An overview of Bluetooth Wireless Technology™ and some competing LAN Standards

Anthony C Davies
School of Computing and Information Systems, Kingston University
Kingston-upon-Thames, Surrey, England, KT1 2EE
tonydavies@ieee.org

Abstract - Bluetooth Wireless Technology™ is a low-cost cable-replacement method for connecting computer-based devices in home and small office environments. Intended as a universal, global standard, it has not developed as fast or as pervasively as initially hoped, but is having a major impact. This tutorial overview presents basic concepts of the Bluetooth standard, the transmission and modulation environments of the unlicensed ISM frequency bands, spread-spectrum communications options, link protocols, data rates, formation of ‘piconets’ and security features.

A review of other standards for Wireless LANs is included, with some indications of implementation methods for Bluetooth Wireless Technology.

Index terms — wireless local area networks, spread-spectrum, mobile communications.

I. Introduction

The increased applications being found for various forms of wireless technology are attributable to a number of factors including:

(1) the wish to provide multiple forms of communications while mobile.

(2) technology advances which have made possible lightweight low-power, low-cost electronic appliances capable of transmission and reception in the GHz frequency bands and

(3) a need to eliminate the inconvenience of cable connections between associated devices in home and office environments.

Operation in the GHz bands has made available substantial amounts of frequency spectrum, leading to schemes to sell this valuable resource to the highest bidder. However the available bandwidth is not unlimited, and given present and anticipated future demands, seems likely to be insufficient. There will therefore continue to be a need for cable and fibre based connectivity for non-mobile applications.

The Bluetooth Wireless Technology [1] is one of a number of methods for implementing wireless-based local area networks (WLANs).

II. Bluetooth origins and limitations

Bluetooth Wireless Technology is a short-range (up to 10m) wireless networking method for personal, office and industrial environments. The name originates from a Danish King, Harald Blátant, who is considered to have succeeded in uniting the Scandinavian people in the 10th century AD. The Bluetooth Standard is supposed to unite personal computing devices. The name was intended to be temporary, but became permanent because apparently no one could think of anything better [1].

It was intended to be a low cost solution for avoiding connecting-cables, etc. with a target price for market-penetration of $5 or less for the hardware (chip) costs. This has not yet been achieved. The initial intention was to achieve 100% domination of the world market by having a universal royalty-free standard.

The development of the Standard originated with the formation of a Bluetooth Special Interest Group (SIG) by IBM, Intel, Nokia and Toshiba in 1998. They aimed for a global standard, which was initially adopted by 70 SIG members, and increased to 3000 SIG members by end of 2001.

560 million Bluetooth devices by 2006 has been predicted by industry-analyst Ovum. ICD predicts (bulletin 25398 [2]) 435 million Bluetooth-enabled mobile phones by 2005. Nevertheless, even this is slower growth than initially predicted, and some SIG members are withdrawing support.

III. The unlicensed bands

The Industrial, Scientific and Medical (ISM) unlicensed bands are 915 MHz, 2.5GHz and 5GHz. In USA there is an additional U-NII band - ‘unlicensed national information infrastructure’ which comprises 300 MHz bandwidth allocated in the 5GHz band. At the present time, Japan does not allow outdoor use of the 5GHz band.

‘Spectrum etiquette’ rules (‘listen before talk’ protocols, low transmitter power, restricted transmit durations) had to be developed for co-existence of Wireless LANs with other users in the un-licensed bands. This led to separate bands being allocated to Asynchronous (data and file transfer) channels and Synchronous (streamed audio or video) channels (this is different from ISDN and ATM). With the anticipated growth of Wireless LAN transmissions in the 2.5GHz band, interference with Bluetooth may become an increasing problem – fortunately, the newer WLAN activity is moving to the 5GHz band, which will help the Bluetooth environment.

Wireless LANs generally have to use a modification of the Ethernet CSMA/CD protocol, called CSMA/CA. The essence of the difference is that collisions have to be predicted and avoided rather than detected, because of the multiple users in the wireless environment.
IV. The IEEE ‘802’ standards

The very extensive ‘802’ group of IEEE standards is concerned with Local Area Networks (LANs) and the development of many of these standards have had a major impact.

