Bluetooth

From Wikipedia, the free encyclopedia

This article is about a wireless technology standard. For the medieval king of Denmark, see Harald Bluetooth.

Bluetooth is a wireless technology standard for exchanging data over short distances (using short-wavelength UHF radio waves in the ISM band from 2.4 to 2.485 GHz[4]) from fixed and mobile devices, and building personal area networks (PANs). Invented by telecom vendor Ericsson in 1994,[5] it was originally conceived as a wireless alternative to RS-232 data cables. It can connect several devices, overcoming problems of synchronization.

Bluetooth is managed by the Bluetooth Special Interest Group (SIG), which has more than 25,000 member companies in the areas of telecommunication, computing, networking, and consumer electronics.[6] The IEEE standardized Bluetooth as **IEEE 802.15.1**, but no longer maintains the standard. The Bluetooth SIG oversees development of the specification, manages the qualification program, and protects the trademarks.[7] A manufacturer must make a device meet Bluetooth SIG standards to market it as a Bluetooth device.[8] A network of patents apply to the technology, which are licensed to individual qualifying devices.

Bluetooth

Developed by	Bluetooth Special Interest Group
Industry	Mobile personal area networks
Compatible hardware	mobile phones, personal computers, gaming consoles[1]
Physical range	Typically less than 10m, up to 100m[2][3]

Contents

Name and logo

The name "Bluetooth" is an Anglicised version of the Scandinavian *Blåtand*/*Blåtann*, (Old Norse *blátǫnn*) the epithet of the tenth-century king Harald Bluetooth who united dissonant Danish tribes into a single kingdom and, according to legend, introduced Christianity as well. The idea of this name was proposed in 1997 by Jim Kardach who developed a system that would allow mobile phones to communicate with computers. At the time of this proposal he was reading Frans G. Bengtsson's historical novel *The Long Ships* about Vikings and King Harald Bluetooth.[9][10] The implication is that Bluetooth does the same with communications protocols, uniting them into one universal standard.[11][12][13]

The Bluetooth logo is a bind rune merging the Younger Futhark runes ᚼ (Hagall) (□) and ᛒ (Bjarkan) (□), Harald's initials.

Implementation

Bluetooth operates at frequencies between 2400 and 2483.5 MHz (including guard bands 2 MHz wide at the bottom end and 3.5 MHz wide at the top).[14] This is in the globally unlicensed (but not unregulated) Industrial, Scientific and Medical (ISM) 2.4 GHz short-range radio frequency band. Bluetooth uses a radio technology called frequency-hopping spread spectrum. Bluetooth divides transmitted data into packets, and transmits each packet on one of 79 designated Bluetooth channels. Each channel has a bandwidth of 1 MHz. Bluetooth 4.0 uses 2 MHz spacing, which accommodates 40 channels. The first channel starts at 2402 MHz and continues up to 2480 MHz in 1 MHz steps. It usually performs 1600 hops per second, with Adaptive Frequency-Hopping (AFH) enabled.[14]

Originally, Gaussian frequency-shift keying (GFSK) modulation was the only modulation scheme available. Since the introduction of Bluetooth 2.0+EDR, π/4-DQPSK (Differential Quadrature Phase Shift Keying) and 8DPSK modulation may also be used between compatible devices. Devices functioning with GFSK are said to be operating in basic rate (BR) mode where an instantaneous data rate of 1 Mbit/s is possible. The term Enhanced Data Rate (EDR) is used to describe π/4-DPSK and 8DPSK schemes, each giving 2 and 3 Mbit/s respectively. The combination of these (BR and EDR) modes in Bluetooth radio technology is classified as a "BR/EDR radio".

Bluetooth is a packet-based protocol with a master-slave structure. One master may communicate with up to seven slaves in a piconet. All devices share the master's clock. Packet exchange is based on the basic clock, defined by the master, which ticks at 312.5 µs intervals. Two clock ticks make up a slot of 625 µs, and two slots make up a slot pair of 1250 µs. In the simple case of single-slot packets the master transmits in even slots and receives in odd slots. The slave, conversely, receives in even slots and transmits in odd slots. Packets may be 1, 3 or 5 slots long, but in all cases the master's transmission begins in even slots and the slave's in odd slots.

The above is valid for "classic" BT. Bluetooth Low Energy, introduced in the 4.0 specification, uses the same spectrum but somewhat differently; see Bluetooth low energy#Radio interface.

Communication and connection

A master Bluetooth device can communicate with a maximum of seven devices in a piconet (an ad-hoc computer network using Bluetooth technology), though not all devices reach this maximum. The devices can switch roles, by agreement, and the slave can become the master (for example, a headset initiating a connection to a phone necessarily begins as master—as initiator of the connection—but may subsequently operate as slave).

