RC 21937 (98632) 22 January 2001 **Computer Science**

IBM Research Report

The Bluetooth™ Wireless Technology

Chatschik Bisdikian
IBM Research Division
Thomas J. Watson Research Center
P.O. Box 704
Yorktown Heights, NY 10598

Research Division
Almaden - Austin - Beijing - Haifa - T. J. Watson - Tokyo - Zurich

The BluetoothÔ Wireless Technology

Abstract:
Bluetooth is the name from the 10th century Danish king Harald Blåtand (Bluetooth) that united Denmark and Norway. The Bluetooth wireless technology aims in uniting personal computing devices into a collaborative, interconnected electronic community. This article highlights the Bluetooth specification.

1 Introduction

In February 1998, Ericsson, IBM, Intel, Nokia, and Toshiba formed the Bluetooth[1] Special Interest Group (SIG) and agreed to work on the development of an international communications standard that will simplify interactivity between personal devices by eliminating connection cables and enabling personal area networking. At the time, there were hardly any knowledge about the hype and emotions that this technology will generate.

Nowadays, there is hardly a day passing when the technology is not mentioned in the various print and electronics media (and not just the technically oriented media). As of this writing (January 2001), the SIG has grown to nine promoters (the previous five plus 3Com, Lucent, Microsoft, and Motorola) and over 2100 adopters including all sorts of industrial, scientific, and educational institutions. Bluetooth adopters are allowed a license-free use of the Bluetooth wireless technology for their qualified products. In the Bluetooth Developer's Conference in San Jose, CA, in December 2000, there were over 3,500 attendees, with over 100 exhibitors demonstrating advanced prototypes and early products covering from simple wireless headsets, to Ethernet bridges with Bluetooth front-ends, to futuristic Bluetooth enabled watches running Linux. The technology has received numerous awards for technical excellence and innovation in trade shows and magazines. What is worth mentioning is that many of these awards not only underscore the technical merits of the technology, but also the hope (or, light at the end of the tunnel) for a seamlessly interconnected world.

Within the SIG, there are several working groups that develop and maintain the specifications for the Bluetooth wireless technology. We will talk about the technology more later in the paper. However, within the SIG, there are additional activities that work together to support of the successful deployment of the technology. There is a program management group comprising representatives of the promoter companies that provides leadership and sets directions for the overall Bluetooth program. There is regulatory group that works with government agencies around the globe to harmonize related to the operation of the technology, regulations, like spectrum assignment for Bluetooth usage. There exists a testing group for developing test specifications for testing Bluetooth products. There exists a qualification program for qualifying Bluetooth devices as compliant to the Bluetooth specification and performing according to the test specifications. There is marketing group for the promotion of the technology and Bluetooth as a universally recognizable brand, and so on.

[1] Bluetooth is a trademark owned by Telefonaktiebolaget L M Ericsson, Sweden.

This paper summarizes the core technology, presented in two volumes and over 1,600 pages. It presents both the protocol stack and early applications considered by the SIG. It also summarizes the current technical activities within the SIG.

2 The Bluetooth protocol stack

The Bluetooth protocol stack can be divided into three groups of protocols as shown in Figure 1.

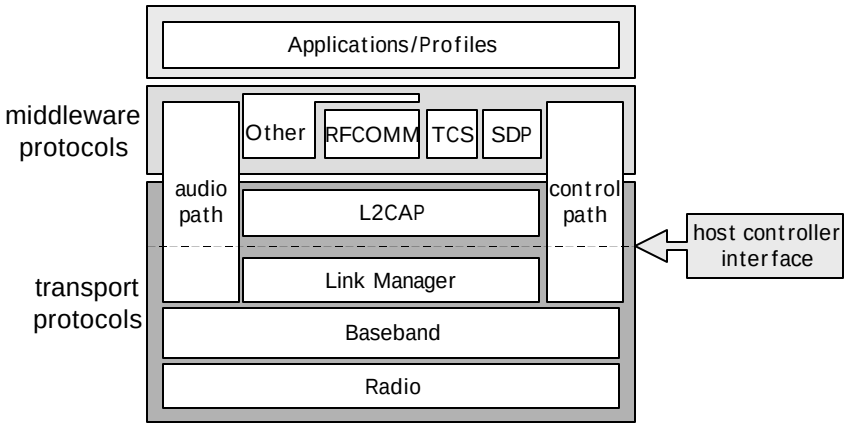

Figure 1: The Bluetooth protocol stack

1. The *transport communication protocols group*: It comprises a set of Bluetooth specific protocols that are present in any end-to-end communication between two Bluetooth devices.