802.3 is the well-known Ethernet (CSMA/CD) LAN standard for wired (copper or fibre) networks and 802.4 is the token-bus wired-LAN standard.

802.11 is for Wireless Local Area Networks, and developed from an 802.4L (wireless) category around 1977.

The original 802.11 was for rates up to 2 Mb/s, and allows Direct-Sequence or Frequency-Hopping Spread-Spectrum (see Sections VII and VIII below) in the unlicensed 2.4 GHz ISM band, or use of the infrared band (850-950 nm). The Direct-Sequence option allows a spreading code of only 11-bit.

Many versions of 802.11 arose, particularly for higher data-rates. 802.11b is a ‘high-rate’ version for up to 11 Mb/s. It uses Direct-Sequence Spread-Spectrum with 26MHz bandwidth and 52 carriers in a 20MHz bandwidth, each modulated carrier being approximately 300 kHz wide. Each carrier is capable of up to 1.5 Mb/s data-rate. 802.11g is for up to 22 Mb/s. 802.11a is more recent, and uses Orthogonal Frequency Division Multiplex (‘OFDM’) [3,4] in the 5 GHz band, and is capable of up to 54 Mb/s. Normal FDM requires ‘guard bands’ to separate the channels, while OFDM uses partially orthogonal carriers, allowing some overlap, as illustrated in Fig. 1.

![Fig. 1. Comparison between FDM and OFDM](image)

A performance comparison between OFDM and use of single-carrier (e.g. FDM) with adaptive equalization at the receiver for broadband wireless systems is given by Falconer et al [5].

The 802.15 working group is developing a family of ‘Wireless Personal Area Networks’ (WPANs) for up to 55Mb/s data-rate, and Bluetooth has been accepted as one of these. In March 2002, Bluetooth was ratified by IEEE for 802.15.1.

V. Competition for Bluetooth

In addition to wireless-based connections there are several alternatives.

The traditional use of ‘wires’ (e.g. plugs, cables, etc) is both inconvenient and costly. Infrared communications has the disadvantage compared to Bluetooth that it is restricted to ‘line of sight’ links.

VI. Will there be Bluetooth everywhere?

Although the take-up of Bluetooth has been slower than predicted, some very ambitious and even extravagant suggestions have been made about future applications that could arise, if the implementation costs are low enough. Whether such applications will really occur remains to be seen.
For example, it has been suggested that domestic refrigerators could be linked to the Internet, providing stock control via bar-coded products. New supplies would be automatically ordered over the Internet from local supermarkets, taking into account any special offers and known preferences of the residents of the house. Additionally, prompts would be given of user needs such as reminders of approaching birthdays, etc. requiring purchase of special supplies.

Perhaps the breakfast toaster could be linked to the Internet, so that in addition to delivering toasted bread, it would print out the local weather forecast with traffic congestion data of local motorway routes, and would advise the refrigerator when to purchase another loaf of bread.

More conventional applications would be for lighting and heating control, using sensors to turn off lights and heat in unoccupied rooms, and detecting movements of occupants and adjusting conditions to match their needs. This is already implemented in some places. It is easy to speculate over extensions. For example, rooms could be pre-heated in advance of the home-owner’s return by detecting an approach of his/her vehicle or mobile phone.

Personal possessions control is another interesting possibility: valuable or portable items could continuously transmit their location, so that they could be tracked and recovered of lost or stolen. This could include children, elderly relatives, pet animals etc. Such a concept could have a big impact in the reduction of insurance premiums.

VIII. Bluetooth Communications Methods

A frequency-hopping spread-spectrum technique is used with 1600 hops/sec at 79 frequencies. These are at (2402 + k) MHz, k = 0,1,2,...,78.

e.g. 2402, 2403, 2404, 2405, 2406,...... 2480

The frequency-sequence is selected in a pseudorandom manner.

All Bluetooth devices share the same frequency space, and the band may be used concurrently by other ISM devices.

In Japan, France and Spain, licensing restrictions require Bluetooth to hop over only 23 frequencies, rather than 79.

