802.15 Personal Area Networks

Greg Hackmann, ghackmann@yahoo.com

Abstract

Recently, low-power wireless networking standards like 802.15.1 (Bluetooth) have driven consumer interest in personal area networks (PANs). These networks are designed for inexpensively connecting low-power devices located within 1 m to 100 m of each other. In this paper, we discuss recent evolutions to the Bluetooth standard, as well as two emerging PAN standards: 802.15.4/ZigBee, and Ultra-Wide Band. We provide a high-level summary of how these standards operate, as well as a brief discussion of what to expect from each technology in the future.

See also:

Table of Contents

---

1 Introduction

Wireless networking standards like 802.11b and Wi-Max typically focus on providing PC-to-PC or PC-to-ISP connectivity over the range of a building or a metropolitan area. However, many applications have far less stringent range requirements, such as connecting peripherals wirelessly to a mobile device or adding components to a home theater system. Personal area networks (PANs) are a perfect fit for these applications: they offer signal ranges in the neighborhood of 1 m to 100 m, and a wide variety of data rates. Moreover, since the kinds of devices we wish to equip with PANs are often mobile and lightweight, power is at a premium. Thus, the low power consumption of PAN radios is very important to their acceptance.

In this paper, we will discuss three different approaches to PAN technology. The first, Bluetooth, has already been widely deployed in hundreds of millions of devices. It offers data rates of up to 3 Mbps and ranges of up to 100 m, with far lower power consumption than 802.11b. Its middleware layer builds on top of the PHY and MAC layers to provide a high degree of interoperability among Bluetooth-equipped devices. This low power consumption and interoperability guarantee have fueled Bluetooth's acceptance in the mobile phone community.

The second of these technologies, 802.15.4, goes even further than Bluetooth in exchanging speed for power. 802.15.4 offers data rates of up to 250 kbps, and can easily support links with a very low duty cycle. Hence, it is suitable for deployment in battery-powered devices that must survive for up to a year between charges. 802.15.4 has already found wide acceptance in the sensor network community, but it is still too early to predict its future in other markets (such as home automation devices).

Finally, ultra-wide band (UWB) radios emit low-power, high-bandwidth pulses that deliver data rates comparable to wired Ethernet. Its high data rates and relatively low power consumption make it ideal for replacing short wired links, like those found among PC peripherals and in home theaters. Unfortunately, IEEE standardization of UWB has failed, resulting in two incompatible standards: DS-UWB, advocated by the UWB Forum; and MB-OFDM, advocated by the WiMedia Alliance. Like 802.15.4, UWB is still in its first stages of deployment, making it difficult to predict its future success.

In this paper, we discuss the three standards described above. We highlight the differences in signaling principles and the various properties of their wireless links. Where applicable, we also describe the support layers that sit on top of the PHY and MAC layers. Finally, we discuss the security features of each technology, describe some current applications, and predict their outlook.

Back to Table of Contents

---

2 802.15.1 (Bluetooth)

802.15.1, more commonly known as Bluetooth, is a low-data-rate, low-power wireless networking standard aimed at replacing cables between lightweight devices [IEEE802.15.1]. The Bluetooth protocol stack, shown in Figure 1, is somewhat unusual compared to other IEEE networking stacks. The Bluetooth stack defines many components above the PHY and MAC layers, some of which are optional. This design permits the Bluetooth Special Interest Group to compose these components into application-specific *profiles*, as discussed below. In this section, we will provide a brief description of several of these components; the interested reader may consult [Prasad06] and [Bluetooth06a] for more details.

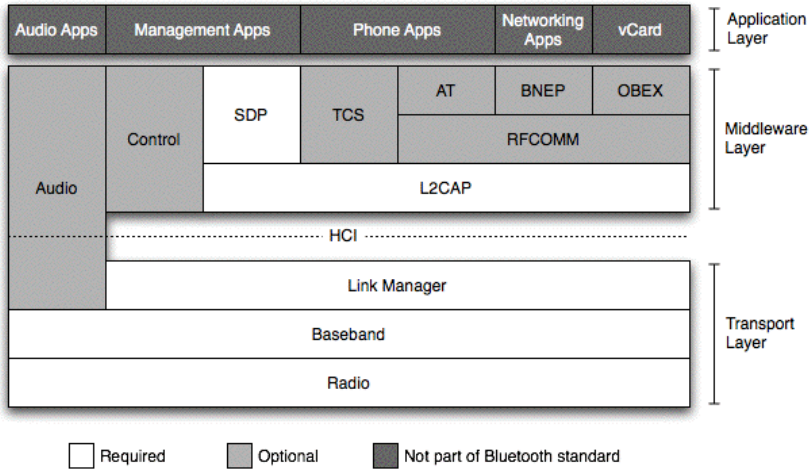

Figure 1: Bluetooth Protocol Stack

2.1 Transport layer

The Bluetooth transport layer is roughly equivalent to the traditional OSI PHY and MAC layers. All Bluetooth devices are required to implement this layer in hardware. The transport layer is composed from the radio, baseband, and link manager layers, which are described below.

2.1.1 Radio Layer

The radio layer dictates the frequency, power, and modulation used by Bluetooth antennas. Bluetooth occupies 79 channels of 1 MHz each in the 2.4 GHz spectrum, from 2.402 GHz to 2.480 GHz. Devices use only one of these channels at a time, hopping between them as described below. There are also guard bands reserved at either end of the spectrum, at 2.400 GHz–2.402 GHz and at 2.480 GHz–2.484 GHz. In the initial revisions of Bluetooth, all devices used BPSK modulation; this offers a maximum data rate of 1 Mbps, or about 723 kbps when all packet overhead is taken into account. (As discussed below, Bluetooth 2.0 adds optional modulations that support increase data rates.) Bluetooth receivers are required to have a bit-error rate (BER) of 0.1% or less.

Bluetooth devices are divided into one of three "Classes", which specify the antenna's output power. Class 1 devices broadcast using 1 mW to 100 mW of power; Class 2 devices broadcast using 0.25 mW to 2.5 mW of power; and Class 3 devices broadcast using up to 1 mW of power. Class 1 devices must be able to change their power output in increments of 2 dB to 8 dB; power control is optional for Class 2 and Class 3 devices. These power classes have signal ranges of approximately 100m, 10m, and 1m, respectively.

2.1.2 Baseband and Link Layers

At the baseband layer, Bluetooth devices form into *piconets* and/or *scatternets*. Piconets consist of one master device that communicates directly with up to 7 active slave devices. Piconets can also have up to 250 parked (i.e., inactive) slave nodes at any given time. Multiple piconets can also be combined into a single multi-hop scatternet.