2. The *middleware communication protocols group*: It comprises a set of non-Bluetooth specific protocols as well as Bluetooth specific protocols that are used to enable new and existing applications to run over Bluetooth links.

3. The *applications group (profiles)*: Not really a communications protocol group, although it can be thought as such. It comprises a set of core applications that run over Bluetooth links that have been developed by the SIG in an effort to help in the development of interoperable applications. These applications are described in a series of specifications referred to as the *profiles* and describe

how specially identified applications will use the transport and middleware communication protocols to accomplish desired usage scenarios.

The set of protocols in these three groups may change or be enhanced in the various future releases of the Bluetooth specification. As of this writing, the specification is in version 1.0B, which includes the initial release of the specification (1.0A) plus a set of errata. Version 1.1, with yet additional errata is expected to be available by the time of this publication. Work on the version 2.0 of the specification is currently under way.

2.1 The transport communication protocols group

2.1.1 The radio

The radio specification defines a frequency hoping spread-spectrum (FHSS) system operating in the license-free 2.4GHz industrial, scientific, and medical (ISM) band. The specification defines a radio transmit power of up to 100mW (20dBm). However, a typical Bluetooth radio is expected to have a 1mW (0dBm) maximum transmit power. This power level would match the cost and power requirements of typical portable consumer devices like cellular phones and PDAs. The radio hops at a nominal rate of 1,600 hopes per second to achieve high noise resilience. The baud rate is 1Msymbols/sec using a binary Gaussian frequency shift-keying (GFSK) modulation technique; hence, the raw link speed is 1Mbps.

The radio hops pseudo-randomly on 1MHz-wide channels over the 79 possible channels (accounting for the guard gaps as well) in the ISM band that occupies the frequency band between 2,400GHz and 2,483.5GHz. The Bluetooth regulatory group is working in harmonizing the frequency band assignments for the 2.4GHz ISM band globally. As of this writing, the North American countries, the countries of the European Community, and Japan, have all agreed to harmonize their 2.4GHz band.

2.1.2 The baseband

The baseband defines the processes for devices to find, connect, and communicate with each other. It also defines low-level bit and packet level operations like error detection and correction, whitening, encryption, and so on.

For Bluetooth devices to communicate with each other, they need to be members of a *piconet*. The piconet comprises a well-defined sequence of frequency hops occurring in a slotted (fixed intervals) fashion over which the members of the piconet can communicate. A piconet has at least one device associated with it and it may contain up to of 8 actively communicating devices. One of the devices of the piconet, called the *master*, regulates the frequency hop sequence and timing of the piconet, and also controls the sequence of transmissions on the piconet. The remaining devices, called the *slaves*, communicate only with the

master and only after the master has transmitted to them. Thus, transmissions on a piconet occur in a slotted *time-division duplex* (TDD) fashion, with even slots occupied by transmissions from the master to a slave, and in the subsequent odd slot occupied by a transmission from the slave back to the master.

Figure 2 shows the transmissions in a piconet with a master and *k* (*k*≤7) slaves. The figure also shows the sequence of successive frequency hops (*f0*, *f1*, …) identifying the particular piconet. Note that for multi-slot packet transmissions (see later on), the frequency does not change through the transmission, however, the next frequency visited is the one that would have been used if only single-slot packets were to be used.

