROFIBUS RS-485 physical layer, there is no preamble and no physical layer header. When a packet is to be forwarded from a PROFIBUS segment to an IEEE 802.11 DSSS wireless segment, the data bits that are received during preamble generation time must be buffered.
- The medium speeds may differ. Because of this difference, buffering is needed in both forwarding directions. In the case of forwarding from a faster medium to a slower one, data bits arrive faster than they can be output, and would get lost without buffering. The case of forwarding from a slower medium to a faster one is different. Most media types require that bits be transmitted without gaps between them. Because of this requirement, the coupling device cannot immediately start transmission on its output medium once the reception of the packet on its input medium has begun. Instead, the coupling device has to buffer the incoming

bits from the slower medium and start packet transmission to the faster medium at a later time. In the optimal case, the time at which this transmission begins is chosen in such a way that the last bit from the slow medium will have been received immediately before its time for transmission to the fast medium has come.
- Different systems can require different numbers of bits to be transmitted when a byte of data is to be sent. In IEEE 802.11, transmission of a byte requires nothing more than transmitting the eight bits of data contained in the byte. In PROFIBUS with an RS-485 medium, on the other hand, three additional bits must be sent along with each byte so that serial communication can take place.

The forwarding delay incurred by a coupling device depends on both the actual combination of these factors as well as on a number of other parameters, such as the processing delay or packet size.

To illustrate the influence of these factors, consider forwarding a packet from a slower RS-485 PROFIBUS physical layer with 1.5-Mb/s data rate (no preambles, no physical layer header) to a faster 2-Mb/s IEEE 802.11 DSSS physical layer with a total physical layer overhead of $128 + 64 = 192$ μs. The PROFIBUS uses 11 b for a byte, the DSSS only eight. When the PROFIBUS packet has a size of $x = 10$ B (110 bits), it remains on the PROFIBUS medium for approximately $110/1\,500\,000 \approx 73.3$ μs. Once the coupling device receives the first bit of the transmitted packet, it can start forwarding the first bit immediately. Due to the physical layer overhead and the transmission time needed for $10 \cdot 8$ b at 2 Mb/s, the packet leaves the forwarder after 232 μs. The forwarding delay is, therefore, ≈ 158.7 μs, more than twice the PROFIBUS packet duration. In contrast, when the packet has a size of $x = 255$ B, it takes 1.87 ms on the PROFIBUS, and only 1.212 ms on the wireless side. If the forwarding device is able to determine the packet length x soon after reception of the packet on the wired side has begun, it will be able to schedule the start of the packet transmission on the wireless side in an optimized way. Specifically, the coupling device can schedule the start of packet transmission such that the last bit of the packet will have been received from the wired medium immediately before it is to be transmitted on the wireless medium. In doing so, the forwarding delay amounts to nothing more than the transmission time of a single bit on the wireless medium, namely, 0.5 μs. In this scenario, forwarding works well for large packets, but not so well for small packets. Since fieldbus systems tend to primarily use smaller packets, the forwarding delays can become quite a serious problem.

A closer investigation of the forwarding delay with cut-through forwarding is presented in [136] for forwarding that occurs between an RS485-based PROFIBUS and a physical layer developed within the European union R-Fieldbus project [40], [137]. This physical layer has a shorter physical overhead than the IEEE 802.11 DSSS. The results, however, can be transferred to other settings as well. One interesting result is that the forwarding delay depends on the forwarding direction. Keeping the wired transmission rate fixed at 1.5 Mb/s, the wired-to-wireless forwarding delay *decreases* as the transmission rate on the wireless side increases. In the reverse direction, however, the wireless-to-wired forwarding delay *increases* as the wireless transmission rate increases. In both cases, the rate of decrease/increase depends on the packet size. Consider a scenario where two wired stations, both with a 1.5-Mb/s data rate, communicate over a single wireless hop (thus having one wired-to-wireless conversion and one wireless-to-wired conversion) [136]. In this scenario, the wireless medium should have a transmission rate between 1.1 and 1.2 Mb/s in order to achieve a close-to-optimal forwarding delay for all packet sizes under consideration. Outside this range, larger packets are subject to high forwarding delays.

Cut-through forwarding schemes typically have the smallest forwarding delays in comparison with S+F or gateway-based approaches.

B. S+F Forwarding

In S+F systems, forwarding devices first receive an entire packet on the input segment before forwarding it to the output segments. The minimum forwarding delay is thus given by the time needed to send the packet on the output segment, plus any additional processing time required by the forwarder. When using the numbers from the example given above, the small packet with $x = 10$ B has a forwarding delay of 232 μs, and the large packet with $x = 255$ B has a forwarding delay of 1.212 ms.

If the forwarding device is a bridge, it might be necessary to contend with other stations on the output segment for the right to transmit. When the output segment is a token-passing ring, for example, the forwarder must receive a token before it can transmit the packet any further. This kind of delay is referred to as *medium access delay*. Frequently, the medium access delay is variable. In this case, the forwarding delay is also variable, even when packets of the same size are the only ones used.

The forwarding delays in S+F approaches tend to be, therefore, larger than for cut-through approaches. The computation of any upper bounds requires knowledge of the upper bounds for the medium access delay.

C. Consequences of Forwarding Delay and Speed Differences

The presence of forwarding delay and different medium speeds has some important consequences.

1) Handling of Link-Layer Timeouts: In systems using master–slave communication, a master unit sends a request packet to a slave unit and expects the response within a certain amount of time (link-layer timeout, or timeout for short). In the presence of forwarding devices, such a request–response exchange takes more time than would be necessary on a single medium. There are two options for setting these timeouts.

- To set it large enough to accommodate the worst case round-trip time between a master and slaves, taking into account all forwarding delays. The drawback of

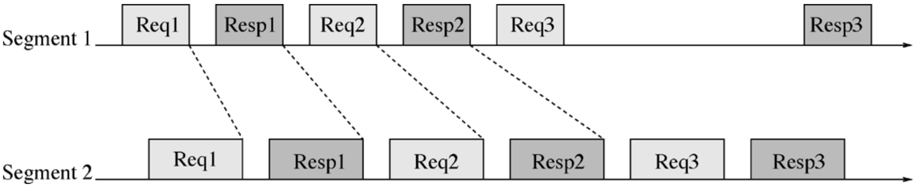

Fig. 3. Example for queueing delay induced by coupling devices.

this approach is the reduced responsiveness to transmission errors. The detection of a missing response (even from a slave within the same segment) takes much longer than it would if there were just a single segment and short timeouts. Due to the probability of transmission errors on wireless media, this delay can become critical if wireless links are involved.