Communication within a piconet occurs directly over the one-hop link between a master and a slave; slaves cannot communicate directly. Bluetooth uses a basic time-division duplexing (TDD) scheme, where time is divided into 625 µs slots. The master may communicate with a slave during the odd-numbered slots, and slaves respond during the even-numbered slots. Each packet may consume 1, 3, or 5 slots. After each packet, the piconet hops to a different Bluetooth channel; the next channel's frequency is determined using a pseudo-random number generator.

Piconet channels can be further subdivided into links that use one of five kinds of transports. The synchronous connection-oriented (SCO) transport reserves slots for synchronous communication; it is most often used to reserve 64 kbps links for voice data. Enhanced SCO (eSCO) links also reserves extra slots for packet retransmission; eSCO links can also steal other links' unused retransmission slots. Most links use the asynchronous connection-oriented logical (ACL) transport, where packets are transmitted during the remaining unreserved slots. Finally, the active slave broadcast (ASB) and parked slave broadcast (PSB) links are used for the master to send control data to active and parked slaves, respectively. All links besides ASB and PSB are reliable: each packet must be acknowledged individually by the receiver, and packets are appended with their CRC to ensure consistency. Links may optionally use 2/3 forward error correction (FEC).

Bluetooth defines three power-saving modes. In *hold mode*, devices only handle slots reserved for synchronous links, and sleep the rest of the time. In *sniff mode*, the device stays asleep most of the time, waking up periodically (from every 1.25 ms to every 40.9 s) to communicate. Finally, in *parked mode*, the device shuts down its links to the master device, excluding the PSB link. The master device can wake up parked devices by beaconing them over the PSB link.

2.2 Middleware Layer

The middleware layer consists of several software components that are designed to encourage interoperability among Bluetooth devices. Many of the components in this layer are optional; generally, only high-powered devices (like PCs) will implement the entire stack. The components in the middleware layer communicate with the transport layer using the standardized Host Controller Interface (HCI). Some of these components include:

- Logical Link Control and Adaptation Protocol (L2CAP): provides TCP- and UDP-like features to ACL links
- RFCOMM: emulates IrDA infrared links on top of L2CAP
- Telephony Control Protocol Specification (TCS): controls phone operations
- AT: controls phone operations using the legacy Hayes ("AT") command set
- Bluetooth Network Encapsulation Protocol (BNEP): encapsulates Ethernet packets in Bluetooth packets
- Object Exchange Protocol (OBEX): supports IrDA's object synchronization features

In the interest of promoting interoperability between Bluetooth devices, the Bluetooth SIG also defines *profiles*, which provide universal protocols for common application-specific tasks. Each profile is created by combining Bluetooth components with profile-specific software. For example, the File Transfer Profile (FTP), which allows Bluetooth-equipped devices to exchange files, consists of a specified client/server protocol built on top of the Radio, Baseband, Link Manager, L2CAP, RFCOMM, SDP, and OBEX components. As of this writing, the Bluetooth SIG defines 24 standard profiles, with several more in draft stages [Bluetooth06a].

2.3 Bluetooth Security

Bluetooth uses a *pairing* process to establish encryption and authentication between two devices. The pairing process is performed using a series of keys as an input to the SAFER+ block cipher. In the interest of brevity, we will not discuss here the inner workings of SAFER+ or the key generation in detail; the interested reader may consult [Shaked05] for more information.

In the first stage of the pairing process, the devices generate a shared 128-bit *initialization key* using the master's 48-bit hardware address; a shared 128-bit random number; and a user-specified PIN of up to 128 bits. The former two values are exchanged in plaintext, and the latter is manually inputted by the user into both devices. The devices then encrypt their link using this key, and negotiate a 128-bit *link key*. The two devices then use the link key to perform a challenge/response protocol. If successful, then the two devices store the link key and discard the initialization key. Any future communication between these two devices is optionally encrypted using a 128-bit session key based on this stored link key.

Unfortunately, it is possible to exploit weaknesses in some Bluetooth implementations in order to attack encrypted links [Shaked05]. If an attacker sniffs the packets used to pair two devices and can figure out the secret PIN, then the link key can easily be computed. Though such an attack is impractical when a 128-bit PIN is used, many Bluetooth devices only allow PINs constructed using 1 to 4 digits. These PINs are very weak and can be easily brute-forced: researchers were able to crack a 4-digit PIN in 63 ms on a 3 GHz Pentium 4 CPU. Fortunately, this attack is somewhat hard for a casual attacker to accomplish, since (s)he must be able to sniff the packets sent during the pairing process. However, a determined attacker may be able to force the two devices to pair again on demand using custom hardware.

There have also been many vendor-specific attacks on Bluetooth devices [Zetter04]. Many of the first Bluetooth-enabled mobile phones allowed attackers to access some Bluetooth components without first pairing with the device. These attacks, known as "Bluebugging" and "Bluesnarfing", have allowed researchers to place calls on other peoples' mobile phones, read their address books, and listen to their phone conversations. (For security reasons, the researchers involved have not publicly disclosed the exact methods used to accomplish these attacks.) Since these attacks exploit vendor-specific bugs in implementations of the Bluetooth stack, they are not an attack on the Bluetooth protocol per se. However, these attacks highlight the need to exhibit caution when implementing wireless network stacks, and the potential problems caused when an implementation is not ready for public consumption.

2.4 Bluetooth 2.0 EDR

As noted in [McCall04], Bluetooth's relatively limited data link rate hindered the combination of multiple Bluetooth devices. For example, simultaneous use of headphones, a mouse, and a keyboard would leave only about a quarter of the 723 kbps link available. Under realistic link conditions, this margin would be insufficient to ensure timely packet retransmissions, resulting in corrupted audio and jumpy mouse motion.

To combat this problem, the Bluetooth 2.0 specification defines two optional Enhanced Data Rate (EDR) extensions. These extensions use π/4-Phase Differential Quaternary Phase-Shift Keying (π/4-DQPSK) and 8-Phase Differential Phase-Shift Keying (8DPSK) modulation to transmit Bluetooth packet payloads, increasing the link rate to approximately 2 Mbps and 3 Mbps respectively. To reduce transmission overhead, EDR also disables Forward Error Correction; EDR devices drop back to the standard 1 Mbps data rate when the BER is above 0.01%. To ensure backwards compatibility with non-EDR compliant devices, the Bluetooth packet headers are always transmitted using BPSK modulation, regardless of the modulation used to transmit the payload. The EDR specification also inserts a short guard band and a synchronization sequence between the header and the payload, to accommodate for the transition between the two modulations.