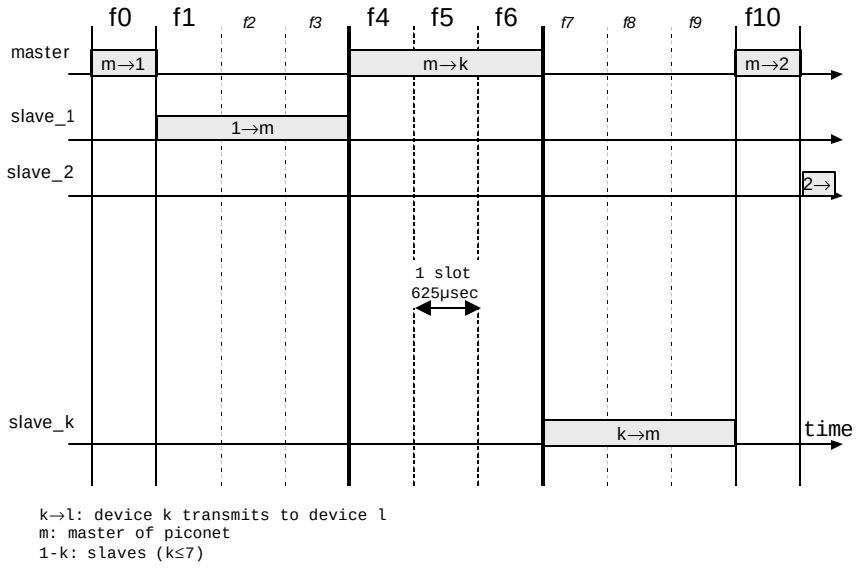

Figure 2: Transmissions in a Bluetooth piconet

Each Bluetooth communications subsystem, which is associated with a Bluetooth host to construct a Bluetooth device[2], has a unique 48-bit address (*BD_ADDR*) assigned to it at manufacture time. Also, every Bluetooth communications subsystem has a Bluetooth clock that ticks at twice the rate (3.2KHz) of the nominal frequency-hopping rate (1.6 Khops/sec). The *BD_ADDR* of the master defines the frequency hopping sequence of a piconet while the Bluetooth clock of the master defines the phase in this sequence. A Bluetooth device may be a member of multiple piconets (what is referred to as *scatterner*) a device can be a

[2] A Bluetooth communication subsystem embedded/integrated in a host system is not excluded.

master of only one piconet. Moreover, several piconets may co-existing in time and space without detrimental degradation in system performance.

To create a piconet Bluetooth devices go through inquiry and page procedures. The potential master and slaves execute these procedures in complementary fashion. A device desiring to communicate with other devices performs an inquiry to search for other devices in its vicinity. Devices listening for inquiry messages respond with inquiry response massages containing among other things its unique *BD_ADDR*. When a Bluetooth device (device A) knows (either through inquiries or previous communication) of the *BD_ADDR* of another Bluetooth device (device B), device A can page device B and invite it to participate in an active communication. The device that initiates a page will become the default master of the resultant piconet. Therefore, the paging device during its pages provides its own *BD_ADDR* and Bluetooth clock value so that the paged devices can instantiate the piconet that they are invited to join. During paging, a master also assigns a temporary 3-bit address to the slave to be used for identification during the continuum that the slave will be active in the piconet.

A Bluetooth piconet supports a single *asynchronous connectionless* (ACL) link between the master and a slave. There is also a broadcast link for transmitting to all active slaves in a piconet. ACL transmissions are typically last one slot, but they may optionally last one, three, or five slots, see figure 2. Using five-slot transmissions in one direction, a maximum one-way transmission-speed of 723Kbps can be reached counting for header overheads at the baseband. In addition to the ACL links, a piconet supports up to three *synchronous connection-oriented* (SCO) links, each SCO link supporting full duplex 64Kbps telephony-grade voice channels. Transmissions on SCO links, which are always single-slot, occur periodically on reserved slots. The use of forward error correction for both ACL and SCO transmissions, and retransmissions of non-broadcast ACL packets through an ARQ and single-bit sequence number scheme, increase the reliability of transmissions.

2.1.3 The link manager

The link manager and the associated protocol, the link manager protocol (LMP), define the characteristics of the Bluetooth link between devices. It defines the message exchanged for authenticating a device and enabling encryption of the link. The actual authentication and encryption algorithms are part of the baseband.

Through LMP transactions, a Bluetooth link can be placed into a low-power mode. There are three low-power modes:

1. *sniff*: a device notifies its communicating partner that it will listen for transmissions for a number of slots every T_{sniff} slots instead of every (other) slot.

2. *hold*: a device notifies its communicating partner that it will be unavailable for communication for a number of slots.

3. *park*: a slave notifies its master that it will be unavailable for communication. However, it will be listening periodically for “beacon” transmissions for possible incoming traffic to the parked slaved that will require it to unpark itself. Parked slave releases its temporary 3-bit address; a new one will be reassigned when in the future the slave is unparked.

The sniff, hold, and park operational modes are optional for Bluetooth devices. They can be activating by a device requesting them from its communicating partner, or by being enforced by the master. Note that for any of these low-power modes of operation, a device may not necessary conserve power. For example, a Bluetooth device may want to participate in several piconets at the same time and thus use any of the low-power modes to notify its communicating partner in a piconet that it will be unavailable for some time in that piconet.

Through LMP transactions, SCO links are defined and other vital information is exchanged associated with the Bluetooth link and device, e.g., whether a device supports multi-slot ACL packets, or what is the user-friendly name of a device.