- Select the timeout to be the same as the timeout for single-segment networks without any forwarders. When a request issued by station A is addressed to station B located in a distant segment, this timeout will be too small to accommodate for the round-trip time. One option to deal with this problem is to avoid letting A retransmit its request packet. The forwarder F_1, closest to A, responds to A's request with a special "response-comes-later" packet [138]. If B is located on another segment attached to F_1, F_1 acquires B's response and forward it on to A. No further action of A is required. If B is not located in a segment attached to F_1, F_1 directs its request to another forwarder F_2, gets a "response-comes-later" packet, and the process continues. A drawback to this approach is that existing fieldbus protocols typically do not contain such a mechanism. Without this mechanism, existing protocols would have to be modified, and wireless links would no longer be able to be seamlessly integrated into them.

2) Queueing Effects: The presence of preambles or different speeds on the medium can have the effect that two identical packets have different transmission times on different media. Because of this fact, queuing delays are now going to be present [139], [140]. An example illustrating these delays can be seen in Fig. 3. Assume a producer–distributor–consumer system. There are two different segment types S_1 and S_2. The distributor and the producers for requests `Req1` and `Req2` are located in segment S_1, the producer for request `Req3` is located in segment S_2, and consumers are spread throughout S_1 and S_2. It is assumed that both production requests and producer responses have a duration of t_1 s on segment S_1. On segment S_2 these same packets have a duration of $t_2 > t_1$ s. As seen in the figure, the forwarding delay (indicated by the dashed lines) increases over time. The packets the coupling device receives from S_1 that it needs to forward to S_2 will be buffered in a queue. If the distributor issues a third production request `Req3` for a variable produced by a station in S_2, the request packet experiences a queueing delay in the forwarding device.

Similar situations can also occur in master–slave systems such as PROFIBUS. A solution developed for such systems (but applicable to other systems as well) is the insertion of extra idle times between requests [139], [140]. With reference to Fig. 3, the distributor, after receiving response one, waits for an additional time before issuing request two.[12]

3) Relative Temporal Consistency: Some systems rely on broadcast packets to achieve relative temporal consistency. The communication between a set of sensors sampling the physical environment, for example, requires such a consistency (see Section II-B1). If the sensors were to belong to different segments, however, the temporal consistency could be jeopardized by the fact that the forwarding delay introduces additional jitter between the sampling instants.

One solution would be to keep all stations synchronized to a common time reference and instruct them to sample at an explicitly specified time. The price to pay, however, is the introduction of a time synchronization protocol (see [29, Ch. 8] for a survey) and the need for hardware clock circuitry even in small sensors.

D. Repeaters Versus Bridges

Repeaters essentially convert the physical representation of signals from one type of medium to another. They usually work in cut-through mode, but S+F is also possible. Since repeaters operate essentially on the physical layer, there are no medium access delays. The segments connected by a repeater run the same MAC protocol and form a single network. The protocol stack of the stations does not need to be changed, except maybe for certain configuration settings such as link-layer timeouts. Repeater-based solutions do, however, expose wired stations to the errors present in the wireless channel.

Bridges operate on the data link layer. Their precise operation depends on the similarity between the layers on either side of them [134], [135]. Bridges often operate in S+F mode and place restrictions on forwarding. As an example: 1) when the input packet is corrupted (e.g., checksum failure), forwarding is suppressed, and 2) when the destination station of a packet is known to be in the input segment, no forwarding is necessary.[13] The ability to avoid forwarding for intrasegment traffic has different benefits.

[12] When there are *only* unicast packets in a master–slave system, there is no need for extra idle times when the forwarding device can filter packets based on addresses. Referring to the example, the forwarder would not forward the first two requests and responses to segment S_2.

[13] To achieve this, the bridge has to learn which stations can be found in which segments. Such detection can be done, for example, by snooping packets and exchanging information with other bridges [134]. Additional mechanisms (spanning tree construction) are needed to avoid forwarding loops. When the address fields of a packet are placed at its beginning (which is common), a filtering bridge can also work in cut-through mode.

- Intrasegment traffic can be handled with the lowest possible response times and small timeouts. In addition, when multiple unacknowledged packets need to be transmitted in a series within the same segment, no extra idle times have to be inserted.
- Intrasegment traffic can be handled simultaneously in different segments, increasing the overall traffic capacity. In order to exploit this increase in capacity, the allocation of stations to various segments should take the anticipated traffic into account.
- As far as intrasegment traffic is concerned, errors on wireless media can be confined completely to a wireless segment.

E. Gateway-Based Approaches

Sometimes it may not be possible to use any forwarding device. In WorldFIP, for example, with its producer–distributor–consumer model, the producer of a data item must respond to a distributor's generation request within 70 bit periods [141], where 1 bit period is equal to the inverse of the data rate. If the distributor's wired segment runs at a speed of 2.5 Mb/s, only 28 μs are available for the request to be answered. Asuming the producer is a wireless station in a neighboring wireless segment, two forwarding steps would be needed, including all the forwarding delay, preambles, and so forth. Going through these steps would take much longer than 28 μs when commercially available equipment is used.

In gateway-based approaches, different segments are typically coupled by a dedicated application running in a gateway station. This application connects to different segments, each running a separate fieldbus protocol stack. The dedicated application interacts with the application layer services of these different protocol stacks to allow communication between segments to take place.

Consider the case where two segments S_1 and S_2, coupled by a gateway, use a fieldbus protocol based on a master–slave scheme. When master A (located in S_1) issues a request addressed to slave B (located in S_2), the gateway can intercept A's request and become a master to B itself. The gateway then receives B's response and generates a response packet for A. Such an approach, however, requires large timeout values for the link-layer of master A. The disadvantages of having such a large timeout value were discussed in Section IV-C.

An alternative to this approach is to let the gateway generate the response to the masters request from a cache, thus acting as a *proxy*. This approach is applicable in master–slave and in producer–(distributor)–consumer systems. The method presented in [142] for WorldFIP uses a wireless-to-wired gateway that serves as a central base station for the wireless part. The MAC protocol on the wireless side is based on a TDMA scheme. The base station is responsible for caching all process variables produced by wireless stations (acting as a consumer here), and for becoming a producer for these variables on the wired part. The same is done in the other direction.

F. Case Study: PROFIBUS

The PROFIBUS is a particularly interesting example for studying hybrid network architectures, since a variety of different approaches have been developed for this system. Some of these approaches were developed in the context of the European Union R-Fieldbus project [40], [137]. In the following sections, these approaches are briefly described.

1) Single-Logical-Ring Solution: All wired and wireless segments are coupled by repeaters into a single broadcast domain. All stations run the PROFIBUS token-passing protocol and are organized into a single logical token-passing ring.