2.5 Applications and Future Outlook

Bluetooth is a mature technology that has been widely adopted by the mobile phone industry. The Bluetooth SIG estimates an installed base of 250 million Bluetooth-equipped devices by the end of 2004, and projected that this would double by the end of 2005 [Edlund05]. Bluetooth has not been accepted as rapidly by PC peripherals as by mobile phone accessories, likely in large part because Microsoft Windows did not provide first-party support for Bluetooth until the release of Windows XP Service Pack 2 in August 2004 [Andersen04].

In 2005, Sony announced that the PlayStation 3 video game console would use Bluetooth to communicate with wireless gamepads and accessories [Smith05]. Sony has sold over 100 million each of its two previous-generation PlayStation consoles since they were released in 1994 and 2000, respectively [Sony05]. If the PlayStation 3 meets with similar success in the marketplace, it could have a significant impact on consumer acceptance of Bluetooth devices beyond the mobile phone market.

Though the Bluetooth standard seems to have a bright future, the days of the 802.15.1 radio layer may be numbered. The Bluetooth SIG has recently announced plans to abandon the 802.15.1 PHY and MAC layers in some future version of the Bluetooth standard, and instead deploy the middleware components on top of a variant of the WiMedia UWB standard discussed in Section 4 [Bluetooth06b]. Depending on how the radio stack is implemented, this shift may increase Bluetooth's data rate by tens or hundreds of times, drastically cut power consumption, or both. However, the success of this shift may depend on other factors that are still being ironed out. Perhaps most importantly, it is not clear whether the Bluetooth SIG will maintain backwards compatibility with existing Bluetooth devices, since UWB radios operate on a very different principle than 802.15.1.

Back to Table of Contents

---

3 802.15.4/ZigBee

Although Bluetooth's power requirements are much lower than that of 802.11b, it is still assumed that Bluetooth-enabled devices will be recharged every few days. The IEEE 802.15.4 standard defines the PHY and MAC for very low-power, low-duty network links [IEEE802.15.4]. This standard is intended for deployment on long-lived systems with low data rate requirements, where devices must be able to operate autonomously for months or even years without recharging the battery. In this section, we will discuss the capabilities of 802.15.4, as well as those of the complementary ZigBee standard [ZigBee]. Many of the technical details discussed here are drawn from [Gutierrez03], where the reader may find further technical details.

3.1 802.15.4 PHY and MAC Layers

802.15.4 offers uses twenty-seven channels spread across three different areas of license-exempt spectrum. One channel is available at 868 MHz. Ten channels are available from 902 MHz to 928 MHz, with a separation of 2 MHz between channels. Sixteen channels are available from 2.4 GHz to 2.4835 GHz, with a channel separation of 5 MHz. Like Bluetooth, these channels are used to avoid interference with neighboring PANs: each PAN uses a single unique channel. However, unlike Bluetooth, devices do not hop across frequencies during the network's lifetime. 802.15.4 radios are required to transmit at a minimum of 1 mW, and must maintain a BER of less than 1%. Depending on the power output, 802.15.4 offers a range of approximately 1m to 100m, which is comparable to Bluetooth.

Direct-sequence spread spectrum modulation is used to minimize data loss due to noise and interference, though the exact parameters differ from spectrum to spectrum. The channels in the 2.4 GHz spectrum use a combination of 32-chip codes and QPSK modulation; these channels have a signal rate of 2.0 Mchips/s and a data rate of 250 kbps. The other channels use BPSK modulation with 15-chip codes. The 868 MHz channel has a signal rate of 300 kchips/sec and a data rate of 20 kbps, whereas the 900 MHz channels have a signal rate of 600 kchips/s and a data rate of 40 kbps.

802.15.4 devices can be divided into two categories, which determine the topology and media access used by the network. Full-function devices (FFDs) can communicate directly with any other devices in the network. In contrast, reduced-function devices (RFDs) can only communicate with FFDs. The 802.15.4 standard allows networks to form either a one-hop star topology, or a multi-hop peer-to-peer topology; the former is most appropriate in networks with few FFDs, whereas the latter is more resilient to node failure when many FFDs are available. Though 802.15.4 defines the allowed topologies, it does not define the layers that actually support them: routing within these topologies is the responsibility of layers above those defined by IEEE.

One FFD can optionally act as a coordinator node, which regulates media access. This node periodically sends beacons that identify the PAN it is coordinating. The interval between these beacons is constant but user-selectable: any multiple of 15.38 ms may separate these beacons, up to 252s. Two beacons form a *superframe* that is partitioned into 16 equally-sized timeslots, as shown in Figure 2. Members of the PAN may request guaranteed time slots (GTSs) in the contention free period at the end of the superframe. All other slots form the contention access period, which is accessed using a CSMA-CA scheme. Since the coordinator node must be relatively powerful, it may not be practical to deploy one in all networks; in this case, all media access is regulated using a CSMA-CA scheme, and the media is always subject to contention.

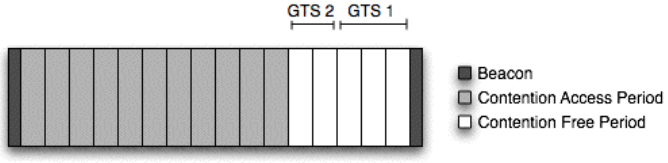

Figure 2: Example 802.15.4 Superframe

3.2 ZigBee

As with many IEEE networking standards, the 802.15.4 standard only defines the PHY and MAC layers. The ZigBee standard extends 802.15.4 to provide Bluetooth-like interoperability features. (Though the term "ZigBee" is often used interchangeably with "802.15.4", this is not quite accurate: devices that implement the 802.15.4 standard are not necessarily ZigBee compatible.) ZigBee builds on top of 802.15.4's radio layer, specifying network, security, and application layers, as described in detail in [Sturek05]. The resulting architecture is shown in Figure 3.

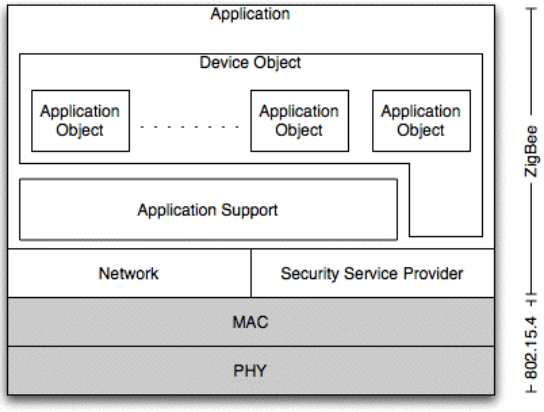

Figure 3: ZigBee Protocol Stack

ZigBee refines 802.15.4's two device categories into three hierarchical device roles. *Coordinators* are 802.15.4 FFDs that act as 802.15.4 coordinator nodes and maintain ZigBee-specific information about the PAN (master encryption keys, etc.). *Routers* are 802.15.4 FFDs that participate in ZigBee's routing protocols. *End devices* are analogous to 802.15.4's RFDs: they must communicate with each other by way of an intermediary coordinator or router.