2.1.4 The host controller interface (HCI)

The Bluetooth specification assumes a reference implementation where the low transport layers, radio, baseband, and link manager, are implemented in hardware and firmware and reside on the same module. This module then attaches to a host that contains the rest of the protocol stack shown in Figure 1 in software. While this reference implementation is not mandated for every Bluetooth device, it is nevertheless highly likely. To permit interoperability between Bluetooth modules and hosts, the Bluetooth specification defines a standardized host controller interface (HCI). Over this HCI, a host can send and receive data (transmitted or received to or from either the ACL and SCO links), as well as send commands and receive events about the status of the radio, the baseband, and the link manager. For example, a host may request a module to enter an inquiry or page state, pass it an authentication key, and so on. The module may pass to the host the results of an inquiry, indicate that a connection request has arrived from a remote device, and so on.

2.1.5 The logical link control and adaptation protocol (L2CAP)

SCO data are funnelled directly from the baseband to an audio application. However, ACL transmissions need to pass through a number of additional protocol layers. The logical link control and adaptation and the associated protocol, logical link control and adaptation protocol (L2CAP), is a Bluetooth specific protocol through which all ACL application data pass.

First of all, L2CAP defines multiple logical channels multiplexed within a single ACL link. Through these logical channels, multiple applications in a Bluetooth device A can communicate to multiple applications in a device B, with each pair of applications in the two devices utilizing exclusively one of the L2CAP logical channels. Furthermore, L2CAP supports protocol multiplexing, thus allowing multiple protocols to utilize a common ACL link.

L2CAP channels can be either connection-oriented, requiring a connection establishment phase to create them, or connectionless. Connection-oriented channels can be qualified with a set of QoS parameters, but in the applications in the current version of the specification, only the best-effort transmissions are exploited.

With a five-slot baseband packet only a few hundred bytes of payload can be transmitted at a time. Hence, to support large packets, commonly used in, say, IP-based communications, L2CAP layer supports segmentation and reassembly of large packets into smaller baseband packets and vice versa.

Last but not least, L2CAP supports the concept of groups, shielding the baseband broadcast groups from the higher layers.

2.2 The middleware communication protocols group

2.2.1 RFCOMM

One of the initial applications for the Bluetooth wireless technology is to serve as a replacement for the ubiquitous serial cables that connect a plethora of personal devices (albeit, using different port designs for different devices). To do so, and take immediate advantage of the myriad of applications written for interactive applications over serial cables, the SIG defined a serial port emulator called RFCOMM.

RFCOMM is based on the ETSI 07.10 standard that defines a multiplexing scheme for serial communications over a common serial medium.

2.2.2 The telephony control signalling protocols (TCS)

The TCS protocols are telephony control protocols used for telephony control commands like ringing, group control (e.g., associating multiple handsets to a single cordless base station), volume control, and so on. They are two such protocols.

1. TCS-AT: it comprises the well known AT-based commands for controlling modems. TCS-AT runs on top of the RFCOMM.

2. TCS-BIN (or, simply TCS): it comprises a packet based telephony control protocol based on the ITU-T Q.931 protocol. This protocol runs on top of L2CAP.

Note that while the telephony control protocols use the data paths of the Bluetooth stack, as mentioned earlier, the actual audio signal bypasses them and is funnelled directly from the audio application to the baseband and vice versa.

2.2.3 The Bluetooth service discovery protocol (SDP)

While the Bluetooth wireless technology is primarily a link level technology, the Bluetooth specification goes well beyond than just defining a new link type. It defines end-to-end communication solutions between Bluetooth devices. The Bluetooth service discovery protocol is a key element in enabling the additional dimensions of the Bluetooth wireless technology.

While the transport protocols presented earlier allow the transfer of information between devices, it is SDP that enables an application in one Bluetooth device to locate a desired complementary application in another Bluetooth device. While SDP does not provide the means for accessing an application, it provides the necessary information (or metadata) for learning which protocol to use to access an application, whether the desired application exists in a device, whether its available, a description of it, and so on.

2.2.4 Other adopted protocols

To support the various Bluetooth usage scenarios identified by the SIG, a number of other protocols have been adopted from existing standards with no additional modification. Adopted protocols include the *infrared object exchange* (IrOBEX, or simply OBEX) and *infrared mobile communications* (IrMC), both developed by the IrDA association. These protocols define transport and synchronization mechanisms for objects like calendar entries, e-mail, and business cards, as well as files. Additional adopted protocols include the *point-to-point protocol* (PPP) that allows packet-based transmissions over serial lines. Since, typically, an IP protocol runs on top of PPP, PPP is used to allow Bluetooth devices to access IP services through a LAN access point.