The Bluetooth Core Specification provides for the connection of two or more piconets to form a scatternet, in which certain devices simultaneously play the master role in one piconet and the slave role in another.

At any given time, data can be transferred between the master and one other device (except for the little-used broadcast mode.) The master chooses which slave device to address; typically, it switches rapidly from one device to another in a round-robin fashion. Since it is the master that chooses which slave to address, whereas a slave is (in theory) supposed to listen in each receive slot, being a master is a lighter burden than being a slave. Being a master of seven slaves is possible; being a slave of more than one master is difficult. The specification is vague as to required behavior in scatternets.

Many USB Bluetooth adapters or "dongles" are available, some of which also include an IrDA adapter.

Uses

Class	Max. permitted power		Typ. range[3] (m)
	(mW)	(dBm)	
1	100	20	~100
2	2.5	4	~10
3	1	0	~1

Bluetooth is a standard wire-replacement communications protocol primarily designed for low-power consumption, with a short range based on low-cost transceiver microchips in each device.[15] Because the devices use a radio (broadcast) communications system, they do not have to be in visual line of sight of each other, however a *quasi optical* wireless path must be viable.[6] Range is power-class-dependent, but effective ranges vary in practice; see the table on the right.

Officially Class 3 radios have a range of up to 1 metre (3 ft), Class 2, most commonly found in mobile devices, 10 metres (33 ft), and Class 1, primarily for industrial use cases,100 metres (300 ft).[3] Bluetooth Marketing qualifies that Class 1 range is in most cases 20–30 metres (66–98 ft), and Class 2 range 5–10 metres (16–33 ft).[2]

Version	Data rate	Max. application throughput
1.2	1 Mbit/s	>80 kbit/s
2.0 + EDR	3 Mbit/s	>80 kbit/s
3.0 + HS	24 Mbit/s	See Version 3.0 + HS
4.0	24 Mbit/s	See Version 4.0 LE

The effective range varies due to propagation conditions, material coverage, production sample variations, antenna configurations and battery conditions. Most Bluetooth applications are for indoor conditions, where attenuation of walls and signal fading due to signal reflections make the range far lower than specified line-of-sight ranges of the Bluetooth products. Most Bluetooth applications are battery powered Class 2 devices, with little difference in range whether the other end of the link is a Class 1 or Class 2 device as the lower powered device tends to set the range limit. In some cases the effective range of the data link can be extended when a Class 2 device is connecting to a Class 1 transceiver with both higher sensitivity and transmission power than a typical Class 2 device.[16] Mostly however the Class 1 devices have a similar sensitivity to Class 2 devices. Connecting two Class 1 devices with both high sensitivity and high power can allow ranges far in excess of the typical 100m, depending on the throughput required by the application. Some such devices allow open field ranges of up to 1 km and beyond between two similar devices without exceeding legal emission limits.[17][18][19]

The Bluetooth Core Specification mandates a range of not less than 10 metres (33 ft), but there is no upper limit on actual range. Manufacturers' implementations can be tuned to provide the range needed for each case.[3]

Bluetooth profiles

Main article: Bluetooth profile

To use Bluetooth wireless technology, a device must be able to interpret certain Bluetooth profiles, which are definitions of possible applications and specify general behaviours that Bluetooth-enabled devices use to communicate with other Bluetooth devices. These profiles include settings to parametrize and to control the communication from start. Adherence to profiles saves the time for transmitting the parameters anew before the bi-directional link becomes effective. There are a wide range of Bluetooth profiles that describe many different types of applications or use cases for devices.[20][21]

List of applications


A typical Bluetooth mobile phone headset.