ZigBee maintains 802.15.4's star topology, but divides the peer-to-peer topology into cluster and mesh formations. Cluster topologies create links between routers and coordinators opportunistically using a beaconing scheme. Mesh topologies maintain a relatively fixed routing infrastructure, using a simplified version of the Ad-hoc On-demand Distance Vector (AODV) routing scheme proposed for ad-hoc networks [RFC3561]. Cluster topologies have the advantage that coordinators

and routers may sleep periodically to extend battery life, whereas their counterparts in mesh networks must maintain constant availability. However, the routing delays in cluster topologies are unpredictable and often much higher than those in mesh networks.

ZigBee also provides Bluetooth-like device and service discovery. Manufacturers describe a device's role and capabilities using a static *device object*. Device objects contain descriptions of the device's type, power profile, and communication endpoints, as well as optional "complex" fields describing device- or manufacturer-specific information. Likewise, each device's service is described using an *application object* that encapsulates its attributes and capabilities. (ZigBee does not define the format of application objects; this is left to the discretion of manufacturers.) ZigBee devices can perform unicast or broadcast queries to discover other devices and/or perform service matchmaking. ZigBee also supports *binding* of some classes of complementary devices (e.g., between ZigBee-enabled light switches and automated light sockets), which automatically creates and maintains links between devices based on their application profiles.

3.3 802.15.4 Security

802.15.4-compliant MAC layers are required to encrypt packets using the AES-128 algorithm when a private key is provided by the upper layers. However, 802.15.4's security features are otherwise unsophisticated. 802.15.4 does not define how AES keys are to be distributed and selected throughout the PAN: as with much of the 802.15.4 standard, this decision is left to the discretion of the upper layers. Likewise, it does not inherently protect nodes from replay attacks; application and/or device developers must manually build replay protection on top of 802.15.4's AES encryption.

ZigBee builds on top of 802.15.4's AES support to provide a much more thorough security layer. We discuss here the high-level details of ZigBee's two security modes. Because of the complexity of ZigBee's security schemes, it is not possible to provide low-level details of these mechanisms here. The interested reader may consult [Reddy05] for further details.

The simpler of ZigBee's two security modes is *residential mode*. Residential mode uses a single, pre-deployed key for the entire PAN and all applications. Because a single static key is used for all links, very little overhead is involved. While residential mode protects the local PAN from eavesdroppers, it does not protect the security of packets from malicious nodes within the same PAN.

Commercial mode, the second of ZigBee's security modes, improves on the security features of residential mode. In commercial mode, two master keys are pre-deployed in a *trust center* that resides on the coordinator node. Other devices negotiate with the trust center to derive per-link keys from one of these two master keys. The trust center maintains a list of these per-link keys along with their corresponding age, which can be used to detect replay attacks using old keys. However, the increased security of commercial node comes at the cost of infrastructure. Network administrators must deploy a powerful coordinator node which can be reached from all devices on the network, and which has enough local resources to maintain the trust center's data structures.

3.4 Applications and Future Outlook

802.15.4 has been rapidly adopted by the sensor network community, where battery life is at a premium and developers are accustomed to radios that transmit at a fraction of 802.15.4's data rate. Telos sensor nodes [Polastre05] and Intel's next-generation Intel Mote 2 sensor platform [Intel] both use 802.15.4-compatible radios. Telos motes are already commercially available, and offer several times the data rate and twice the expected battery life of previous-generation sensors. Researchers have proposed using 802.15.4- or ZigBee-enabled sensors joined by a Bluetooth or 802.11b backbone to create powerful systems for healthcare monitoring [Eklund05] and industrial automation [Neelakanta03].

ZigBee has also been positioned as a standard for communication among home automation devices, such as wireless electrical switches. In 2005, several ZigBee-enabled devices were demonstrated at the ZigBee Alliance Open House and Member Meeting [Louderback05]. However, as of this writing, no ZigBee-enabled home automation devices appear to be available for purchase. Moreover, existing home automation protocols like X10 have existed in one form or another for decades, but devices based on these protocols have become little more than a niche market. Thus, ZigBee's future in household devices is still somewhat unclear.

Back to Table of Contents

---

4 Ultra-Wide Band

Ultra-wide band (UWB) radios take a drastically different approach from Bluetooth and 802.15.4. Where the latter two radios emit signals over long periods using a small part of the spectrum, UWB takes the opposite approach: UWB uses short pulses (in the ps to ns range) over a large bandwidth (often many GHz). According to Shannon's Law, the maximum data rate of a radio link can be increased much more efficiently by increasing its bandwidth than by increasing its power; hence, UWB radios offer very high data rates (hundreds of Mbps or even several Gbps) with relatively low power consumption. The use of short pulses over a wide spectrum also means that the signal is below the average power output defined as noise by the FCC (-41.3 dBm/MHz), and that UWB signals are not susceptible to noise or jamming.

UWB is a much simpler technology than Bluetooth and ZigBee, since there are currently no mandatory or optional middleware layers that build on top of the basic PHY and MAC layers. There are currently two major competing UWB standards. In this section, we will describe how these two standards specify these two layers. We will also briefly discuss IEEE efforts to create a unified UWB standard, as well as potential future applications for UWB technology.

4.1 Direct Sequence-UWB (UWB Forum)

Direct Sequence-UWB (DS-UWB) is the more straightforward of the two approaches. DS-UWB radios use a single pulse, like one shown in Figure 4, in one of two different spectra. These pulses may occur in the spectrum from 3.1 GHz - 4.85 GHz, or at 6.2 GHz - 9.7 GHz.

