MITSUBISHI ELECTRIC RESEARCH LABORATORIES
http://www.merl.com

UWB-based Sensor Networks and the IEEE 802.15.4a Standard - A Tutorial

A.F. Molisch, P. Orlik, Z. Sahinoglu, J. Zhang

TR2006-117 October 2006

Abstract

This paper gives a tutorial overview of ultrawideband communications systems for sensor networks. In particular, we describe the IEEE 802.15.4a standards, which is currently being developed. While most nodes (reduced-function devices) in sensor networks usually have to consume little energy, and are constrained with respect to the complexity of the processing they can perform, some nodes (full-function devices) do not show these restrictions. We describe a hybrid modulation, coding, and multiple access scheme that is particulary suited for heterogeneous networks that contain both FFDs and RFDs. The scheme is a generalization of the well-known time-hopping impulse radio (TH-IR). It employs systematic coding, joint pulse-position modulation and phase shift keying, as well as a combination of polarity scrambling and time-hopping. We also describe two-way ranging algorithms that serve as the basis for geolocation in 802.15.4a, and we discuss the methods for how the ranging information can be kept secret from snoopers.

International Conference on Communications and Networking in China

UWB-based sensor networks and the IEEE 802.15.4a standard - a tutorial

(invited paper)

Andreas F. Molisch, *Fellow IEEE*, Philip Orlik, *Member, IEEE,*
Zafer Sahinoglu, *Senior Member, IEEE,* and Jin Zhang, *Senior Member, IEEE*

***Abstract*— This paper gives a tutorial overview of ultrawideband communications systems for sensor networks. In particular, we describe the IEEE 802.15.4a standard, which is currently being developed. While most nodes (reduced-function devices) in sensor networks usually have to consume little energy, and are constrained with respect to the complexity of the processing they can perform, some nodes (full-function devices) do not show these restrictions. We describe a hybrid modulation, coding, and multiple access scheme that is particularly suited for heterogeneous networks that contain both FFDs and RFDs. The scheme is a generalization of the well-known time-hopping impulse radio (TH-IR). It employs systematic coding, joint pulse-position modulation and phase shift keying, as well as a combination of polarity scrambling and time-hopping. We also describe two-way ranging algorithms that serve as the basis for geolocation in 802.15.4a, and we discuss the methods for how the ranging information can be kept secret from snoopers.**

I. Introduction

In recent years, sensor networks have drawn great interest in the wireless community [1], [2], [3]. In sensor networks, different nodes usually communicate with each other without having a fixed infrastructure. The main goal of the network is the transmission of data within given quality- and delay-constraints. The transmission of data from the source to the destination usually occurs in several hops, where some nodes in the network operate as relay for the transmission of the information. Such relaying makes it easier to transmit information in networks that do not have any a-priori cellplanning, and also increase the robustness with respect to node failure. The Zigbee-standard [4] is the most widely used standard for the network layer (including the routing) of such sensor networks.

The key requirements for transceivers in sensor networks are

- low cost: since a large number of nodes are to be used, the cost of each node must be kept small. For example, the cost of an RFID node should be less than 1% of the cost of the product they tag.
- small form factor: the total transceiver (including power supply and antenna) must be small, so that it can be put in locations where the sensing actually takes place.
- low power consumption: a sensor usually has to work for several years without a change of battery. This entails that the power consumption must be extremely low.
- robustness: robustness of the transmission scheme against interference, small-scale fading, and shadowing is required so that delay- and quality constraints can be fulfillfed.

The authors are with Mitsubishi Electric Research Labs, Cambridge, MA, USA, email: {molisch, porlik, zafer, jzhang}@merl.com. A. F. Molisch is also at the Department of Electroscience, Lund University, Sweden.

Furthermore, geolocation is a key requirement. In sensor networks, a number of nodes communicate their sensing (measurement) results to each other and/or a central backhaul node. In many cases, the receiving nodes have to have knowledge of the exact location of the transmitter. For example, a fire sensor should include in its message not only that there is a fire, but also at which location. Furthermore, the receiving nodes often perform estimation of the target function based on $correlated$ data from closely-spaced sensors. Full exploitation of this correlation is possible only when the location of the sensors is known. Thus, geolocation capabilities of the nodes are very important for sensor network applications.