The worst case response times for this solution clearly depend on the number of media boundaries that need to be crossed [143] as well as their respective forwarding delays [136], [140]. The idle times needed to avoid queueing in repeaters due to different medium speeds have been investigated in [140]. The influence on the setting of link-layer timeouts (called *slot time* in PROFIBUS) is considered in [138].

In PROFIBUS, the slot time T_{SL} serves not only as a link-layer timeout, but also plays a role in the detection of lost tokens. When the token owner crashes, the transmission medium remains silent, since no other station currently has the right to initiate transmissions. To detect this, a station i is required to listen to the medium. If the medium is idle for longer than the duration $\tau_i = (6 + 2 \cdot i) \cdot T_{SL}$ [9], station i concludes token loss, generates a new token, and starts transmissions immediately. Increased slot times thus lead to decreased responsiveness to token losses. Assignment of station addresses with small i can reduce this problem.

2) Multiple Logical Ring (MLR) Solution: As an alternative to the single logical ring solution adopted in the R-Fieldbus project, the approach to use MLRs has also been investigated [138], [144], [145]. The stations are grouped into segments, also referred to as *domains*.

There are different kinds of coupling stations between segments of different types. A *brouter* (bridge/router) is a master station for two separate token-passing rings on two different segments. In contrast, a repeater can be used, for example, for coupling a segment consisting of only wireless slave stations to a wired segment that has master stations or to connect multiple segments into a single logical ring.

Different strategies can be applied for allocating stations to segments and for allocating segments to logical rings. In the *domain-driven MLR* approach, there is a separate logical ring for each segment. Segments are coupled through brouters. If a wireless master station x is not reachable or loses the token, then only its own logical ring is affected, and the other rings remain functional. It may, however, still not be acceptable to distort the operation of other wireless master stations in the segment of station x. In the *wireless-master-driven MLR* approach, each wireless master station is therefore allocated its own segment and runs its own token-passing ring. Such a segment is coupled to wired segments through its own brouter. Finally, in the *domain-group-driven MLR*, multiple segments can be allocated into a single ring. The goal of the allocation is to minimize interring traffic. Segments belonging to the same ring are coupled through repeaters, whereas brouters are used to couple segments belonging to different rings.

The MLR approach shares advantages with bridge-based solutions (see Section IV-D). Specifically, token losses and ring instabilities induced by repeated losses of tokens are confined to a single logical ring.

In the MLR solution, link-layer timeouts are configured for good responsiveness in intraring transactions. Interring transactions are handled by other means. Two proposals are as follows.

- The "response-comes-later" approach (see also Section IV-C) has been proposed in [138].
- The proposal in [144] is based on the presence of different types of responses/acknowledgment. The receiver of a request has the freedom to send an acknowledgment packet without any data. It is therefore not necessary for the master (initiator) to *immediately* retransmit this request a number of times. Instead, the initiator can postpone the next transmission trial to its next token holding time.

  Suppose that station A is the initiator, station B the intended responder, F_1 the neighboring brouter to A, and F_2 the neighboring brouter to B. Station A sends a request to station B's address. Brouter F_1 intercepts this request and sends an empty response to station A. Brouter F_1 then encapsulates A's request packet into a packet belonging to a specific protocol *running between brouters*, and directs this packet to brouter F_2. Brouter F_2 decapsulates the request, sends it to station B, acquires B's response, encapsulates B's response, and then forwards the encapsulated response to brouter F_1. Brouter F_1 then buffers this response and sends it to station A the next time it repeats the same request. This approach requires no change to station A and B's protocol stacks, but requires the brouters to perform routing procedures. Brouter F_1 must now know that station B can be found behind brouter F_2. A disadvantage of this approach is that the time needed for A to get the final answer is not only influenced by medium access delays (a brouter must wait for the token), but also influenced by queueing delays in the brouters. The queueing delays can occur because of cross traffic passing through the brouters F_1 and F_2. This cross traffic could, for example, originate from other rings.

If brouters forward without using additional protocol mechanisms, deadlock scenarios can occur [140, Ch. 4]. Consider two logical PROFIBUS token passing rings, R_1 and R_2, coupled by a brouter F. A master station A acquires the token in ring R_1 and sends a request to a slave station in R_2. At almost the same time, a master station B in ring R_2 captures the token and sends a request to a slave in R_1. The brouter F cannot forward master station A's request packet to ring R_2 because master station B has the token and is waiting for an answer. Similarly, brouter F cannot forward master station B's request to ring R_1.

3) Virtual Ring Extension Solution: A coupling architecture for coupling a wireless segment to a token-passing PROFIBUS segment was proposed in [146]. This architecture is mainly useful where "wireless last-hop" segments are to be attached to a wired backbone segment. The coupling device is bridge-like, running two different protocols on the wireless and wired sides. Specifically, on the wired side the PROFIBUS token-passing protocol is used, whereas on the wireless side a polling-based MAC is employed.

The coupling device uses cut-through forwarding for intersegment data and response frames. All other packets originating from the wired segments, especially the token packet and ring-maintenance packets, are not forwarded. Instead, the coupling device acts as the wired segment *on behalf* of the wireless stations. Specifically, it pretends to accept and transmit token frames, it participates in ring maintenance and so forth.

4) Application Layer Gateway Solutions: Examples of the application layer gateway approach are described in [147] and [148]. In [147], a PROFIBUS network is augmented with wireless stations by means of a *protocol converter*. This protocol converter acts as a PROFIBUS master on the wired part and as a *virtual master* on the wireless part. On the wireless side, an application layer instance runs a polling protocol that utilizes IP datagrams on top of IEEE 802.11 with DCF (*virtual polling algorithm*). Running this protocol effectively eliminates the need for contention between wireless stations, as well as the presence of collisions between them. The protocol converter puts all the packets that are destined for a certain (wired or wireless) station into a separate message queue and transmits them when appropriate (defined by the length of the polling cycle and the allowable service time per station).

V. Conclusion

Selected issues related to wireless fieldbus systems have been discussed in this paper. Wireless technologies can bring many benefits to industrial applications, one of them being the ability to reduce machine setup times by avoiding cabling. The market offers mature wireless solutions, such as the IEEE 802.11 standard, the IEEE 802.15.4 standard, or BT. So far, however, wireless technologies have not gained widespread acceptance on the factory floor. One reason for this lack of acceptance is the difficulty in achieving the timely and successful transmission of packets over error-prone wireless channels. With the design of suitable protocol mechanisms and transmission schemes, along with the careful combination of these schemes, important steps toward increasing the acceptance of wireless technologies for industrial applications can be made.