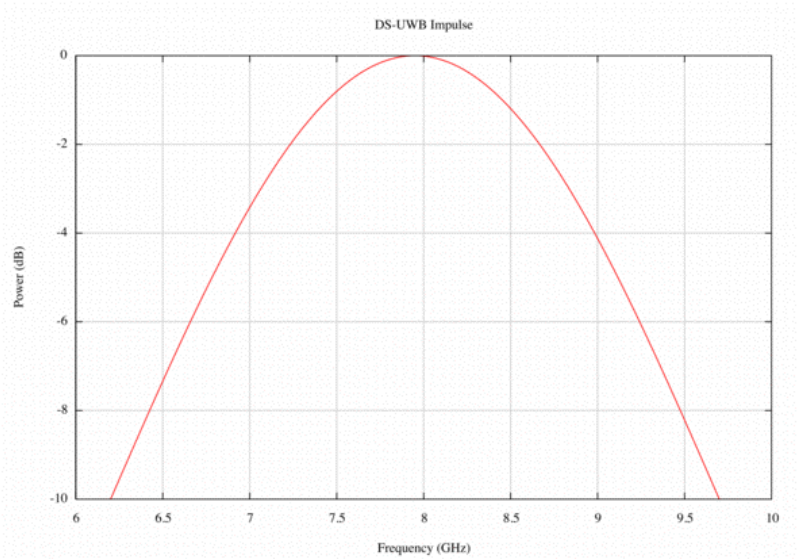

Figure 4: DS-UWB Impulse

Aside from the two different ranges of spectrum, the DS-UWB spectrum supports a wide range of parameters that have a significant effect on the link's usable data rate. Implementers may use 4-BOK modulation (2 bits/signal) where the signal quality permits, or BPSK modulation (1 bit/signal) where the signal quality is poorer or the higher data rate is not needed. To further combat noise, DS-UWB allows optional forward error correction with rates of 1/2, 3/4, or 1. Finally, DS-UWB radios employ code sequences that use anywhere from 1 to 24 pulses to transmit a bit, again depending on the signal quality. Depending on the parameters selected, DS-UWB radios can achieve a data rate between 55 Mbps to 1.32 Gbps in the 3.1 GHz band, or 55 Mbps to 2 Gbps in the 6.2 GHz band.

The DS-UWB approach has been standardized by the UWB Forum, which specifies a standard MAC for DS-UWB-based devices [UWB]. The UWB Forum FAQ notes that this MAC layer would use "a combination of code division, offset operating frequencies, and FDM to allow multiple piconets to appear as white noise to each other", thus fully or partially avoiding the need to resolve media contention among nearby PANs [UWB06]. Unfortunately, the UWB Forum does not make its specifications available to the public, so it is not possible to discuss more in-depth technical details of the MAC layer here.

4.2 Multi-Band OFDM (WiMedia)

Multi-Band Orthogonal Frequency Division Multiplexing (MB-OFDM) uses a slightly different approach to signaling from DS-UWB. Rather than using a single pulse over a wide band, MB-OFDM divides the spectrum into multiple sub-bands, as shown in Figure 5. As with Bluetooth, MB-ODFM signals hop across these sub-bands in a predictable fashion: the radio hops between frequencies every 312.5 ns, with a 9.5 ns guard in-between hops. The MB-OFDM standard as defined by the WiMedia Alliance [WiMedia] uses the spectrum from 3.1 GHz to 10.6 GHz, which is divided into 14 equally-sized sub-bands of 528 MHz each.

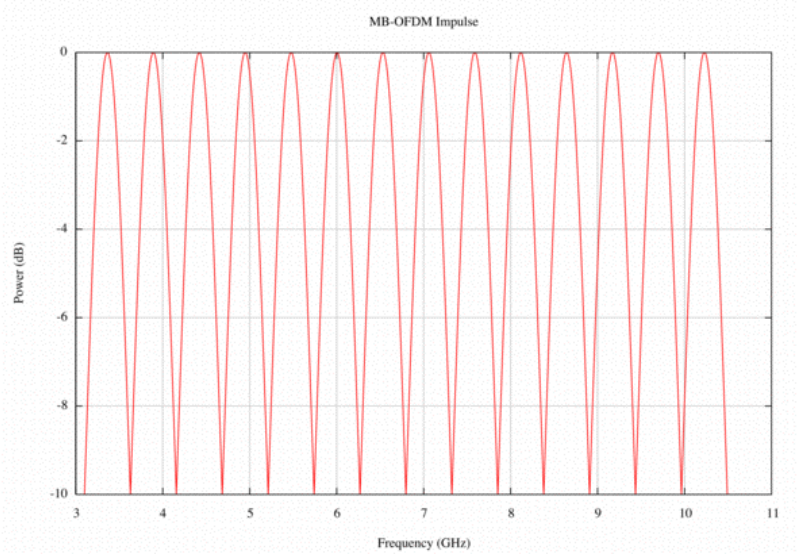

Figure 5: MB-OFDM Impulse

Like DS-UWB, MB-OFDM's data rate varies depending on the encoding chosen. However, MB-OFDM offers implementers fewer tunable parameters than DS-UWB. MB-OFDM signals use QPSK modulation (2 bits/signal) and support forward error correction rates of 1/3, 1/2, 5/8, or 3/4. MB-OFDM radios may interleave these coded transmissions over three sub-bands simultaneously, or they may use only a single band. Depending on the selected parameters, MB-OFDM offers data rates ranging from 53.3 Mbps to 480 Mbps.

The WiMedia Alliance defines a MAC layer to be used in conjunction with MB-OFDM radios. Though the WiMedia standard is not IEEE-certified, it has been submitted to Ecma International, and is available to the public [Ecma05]. In the interest of brevity, we will only provide a high-level discussion of the MAC layer's

features here; the reader may consult [Ecma05] for more low-level details.

WiMedia packets may be sent in either unicast or broadcast fashion. Unicast packets are directed to their destination based on a 16-bit device address; certain addresses are also reserved for broadcast groups. Unlike Ethernet MAC addresses — which are assumed to be globally unique — WiMedia makes no guarantees about the uniqueness of device addresses. Instead, the WiMedia standard defines a scheme for resolving address conflicts. Like ZigBee, WiMedia devices can transmit special packets to reserve transmission slots or contend for non-reserved slots. Unlike ZigBee, WiMedia's reservations are carried out in a decentralized fashion, rather than using a centralized coordinator node.

4.3 UWB Security

UWB radios are somewhat inherently secure, because their low output power and short pulses make their transmissions appear to be white noise from a distance. Nevertheless, UWB signals could potentially be sniffed by a determined attacker who is located close to the transmitter; this mandates the use of security at the MAC layer. As described above, the UWB Forum's specifications are not open to the public, so a discussion of security features employed by their DS-UWB standard is not possible here. However, it is possible to discuss WiMedia's MAC-level security features. Again, due to the complexity of the topic, we refer the reader to [Ecma05] for more in-depth discussion than is possible here.