Both the IrDA based and the PPP protocols are currently defined to run on top of RFCOMM.

2.3 The Bluetooth profiles

To provide value-add and good user experience right out-of-the-box to the users of the technology and promote application interoperability from the outset of the deployment of the technology, the Bluetooth SIG decided to develop complete application solutions for a set of usage scenarios. For each of the scenarios identified as (a) useful to the users of the technology, and (b) feasible within the timeframe set-up for the release of the specification, a specification was developed referred to as a *profile*. There are protocol profiles and application profiles. Each of the profiles defines how the Bluetooth protocol stack is to be used and configured so that the Bluetooth devices supporting the specific profile will exchange information in a legible manner.

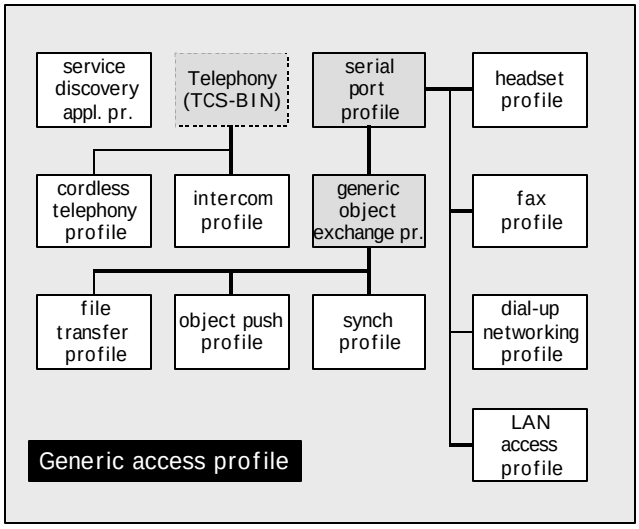

Figure 3: The Bluetooth profiles

Figure 3 shows the collection of Bluetooth defines defined in the version 1.0 of the specification and the dependencies of each other.

1. *Generic Access Profile* (GAP): It defines how Bluetooth device create piconets and communication with each other. Furthermore, it defines security modes according to which a device may be discoverable by other devices,

connectable with other devices, whether it establishes Bluetooth links only with trusted devices, or not, and so on. Trust relations between devices is achieved through the use of stored link keys generated by entering PINs to the devices that are to trust each other.

All other profiles depend on GAP. All Bluetooth devices must support GAP.

2. *Service Discovery Application Profile* (SDAP): It determines how a service discovery application in a Bluetooth device uses SDP to search for services in its vicinity. In addition, it determines how SDP utilizes the Bluetooth transport protocols to carry SDP messages over-the-air.

3. *TCS-BIN-based profiles*: There are two profiles that use TCS-BIN in their implementation.

   - The *cordless telephony profile* defines the use of cellular phones as cordless handsets in the vicinity of cordless base-station.

   - The *intercom profile* defines the use of cellular phones as intercoms for direct communication to each other.

   These two profiles are sometimes refer to as the “3 in 1 usage scenario”, where a cellular phone has triple role based on where it is used as (a) cellular phone, (b) a cordless handset, and (c) an intercom device.

4. *Serial Port Profile*: It determines how the RFCOMM layer is configured and utilizes the Bluetooth transport protocols to create a virtual serial pipe between two devices. A number of additional profiles are defined to run on top of the serial port profile.

5. *Generic Object Exchange Profile* (GEOP): It determines how peer OBEX protocol layers use the RFCOMM profile to establish an interactive session for transporting objects. The following three profiles are based on GEOP.

   The serial port and generic object exchange profiles are two protocol profiles. With the exception of the GAP, all the rest of the profiles are application profiles.

6. *File Transfer Profile*: It defines an application for the transfer of files between devices. It identifies the pushing and the pulling of files, folder creation, and deletion and browsing of file folders.

7. *Object Push Profile*: It defines a simple application for pushing objects, and in particular business cards, between personal devices.

8. *Synchronization Profile*: It defines the process for synchronizing personal data (callendars, address books, etc) among personal devices.

9. *Headset Profile*: It defines the use of cordless headsets for cellular phones and other personal devices.

10. *Fax Profile*: It defines how to send faxes wirelessly. It relates to the next profile which also deals with the transmission and access to data services.