- Wireless control of and communication between a mobile phone and a handsfree headset. This was one of the earliest applications to become popular.[22]
- Wireless control of and communication between a mobile phone and a Bluetooth compatible car stereo system.
- Wireless control of and communication with tablets and speakers such as iOS and Android devices.
- Wireless Bluetooth headset and Intercom. Idiomatically, a headset is sometimes called "a Bluetooth".
- Wireless streaming of audio to headphones with[23] or without[24] communication capabilities.
- Wireless networking between PCs in a confined space and where little bandwidth is required.[25]
- Wireless communication with PC input and output devices, the most common being the mouse, keyboard and printer.
- Transfer of files, contact details, calendar appointments, and reminders between devices with OBEX.
- Replacement of previous wired RS-232 serial communications in test equipment, GPS receivers, medical equipment, bar code scanners, and traffic control devices.
- For controls where infrared was often used.
- For low bandwidth applications where higher USB bandwidth is not required and cable-free connection desired.
- Sending small advertisements from Bluetooth-enabled advertising hoardings to other, discoverable, Bluetooth devices.[26]
- Wireless bridge between two Industrial Ethernet (*e.g.*, PROFINET) networks.
- Three seventh and eighth generation game consoles, Nintendo's Wii.[27] and Sony's PlayStation 3, use Bluetooth for their respective wireless controllers.
- Dial-up internet access on personal computers or PDAs using a data-capable mobile phone as a wireless modem.
- Short range transmission of health sensor data from medical devices to mobile phone, set-top box or dedicated telehealth devices.[28]
- Allowing a DECT phone to ring and answer calls on behalf of a nearby mobile phone.
- Real-time location systems (RTLS), are used to track and identify the location of objects in real-time using “Nodes” or “tags” attached to, or embedded in the objects tracked, and “Readers” that receive and process the wireless signals from these tags to determine their locations.[29]
- Personal security application on mobile phones for prevention of theft or loss of items. The protected item has a Bluetooth marker (*e.g.*, a tag) that is in constant communication with the phone. If the connection is broken (the marker is out of range of the phone) then an alarm is raised. This can also be used as a man overboard alarm. A product using this technology has been available since 2009.[30]

- Calgary, Alberta, Canada's Roads Traffic division uses data collected from travelers' Bluetooth devices to predict travel times and road congestion for motorists.[31]
- Wireless transmission of audio,[32] (a more reliable alternative to FM transmitters)

Bluetooth vs. Wi-Fi (IEEE 802.11)

Bluetooth and Wi-Fi (the brand name for products using IEEE 802.11 standards) have some similar applications: setting up networks, printing, or transferring files. Wi-Fi is intended as a replacement for high speed cabling for general local area network access in work areas. This category of applications is sometimes called wireless local area networks (WLAN). Bluetooth was intended for portable equipment and its applications. The category of applications is outlined as the wireless personal area network (WPAN). Bluetooth is a replacement for cabling in a variety of personally carried applications in any setting, and also works for fixed location applications such as smart energy functionality in the home (thermostats, etc.).

Wi-Fi and Bluetooth are to some extent complementary in their applications and usage. Wi-Fi is usually access point-centered, with an asymmetrical client-server connection with all traffic routed through the access point, while Bluetooth is usually symmetrical, between two Bluetooth devices. Bluetooth serves well in simple applications where two devices need to connect with minimal configuration like a button press, as in headsets and remote controls, while Wi-Fi suits better in applications where some degree of client configuration is possible and high speeds are required, especially for network access through an access node. However, Bluetooth access points do exist and ad-hoc connections are possible with Wi-Fi though not as simply as with Bluetooth. Wi-Fi Direct was recently developed to add a more Bluetooth-like ad-hoc functionality to Wi-Fi.

Devices

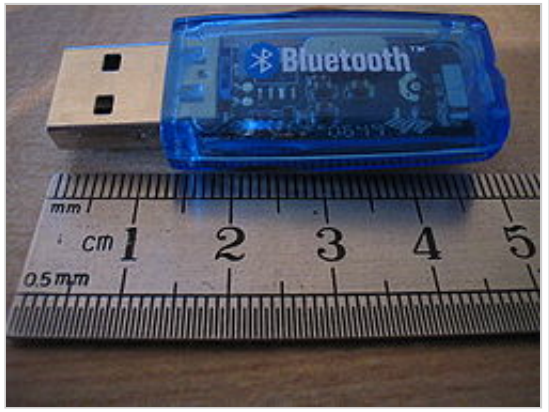
Bluetooth exists in many products, such as telephones, tablets, media players, robotics systems, handheld, laptops and console gaming equipment, and some high definition headsets, modems, and watches.[33] The technology is useful when transferring information between two or more devices that are near each other in low-bandwidth situations. Bluetooth is commonly used to transfer sound data with telephones (i.e., with a Bluetooth headset) or byte data with hand-held computers (transferring files).

A Bluetooth USB dongle with a 100 m range.

Bluetooth protocols simplify the discovery and setup of services between devices.[34] Bluetooth devices can advertise all of the services they provide.[35] This makes using services easier, because more of the security, network address and permission configuration can be automated than with many other network types.[34]

Computer requirements

A personal computer that does not have embedded Bluetooth can use a Bluetooth adapter that enables the PC to communicate with Bluetooth devices. While some desktop computers and most recent laptops come with a built-in Bluetooth radio, others require an external adapter, typically in the form of a small USB "dongle."



A typical Bluetooth USB dongle.

Unlike its predecessor, IrDA, which requires a separate adapter for each device, Bluetooth lets multiple devices communicate with a computer over a single adapter.[36]

Operating system implementation

For more details on this topic, see Bluetooth stack.