There are two main classes of frequency-hopper, those that have many bits per hop and those that have many hops per bit. Bluetooth uses the first class.

As an example of an algorithm for selecting the sequence of frequencies used in a frequency-hopper, an illustration from the ’SWAN’ hopper [6] is given. The ‘frequency-jumps’ are required to be to at least six frequency slots on each hop.

There are 79 frequencies f[i] per sequence and 22 different sequences F[j] per family, chosen as:

\[ F[j] = \{ f_{[0]}, f_{[1]}, f_{[2]}, \ldots \ldots f_{[79]} \} \]

\[ f[i] = (i \times j) \mod 79 \]

\[ i = 0, 1, 2, 3, \ldots 79 \]

\[ j = 7, 10, 13, 16, 19, \ldots 67, 70 \]

\[ i \] is the sequence-step, and \( j \) is the sequence-identifier in the family. Thus,

\[ F[7] = 0, 7, 14, 21, 28, 35, 42, 49, 56, 63, 70, 77, 5, 12, 19, 27, 34, 41, 48, \ldots \]

\[ F[10] = 0, 10, 20, 30, 40, 50, 60, 70, 7, 1, 11, 21, 31, 41, 51, 61, 71, 2, 12, 22, \ldots \]

\[ F[13] = 0, 13, 26, 39, 52, 65, 78, 12, 25, 38, 51, 64, 77, 11, 24, 37, 50, 63, \ldots \]

et. continuing up to F[70].

Two other families exist. The sequences in any family are weakly-orthogonal to one another, but there is no orthogonality property between families, so that it is only possible to use one family in one environment.

This is a somewhat simplistic algorithm, and contrasts with the very sophisticated and sometimes very long-period sequences with remarkable correlation properties which are used in some spread-spectrum systems.

The sequences used to support the direct-sequence spread-spectrum of the 802.11b standard is based on a Barker code of 11 bits:

\[ +, -, +, - , +, - , +, - , +, +, - \]

Barker codes [10,11] have the special property that the magnitude of the aperiodic autocorrelation for all off-peak time-shifts is limited to a maximum of ±1, which makes them useful for many communications applications.

The reason for selecting frequency hopping rather than Direct-Sequence Spread-Spectrum for Bluetooth may be because of improved dynamic range and reduction of the near-far problem (a transmitter using one sequence which is close to a receiver attempting to receive a transmission based on an uncorrelated sequence may cause unacceptable interference).

The Bluetooth standard allows three transmit-power classes: 1mW, 2.5mW and 100mW. Most applications are in the first two classes, which provide ranges of 100mm to 10m respectively.
Each device has a unique 48 bit hard-wired device-address for identity. Many devices are possible since \( 2^{48} = 281474976710656 \approx 2.815 \times 10^{14} \).

Additionally (Fig. 2) each device has a 28 bit clock running at twice the nominal hopping-frequency (e.g. 3200Hz, period 312.5\( \mu \)s).

Fig 2. Device clock and frequency-hopping

IX. Modulation

The maximum data rate for Bluetooth is 1 Mbit/sec, using Gaussian binary frequency shift keying (FSK). Binary ASK, FSK, and PSK all carry one bit per transmitted symbol, and the key to getting more bits in a given bandwidth is to send more bits per symbol – but immunity to interference is worse, so that this must normally be associated with more sophisticated equalisation. The various standards which offer much higher data rates than Bluetooth use a variety of modulation techniques which increase the bits per symbol.

Fig. 3 illustrates this for the simple cases of Binary PSK and Quad PSK. The bit rate for QPSK is thus double that of BPSK for the same symbol rate.

Fig. 3. BPSK and QPSK

The 802.15.3 standard specifies various QAM alternatives all with a symbol rate of 11Mbaud.

16-QAM achieves 33Mb/sec, and 64-QAM achieves 55Mb/sec.

X. Links and Data Rates

Each device supports one Asynchronous Connectionless Communications link (ACL) for file and data transfers and Two Synchronous Connection-oriented Communications links (SCL) for digital audio, etc. (Fig. 4). The Asynchronous links support a maximum data-rate of 732.2 kbits/sec in an asymmetrical mode or 433.9 kbits/sec in a symmetric mode (e.g. the same rate in both directions). The Synchronous links support two bi-directional 64 kbits/sec connections.