The approach based on "hardening" the protocol stack can benefit from relaxing user requirements and making applications more tolerant against errors. In fact, a key observation from the field of wireless sensor networks [29] is that the *joint* design of applications (here: controllers) and the networking stack, along with careful cross-layer design within the networking stack itself, is more likely to give better results than designing each element in isolation.

There are many research opportunities in the fields of wireless fieldbus systems and wireless industrial communications. One such opportunity involves the search for new protocol mechanisms to improve real-time capabilities. A key component in the design and evaluation of such mechanisms is the formulation of appropriate performance measures, benchmark applications, and wireless channel models that have been adapted to industrial environments. Another opportunity involves the assessment of the many emerging wireless technologies (ultrawideband, MIMO techniques, smart antennas, wireless ad hoc and sensor networks) from both a technological and a market perspective in terms of their potential use in industrial applications. Yet another research opportunity concerns a trend in fieldbus systems to carry multimedia and TCP traffic in addition to control traffic. As a consequence, there is a need for wireless-adapted protocol support for these data types, which would not degrade the quality of service rendered to the control traffic. From a practical perspective, plant engineers need software tools for planning, configuration, and maintenance of wireless industrial networks. One component of such a software suite would need to determine the placement of wireless stations and coupling devices. An optimization goal might be to minimize the installation costs while satisfying the real-time requirements of individual stations. Further areas of research include security, mobility support, and the joint consideration of real-time transmission and energy efficiency.

Acknowledgment

The authors would like to thank the reviewers and the editor for their helpful comments. The authors would also like to thank K. Klues from TKN for helping to proofread the paper.

References

[1] P. E. Rybski, S. E. Stoeter, M. Gini, D. F. Hougen, and N. P. Papanikolopoulos, “Performance of a distributed robotic system using shared communications channels,” *IEEE Trans. Robot. Autom.*, vol. 18, no. 5, pp. 713–727, Oct. 2002.

[2] V. K. Kongezos and C. R. Allen, “Wireless communication between A.G.V.’s (autonomous guided vehicle) and the industrial network C.A.N. (controller area network),” in *Proc. IEEE Int. Conf. Robotics and Automation*, 2002, pp. 434–437.

[3] J. A. Janet, W. J. Wiseman, R. D. Michelli, A. L. Walker, and S. M. Scoggins, “Using control networks for distributed robotic systems,” in *Proc. IEEE Int. Conf. Robotics and Automation*, 1999, pp. 1138–1143.

[4] J. R. Pimentel, *Communication Networks for Manufacturing*. Englewood Cliffs, NJ: Prentice-Hall, 1990.

[5] N. P. Mahalik, Ed., *Fieldbus Technology—Industrial Network Standards for Real-Time Distributed Control*. Berlin, Germany: Springer, 2003.

[6] P. Pleineveaux and J.-D. Decotignie, “Time critical communication networks: Field buses,” *IEEE Network*, vol. 2, no. 3, pp. 55–63, May 1988.

[7] J.-D. Decotignie and P. Pleineveaux, “A survey on industrial communication networks,” *Ann. Telecomm.*, vol. 48, no. 9, p. 435ff, 1993.

[8] R. Zurawski, Ed., *The Industrial Information Technology Handbook*. Boca Raton, FL: CRC, 2005.

[9] *General Purpose Field Communication System, EN 50170, Volume 2: PROFIBUS*, Union Technique de l’Electricité, 1996.

[10] U. Jecht, W. Stripf, and P. Wenzel, “Profibus—Open solutions for the world of automation,” in *The Industrial Information Technology Handbook*, R. Zurawski, Ed. Boca Raton, FL: CRC, 2005.

[11] *General Purpose Field Communication System, EN 50170, Volume 3: WorldFIP*, Union Technique de l’Electricité, 1996.

[12] J.-P. Thomesse, “The WorldFIP fieldbus,” in *The Industrial Information Technology Handbook*, R. Zurawski, Ed. Boca Raton, FL: CRC, 2005.

[13] *ISO Standard 11 898—Road Vehicle—Interchange of Digital Information—Controller Area Network (CAN) for High-Speed Communication*, 1993.

[14] G. Cena and A. Valenzano, “Operating principles and features of CAN,” in *The Industrial Information Technology Handbook*, R. Zurawski, Ed. Boca Raton, FL: CRC Press, 2005.

[15] *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*, 1999.

[16] *IEEE Standard for Telecommunications and Information Exchange Between Systems—LAN/MAN Specific Requirements—Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: High Speed Physical Layer in the 5 GHz Band*, 1999.

[17] *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher Speed Physical Layer (PHY) Extension in the 2.4 Ghz Band*, 1999.

[18] *Specification of the Bluetooth System, Version 1.1*, Dec. 1999.

[19] J. C. Haartsen, “The Bluetooth radio system,” *IEEE Pers. Commun.*, vol. 7, no. 1, pp. 28–36, Feb. 2000.

[20] *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-WPAN’s)*, Oct. 2003.

[21] E. Callaway, P. Gorday, L. Hester, J. A. Gutierrez, M. Naeve, B. Heile, and V. Bahl, “Home networking with IEEE 802.15.4: A developing standard for low-rate wireless personal area networks,” *IEEE Commun. Mag.*, vol. 40, no. 8, pp. 70–77, Aug. 2002.

[22] C. Schwaiger and T. Sauter, “Security strategies for field area networks,” in *Proc. IEEE 2002 28th Annu. Conf. Industrial Electronics Society (IECON)*, 2002, pp. 2915–2920.

[23] A. Treytl, T. Sauter, and C. Schwaiger, “Security measures for industrial fieldbus systems—State of the art and solutions for IP-based approaches,” in *Proc. 2004 IEEE Int. Workshop Factory Communication Systems (WFCS)*, pp. 201–209.

[24] C. Schwaiger and T. Sauter, “A secure architecture for fieldbus/internet gateways,” in *Proc. 8th IEEE Int. Conf. Emerging Technologies and Factory Automation (ETFA)*, 2001, pp. 279–285.

[25] J. Hirai, T.-W. Kim, and A. Kawamura, “Practical study on wireless transmission of power and information for autonomous decentralized manufacturing system,” *IEEE Trans. Ind. Electron.*, vol. 46, no. 2, pp. 349–359, Apr. 1999.

[26] D. Dzung, C. Apneseth, G. Scheible, and W. Zimmermann, “Wireless sensor communication and powering system for real-time industrial applications,” presented at the 2002 IEEE Workshop Factory Communication Systems (WFCS 2002), Västerås, Sweden.