Until recently, most sensor networks used conventional narrowband modulation- and multipleaccess- techniques. For example, the PHY layer of the Zigbee networking standard,[1] employs a 1 MHz wide code-shift keying modulation. However, it is now recognized that ultrawideband (UWB) transmission techniques [6] in general are better at meeting the abovementioned requirements for sensor networks (low cost, low power consumption, robustness, geolocation) [7]. UWB uses a spreading of the transmit signal over a very large bandwidth (typically 500 MHz or more) [6]. By using a large spreading factor, robustness against interference and fading is achieved. Furthermore, the precision of ranging measurements (which form the basis of geolocation) is proportional to the bandwidth that can be employed; thus UWB also offers considerable advantages for geolocation.

Recognizing these facts, the IEEE has established the standardization group IEEE 802.15.4a, with the mandate to develop a new physical layer for sensor networks,[2] which should provide better communications capability than the existing 802.15.4 physical layer, and also should provide geolocation capability. This new physical layer is based on UWB transmission techniques, namely time-hopping impulse radio (TH-IR). The group started its work in 2003, first developing application scenarios (from which the requirements for the capabilities of the physical layer were deduced), and channel models. In March 2004, a baseline proposal [8] was approved, and in the subsequent months, a number of subgroups developed the details of the modulation/coding schemes, multiple access, ranging waveforms, and required modifications of the MAC layer. In December 2005, the standard was sent out for its first letter ballot, and is expected to receive its final approval in early 2007 [9].

[1] The Zigbee standard uses the IEEE 802.15.4 standard [5] for the PHY layer and networking layer.

[2] generally, the standard is intended for "personal area networks", which refers to the range over which two nodes can communicate.

1-4244-0463-0/06/$20.00 ©2006 IEEE

In this paper, we describe the basic structure of the standard PHY layer, and in particular address the properties that make it especially suitable for heterogeneous sensor networks.[3] Section II describes the basic principles of UWB communications, and we point out the properties that make it more robust to interference and other detrimental effects than narrowband systems. We also analyze the properties of UWB channels, which determine the performance limits of the PHY layer. Sec. III investigates the UWB *communications* methods of the 802.15.4a standard. We show how the chosen modulation and multiple-access formats are especially suitable for heterogeneous networks, i.e., work well with both coherent and noncoherent receivers. Section IV then describes the ranging and geolocation methods of the standard; in particular we discuss methods that allow for "secure" or "private" ranging. A summary and conclusions wrap up this paper.

II. Principles of UWB

A. Frequency regulation

Ultrawideband signals are defined as having an absolute bandwidth larger than 500 MHz, or a relative bandwidth larger than 20 % [10]. The spreading over a large bandwidth allows the construction of systems that interfere less with existing systems. For this reason, frequency regulators all over the world have issued (or will soon issue) rulings that allow the unlicensed operation of UWB systems, even if the UWB spectrum overlaps with the spectrum assigned to existing (legacy) systems. Of course, adherence to a frequency mask (limits on the power spectral density) has to be guaranteed. In the USA, emissions between 3.1 and 10.6 GHz are allowed. In Japan, operation between 3.4 and 4.8 GHz is admissible if the UWB transmitter uses DAA (detect and avoid), i.e., monitors the possible victim devices in its vicinity, and ceases transmission if it would interfere significantly with such a victim device. However, for 4.2 GHz through 4.8 GHz, interference mitigation techniques are not required until the end of December, 2008. Operation between 7.25 and 10.25 GHz is admissible also without DAA. Envisioned regulations in Europe define that operation of UWB devices in the frequency range from 4.2 to 4.8 GHz is permissible without DAA until the year 2010; afterwards, DAA must be used. The frequency band from 6 to 8.5 GHz can be used without DAA. Additionally, if DAA or low duty cycle (LDC) are used then the band from 3.1 to 4.8 GHz is available for UWB systems. In all cases, the power spectral density in the operating frequency band has to remain below 41.3 dBm/MHz; requirements for the out-of-band emissions vary.[4]

The large absolute bandwidth of UWB transmission means that the spreading factor of low-rate data transmission is very large (on the order of 1000). This large spreading not only allows transmission over reasonable distances ($10 - 50$ m) despite the restrictions on the power spectral density, but also improves the robustness to interference from narrowband interferers (jammers) and/or other UWB devices. Furthermore, a large absolute bandwidth allows very precise ranging, since the ranging accuracy is proportional to the bandwidth of the emitted signal.

[3]This paper describes the status as of summer 2006. While the essential structure of the standard has been fixed by this time, minor modifications might occur in the future.

[4]European regulations have not been finalized by the time of this writing. Also, Japanese regulations might still be changed in the near future.