Apple products have worked with Bluetooth since Mac OS X v10.2, which was released in 2002.[37]


An internal notebook Bluetooth card (14×36×4 mm).

For Microsoft platforms, Windows XP Service Pack 2 and SP3 releases work natively with Bluetooth v1.1, v2.0 and v2.0+EDR.[38] Previous versions required users to install their Bluetooth adapter's own drivers, which were not directly supported by Microsoft.[39] Microsoft's own Bluetooth dongles (packaged with their Bluetooth computer devices) have no external drivers and thus require at least Windows XP Service Pack 2. Windows Vista RTM/SP1 with the Feature Pack for Wireless or Windows Vista SP2 work with Bluetooth v2.1+EDR.[38] Windows 7 works with Bluetooth v2.1+EDR and Extended Inquiry Response (EIR).[38]

The Windows XP and Windows Vista/Windows 7 Bluetooth stacks support the following Bluetooth profiles natively: PAN, SPP, DUN, HID, HCRP. The Windows XP stack can be replaced by a third party stack that supports more profiles or newer Bluetooth versions. The Windows Vista/Windows 7 Bluetooth stack supports vendor-supplied additional profiles without requiring that the Microsoft stack be replaced.[38]

Linux has two popular Bluetooth stacks, BlueZ and Affix. The BlueZ stack is included with most Linux kernels and was originally developed by Qualcomm.[40] The Affix stack was developed by Nokia. FreeBSD features Bluetooth since its v5.0 release. NetBSD features Bluetooth since its v4.0 release. Its Bluetooth stack has been ported to OpenBSD as well.

Specifications and features

The development of the short link radio technology, later named Bluetooth, was initiated by Nils Rydbeck CTO at Ericson Mobile in Lund. The purpose was to create a wireless headset, according to two inventions, presented in 1989, SE 8902098-6 (http://worldwide.espacenet.com/textdoc?DB=EPODOC&IDX=SE8902098-6), issued 1989-06-12 and 1992 SE 9202239 (http://worldwide.espacenet.com/textdoc?DB=EPODOC&IDX=SE9202239), issued 1992-07-24 by Dr. Johan Ullman. Nils Rydbeck tasked Tord Wingren with specifying and Jaap Haartsen and Sven Mattisson with developing, who were working for Ericsson in Lund, Sweden.[41] The specification is based on frequency-hopping spread spectrum technology.

The specifications were formalized by the Bluetooth Special Interest Group (SIG). The SIG was formally announced on 20 May 1998. Today it has a membership of over 20,000 companies worldwide.[42] It was established by Ericsson, IBM, Intel, Toshiba and Nokia, and later joined by many other companies.

All versions of the Bluetooth standards support downward compatibility. That lets the latest standard cover all older versions.

The Bluetooth Core Specification Working Group (CSWG) produces mainly 4 kinds of specifications

- The Bluetooth Core Specification, release cycle is typically a few years in between
- Core Specification Addendum (CSA), release cycle can be as tight as a few times per year
- Core Specification Supplements (CSS), can be released very quickly
- Errata

Bluetooth v1.0 and v1.0B

Versions 1.0 and 1.0B had many problems and manufacturers had difficulty making their products interoperable. Versions 1.0 and 1.0B also included mandatory Bluetooth hardware device address (BD_ADDR) transmission in the Connecting process (rendering anonymity impossible at the protocol level), which was a major setback for certain services planned for use in Bluetooth environments.

Bluetooth v1.1

- Ratified as IEEE Standard 802.15.1–2002[43]
- Many errors found in the v1.0B specifications were fixed.
- Added possibility of non-encrypted channels.
- Received Signal Strength Indicator (RSSI).

Bluetooth v1.2

Major enhancements include the following:

- Faster Connection and Discovery
- *Adaptive frequency-hopping spread spectrum (AFH)*, which improves resistance to radio frequency interference by avoiding the use of crowded frequencies in the hopping sequence.
- Higher transmission speeds in practice, up to 721 kbit/s,[44] than in v1.1.
- Extended Synchronous Connections (eSCO), which improve voice quality of audio links by allowing retransmissions of corrupted packets, and may optionally increase audio latency to provide better concurrent data transfer.
- Host Controller Interface (HCI) operation with three-wire UART.
- Ratified as IEEE Standard 802.15.1–2005[45]
- Introduced Flow Control and Retransmission Modes for L2CAP.