[27] S. Roundy, D. Steingart, L. Frechette, P. Wright, and J. Rabaey, “Power sources for wireless sensor networks,” presented at the Wireless Sensor Networks 1st Eur. Workshop (EWSN 2004), Berlin, Germany.

[28] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: A survey,” *Comput. Netw.*, vol. 38, pp. 393–422, 2002.

[29] H. Karl and A. Willig, *Architectures and Protocols for Wireless Sensor Networks*. Chichester, U.K.: Wiley, 2005.

[30] A. J. Goldsmith and S. B. Wicker, “Design challenges for energy-constrained ad hoc wireless networks,” *Wireless Commun.*, vol. 9, pp. 8–27, Aug. 2002.

[31] J. A. Stankovic, T. F. Abdelzaher, C. Lu, L. Sha, and J. C. Hou, “Real-time communication and coordination in embedded sensor networks,” *Proc. IEEE*, vol. 91, no. 7, pp. 1002–1022, Jul. 2003.

[32] A. Lessard and M. Gerla, "Wireless communication in the automated factory environment," *IEEE Network*, vol. 2, no. 3, pp. 64–69, May 1988.

[33] D. A. Roberts, "'OLCHFA': A distributed time-critical fieldbus," in *Proc. IEE Colloq. Safety Critical Distributed Systems*, 1993, pp. 6/1–6/3.

[34] I. Izikowitz and M. Solvie, "Industrial needs for time-critical wireless communication & wireless data transmission and application layer support for time critical communication," presented at the Euro-Arch'93 Conf., Munich, Germany.

[35] T. S. Rappaport, *Wireless Communications—Principles and Practice*. Upper Saddle River, NJ: Prentice-Hall, 2002.

[36] ——, "Characterization of UHF multipath radio channels in factory buildings," *IEEE Trans. Antennas Propag.*, vol. 37, no. 8, pp. 1058–1069, Aug. 1989.

[37] ——, "Indoor radio communications for factories of the future," *IEEE Commun. Mag.*, vol. 27, no. 5, pp. 15–24, May 1989.

[38] J. K. Cavers, *Mobile Channel Characteristics*. Boston, MA: Kluwer, 2000.

[39] A. Neskovic, N. Neskovic, and G. Paunovic. (2000) Modern approaches in modeling of mobile radio systems propagation environment. *IEEE Commun. Surveys Tuts.* [Online]. Available: http://www.comsoc.org/livepubs/surveys

[40] J. Hähniche and L. Rauchhaupt, "Radio communication in automation systems: The R-fieldbus approach," in *Proc. 2000 IEEE Int. Workshop Factory Communication Systems (WFCS 2000)*, pp. 319–326.

[41] C. Koulamas, A. Lekkas, G. Papandopoulos, G. Kalivas, and S. Koubias, "Delay performance of radio physical layer technologies as candidates for wireless extensions to industrial networks," in *Proc. IEEE Int. Conf. Emerging Technologies and Factory Automation (ETFA '01)*, pp. 133–142.

[42] T. S. Rappaport, S. Y. Seidel, and K. Takamizawa, "Statistical channel impulse response models for factory and open plan building radio communication system design," *IEEE Trans. Commun.*, vol. 39, no. 5, pp. 794–807, May 1991.

[43] D. Hampicke, A. Richter, A. Schneider, G. Sommerkorn, R. Thomä, and U. Trautwein, "Characterization of the directional mobile radio channel in industrial scenarios, based on wide-band propagation measurements," in *Proc. IEEE Vehicular Technology Conf.*, 1999, pp. 3358–3362.

[44] B. O'Hara and A. Petrick, *IEEE 802.11 Handbook—A Designer's Companion*. New York: IEEE Press, 1999.

[45] 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.

[46] Funbus-Projektkonsortium. (2000, Oct.) Das Verbundprojekt Drahtlose Feldbusse im Produktionsumfeld (Funbus)—Abschlußbericht. [Online]. Available: http://www.softing.de/d/NEWS/Funbusbericht.pdf

[47] D. A. Eckhardt and P. Steenkiste, "A trace-based evaluation of adaptive error correction for a wireless local area network," *MONET—Mobile Networks and Applications*, vol. 4, pp. 273–287, 1999.

[48] G. T. Nguyen, R. H. Katz, B. Noble, and M. Satyanarayanan, "A trace-based approach for modeling wireless channel behavior," presented at the Winter Simulation Conf., Coronado, CA, 1996.

[49] D. Duchamp and N. Reynolds, "Measured performance of wireless LAN," presented at the 17th Conf. Local Computer Networks, Minneapolis, MN, 1992.

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

[51] A. Willig and A. Wolisz, "Ring stability of the PROFIBUS token-passing protocol over error-prone links," *IEEE Trans. Ind. Electron.*, vol. 48, no. 5, pp. 1025–1033, Oct. 2001.

[52] H. ju Moon, H. S. Park, S. C. Ahn, and W. H. Kwon, "Performance degradation of the IEEE 802.4 token bus network in a noisy environment," *Comput. Commun.*, vol. 21, pp. 547–557, 1998.

[53] *Information Processing Systems—Local Area Networks—Part 4: Token-Passing Bus Access Method and Physical Layer Specifications*, Aug. 1990.

[54] N. Malpani, Y. Chen, N. Vaidya, and J. Welch, "Distributed token circulation in mobile ad hoc networks," *IEEE Trans. Mobile Comput.*, vol. 4, no. 2, pp. 154–165, Mar.–Apr. 2005.

[55] L. Kleinrock and F. A. Tobagi, "Packet switching in radio channels: Part I—Carrier sense multiple access modes and their throughput-delay characteristics," *IEEE Trans. Commun.*, vol. COM-23, no. 12, pp. 1400–1416, Dec. 1975.

[56] A. Kutlu, H. Ekiz, and E. T. Powner, "Performance analysis of MAC protocols for wireless control area network," in *Proc. Int. Symp. Parallel Architectures, Algorithms and Networks*, 1996, pp. 494–499.

[57] A. Kutlu, H. Ekiz, M. D. Baba, and E. T. Powner, "Implementation of "comb" based wireless access method for control area network," in *Proc. 11th Int. Symp. Computer and Information Science*, 1996, pp. 565–573.

[58] F. A. Tobagi and L. Kleinrock, "Packet switching in radio channels: Part II—The hidden terminal problem in carrier sense multiple-access and the busy-tone solution," *IEEE Trans. Commun.*, vol. COM-23, no. 12, pp. 1417–1433, Dec. 1975.

[59] S. Lin and D. J. Costello, *Error Control Coding*, 2nd ed. Englewood Cliffs, NJ: Prentice-Hall, 2004.