UWB signals with large relative bandwidth also have the advantage that some frequency components have a better chance of propagating through (or around) obstacles. Thus, the wide relative bandwidth provides a diversity of propagation paths that leads to a higher robustness of the transmit signal. However, we note that this effect is most pronounced in the frequency range below 1 GHz. At microwave frequencies, a large *relative* bandwidth does not show significant advantages, while it complicates the design of the circuits and antennas of the transceivers.

B. Transmission schemes for UWB

There are a number of different ways to spread signals to large bandwidths. From a signal processing point of view, UWB is just spread-spectrum with a very large spreading bandwidth; for this reason, any of the well-known spread-spectrum approaches [11] can be employed. For UWB systems with high data rates, two approaches are currently used: (i) direct-sequence code division multiple access [12] is used in the high-data-rate UWB system of the UWB Forum [13]; (ii) a combination of frequency hopping, error-correction coding, and repetition coding, together with OFDM modulation, is used in the ECMA 268 standard for high-data-rate UWB systems [14].

For low data rates, time-hopping impulse radio (TH-IR) offers the best trade-off between complexity and performance. TH-IR was first proposed, and then investigated in detail, in the pioneering work of Win and Scholtz in the 1990s [15], [16], [17]. It is based on the following principle: each data symbol is represented by a sequence of pulses with pseudorandom delays; the modulation (either pulse position modulation PPM or quadrature amplitude modulation QAM) is applied to the whole pulse sequence. The sequence is chosen differently for each user; this allows the receiver to distinguish between different users. The duration of the pulses essentially determines the width of the transmit spectrum. We will see in Sec. III that the 802.15.4a standard builds on this principle, but includes some additional features.

C. UWB channels

The propagation channels over which the UWB systems are to operate have a dramatic impact on the design [18]. If the system were to operate only in an AWGN channel, then the receiver could be a simple energy detector (assuming pulse position modulation), which just detects whether a pulse is present at a given moment or not. However, UWB channels are delay dispersive, with rms delay spreads on the order of 5-50 ns. Due to the large bandwidth and resulting fine delay resolution, a coherent (Rake) receiver sees a large number of multipath components. This has the advantage of a high degree of delay diversity, so that small-scale fading fluctuations are almost completely eliminated [19]. On the downside, a Rake receiver needs to have a large number of fingers in order to collect all of the available multipath energy. The wider the spreading bandwidth, the more dramatic this effect; for 7.5 GHz spreading bandwidth, several hundred Rake fingers might be necessary just to collect half of the available energy [20].

Another important effect of the UWB propagation channel is that it makes ranging more difficult, because its power delay profile (PDP) shows a "soft onset". In UWB NLOS (non-line-of-sight) channels, the (easily identified) *strongest* component

can be several tens of nanoseconds after the first component [21]. For ranging purposes, we need to find the delay of the $first$ multipath component. Misidentifying the first multipath component (MPC) leads to errors in the range estimation.[5] Sec. IV will discuss sophisticated algorithms that can identify the first component even if it is relatively weak.

III. UWB COMMUNICATIONS IN SENSOR NETWORKS

A. Heterogeneous networks

Most sensor networks are heterogeneous, i.e., there are nodes with different capabilities and requirements. Typically, the network has one or several full-function device (FFD) that collects data from different sensors, processes them, and forwards them to some central monitoring station. A FFD has few restrictions with respect to processing complexity (as there are few of them, cost is not such an important factor), and energy consumption (since an FFD is usually connected to a permanent power supply). The sensor nodes themselves, on the other hand, are usually reduced-function devices with extremely stringent limits on complexity and power consumption. The distinction between FFD and RFD was also introduced in the Zigbee standard for networking and routing purposes.

For UWB devices, the goals and limits of FFDs and RFDs can be best achieved if FFD devices employ coherent reception, while RFDs use simple energy detectors (noncoherent receivers). As a consequence, the modulation, coding, and multiple access schemes (MCM) have to be designed in such a way that they work $both$ for coherent and noncoherent receivers. Furthermore, it is required that such a flexible MCM scheme does not deteriorate the possible performance of the FFDs, i.e., that the performance of FFDs with flexible MCM is (almost) as good as with an MCM that is designed for homogeneous coherent-receiver networks.

B. Bandplan

As a first step, the bandwidth of the UWB signals must be selected. As the frequency regulators prescribe the power spectral $density$, the total transmit power can be increased by increasing the signal bandwidth. Furthermore, a higher bandwidth implies a higher degree of delay diversity.