Bluetooth v2.0 + EDR

This version of the Bluetooth Core Specification was released in 2004. The main difference is the introduction of an Enhanced Data Rate (EDR) for faster data transfer. The nominal rate of EDR is about 3 Mbit/s, although the practical data transfer rate is 2.1 Mbit/s.[44] EDR uses a combination of GFSK and Phase Shift Keying modulation (PSK) with two variants, π/4-DQPSK and 8DPSK.[46] EDR can provide a lower power consumption through a reduced duty cycle.

The specification is published as *Bluetooth v2.0 + EDR*, which implies that EDR is an optional feature. Aside from EDR, the v2.0 specification contains other minor improvements, and products may claim compliance to "Bluetooth v2.0" without supporting the higher data rate. At least one commercial device states "Bluetooth v2.0 without EDR" on its data sheet.[47]

Bluetooth v2.1 + EDR

Bluetooth Core Specification Version 2.1 + EDR was adopted by the Bluetooth SIG on 26 July 2007.[46]

The headline feature of v2.1 is secure simple pairing (SSP): this improves the pairing experience for Bluetooth devices, while increasing the use and strength of security. See the section on Pairing below for more details.[48]

Version 2.1 allows various other improvements, including "Extended inquiry response" (EIR), which provides more information during the inquiry procedure to allow better filtering of devices before connection; and sniff subrating, which reduces the power consumption in low-power mode.

Bluetooth v3.0 + HS

Version 3.0 + HS of the Bluetooth Core Specification[46] was adopted by the Bluetooth SIG on 21 April 2009. Bluetooth v3.0 + HS provides theoretical data transfer speeds of up to **24 Mbit/s,** though not over the Bluetooth link itself. Instead, the Bluetooth link is used for negotiation and establishment, and the high data rate traffic is carried over a colocated 802.11 link.

The main new feature is AMP (Alternative MAC/PHY), the addition of 802.11 as a high speed transport. The High-Speed part of the specification is not mandatory, and hence only devices that display the "+HS" logo actually support Bluetooth over 802.11 high-speed data transfer. A Bluetooth v3.0 device without the "+HS" suffix is only required to support features introduced in Core Specification Version 3.0[49] or earlier Core Specification Addendum 1.[50]

L2CAP Enhanced modes
: Enhanced Retransmission Mode (ERTM) implements reliable L2CAP channel, while Streaming Mode (SM) implements unreliable channel with no retransmission or flow control. Introduced in Core Specification Addendum 1.

Alternative MAC/PHY
: Enables the use of alternative MAC and PHYs for transporting Bluetooth profile data. The Bluetooth radio is still used for device discovery, initial connection and profile configuration. However, when large quantities of data must be sent, the high speed alternative MAC PHY 802.11 (typically associated with Wi-Fi) transports the data. This means that Bluetooth uses proven low power connection models when the system is idle, and the faster radio when it must send large quantities of data. AMP links require enhanced L2CAP modes.

Unicast Connectionless Data
: Permits sending service data without establishing an explicit L2CAP channel. It is intended for use by applications that require low latency between user action and reconnection/transmission of data. This is only appropriate for small amounts of data.

Enhanced Power Control
: Updates the power control feature to remove the open loop power control, and also to clarify ambiguities in power control introduced by the new modulation schemes added for EDR. Enhanced power control removes the ambiguities by specifying the behaviour that is expected. The feature also adds closed loop power control, meaning RSSI filtering can start as the response is received. Additionally, a "go straight to maximum power" request has been introduced. This is expected to deal with the headset link loss issue typically observed when a user puts their phone into a pocket on the opposite side to the headset.

Ultra-wideband

The high speed (AMP) feature of Bluetooth v3.0 was originally intended for UWB, but the WiMedia Alliance, the body responsible for the flavor of UWB intended for Bluetooth, announced in March 2009 that it was disbanding, and ultimately UWB was omitted from the Core v3.0 specification.[51]

On 16 March 2009, the WiMedia Alliance announced it was entering into technology transfer agreements for the WiMedia Ultra-wideband (UWB) specifications. WiMedia has transferred all current and future specifications, including work on future high speed and power optimized implementations, to the Bluetooth Special Interest Group (SIG), Wireless USB Promoter Group and the USB Implementers Forum. After successful completion of the

technology transfer, marketing, and related administrative items, the WiMedia Alliance ceased operations.[52][53][54][55][56][57]

In October 2009 the Bluetooth Special Interest Group suspended development of UWB as part of the alternative MAC/PHY, Bluetooth v3.0 + HS solution. A small, but significant, number of former WiMedia members had not and would not sign up to the necessary agreements for the IP transfer. The Bluetooth SIG is now in the process of evaluating other options for its longer term roadmap.[58][59][60]

Bluetooth v4.0

See also: Bluetooth low energy

The Bluetooth SIG completed the Bluetooth Core Specification version 4.0 (called Bluetooth Smart) and has been adopted as of 30 June 2010. It includes *Classic Bluetooth*, *Bluetooth high speed* and *Bluetooth low energy* protocols. Bluetooth high speed is based on Wi-Fi, and Classic Bluetooth consists of legacy Bluetooth protocols.