WiMedia defines three levels of link-layer security. In Security Level 0, devices send data fully unencrypted. Devices that support Security Level 1 establish encrypted links with other Security Level 1 devices, but can also establish unencrypted links with devices that do not support encryption. Finally, Security Level 2 mandates that all links must be encrypted; devices at this security level cannot establish links with devices in the previous two levels.

WiMedia devices use AES-128 to encrypt packets at the link level. Each device is equipped with one or more pre-defined 128-bit master keys. To prevent devices from sending this key in plaintext, each master key has a corresponding master key ID (MKID). When two devices connect, they exchange their MKIDs to establish a common master key, and then use this common key to negotiate a unique per-link key. AES-128 is used in counter mode, which XORs the plaintext with a counter that is incremented for each message; this effectively converts the fixed master and link keys to temporal keys. Devices use a basic challenge/response handshaking protocol during link establishment; they exchange random nonces during this protocol in order to prevent replay attacks.

In order to secure broadcast transmissions, each group also has a common group transient key (GTK). The GTK is exchanged using a gossiping scheme when two devices establish an encrypted link. During the handshaking process, devices in common groups exchange the corresponding GTKs if one of the two devices has it in local storage. It is unclear from the WiMedia specification how the GTK is created in the first place, but presumably it is generated by the first device to join the group.

4.4 Standardization Efforts

The IEEE 802.15.3a Task Group [IEEE802.15.3a] was formed in 2003 to create a common, industry-wide standard for UWB devices. Unfortunately, the group quickly divided into opposing camps. Some companies promoted DS-UWB, arguing that MB-OFDM's frequency-hopping required complicated synchronization schemes. Other companies preferred MB-OFDM, arguing that its frequency-hopping scheme made it less susceptible to interference from neighboring UWB PANs. Ultimately, efforts to create a hybrid standard failed, and the group disbanded in January 2006 [Mannion06]. The two camps decided to commercialize their respective standards anyway, forming the UWB Forum and WiMedia Alliance industry groups to drive standardization and interoperability efforts.

IEEE has since moved forward with the 802.15.3c Task Group [IEEE802.15.3c]. This group aims to derive a standard for millimeter-wave UWB devices, which are projected to offer data rates of over 2 Gbps. Because this group was established in March 2005, very little headway has been made as of this writing. However, IBM has recently announced the first prototype millimeter-wave chipset [IBM06], which it proposes using as a basis for the 802.15.3c standard.

4.5 Applications and Future Outlook

UWB is mainly advocated as a cable-replacement technology like Bluetooth, except for devices with much higher data-rate requirements. In January 2006, Belkin announced the very first UWB-enabled product, a wireless USB hub using the DS-UWB-based CableFree protocol [Belkin06]. The USB Implementers Forum is developing an official Wireless USB standard, which will sit on top of the WiMedia stack and provide USB 2.0-like speeds of 480 Mbps when devices are within 3 m [USB06]. As discussed above, the WiMedia standard will form the basis for a future version of the Bluetooth radio layer. Finally, because UWB's data rate is high enough to support HDTV streams, it has been suggested as a replacement for audio/video cables in home theaters [Nekoogar05].

However, like 802.15.4/ZigBee, UWB technology is still in its infancy. As of this writing, only a handful of UWB-enabled products have been announced, and none have shipped. UWB also faces challenges that may affect its commercial acceptance. First, UWB technology has already been divided into two incompatible standards. The recent announcement of Freescale's plans to develop its CableFree standard independently of the UWB Forum may divide the market even further [Judge06]. Unless one UWB standard becomes dominant very quickly, consumers may hesitate to buy UWB devices.

Second, because of the low average power of UWB radios, signal quality drops off rapidly as the transmitter and receiver move apart, which may frustrate consumers who are used to longer-range technologies like Bluetooth. For example, Wireless USB's projected data rate drops from 480 Mbps to 110 Mbps when the devices are separated by 10 m, a loss of almost 80%. This issue may be partially-addressed by the forthcoming 802.15.5 standard [IEEE802.15.5], which will allow UWB devices to form mesh networks. In principle, this will allow two UWB devices located far apart to form a multi-hop link using a series of shorter, higher-quality links among intermediate nodes. However, like the 802.15.3c Task Group, the 802.15.5 Task Group has not yet produced any standards as of this writing. Moreover, the 802.15.5 standard may require MAC layer changes for full functionality [Sim06]; devices that have been deployed before the standard is finalized might not be able to take advantage of its features.

Back to Table of Contents

---

5 Summary

PANs represent a dramatic shift in wireless networking technology, which has generally been targeted at devices like laptops where power consumption is not a major issue. PAN technology emphasizes constructing reliable links over low-power radios, but often at the cost of a reduced data rate compared to Wi-Fi. In this paper, we have discussed three prominent PAN technologies, whose features and characteristics are summarized below in Figure 6.

	Bluetooth	802.15.4		UWB	
		standard	w/ZigBee	UWB Forum	WiMedia

Radio Spectrum	2.4 GHz	868 MHz, 915 MHz, 2.4 GHz		3.1 GHz - 4.85 GHz, 6.2 GHz - 9.7 GHz	3.1 GHz - 10.6 GHz
Max. Data Rate	3 Mbps	250 kbps		2 Gbps	480 Mbps
Radio Power	< 100 mW	> 1 mW		Depends on bandwidth; < 0.074 mW/GHz	
Max. Range	1 m - 100 m	1 m - 100 m		Unknown, probably low[1]	
Network Topologies	Cluster, multi-hop cluster	Star, peer-to-peer[2]	Star, cluster, mesh	Unknown[3]	Peer-to-peer
Media Access	TDD, frequency hopping	CSMA-CA, optional TDD		Unknown[3]	CSMA-CA, OFDM, optional TDD
Optional Security Features	SAFER+, key negotiation (known weaknesses)	AES-128	AES-128, key authority	Unknown[3]	AES-128, key negotiation
Applications	Low-bandwidth cable replacement	Sensors, home automation		High-bandwidth cable replacement	

[1] Neither the UWB Forum nor WiMedia Alliance disclose exact ranges. Due to UWB's low power output, its range should be much lower than Bluetooth's or 802.15.4's.
[2] IEEE 802.15.4 defines these topologies, but upper layers are responsible for actually supporting and maintaining them.
[3] The UWB Forum does not publicly disclose technical specifications.

Figure 6: A Comparison of PAN Technologies

Currently, by far the most widely-accepted of these technologies is Bluetooth, which has been deployed in hundreds of millions of devices worldwide. The initial revisions of Bluetooth featured a ~1Mbps data rate along with several days of battery life; these characteristics are a good fit for the mobile phone market, where Bluetooth has found its greatest success. Its middleware layer also simplifies coupling phones with PCs and wireless accessories, further fueling its acceptance. Bluetooth's success has not yet been replicated outside of the mobile phone market; but recent data rate increases to Bluetooth 2.0 aim to rectify this, as do plans to move to a UWB-based radio.