On the other hand, receiver design considerations lead to a requirement for lower signal bandwidths. For noncoherent receivers, the bandwidth should be less than the channel delay spread, since the receiver cannot optimally combine the resolved MPCs, anyway. For a coherent receiver, we have to perform a tradeoff between the delay diversity, and the amount of energy that can be collected with a given number of Rake fingers [22]. For typical UWB channels, the optimum lies between 100 MHz and 2 GHz. We must also keep in mind that the bandwidth of the system determines the required clockspeed and the speed of the receiver electronics in a coherent receiver. Cost requirements also imply that the bandwidth should be as low as possible.

[5]It must be emphasized that a "soft onset" of the power delay profile is a property of the channel itself, does not depend on the bandwidth of the system operating over the channel.. However, after lowpass filtering by a narrowband receiver (delay resolution on the order of hundreds of nanoseconds), the maximum of the PDP is industinguishable from the first MPC. Thus, a correct modeling of the soft onset is much more important for UWB channels.

freq. band	f_c (MHz)	BW (MHz)	admissible region
0	399.36	499.2	USA,
1	3494.4	499.2	USA,Europe
2	3993.6	499.2	USA,Europe, Japan
3	4492.8	499.2	USA,Europe, Japan
4	3993.6	1331.1	USA,Europe, Japan
5	6489.6	499.2	USA,Europe
6	6988.8	499.2	USA,Europe
7	6489.6	1081.6	USA,Europe
8	7488.0	499.2	USA,Europe, Japan
9	7987.2	499.2	USA,Europe, Japan
10	8486.4	499.2	USA, Japan
11	7987.2	1331.2	USA, Japan
12	8985.6	499.2	USA, Japan
13	9484.8	499.2	USA, Japan
14	9984.0	499.2	USA, Japan
15	9484.8	1354.9	USA, Japan

Table 1 IEEE 802.15.4a UWB frequency bands. f_c: center frequency

Based on all these considerations, IEEE 802.15.4a decided on a signal bandwidth (BW) of 500 MHz for the mandatory modes; optional frequency bands whose bandwidths are greater than 1 GHz width are also defined. Table 1 gives the center frequencies and bandwidths of the admissible bands, as well as the regulatory domains in which they are admissible. The center frequencies are chosen in such a way that they can be derived from a variety of readily available crystal oscillators.

C. Hybrid modulation and multiple access

As we have mentioned before, the MCM has to work with both coherent and noncoherent receivers. This is achieved by choosing the following transmit waveform

$$w^{(k)}(t) = \sum_i \sum_{n=0}^{N-1} \widetilde{b}_i^{(k)} p(t - nT_c - c_i^{(k)} T_b - iT_s - \frac{1 + b_i^{(k)}}{2} T_{ppm}) d_{i,n}^{(k)} \quad (1)$$

where superscript $^{(k)}$ denotes the $k-$th user, b_i and $\widetilde{b}_i$ are the i-th (coded) bit that is to be transmitted (we note here that $\widetilde{b}_i$ is used to indicate a parity check bit that is modulated onto the phase of the pulses while b_i is the uncoded bit that modulates the position of the bits). Furthermore, n indices the N pulses that are transmitted during each symbol, c is the time (bulk)-hopping sequence, T_c is the chip (pulse) duration of approximately 2 ns, T_b is the burst-hopping duration, which equals $T_b = NT_c = 32$ ns, T_{ppm} is the modulation interval for the pulse position modulation $T_{ppm} = 16T_b$, and T_s is the symbol duration. The $d_{i,n}$ denote a pseudorandom scrambling sequence. The pulse $p(t)$ is the "basis pulse" that is a raised-cosine pulse.[6]

Let us now describe the reasons for choosing this specific waveform. We first turn our attention to the modulation (see Fig. 1): for a noncoherent receiver, it provides a PPM modulation signal with a 32 ns excitation signal and a 512 ns modulation interval. In addition a coherent receiver may despread the excitation signal by correlating with $d_{i,n}^{(k)}$ resulting in an SNR gain. Furthermore, the coherent receiver can extract the parity

[6]To be exact, the basis pulse has to have a correlation with a raised-cosine pulse of better than 0.8. Alternative pulseshapes, which allow better spectral shaping and improved multiple access, have also been defined in the standard.