Bluetooth low energy, previously known as Wibree,[61] is a subset of Bluetooth v4.0 with an entirely new protocol stack for rapid build-up of simple links. As an alternative to the Bluetooth standard protocols that were introduced in Bluetooth v1.0 to v3.0, it is aimed at very low power applications running off a coin cell. Chip designs allow for two types of implementation, dual-mode, single-mode and enhanced past versions.[62] The provisional names *Wibree* and *Bluetooth ULP* (Ultra Low Power) were abandoned and the BLE name was used for a while. In late 2011, new logos "Bluetooth Smart Ready" for hosts and "Bluetooth Smart" for sensors were introduced as the general-public face of BLE.[63]

- In a single-mode implementation, only the low energy protocol stack is implemented. STMicroelectronics,[64] AMICCOM,[65] CSR,[66] Nordic Semiconductor[67] and Texas Instruments[68] have released single mode Bluetooth low energy solutions.
- In a dual-mode implementation, Bluetooth Smart functionality is integrated into an existing Classic Bluetooth controller. As of March 2011, the following semiconductor companies have announced the availability of chips meeting the standard: Qualcomm-Atheros, CSR, Broadcom[69][70] and Texas Instruments. The compliant architecture shares all of Classic Bluetooth's existing radio and functionality resulting in a negligible cost increase compared to Classic Bluetooth.

Cost-reduced single-mode chips, which enable highly integrated and compact devices, feature a lightweight Link Layer providing ultra-low power idle mode operation, simple device discovery, and reliable point-to-multipoint data transfer with advanced power-save and secure encrypted connections at the lowest possible cost.

General improvements in version 4.0 include the changes necessary to facilitate BLE modes, as well the Generic Attribute Profile (GATT) and Security Manager (SM) services with AES Encryption.

Core Specification Addendum 2 was unveiled in December 2011; it contains improvements to the audio Host Controller Interface and to the High Speed (802.11) Protocol Adaptation Layer.

Core Specification Addendum 3 revision 2 has an adoption date of 24 July 2012.

Core Specification Addendum 4 has an adoption date of 12 February 2013.

Bluetooth v4.1

The Bluetooth SIG announced formal adoption of the Bluetooth v4.1 specification on 4 December 2013. This specification is an incremental software update to Bluetooth Specification v4.0, and not a hardware update. The update incorporates Bluetooth Core Specification Addenda (CSA 1, 2, 3 & 4) and adds new features that improve consumer usability. These include increased co-existence support for LTE, bulk data exchange rates—and aid developer innovation by allowing devices to support multiple roles simultaneously.[71]

New features of this specification include:

- Mobile Wireless Service Coexistence Signaling
- Train Nudging and Generalized Interlaced Scanning
- Low Duty Cycle Directed Advertising
- L2CAP Connection Oriented and Dedicated Channels with Credit Based Flow Control
- Dual Mode and Topology
- LE Link Layer Topology
- 802.11n PAL
- Audio Architecture Updates for Wide Band Speech
- Fast Data Advertising Interval
- Limited Discovery Time[72]

Notice that some features were already available in a Core Specification Addendum (CSA) before the release of v4.1.

Bluetooth v4.2

Bluetooth v4.2 was released on December 2, 2014. It Introduces some key features for IoT. Some features, such as Data Length Extension, require a hardware update.[73] But some older Bluetooth hardware may receive some Bluetooth v4.2 features, such as privacy updates via firmware.[74]

The major areas of improvement are:

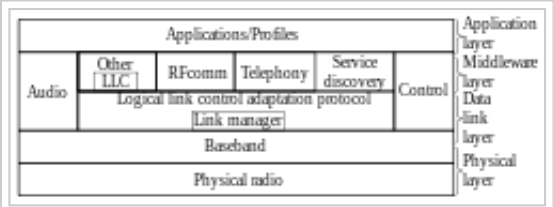
- LE Data Packet Length Extension
- LE Secure Connections
- Link Layer Privacy
- Link Layer Extended Scanner Filter Policies
- IP connectivity for Bluetooth Smart devices to become available soon after the introduction of BT v4.2 via the new Internet Protocol Support Profile (IPSP).
- IPSP adds an IPv6 connection option for Bluetooth Smart, to support connected home and other IoT implementations.