[60] R. van Nee and R. Prasad, *OFDM for Wireless Multimedia Communications*. Boston, MA: Artech House, 2000.

[61] S. Glisic and B. Vucetic, *Spread Spectrum CDMA Systems for Wireless Communications*. Boston, MA: Artech House, 1997.

[62] L. B. Milstein and M. K. Simon, "Spread spectrum communications," in *The Communications Handbook*, J. D. Gibson, Ed. Boca Raton, FL: CRC/IEEE Press, 1996, pp. 199–212.

[63] K.-S. Tang, K.-F. Man, and S. Kwong, "Wireless communication network design in IC factory," *IEEE Trans. Ind. Electron.*, vol. 48, no. 2, pp. 452–459, Apr. 2001.

[64] D. Stamatelos and A. Ephremides, "Spectral efficiency and optimal base placement for indoor wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 14, no. 4, pp. 651–661, May 1996.

[65] S. Lin, D. J. Costello, and M. J. Miller, "Automatic-repeat-request error-control schemes," *IEEE Commun. Mag.*, vol. 22, no. 12, pp. 5–17, Dec. 1984.

[66] A. Paulraj, "Diversity techniques," in *The Communications Handbook*, J. D. Gibson, Ed. Boca Raton, FL: CRC/IEEE Press, 1996, pp. 213–223.

[67] S. M. Alamouti, "A simple transmit diversity technique for wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 16, no. 8, pp. 1451–1458, Oct. 1998.

[68] A. Willig, "Exploiting redundancy concepts to increase transmission reliability in wireless industrial LANs," *IEEE Trans. Ind. Electron.*, submitted for publication.

[69] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3062–3080, Dec. 2004.

[70] H. Liu, H. Ma, M. E. Zarki, and S. Gupta, "Error control schemes for networks: An overview," *MONET—Mobile Netw. Appl.*, vol. 2, no. 2, pp. 167–182, 1997.

[71] E. Uhlemann, P.-A. Wiberg, T. M. Aulin, and L. K. Rasmussen, "Deadline-dependent coding—A framework for wireless real-time communication," in *Proc. Int. Conf. Real-Time Computing Systems and Applications*, 2000, pp. 135–142.

[72] P.-A. Wiberg and U. Bilstrup, "Wireless technology in industry—Applications and user scenarios," in *Proc. IEEE Int. Conf. Emerging Technologies and Factory Automation (ETFA '01)*, pp. 123–133.

[73] X. Wang and M. T. Orchard, "On reducing the rate of retransmission in time-varying channels," *IEEE Trans. Commun.*, vol. 51, no. 6, pp. 900–910, Jun. 2003.

[74] S. Kallel, "Analysis of a type II hybrid ARQ scheme with code combining," *IEEE Trans. Commun.*, vol. 38, no. 8, pp. 1133–1137, Aug. 1990.

[75] E. Uhlemann, "Adaptive concatenated coding for wireless real-time communications," Ph.D. dissertation, School Inf. Sci., Comput. Elect. Eng., Halmstad University, Halmstad, Sweden, Sep. 2004.

[76] M. Elaoud and P. Ramanathan, "Adaptive use of error-correcting codes for real-time communication in wireless networks," presented at the INFOCOM 1998, San Francisco, CA.

[77] C. Schurgers, V. Raghunathan, and M. B. Srivastava, "Power management for energy-aware communication systems," *ACM Trans. Embedded Comput. Syst.*, vol. 2, pp. 431–447, Aug. 2003.

[78] A. Honarbacht and A. Kummert, "WSDP: Efficient, yet reliable, transmission of real-time sensor data over wireless networks," presented at the Wireless Sensor Networks 1st Eur. Workshop (EWSN 2004), Berlin, Germany.

[79] "Special issue on networked control systems," *IEEE Trans. Autom. Control*, vol. 49, no. 9, pp. 1421–1603, Sep. 2004.

[80] X. Liu and A. Goldsmith, "Wireless communication tradeoffs in distributed control," in *Proc. 42nd IEEE Conf. Decision and Control*, 2003, pp. 688–694.

[81] ——, "Kalman filtering with partial observation losses," presented at the IEEE Conf. Decision and Control, Atlantis, Paradise Island, Bahamas, 2004.

[82] (2005) Bluetooth. [Online]. Available: http://www.bluetooth.com

[83] J. Haartsen, "Bluetooth—The universal radio interface for ad hoc, wireless connectivity," *Ericsson Rev.*, no. 3, pp. 110–117, 1998.

[84] J. Bray and C. F. Sturman, *Bluetooth: Connect Without Cables*. Eaglewood Cliffs, NJ: Prentice-Hall, 2000.

[85] C. Bisdikian, "An overview of the Bluetooth wireless technology," *IEEE Commun. Mag.*, vol. 39, no. 12, pp. 86–94, Dec. 2001.

[86] *Bluetooth 1.2 Core Specification*, Nov. 2003.

[87] G. Miklòs, A. Ràcz, Z. Turànyi, A. Valkò, and P. Johansson, "Performance aspects of Bluetooth scatternet formation," in *Proc. 1st ACM Int. Symp. Mobile Ad Hoc Networking and Computing*, 2000, pp. 147–148.

[88] A. C. V. Gummalla and J. O. Limb. (2000) Wireless medium access control protocols. *IEEE Commun. Surveys Tuts.* [Online]. Available: http://www.comsoc.org/pubs/surveys

[89] J. Greenfkes and K. Riemen, "Code modulation with digitally controlled companding for speech transmission," *Philips Tech. Rev.*, pp. 335–353, 1970.

[90] S. Zürbes, W. Stahl, K. Matheus, and J. Haartsen, "Radio network performance of bluetooth," presented at the IEEE Int. Conf. Communication (ICC), New Orleans, LA, 2000.

[91] S. Zürbes, "Considerations on link and system throughput of bluetooth networks," in *Proc. IEEE Int. Symp. Personal, Indoor and Mobile Radio Commun. (PIMRC)*, 2000, pp. 1315–1319.

[92] K. Matheus, S. Zürbes, R. Taori, and S. Magnusson, "Fundamental properties of ad hoc networks like Bluetooth: A radio network perspective," presented at the IEEE Vehicular Technology Conf. (VTC), Orlando, FL, 2003.

[93] K. Matheus and S. Magnusson, "Bluetooth radio network performance: Measurement results and simulation models," presented at the Int. Workshop Wireless Ad Hoc Networking (IWWAN), Oulu, Finland, 2004.

[94] *Bluetooth 2.0 Core Specification cdr.*, Nov. 2004.