11. *Dial-up Networking Profile* (DUNP): It defines the use of a wireless modem for a dial-up access to data services, say, and internet service provider. The profile focus primarily on the wireless modem functionality of cellular phones. This profile transforms one's cellular phone into a personal communications gateway, permitting one to connect its personal device (a PDA, or a laptop computer) to data services from any place where there is cellular phone coverage.

    The three previous profiles using the AT commands as a control protocol supporting either voice or data communications.

12. *LAN Access Profile* (LAP): It defines the process by which a personal device connects to a LAN infrastructure via a LAN access point (LAP). This profile uses PPP to establish connectivity with a LAN infrastructure. In the case of IP-based communications, the widely used PPP solution simplifies the process for connecting to a "point-of-presence" of an IP network. The ad-hoc creation of peer-to-peer IP networks is still an open issue.

Currently, the SIG is has working groups (WGs) investigating a number of new profiles, but the corresponding specifications are not finalized or publicized yet.

1. Radio 2 (next generation radio) WG: it develops a backward compatible higher-speed (≥10Mbps) communications subsystem.

2. Car Profile WG: it develops applications for in-car communications between personal devices and in-car systems.

3. Personal Area Network Profile WG: it develops solutions to support ad hoc, peer-to-peer communications.

4. Human Interface Device WG: it develops solutions for cordless computers.

5. Co-existence WG: it studies coexistence issues between Bluetooth devices and other wireless solutions for the 2.4GHz ISM band.

6. Richer Audio/Voice/Video Profile WG: it develops solutions for (near) CD-quality audio and VGA-level video.

7. Printing Profile WG: it develops solutions for access and control of printers.

8. Still Image Profile WG: it develops solutions for transferring digital images from a digital camera to other devices, e.g., a notebook computer.

9. Extended Service Discovery Profile WG: it develops support for additional service discovery protocols on top of SDP. Initial focus is on UPnP and Salutation.

10. Local Positioning Profile WG: it develops solutions that would provide GPS-like positioning information for Bluetooth devices indoors.

11. Unrestricted Digital Information Extension for Japanese 3G Handsets WG.

3 Concluding remarks

The Bluetooth wireless technology has been developed to simplify the interconnection of personal devices by using a single, globally available, air-interface. This technology is geared not only to the business executives and professionals, but to the consumer population as well. It aims in freeing people from having to worry about connecting their devices amongst themselves, or with other people's devices, or with a third party's devices. Its widespread use would greatly enhance one's experience in using computing devices. The Bluetooth wireless technology presents the first real opportunity to realize the vision of pervasive, persistent, ubiquitous, unconscious (use your favorite term here) computing and communication.

Today, the young generation seems to be oblivious to the fact that the "Web" was not even existent just a few years ago. Similarly, using devices capable of Bluetooth wireless communications, it would not be hard to envisage that in few years the (then) young generation will be oblivious to the fact that devices didn't use to communicate with each other, or that device communications was even a point of concern.

The ultimate success of the technology depends on many parameters, many of which are either unknown or they are, in turn, dependent on unpredictable market forces and interests. However, the SIG made any effort to create the framework for the successful deployment of this new technology. It has defined a license-free, low cost (when deployed in numbers) communications technology, that can be used around the globe. It has defined a set of interoperable seed applications that can add value to the technology from day one of its deployment. It has used a lot of marketing muscle to spread the word and the vision of a seamlessly interconnected world. The first products have just starting appearing in the market while a lot more have been promised for this year. Bluetooth chip manufacturers are projecting massive production increases for the year. We now need to wait and see.

4 Additional resources

For detailed description of the technology, one can download the whole specification at no cost from the Bluetooth web-site at *http://www.bluetooth.com*. A trade magazine devoted to the technology and the latest products and gadgets is *Bluetooth World* available at *http://www.thebluelink.com*. A very good technical article written by one of the innovators of the Bluetooth wireless technology, Dr. Jaap C. Haartsen, titled *The Bluetooth Radio System*, can be found in the special issue on "Connectivity and Applications Enablers for Ubiquitous Computing and Communications" of *IEEE Personal Communications*, February 2000. *Bluetooth Revealed* (Prentice-Hall PTR, 2001), authored by Brent A. Miller and myself, contains an extended introduction and summary of the 1,600 pages of the specification containing tidbits from our personal experiences working on the development of the specification. A good article highlighting the technology with emphasis the qualification program is *Bluetooth's slow dawn*, by Ron Schneiderman, in *IEEE Spectrum*, November 2000.