Technical information

Bluetooth protocol stack

Main articles: Bluetooth stack and Bluetooth protocols

Bluetooth is defined as a layer protocol architecture consisting of core protocols, cable replacement protocols, telephony control protocols, and adopted protocols.[75] Mandatory protocols for all Bluetooth stacks are: LMP, L2CAP and SDP. In addition, devices that communicate with Bluetooth almost universally can use these protocols: HCI and RFCOMM.



Bluetooth Protocol Stack

LMP

The *Link Management Protocol* (LMP) is used for set-up and control of the radio link between two devices. Implemented on the controller.

L2CAP

The *Logical Link Control and Adaptation Protocol* (L2CAP) Used to multiplex multiple logical connections between two devices using different higher level protocols. Provides segmentation and reassembly of on-air packets.

In *Basic* mode, L2CAP provides packets with a payload configurable up to 64 kB, with 672 bytes as the default MTU, and 48 bytes as the minimum mandatory supported MTU.

In *Retransmission and Flow Control* modes, L2CAP can be configured either for isochronous data or reliable data per channel by performing retransmissions and CRC checks.

Bluetooth Core Specification Addendum 1 adds two additional L2CAP modes to the core specification. These modes effectively deprecate original Retransmission and Flow Control modes:

- **Enhanced Retransmission Mode** (ERTM): This mode is an improved version of the original retransmission mode. This mode provides a reliable L2CAP channel.
- **Streaming Mode** (SM): This is a very simple mode, with no retransmission or flow control. This mode provides an unreliable L2CAP channel.

Reliability in any of these modes is optionally and/or additionally guaranteed by the lower layer Bluetooth BDR/EDR air interface by configuring the number of retransmissions and flush timeout (time after which the radio flushes packets). In-order sequencing is guaranteed by the lower layer.

Only L2CAP channels configured in ERTM or SM may be operated over AMP logical links.

SDP

The *Service Discovery Protocol* (SDP) allows a device to discover services offered by other devices, and their associated parameters. For example, when you use a mobile phone with a Bluetooth headset, the phone uses SDP to determine which Bluetooth profiles the headset can use (Headset Profile, Hands Free Profile, Advanced Audio Distribution Profile (A2DP) etc.) and the protocol multiplexer settings needed for the phone to connect to the headset using each of them. Each service is identified by a Universally Unique Identifier (UUID), with official services (Bluetooth profiles) assigned a short form UUID (16 bits rather than the full 128).

RFCOMM

Radio Frequency Communications (RFCOMM) is a cable replacement protocol used to generate a virtual serial data stream. RFCOMM provides for binary data transport and emulates EIA-232 (formerly RS-232) control signals over the Bluetooth baseband layer, i.e. it is a serial port emulation.

RFCOMM provides a simple reliable data stream to the user, similar to TCP. It is used directly by many telephony related profiles as a carrier for AT commands, as well as being a transport layer for OBEX over Bluetooth.

Many Bluetooth applications use RFCOMM because of its widespread support and publicly available API on most operating systems. Additionally, applications that used a serial port to communicate can be quickly ported to use RFCOMM.

BNEP

The *Bluetooth Network Encapsulation Protocol* (BNEP) is used for transferring another protocol stack's data via an L2CAP channel. Its main purpose is the transmission of IP packets in the Personal Area Networking Profile. BNEP performs a similar function to SNAP in Wireless LAN.

AVCTP

The *Audio/Video Control Transport Protocol* (AVCTP) is used by the remote control profile to transfer AV/C commands over an L2CAP channel. The music control buttons on a stereo headset use this protocol to control the music player.

AVDTP

The *Audio/Video Distribution Transport Protocol* (AVDTP) is used by the advanced audio distribution profile to stream music to stereo headsets over an L2CAP channel intended for video distribution profile in the bluetooth transmission.

TCS

The *Telephony Control Protocol – Binary* (TCS BIN) is the bit-oriented protocol that defines the call control signaling for the establishment of voice and data calls between Bluetooth devices. Additionally, "TCS BIN defines mobility management procedures for handling groups of Bluetooth TCS devices."

TCS-BIN is only used by the cordless telephony profile, which failed to attract implementers. As such it is only of historical interest.

Adopted protocols

Adopted protocols are defined by other standards-making organizations and incorporated into Bluetooth's protocol stack, allowing Bluetooth to code protocols only when necessary. The adopted protocols include:

- **Point-to-Point Protocol (PPP)**: Internet standard protocol for transporting IP datagrams over a point-to-point link.
- **TCP/IP/UDP**: Foundation Protocols for TCP/IP protocol suite
- **Object Exchange Protocol (OBEX)**: Session-layer protocol for the exchange of objects, providing a model for object and operation representation
- **Wireless Application Environment/Wireless Application Protocol (WAE/WAP)**: WAE specifies an application framework for wireless devices and WAP is an open standard to provide mobile users access to telephony and information services.[75]

Baseband error correction

Depending on packet type, individual packets may be protected by error correction, either 1/3 rate forward error correction (FEC) or 2/3 rate. In addition, packets with CRC will be retransmitted until acknowledged by automatic repeat request (ARQ).