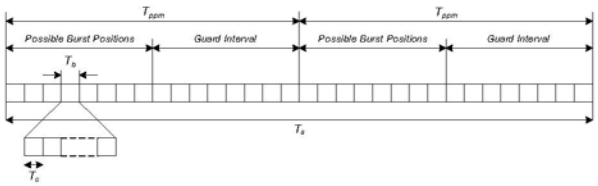

Fig. 1. Modulation and time-hopping of the 802.15.4a standard.

check bit bit, $\widetilde{b}_i$, from which it can obtain additional coding gain (see Sec. III. D). To see this, let us denote the sum of N pulses as prototype waveform $S(t)$

$$S(t) = \sum_{n=0}^{N-1} p(t - nT_c) d_{i,n}^{(k)} \tag{2}$$

Then this waveform is modulated with both PPM and BPSK. The modulation interval T_{ppm}=512 ns is chosen much larger than the typical channel delay spreads, so that a noncoherent receiver can detect the PPM even in channels with heavy delay dispersion. On the other hand, the duration of the prototype waveform is on the order of, or shorter than, typical delay spreads. Thus, the duration over which a noncoherent receiver has to integrate the received signal is essentially determined by the propagation channel. Shortening the duration of the prototype waveform would not significantly reduce the optimum integration duration (and thus, the time over which the receiver collects noise). A coherent receiver can perform a correlation (matched filtering) with $S(t)$, and thus enhance the signal-to-noise ratio by a factor of N. Furthermore, additional information is available for the coherent receiver from the detection of the bit $\widetilde{b}_i$, which is different from b_i. We will discuss in the following subsection how this extra bit is used.

Now let us turn our attention to the multiple-access format. For the noncoherent receiver, the signal provides time hopping, while for the coherent receiver, an extra scrambling gain is obtained. Figure 1 shows the time hopping: the position of the prototype waveform $S(t)$ is shifted by multiples of $T_{\text{b}} = 32$ ns in a pseudorandom way; the shifts are different for different users. Note that the maximum possible shift is $8T_{\text{b}}$, while the time shift for the PPM is $16T_{\text{b}}$. Thus, a duration of $8T_{\text{b}} = 256$ ns serves as a guard interval for channels with heavy delay dispersion.

The coherent receiver obtains additional multiuser separation by the despreading of the prototype waveform $S(t)$. As each user has a different prototype waveform, the matched filtering at the receiver input provides multiaccess interference suppression. The amount of suppression depends on the crosscorrelation between the prototype waveforms.

D. Coding for hybrid modulation

As we have outlined in the previous section, the modulation scheme enables a coherent receiver to receive two bits per transmit symbol, while it enables one bit per symbol for noncoherent receivers. An obvious idea would be to double the data rate of the payload data if the transmitter knows that the receiver can perform coherent detection. However, such an approach is not practical for sensor networks: first, multicast transmission often requires that coherent and noncoherent recievers can transmit the same information; secondly, relay nodes often are noncoherent receivers even if the the ultimate destination of the message is a coherent receivers.

Thus, a better approach is to use the extra bits for coherent receivers to provide higher coding gain. In order to ensure that the signals can still be decoded by noncoherent receivers, a $systematic$ code has to be used: the systematic bits are mapped onto the bits to determine the PPM, and are thus visible to all receivers. The redundant bits are transmitted on the BPSK, and are thus visible only for coherent receivers. The convolutional code has generator functions

$$g_1 = [010], \quad g_2 = [101] \tag{3}$$

In addition, the information is also protected with a systematic (51,43,8) Reed-Solomon code.

The structure of the coding scheme allows to implement a variety of decoders that have different tradeoffs between complexity and performance. We list them in order of ascending performance

- no decoding: since the RS code is systematic, the receiver can just ignore the redundant bits of the RS (as well as the systematic convolutional) code, and decode the information bit by bit
- hard decoding of the RS code: using standard decoding of RS codes, the receiver can decode the signal without using the redundant information of the convolutional code
- hard decoding of convolutional code followed by hard decoding of RS code
- soft decoding of convolutional code followed by decoding of RS code

E. Synchronization for heterogeneous networks

Before data detection can be performed, it is first necessary to acquire, synchronize, and perform channel estimation. Also the preamble, which is used for those two purposes, has to be detectable by both coherent and noncoherent receivers. This goal is achieved by an ingenious scheme first suggested by [23], [24], namely "perfectly balanced ternary sequences" (PBTS). Those sequences have the property that both the periodic autocorrelation function for coherent receivers

$$ACF_k = \sum_n \sum_j \sum_m c_{i+mN} c_{k-i+jN} \tag{4}$$

and the periodic autocorrelation function as observed by noncoherent receivers

$$\overline{ACF}_k = \sum_n \sum_j \sum_m |c_{i+mN}| \cdot (2|c_{k-i+jN}| - 1) \tag{5}$$

are perfect, i.e., proportional to a delta comb $\sum_i \delta_{k+iN}$. Of course, the coherent receiver has a 3 dB advantage over the non-coherent receiver. The preamble uses a large number of repetitions of the PBTS; the resulting signal is thus well-suited both for synchronization, and channel estimation (the received signal is the periodic repetition of the impulse response).