[95] I. Howitt and J. A. Gutierrez, "IEEE 802.15.4 low rate—Wireless personal area network coexistence issues," in *Proc. Wireless Communications and Networking Conference 2003 (WCNC 2003)*, pp. 1481–1486.

[96] G. Lu, B. Krishnamachari, and C. S. Raghavendra, "Performance evaluation of the IEEE 802.15.4 MAC for low-rate low-power wireless networks," in *Proc. 2004 IEEE Int. Conf. Performance, Computing, and Communications*, pp. 701–706.

[97] *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band*, ANSI/IEEE Std 802.11, Jun. 2003.

[98] *International Standard ISO/IEC 8802-2:1998: Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements—Part 2: Logical Link Control*, 1998.

[99] *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Amendment 5: Spectrum and Transmit Power Management Extensions in the 5 GHz Band in Europe*, Oct. 2003.

[100] K. Matheus, "Wireless local and wireless personal area network technologies for industrial deployment," in *The Industrial Communication Technology Handbook*, R. Zurawski, Ed. Boca Raton, FL: CRC, 2004.

[101] Mobilian. (2001) Wi-Fi (802.11b) and Bluetooth: An examination of coexistence approaches. [Online]. Available: http://www.mobilian.com

[102] K. Matheus and S. Zürbes, "Co-existence of Bluetooth and IEEE 802.11b WLANs: Results from a radio network testbed," in *Proc. IEEE Int. Symp. Personal, Indoor and Mobile Radio Communications (PIMRC)*, vol. 1, 2002, pp. 151–155.

[103] M. A. Visser and M. E. Zarki, "Voice and data transmission over an 802.11 wireless network," in *Proc. IEEE Personal, Indoor and Mobile Radio Conf. (PIMRC) '95*, pp. 648–652.

[104] M. Veeraraghavan, N. Cocker, and T. Moors, "Support of voice services in IEEE 802.11 wireless LANs," presented at the INFOCOM 2001, Anchorage, AK.

[105] *Draft Supplement to Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Medium Access Control (MAC) Enhancements for Quality of Service (QoS)*, Nov. 2002.

[106] A. Grilo and M. Nunes, "Performance evaluation of IEEE 802.11e," in *Proc. 2002 IEEE Int. Symp. Personal, Indoor and Mobile Radio Communications (PIMRC)*, vol. 1, pp. 511–517.

[107] P. Garg, R. Doshi, R. Greene, M. Baker, M. Malek, and X. Cheng, "Using IEEE 802.11e MAC for QoS over wireless," in *Proc. 2003 IEEE Int. Performance, Computing, and Communications Conf.*, pp. 537–542.

[108] R. van Nee, G. Awater, M. Morikura, H. Takanashi, M. Webster, and K. W. Halford, "New high-rate wireless LAN standards," *IEEE Commun. Mag.*, vol. 37, no. 12, pp. 82–88, Dec. 1999.

[109] M. V. Clark, K. K. Leung, B. McNair, and Z. Kostic, "Outdoor IEEE 802.11 cellular networks: Radio link performance," in *Proc. IEEE Int. Conf. Commun. (ICC)*, vol. 1, 2002, pp. 512–516.

[110] K. K. Leung, B. McNair, L. J. Cimini, and J. H. Winters, "Outdoor IEEE 802.11 cellular networks: MAC protocol design and performance," presented at the IEEE Int. Conf. Communications (ICC), New York, 2002.

[111] G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function," *IEEE J. Sel. Areas Commun.*, vol. 18, no. 3, pp. 535–547, Mar. 2000.

[112] S. Sadalgi. (2000, May) A performance analysis of the basic access IEEE 802.11 wireless LAN MAC protocol (CSMA/CA). [Online]. Available: http://paul.rutgers.edu/~sadalgi/network.pdf

[113] G. Ennis, "Impact of Bluetooth on 802.11 direct sequence," IEEE, Tech. Rep. IEEE 802.11-98/319, Sep. 1998.

[114] J. Zyren, "Extension of Bluetooth and 802.11 direct sequence interference model," IEEE, Tech. Rep. IEEE 802.11-98/378, Nov. 1998.

[115] N. Golmie, R. van Dyck, and A. Soltanian, "Bluetooth and 802.11b Interference: Simulation Model and System Results," IEEE, Tech. Rep. IEEE802.15-01/195R0, Apr. 2001.

[116] D. Fumolari, "Link performance of an embedded bluetooth personal area network," presented at the IEEE Int. Conf. Communications (ICC), Helsinki, Finland, 2001.

[117] I. Howitt, "IEEE 802.11 and Bluetooth coexistence analysis methodology," in *Proc. IEEE Vehicular Technology Conf. (VTC)*, vol. 2, 2001, pp. 1114–1118.

[118] I. Howitt, V. Mitter, and J. Gutierrez, "Empirical study for IEEE 802.11 and Bluetooth interoperability," in *Proc. IEEE Vehicular Technology Conf. (VTC)*, vol. 2, 2001, pp. 1109–1113.

[119] H. Velayos and G. Karlsson, "Techniques to reduce IEEE 802.11b MAC layer hand-over time," presented at the IEEE Int. Conf. Communications (ICC), Paris, France, 2004.

[120] J.-D. Decotignie, "Which network for which application," in *The Industrial Information Technology Handbook*, R. Zurawski, Ed. Boca Raton, FL: CRC, 2005.

[121] D. Miorandi and S. Vitturi, "Performance analysis of producer/consumer protocols over IEEE 802.11 wireless links," presented at the Proc. IEEE Workshop Factory Communication Systems (WFCS), Vienna, Austria, 2004.

[122] ——, "Analysis of master–slave protocols for real-time industrial communications over IEEE 802.11 WLANs," presented at the IEEE Industrial Informatics Conf. (INDIN '04), Berlin, Germany.

[123] R. O. Baldwin, "Improving the real-time performance of a wireless local area network," Ph.D. dissertation, Faculty Elect. Eng., Virginia Polytechnic Inst. State Univ., , Blacksburg, Jun. 1999.

[124] J. L. Sobrinho and A. S. Krishnakumar, "Real-time traffic over the IEEE 802.11 medium access control layer," *Bell Labs Tech. J.*, vol. 1, no. 2, pp. 172–187, 1996.

[125] G.-S. Ahn, A. T. Campbell, A. Veres, and L.-H. Sun, "Swan: Service differentiation in stateless wireless ad hoc networks," presented at the INFOCOM 2002, New York.