802.15.4 takes an even further step in the low-data-rate, low-power direction characterized by PAN technology. It offers 250 Kbps data rates at a power consumption rate even lower than that of Bluetooth's. ZigBee extends 802.15.4 to offer some middleware functionality comparable to Bluetooth's middleware layer. Because of 802.15.4's low power consumption, it has been quickly accepted by the sensor network community. However, its future as a home automation standard still stands to be seen.

UWB attempts to reverse the trend of trading power efficiency for data rate, by using low-power, high-bandwidth bursts instead of the medium-power, low-bandwidth streams used by other wireless radios. This allows UWB links to deliver data rates in the Mbps to Gbps range at close range, which is ideal for replacing high-bandwidth cables. UWB technology is still in its infancy, so its fate is difficult to predict. Though the technology is sound for many applications, the splintering of UWB into at least two incompatible standards may hurt its chances for long-term success.

Back to Table of Contents

References

[Bluetooth06a] Bluetooth SIG, "Specification documents", Bluetooth specifications, 2006, https://www.bluetooth.org/spec/. A list of Bluetooth SIG specifications.

[ECMA05] ECMA, "Standard ECMA-386: High Rate Ultra Wideband PHY and MAC Standard", Ecma standard, December 2005, http://www.ecma-international.org/publications/files/ECMA-ST/ECMA-368.pdf. The WiMedia specification, published by Ecma International.

[Gutierrez03] J. Gutierrez, "P802.15.4 TG4 tutorial", IEEE submission, January 2003, http://grouper.ieee.org/groups/802/15/pub/2003/Jan03/03036r0P802-15_WG-802-15-4-TG4-Tutorial.ppt. An IEEE presentation describing 802.15.4 overall.

[Sturek05] D. Sturek, "ZigBee architecture and specifications overview", ZigBee Alliance presentation, December 2005, http://www.zigbee.org/en/events/documents/December2005_Open_House_Presentations/043120r008ZB_Architecture-ZigBeeV1-0Architecture.pdf. A presentation describing ZigBee's general features.

[Reddy05] J. Reddy, "ZigBee security layer technical overview", ZigBee Alliance presentation, December 2005, http://www.zigbee.org/en/events/documents/December2005_Open_House_Presentations/ZigBee_Security_Layer_Technical_Overview.pdf. A presentation describing ZigBee's security features in further depth.

[Fisher05] R. Fisher, R. Kohno, H. Ogawa, H. Zhang, K. Takizawa, M. M. Laughlin, and M. Welborn, "DS-UWB physical layer submission to 802.15 task group 3a", IEEE submission, January 2005, http://www.decawave.com/15-04-0137-04-003a-merger2-proposal-ds-uwb-update.doc. An IEEE presentation with a high-level overview of DS-UWB.

[Prasad06] R. Prasad, *From WPANs to personal networks: technologies and applications*, Artech House, 2006. A book that discusses various WPAN technologies.

[Nekoogar05] F. Nekoogar, *Ultra-Wideband Communications: Fundamentals and Applications,* Prentice Hall, 2005, http://proquest.safaribooksonline.com/0131463268. A book that describes the fundamentals of UWB.

[IEEE802.15.1] IEEE, "IEEE 802.15 WPAN Task Group 1 (TG1)", IEEE Task Group, http://www.ieee802.org/15/pub/TG1.html.

[IEEE802.15.3a] IEEE, "IEEE 802.15 WPAN High Rate Wave Alternative PHY Task Group 3a (TG3a)", IEEE Task Group, http://www.ieee802.org/15/pub/TG3a.html.

[IEEE802.15.3c] IEEE, "IEEE 802.15 WPAN Millimeter Wave Alternative PHY Task Group 3c (TG3c)", IEEE Task Group, http://www.ieee802.org/15/pub/TG3c.html.

[IEEE802.15.4] IEEE, "IEEE 802.15 WPAN Task Group 4 (TG4)", IEEE Task Group, http://www.ieee802.org/15/pub/TG4.html.

[ZigBee] ZigBee Alliance, "ZigBee Alliance", WPAN industry group, http://www.zigbee.org/. The industry group responsible for the ZigBee standard and certification.

[WiMedia] WiMedia Alliance, "WiMedia Alliance", UWB industry group, http://www.wimedia.org/. The industry group responsible for the WiMedia standard and certification.

[UWB] UWB Forum, "UWB Forum", UWB industry group, http://www.uwbforum.org/. An industry group responsible for various UWB standards, most notably one based on DS-UWB.

[IEEE802.15.5] IEEE, "IEEE 802.15 WPAN Task Group 5 (TG5)", IEEE Task Group, http://www.ieee802.org/15/pub/TG5.html.

[Sim06] M. Sim, "Mesh networking considerations for IEEE 802.15.3", IEEE submission, January 2006, ftp://ieee:wireless@ftp.802wirelessworld.com/15/06/15-06-0056-00-0005-mesh-networking-considerations-ieee-802-15-3.ppt. An IEEE presentation describing the high-level goals that the 802.15.5 standard should address.

[McCall04] D. McCall, "Taking a walk inside Bluetooth EDR", CommsDesign article, December 2004, http://www.commsdesign.com/printableArticle/?articleID=55800768. A discussion of the changes made to Bluetooth to support EDR.

[Shaked05] Y. Shaked and A. Wool, "Cracking the Bluetooth PIN", in *MobiSys '05: Proceedings of the 3rd international conference on Mobile systems, applications, and services*, pp. 39-50, 2005, http://www.eng.tau.ac.il/~yash/mobisys05.pdf. A MobiSys paper about brute-force attacks on Bluetooth link keys.

[RFC3561] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing", IETF Request for Comments, July 2003, http://www.ietf.org/rfc/rfc3561.txt. An ad-hoc routing protocol, which is used in modified form by ZigBee.

[Zetter04] K. Zetter, "Security cavities ail Bluetooth," Wired News article, August 2004, http://wired.com/news/privacy/0,1848,64463,00.html. A Wired News article about various attacks on specific vendors' Bluetooth stacks.