The 802.15.4a standard foresees the use of either length-31, or length-127 PBTS. Table 2 shows the 31-bit sequences defined in the standard; they have finite cross correlation. Note that different networks use different preamble sequences.

sequence number	sequence
1	-0000+0-0+++0+-000+-+++00-+0-00
2	0+0+-0+0+000-++0-+—00+00++000
3	-+0++000-+-++00++0+00-0000-0+0-
4	0000+-00-00-++++0+-+000+0-0++0-
5	-0+-00+++-+000-+0+++0-0+0000-00
6	++00+00—+-0++-000+0+0-+0+0000
7	+0000+-0+0+00+000+0++—0-+00-+
8	0+00-0-0++0000–+00-+0++-++0+00

Table 2: Preamble sequences

In heavy multipath (long delay spread), the ideal periodic autocorrelation properties get distorted due to inter symbol interference. In order to deal with this situation, the 802.15.4a standard foresees an adaptive choice of the pulse repetition frequency in the sequence. Either 15.6, or 3.90 MHz can be chosen.

F. Packet transmission

The 802.15.4a standard uses a number of different schemes for multiple access. Different networks are distinguished by using different frequency bands, and by different codes (PBTS sequences for the preambles, time-hopping codes and scrambling codes for the data). Within a network, multiple-access is achieved by an ALOHA scheme, i.e., each user transmits without checking whether other users are on the air.[7]

G. Beyond 15.4a: transmitted reference

The MCM that allows coherent as well as noncoherent receivers provides considerable flexibility for system designers. The principle could be taken one step further, by enabling transmitted-reference (TR) receivers as well. In TR, the transmitter sends all information as a sequence of pulse *pairs* in such a way that the information is encoded as the phase difference between the first and the second pulse. A receiver then just has to multiply the received signal with a delayed copy of itself [25], [26]. TR systems also have a number of drawbacks, which have, however, been partly resolved by recent research results:

- energy expended on the first pulse (reference pulse) in the pulse pair is wasted, as only the phase of the second pulse is information-bearing. However, [27] showed how the reference pulse can be made information-bearing.
- the noise-noise crossterms at the receiver (when the received signal is multiplied with the delayed version of itself) can dominate the performance. Using "cleaned-up" (averaged) reference signals [26], or performing sequence-matched filtering before the multiplication [28] greatly alleviates these problems.
- the implementation of the delays can be problematic; however, this problem has been solved for low-rate systems by a recent scheme of [29] that uses frequency-shifted pulse pairs (instead of the usual time-delayed pulse pairs).

IV. UWB GEOLOCATION IN SENSOR NETWORKS

A. Operating principle - two-way ranging

UWB networks mostly use time-of-arrival for determining the range between different nodes; those ranges form the basis of the actual location estimation [30]. According to the ranging protocol in IEEE 802.15.4a standard, an originating device A first transmits a signal to target node B. After reception, node B prepares and sends an acknowledgment packet back to node A. In a separate packet node B also reports to A the arrival time of the packet from A and the departure time of the ACK. Node A can then compute the range since it knows the total round-trip time and the turn around time of the ACK. (see Fig. 2).

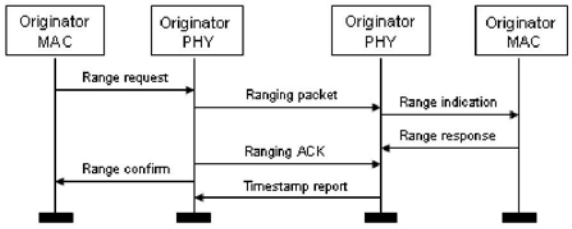

Fig. 2. Two-way ranging in IEEE 802.15.4a.

B. Detection in LOS and NLOS

The key task for the receivers is the determination of the roundtrip time of the packet, which in turn requires the identification of the first arriving MPC. This task is relatively easy in channels where the first MPC is also the strongest one, as is usually the case in LOS situations. However, it becomes much more difficult in NLOS situations. As discussed in Sec. II.C, the delay between the first and strongest component can be several tens of nanoseconds, which leads to a corresponding inaccuracy of the range estimate. Accurate identification of the first MPC is thus vital.