[126] (1999) Specification of the Bluetooth System. Bluetooth Consortium. [Online]. Available: http://www.bluetooth.org

[127] C. de Morais Cordeiro, D. P. Agrawal, and D. H. Sadok, "Interference modeling and performance of Bluetooth MAC protocol," *IEEE Trans. Wireless Commun.*, vol. 2, no. 6, pp. 1240–1246, Nov. 2003.

[128] U. Bilstrup and P.-A. Wiberg, "Bluetooth in industrial environment," in *Proc. 2000 IEEE Workshop Factory Communication Systems (WFCS 2000)*, pp. 239–246.

[129] A. El-Hoiydi and J.-D. Decotignie, "Soft deadline bounds for two-way transactions in Bluetooth piconets under co-channel interference," in *Proc. 8th IEEE Int. Conf. Emerging Technologies and Factory Automation (ETFA)*, 2001, pp. 143–150.

[130] D. Miorandi and S. Vitturi, “A wireless extension of PROFIBUS DP based on the Bluetooth radio system,” *J. Ad Hoc Netw.*, to be published.

[131] ——, “Hybrid wired/wireless implementations of profibus DP: A feasibility study based on ethernet and bluetooth,” *Comput. Commun.*, vol. 27, pp. 946–960, Jun. 2004.

[132] S. Cavalieri and D. Panno, “On the integration of fieldbus traffic within IEEE 802.11 wireless LAN,” presented at the 1997 IEEE Int. Workshop Factory Communication Systems (WFCS’97), Barcelona, Spain.

[133] A. S. Tanenbaum, *Computer Networks*, 3rd ed. Englewood Cliffs, NJ: Prentice-Hall, 1997.

[134] R. Perlman, *Interconnections Second Edition—Bridges, Routers, Switches and Internetworking Protocols*. Reading, MA: Addison-Wesley, 1999.

[135] J.-D. Decotignie, “Interconnection of wireline and wireless fieldbusses,” in *The Industrial Information Technology Handbook*, R. Zurawski, Ed. Boca Raton, FL: CRC, 2005.

[136] C. Koulamas, S. Koubias, and G. Papadopoulos, “Using cut-through forwarding to retain the real-time properties of profibus over hybrid wired/wireless architectures,” *IEEE Trans. Ind. Electron.*, vol. 51, no. 6, pp. 1208–1217, Dec. 2004.

[137] L. Rauchhaupt, “System and device architecture of a radio-based fieldbus—The RFieldbus system,” presented at the 4th IEEE Workshop Factory Communication Systems 2002 (WFCS 2002), Västerås, Sweden.

[138] L. Ferreira, M. Alves, and E. Tovar, “Hybrid wired/wireless profibus networks supported by bridges/routers,” in *Proc. 2002 IEEE Workshop Factory Communication Systems (WFCS 2002)*, pp. 193–202.

[139] M. Alves, E. Tovar, F. Vasques, G. Hammer, and K. Röther, “Real-time communications over hybrid wired/wireless PROFIBUS-based networks,” in *Proc. 14th Euromicro Conf. Real-Time Systems*, 2002, pp. 142–151.

[140] M. F. Alves, “Real-Time Communications Over Hybrid Wired/Wireless PROFIBUS-Based Networks,” PhD dissertation, Faculty of Engineering, Univ. Porto, Porto, Portugal, Feb. 2003.

[141] P. Morel, A. Croisier, and J.-D. Decotignie, “Requirements for wireless extensions of a FIP fieldbus,” in *Proc. IEEE Int. Conf. Emerging Technologies and Factory Automation (ETFA ’96)*, pp. 116–122.

[142] P. Morel and A. Croisier, “A wireless gateway for fieldbus,” in *Proc. 6th Int. Symp. Personal, Indoor and Mobile Radio Communications (PIMRC ’95)*, vol. 1, pp. 105–109.

[143] M. Alves, E. Tovar, and F. Vasques, “Evaluating the duration of message transactions in broadcast wired/wireless fieldbus networks,” in *Proc. 27th Annu. Conf. IEEE Industrial Electronics Soc. (IECON ’01)*, pp. 243–248.

[144] L. Ferreira, E. Tovar, and M. Alves, “Enabling-inter-domain transactions in bridge-based hybrid wired/wireless PROFIBUS networks,” in *Proc. IEEE Int. Conf. Emerging Technologies and Factory Automation (ETFA ’03)*, pp. 15–22.

[145] L. Ferreira and E. Tovar, “Timing analysis of a multiple logical ring wired/wireless PROFIBUS network,” in *Proc. 2004 IEEE Int. Workshop Factory Communication Systems (WFCS)*, pp. 81–90.

[146] A. Willig, “An architecture for wireless extension of PROFIBUS,” in *Proc. 29th Annu. Conf. IEEE Industrial Electronics Society (IECON ’03)*, vol. 3, pp. 2369–2375.

[147] K. C. Lee and S. Lee, “Integrated network of PROFIBUS-DP and IEEE 802.11 wireless LAN with hard real-time requirement,” in *Proc. IEEE 2001 Int. Symp. Industrial Electronics*, vol. 3, pp. 1484–1489.

[148] 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.

Andreas Willig (Member, IEEE) received the diploma degree in computer science from the University of Bremen, Bremen, Germany, in 1994 and the Dr.-Ing. degree in electrical engineering from the Technical University Berlin, Berlin, Germany, in 2002.

He is with the Hasso-Plattner-Institute at University of Potsdam, Potsdam, Germany. His research interests include wireless networks, fieldbus and real-time systems, ad hoc and sensor networks, all with specific focus on protocol design and performance aspects.

Kirsten Matheus (Member, IEEE) received the Diploma degree in electrical engineering from the Technical University of Aachen, Aachen, Germany, in 1995 and the Dr.-Ing. degree in electrical engineering from the University of Bremen, Bremen, Germany, in 1998.

From 1998 to 2003, she worked for the Ericsson Eurolab Research department on the standardization of HIPERLAN/2 and Bluetooth technologies. She is currently working as a developer with CARMEQ GmbH, Berlin, Germany, a Volkswagen subsidiary. Since 2003, she has worked on various aspects concerning wireless technologies in the automotive industry. Her research interest is the optimization of radio network capacities in uncoordinated ad hoc networks.

Adam Wolisz (Senior Member, IEEE) received the Dr.—Ing. degree from the Silesian Technical University, Gliwice, Poland, in 1983.

He is currently a Professor of Electrical Engineering and Computer Science at the Technical University Berlin, Berlin, Germany, where he is directing the Telecommunication Networks Group (TKN). He is also a Member of the Senior Board of GMD Fokus, being especially in charge of the Competence Centers GLONE and TIP. His research interests are in architectures and protocols of communication networks as well as protocol engineering with impact on performance and QoS aspects.