[Neelakanta03] P. S. Neelakanta and H. Dighe, "Robust factory wireless communications: a performance appraisal of the Bluetooth and the ZigBee colocated on an industrial floor," in *Proc. 29th Annual Conference of the IEEE Industrial Electronics Society (IECON '03)*, volume 3, pp. 2381-2386, 2003, http://ieeexplore.ieee.org/iel5/9011/28610/01280617.pdf (subscription to IEEE online library required). An IECON paper describing how well Bluetooth and ZigBee share the same spectrum; also, a brief discussion of why both are useful for industrial applications.

[Eklund05] J. M. Eklund, T. R. Hansen, J. Sprinkle, and S. Sastry, "Information technology for assisted living at home: building a wireless infrastructure for assisted living," in *Proc. 27th International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC 2005)*, September 2005, http://www.eecs.berkeley.edu/~eklund/Papers/EMBC2005_SensorNet.pdf. An EMBC paper discussing the use of wireless networks, including WPANs like Bluetooth, to monitor elderly patients.

[UWB06] UWB Forum, "Technical FAQ", 2006, http://www.uwbforum.org/index.php?option=com_content&task=view&id=25&Itemid=50. Brief, high-level information about the UWB Forum's standards.

[USB06] USB Implementers Forum, "Certified Wireless USB from the USB-IF", USB Implementers Forum standard, 2006, http://www.usb.org/developers/wusb/. Information and specifications about the official Wireless USB standard.

[Edlund05] A. Edlund, "Bluetooth wireless technology — 2005 update," Bluetooth SIG report, 2005, http://www.touchbriefings.com/pdf/1433/Edlund.pdf. A look at the state of Bluetooth deployments in 2005

[Mannion06] P. Mannion, "Ultrawideband standards committee disbanding", EE Times article, January 2006, http://www.eetimes.com/article/showArticle.jhtml?articleID=177101766. An EE Times article noting the dissolution of the IEEE 802.15.3a task group.

[Bluetooth06b] Bluetooth SIG, "Bluetooth SIG selects WiMedia Alliance ultra-wideband technologoy for high speed Bluetooth applications", Bluetooth SIG press release, March 2006, http://www.bluetooth.com/Bluetooth/Press/SIG/BLUETOOTH_SIG_SELECTS_WIMEDIA_ALLIANCE_ULTRAWIDEBAND_TECHNOLOGY_FOR_HIGH_SPEED_BLUETOOTH_APPLICATION.htm. A Bluetooth SIG/WiMedia press release describing plans to use WiMedia radios in a future version of Bluetooth.

[Judge06] P. Judge, "Freescale flounces out of own UWB club", Techworld article, April 2006, http://www.techworld.com/news/index.cfm?newsID=5756. A Techworld article describing Freescale's plans to leave the UWB Forum.

[Polastre05] J. Polastre, R. Szewczyk, and D. Culler, "Telos: Enabling ultra-low power wireless research", in *Proc. 4th International Symposium on Information Processing in Sensor Networks (IPSN'05)*, pp. 364 - 369, April 2005, http://www.polastre.com/papers/spots05-telos.pdf. An IPSN paper describing an 802.15.4-enabled mote.

[Intel] Intel Research, "Intel Mote 2 Overview", Intel Research whitepaper, http://www.intel.com/research/downloads/imote_overview.pdf. An Intel whitepaper discussing their ZigBee-enabled mote platform.

[Louderback05] J. Louderback, "ZigBee ushers in age of connected devices", ExtremeTech article, March 2005, http://www.extremetech.com/article2/0,1558,1771993,00.asp. An overview of the home automation devices demonstrated at ZigBee Alliance's open house in 2005.

[IBM06] IBM Research, "IBM scientists demonstrate chipset to boost wireless communications", IBM Research press release, February 2006, http://domino.research.ibm.com/comm/pr.nsf/pages/news.20060206_mmwave.html. A press release announcing the first prototype milimeter-wave chipset.

[Smith05] T. Smith, "Sony details PlayStation 3," The Register article, May 2005, http://www.theregister.co.uk/2005/05/17/sony_unveils_ps3/. A list of announced features for the PlayStation 3 video game console, including its use of Bluetooth.

[Belkin06] Belkin Corporation, "Belkin CableFree USB hub enables instant wireless connectivity of USB devices", Belkin press release, January 2006, http://www.belkin.com/pressroom/releases/uploads/01_03_06CableFreeUSB.html. An announcement of the first UWB device.

[Andersen04] S. Andersen and V. Abella, "Changes to functionality in Microsoft Windows XP service pack 2", Microsoft technical document, August 2004,

http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/sp2netwk.mspx. A list of the networking features changed by Windows XP SP2, including the introduction of a first-party Bluetooth stack.

[Sony05] Sony Computer Entertainment, "PlayStation 2 breaks record as the fastest computer entertainment platform to reach cumulative shipment of 100 million units", Sony press release, November 2005, http://www.scei.co.jp/corporate/release/pdf/051130e.pdf. A press release highlighting the sales of the PlayStation series of video game consoles.

Back to Table of Contents

List of Acronyms

π/4-DQPSK	π/4-Phase Differential Quaternary Phase-Shift Keying
4-BOK	Quaternary Bi-Orthogonal Keying
8DPSK	8-Phase Differential Phase-Shift Keying
ACL	Asynchronous Connection-oriented Logical [Bluetooth transport]
AODV	Ad-hoc On-demand Distance Vector [routing]
ASB	Active Slave Broadcast [logical Bluetooth transport]
BER	Bit-Error Rate
BNEP	Bluetooth Network Encapsulation Protocol
BPSK	Bi-Phase Shift Keying
CSMA-CA	Carrier Sense Multiple Access, Contention Avoidance
DSSS	Direct-Sequence Spread Spectrum
DS-UWB	Direct-Sequence Ultra-Wide Band
EDR	[Bluetooth 2.0] Enhanced Data Rate
eSCO	Extended SCO
FFD	[802.15.4] Full-Function Device
GTK	[WiMedia] Group Transient Key
GTS	[802.15.4] Guaranteed Time Slot
HCI	[Bluetooth] Host Controller Interface
L2COM	Logical Link Control and Adaptation Protocol
MAC	Media Access Control [networking layer]
MB-OFDM	Multi-Band OFDM
MKID	[WiMedia] Master Key ID
PHY	PHYsical [networking layer]
PSB	Parked Slave Broadcast [logical Bluetooth transport]
OBEX	Object Exchange Protocol
OFDM	Orthogonal Frequency Division Multiplexing
RFD	[802.15.4] Reduced-Function Device
SCO	Synchronous Connection-Oriented [logical Bluetooth transport]
SIG	Special Interest Group
TCS	Telephony Control Protocol Specification
UWB	Ultra-Wide Band

Back to Table of Contents

Last modified: March 21, 2006.