Fig. 4. Links between Bluetooth devices

Some error handling is provided. In the case of the asynchronous links, packet-sequence numbers are transmitted, and the receiver can request a retransmission. Flow-control is used, and a 16 bit CRC is included. In the case of the synchronous links, retransmission is not possible and the received packets have to be accepted as they arrive. To achieve lower error rates, forward error control coding can be incorporated in what is transmitted.

The data rates provided by the Bluetooth standard are inadequate for some consumer applications [8]. For example, downloading images from digital cameras could be unacceptably slow at the Bluetooth rates. High definition DVD requires 9.8 Mbit/sec. An MPEG2 video data stream for a high-definition TV display requires 19.2 Mbit/sec. Real-time 1024x768 60Hz computer graphics requires 38 Mbit/sec. There will be an increasing need to support game-consoles linked to virtual-reality 3D viewing spectacles. For all these applications, Bluetooth rates are insufficient.

XI. Forming Networks

Bluetooth devices form ‘piconets’ in order to communicate. A piconet comprises up to 8 actively-participating devices, in which one takes the role of ‘master’, and the others are ‘slaves’. In order to establish a piconet, the master transmits ‘enquiry messages’ at 1.28 second intervals in order to locate Bluetooth devices within range. This is followed by ‘invitations to join the piconet’ addressed to the specific devices within range that the master wishes to have in the net.

Fig. 5. Piconet with some parked devices

The master allocates a member-address to each of the active slaves, and controls their transmissions.

The clock of the master provides the time-synchronisation of the whole piconet. The master always transmits in ‘even-numbered’ time-slots and the
slaves transmit in ‘odd-numbered’ time-slots in accordance with permission given by the master. This timing is based upon the second-least-significant bit of the master clock (since the clock runs at twice the hop-rate, this bit determines which are odd and even slots).

Additional devices (above the maximum of 8 active ones) may be registered with the master and ‘parked’ in an inactive mode (Fig. 5). At some later time they may be asked by the master to become active. Still more devices may be in a ‘standby’ mode.

There is no essential difference between a master and a slave device – indeed, once a piconet has become operational, the master and a specific slave may agree to reverse their roles.

A device can belong concurrently to more than one piconet. The combination of two or more piconets in this way forms a ‘scatternet’.

As explained above, the nominal time per frequency hop is 625μs. The devices normally transmit each packet wholly within one of these hops. Longer packets are allowed, and since the master controls the hop-sequence, whenever a longer packet is to be transmitted, the master suspends the frequency hopping, so as to provide a constant transmission frequency for the duration of the packet message.

XII. Bluetooth Packets and Protocols

There is a large range of baseband packet types of various lengths. Some of these have options for the addition of forward error correcting codes in addition to the header and payload fields. The standard Bluetooth packet has a 72 bit Access code field, a 54 bit header field and a payload (which may include a 16 bit CRC) of 0 to 2745 bits. The Specification lists 17 different packet types.

A special class of Bluetooth transactions are those of the Link Manager Protocol (LMP), used to establish the properties of a Bluetooth link and to enable the features of the various devices forming a piconet to be established and configuration properties to be set-up.

The higher-level protocols supported by Bluetooth include RFCOMM, which provides an emulation of the RS-232 nine-wire serial connection used in many personal computers. There is also a Telephony Control Signalling protocol (TCS-AT) which uses the RFCOMM protocol to transmit the AT commands (as used in modems, for example)

XIII. Security of Bluetooth

Bluetooth provides some security features. It does not use public-key cryptography for this purpose. Instead, a shared secret key is used.

For authentication the key is 128 bits. The challenging device sends a ‘challenge packet’ to the ‘claimant’ device, which adds the 128 bit key and returns the packet. The challenger does the same locally, and then compares its locally generated version with the version returned from the claimant. If both are using the same key this process verifies the claimant-identity to the challenger. This is illustrated by Fig. 6.