The standard uses the preamble (which is also used for synchronization and channel estimation) also for ranging purposes. Remember that this preamble allows to estimate the different MPCs, since the received signal is a periodic repetition of the channel impulse response. The receiver thus has a noisy estimate of the impulse response available; from the synchronization phase, it usually also has the arrival time of the stongest MPC. Starting from that arrival time, the receiver can now "search back" to find possible earlier MPCs.

The searchback is complicated by two issues:

- the received signal is noisy; only components that exceed a certain threshold are considered . Still, the task remains to determine whether a component above the threshold is an actual MPC, or just a noise spike. The longer the duration over which the searchback is done, the higher the chance that a large noise spike occurs. The placing of the threshold is thus a tradeoff between the false-alarm probability (i.e., the probability of confusing a noise threshold with a MPC), and the probability of missing an MPC.
- the received signal arrives in clusters. The strongest MPC is not necessarily in the first arriving cluster. This complicates the search-back algorithm: when finding an MPC that is not preceded by another MPC, we have to determine whether we have found really the first MPC, or just the first MPC of the current cluster. An algorithm for this backward search is given in [31].

C. Private ranging

Ranging is very useful in sensor networks, but can be subject to hostile attacks especially in security-related networks. A

[7] There is an optional method for determining when other nodes in the network are on the air.

number of attacks is possible:

- Snooper attack: hostile device listens to ranging exchanges
- Impostor attacks:
  - hostile device sends range request, finds out range
  - hostile device gives answer, providing wrong range to inquirer
- Jamming attack: hostile device jams during transmission of ranging signal

In order to make such attacks more difficult, the 802.15.4a standard foresees a "private ranging" mode. In this mode, the ranging preamble uses one of 127 possible sequences. Prior to ranging, the nodes exchange via a secure protocol which of the sequences will be used in the next ranging cycle. This prevents impostor attacks, and makes snooper attacks more difficult (a snooper now has to listen to all length-127 ranging waveforms specified by the standard).

V. Summary and conclusions

In this paper, we have argued that UWB transmission techniques are especially suitable for the implementation of sensor networks. They offer

- good geolocation capabilities.
- high robustness to interference and small-scale fading (when using coherent receivers).
- low-complexity receivers (when using noncoherent receivers) and transmitters; similarly, low energy consumption can be achieved.

UWB in the microwave range does not offer a high restistance to shadowing, but this problem can be mitigated in sensor networks by appropriate routing, and possible collaborative communications.

The IEEE has been developing a standard, 802.15.4a, for UWB-based sensor networks. It offers a high degree of flexibility. It uses a modulation, coding, and multiple access scheme that allows reception with either coherent or noncoherent receivers, and can adapt to environments with different delay spreads.

The standard also works well together with the IEEE 802.15.4a MAC standard and the Zigbee networking standard. Fitting into this established framework, and providing excellent performance and flexibility, it seems poised for widespread acceptance in industry.

References

[1] V. Raghunathan, S. Ganeriwal, and M. Srivastava, "Emerging techniques for long lived wireless sensor networks," *IEEE Communications Magazine*, pp. 108–114, 2006.

[2] D. Puccinelli and M. Haenggi, "Wireless sensor networks: applications and challenges of ubiquitous sensing," *IEEE Circuits and Systems Magazine*, pp. 19–31, 2005.

[3] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, pp. 102–114, 2002.

[4] "Zigbee specification version 1.0," tech. rep. available at "http://www.zigbee.org".

[5] IEEE Working Group 802.15.4, "IEEE Std 802.15.4 -2003, Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)," tech. rep., 2003.

[6] M. G. diBenedetto, T. Kaiser, A. F. Molisch, I. Oppermann, C. Politano, and D. Porcino (eds.), *UWB Communications Systems: A Comprehensive Overview*. EURASIP Publishing, 2005.

[7] I. Oppermann, L. Stoica, A. Rabbachin, Z. Shelby, and J. Haapola, "Uwb wireless sensor networks: Uwen - a practical example," *IEEE Communications Magazine*, pp. S27–S32, 2004.

[8] A. F. Molisch, et.al, "UWB PHY proposal for IEEE 802.15.4a Alt-PHY Project," tech. rep., 2005. doc.: IEEE 802.15-05-0172-02-004a.

[9] IEEE Working Group 802.15.4a, "Draft specifications for IEEE 802.15.4a standard", 2006, at www.802wirelessworld.com

[10] Federal Communications Commission, "First report and order 02-48," 2002.