Following successful authentication, link encryption may follow. Encryption uses a key of not more than 128 bits. The upper limit is controlled in many countries by Government regulations in order to allow interception by security agencies. The key length permitted may differ in different countries.

The encryption key changes with each packet transmitted.

If encryption is used, the whole connection is encrypted e.g. the asynchronous and synchronous links are either all encrypted or else none are encrypted.

The security provided is claimed to be adequate for financial transactions.

XIV. Implementing Bluetooth

The component parts of a Bluetooth chip include the 2.4GHz transmitter and receiver, a minimum of other analogue parts, a digital signal processor to carry out the Baseband processing including FFT and other signal processing operations, a microcontroller and sufficient RAM and ROM. Low-power is a major requirement, because of the portable nature of the majority of applications. The transmitter power amplifier is a major contributor to the overall power consumption, and as well as power-efficiency, must meet stringent linearity requirements and also provide for power control. The Bluetooth specification requires that the transmitter output power is controlled in accordance with signal-strength information provided from the remote receiver.

The basic circuit design principles are described by a number of authors [12,13,14]. Many of these describe multi-chip solutions with some discrete components, which can now be considered to be commercially out-of-date, because of the need to integrate the whole of the Bluetooth electronics within a single chip in order to meet cost constraints.

In accordance with normal System-on-Chip design methods, the Bluetooth chip is typically made from a configuration including imported blocks of pre-designed IP, where the designer/manufacturer may or may not have access to the internal details of these blocks, and obtains the rights to use them on either a license or royalty basis.
The following design goals and results have been provided by Cambridge Silicon Radio, one of the major manufacturers and providers of IP for Bluetooth products [15]. In April 2002, Cambridge Silicon Radio claimed to have their chips in 60% of all Bluetooth products.

The requirement is for the integrated circuit dies to cost less than $2 each by 2001, and to manufacture 10^9 units per year, with an end-product test time of not more than 3 secs.

The implications are choice of a pure CMOS technology with no production trimming and a 90% yield. A single chip has to be designed with radio-frequency and baseband parts and DSP and microcontroller and memory.

Preferably there should be no r.f. components off-chip, although this had not been achieved at Cambridge Silicon Radio by the end of 2001.

Particular design problems arise from the low Q of on-chip inductors, and the need to have a receiver only a few cm from a +33dBm mobile phone transmitter. The r.f. transmission must reach the receivers of other Bluetooth devices, and yet must not have any impact upon the behaviour of the local integrated circuit chip.

The receiver is required to achieve a bit error rate of 1 in 1000.

Cambridge Silicon Radio now has a single-chip implementation (BlueCore2) which meets the target $5 price, and consumes less than 50mW with a 1.8V supply. In ‘sleep mode’ the power drops to 27µW. The chip is fabricated in 0.35µ CMOS, and will soon be available in 0.18µ CMOS.

The Bluetooth Network Encapsulation Protocol (BNEP) provides an emulation of Ethernet over Bluetooth links [2]. This will enable mobile phones to be Ethernet terminals, so providing TCP/IP and voice-over-IP services. The trends appear to be towards increasing use of the TCP/IP environment, brought as close as possible to the end-user of the communications network.

Combining the Ethernet medium access controller with the Bluetooth components and full real-time TCP/IP facilities on a single chip will become an inevitable development for economic viability.

Conclusions

The Bluetooth Wireless Technology is providing a low-cost method of wireless connectivity for all kinds of digital and computing devices, and although the supported data rates are moderate and insufficient for many applications, it seems certain that Bluetooth devices will become very widespread.

Acknowledgements

The information in this tutorial overview has been compiled from a range of publicly-available sources including some commercial advertising material. It is believed to be accurate but the author takes full responsibility for any errors of detail or interpretation in deriving the material and putting it into the form of this tutorial. The UK Engineering and Physical Sciences Research Council (EPSRC) is thanked for financial support (grant number GR/R32895/01)

References


Relevant Websites:

www.bluetooth.com
www.homeplug.org
www.hiperlan2.com
www.homepna.org
www.wi-fi.org
www.palowireless.com