[11] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications Handbook*. McGraw-Hill,Inc., 1994.

[12] A. J. Viterbi, *CDMA: Principles of Spread Spectrum Communications*. New York: Addison-Wesley, 1995.

[13] J. McCorkle et al., "Xtreme spectrum cpf document," 2003. Document IEEE 802.15-03/154r0.

[14] ECMA, "Uwb: High rate ultra wideband phy and mac standard," tech. rep., 2005. www.ecma-international.org.

[15] R. A. Scholtz, "Multiple access with time-hopping impulse modulation," in *Proc. IEEE Military Commun. Conf. (MILCOM)*, vol. 2, pp. 447–450, Oct 1993. Boston, MA, USA.

[16] M. Z. Win and R. A. Scholtz, "Impulse radio: How it works," *IEEE Commun. Lett.*, vol. 2, pp. 36–38, Feb 1998.

[17] M. Z. Win and R. A. Scholtz, "Ultra-wide bandwidth time-hopping spread-spectrum impulse radio for wireless multiple-access communications," *IEEE Trans. Commun.*, vol. 48, pp. 679–691, Apr 2000.

[18] A. F. Molisch, "Ultrawideband propagation channels - theory, measurement, and modeling," *IEEE Trans. Veh. Techn.*, vol. 54, pp. 1528 – 1545, Sept 2005.

[19] M. Z. Win and R. A. Scholtz, "On the energy capture of ultra-wide bandwidth signals in dense multipath environments," *IEEE Commun. Lett.*, vol. 2, pp. 245–247, Sept 1998.

[20] J. Karedal, S. Wyne, P. Almers, F. Tufvesson, and A. F. Molisch, "Statistical analysis of the uwb channel in an industrial environment," in *Proc. IEEE Veh. Tech. Conf. (VTC-Fall)*, vol. 1, pp. 81–85, Sept. 2004. Los Angeles, CA, USA.

[21] A. F. Molisch, K. Balakrishnan, C. C. Chong, D. Cassioli, S. Emami, A. Fort, J. Karedal, J. Kunisch, H. Schantz, , and K. Siwiak, "A comprehensive model for ultrawideband propagation channels," *IEEE Trans. Antennas Prop.*, p. submitted, 2006.

[22] D. Cassioli, M. Z. Win, A. F. Molisch, and F. Vatelaro, "Performance of selective Rake reception in a realistic UWB channel," in *Proc. ICC 2002*, pp. 763–767, 2002.

[23] F. Chin, et. al., "Impulse radio signaling for communication and ranging," tech. rep. IEEE P802.15-05-0231-03-004a, available at http://802wirelessworld.com.

[24] I. Lakkis, "Pulse compression," tech. rep. IEEE P802.15-05-0456-02-004a, available at http://802wirelessworld.com.

[25] R. Hoctor and H. Tomlinson, "Delay-hopped transmitted reference rf communications," in *IEEE conf. on Ultra Wideband Systems and Technologies 2002*, pp. 265–270, 2002.

[26] J. D. Choi and W. E. Stark, "Performance of ultra-wideband communications with suboptimal receivers in multipath channels," *IEEE J. Selected Areas Comm.*, vol. 20, pp. 1754–1766, Dec. 2002.

[27] S. Zhao, P. Orlik, A. F. Molisch, H. Liu, and J. Zhang, "Hybrid ultrawideband modulations compatible for both coherent and transmit-reference receivers," *IEEE Trans. Wireless Comm.*, p. in press, 2006.

[28] F. Tufvesson and A. F. Molisch, "Ultra-wideband communication using hybrid matched filter correlation receivers," in *Proc. VTC spring 2004*, pp. 1290–1294, 2004.

[29] D. L. Goeckel and Q. Zhang, "Slightly frequency-shifted reference ultrawideband (uwb) radio: Tr-uwb without the delay element," in *Proc. IEEE Military Communications Conference 2005*.

[30] S. Gezici, Z. Tian, G. B. Giannakis, H. Kobayashi, A. F. Molisch, H. V. Poor, and Z. Sahinoglu, "Localization via ultra-wideband radios: a look at positioning aspects for future sensor networks," *IEEE Signal Processing Magazine*, vol. 22, pp. 70 – 84.

[31] I. Guvenc, Z. Sahinoglu, P. Orlik, and A. F. Molisch, "Waveform design and threshold selection for non-coherent ir-uwb ranging," *IEEE Trans. Vehicular Techn.*, p. submitted, 2006.