Setting up connections

Any Bluetooth device in *discoverable mode* transmits the following information on demand:

- Device name
- Device class
- List of services
- Technical information (for example: device features, manufacturer, Bluetooth specification used, clock offset)

Any device may perform an inquiry to find other devices to connect to, and any device can be configured to respond to such inquiries. However, if the device trying to connect knows the address of the device, it always responds to direct connection requests and transmits the information shown in the list above if requested. Use of a device's services may require pairing or acceptance by its owner, but the connection itself can be initiated by any device and held until it goes out of range. Some devices can be connected to only one device at a time, and connecting to them prevents them from connecting to other devices and appearing in inquiries until they disconnect from the other device.

Every device has a unique 48-bit address. However, these addresses are generally not shown in inquiries. Instead, friendly Bluetooth names are used, which can be set by the user. This name appears when another user scans for devices and in lists of paired devices.

Most cellular phones have the Bluetooth name set to the manufacturer and model of the phone by default. Most cellular phones and laptops show only the Bluetooth names and special programs are required to get additional information about remote devices. This can be confusing as, for example, there could be several cellular phones in range named T610 (see Bluejacking).

Pairing and bonding

Motivation

Many services offered over Bluetooth can expose private data or let a connecting party control the Bluetooth device. Security reasons make it necessary to recognize specific devices, and thus enable control over which devices can connect to a given Bluetooth device. At the same time, it is useful for Bluetooth devices to be able to establish a connection without user intervention (for example, as soon as in range).

To resolve this conflict, Bluetooth uses a process called *bonding*, and a bond is generated through a process called *pairing*. The pairing process is triggered either by a specific request from a user to generate a bond (for example, the user explicitly requests to "Add a Bluetooth device"), or it is triggered automatically when connecting to a service where (for the first time) the identity of a device is required for security purposes. These two cases are referred to as dedicated bonding and general bonding respectively.

Pairing often involves some level of user interaction. This user interaction confirms the identity of the devices. When pairing successfully completes, a bond forms between the two devices, enabling those two devices to connect to each other in the future without repeating the pairing process to confirm device identities. When desired, the user can remove the bonding relationship.

Implementation

During pairing, the two devices establish a relationship by creating a shared secret known as a *link key*. If both devices store the same link key, they are said to be *paired* or *bonded*. A device that wants to communicate only with a bonded device can cryptographically authenticate the identity of the other device, ensuring it is the same device it previously paired with. Once a link key is generated, an authenticated Asynchronous Connection-Less (ACL) link between the devices may be encrypted to protect exchanged data against eavesdropping. Users can delete link keys from either device, which removes the bond between the devices—so it is possible for one device to have a stored link key for a device it is no longer paired with.

Bluetooth services generally require either encryption or authentication and as such require pairing before they let a remote device connect. Some services, such as the Object Push Profile, elect not to explicitly require authentication or encryption so that pairing does not interfere with the user experience associated with the service use-cases.

Pairing mechanisms

Pairing mechanisms changed significantly with the introduction of Secure Simple Pairing in Bluetooth v2.1. The following summarizes the pairing mechanisms:

- *Legacy pairing*: This is the only method available in Bluetooth v2.0 and before. Each device must enter a PIN code; pairing is only successful if both devices enter the same PIN code. Any 16-byte UTF-8 string may be used as a PIN code; however, not all devices may be capable of entering all possible PIN codes.
  - *Limited input devices*: The obvious example of this class of device is a Bluetooth Hands-free headset, which generally have few inputs. These devices usually have a *fixed PIN*, for example "0000" or "1234", that are hard-coded into the device.
  - *Numeric input devices*: Mobile phones are classic examples of these devices. They allow a user to enter a numeric value up to 16 digits in length.
  - *Alpha-numeric input devices*: PCs and smartphones are examples of these devices. They allow a user to enter full UTF-8 text as a PIN code. If pairing with a less capable device the user must be aware of the input limitations on the other device, there is no mechanism available for a capable device to determine how it should limit the available input a user may use.
- *Secure Simple Pairing* (SSP): This is required by Bluetooth v2.1, although a Bluetooth v2.1 device may only use legacy pairing to interoperate with a v2.0 or earlier device. Secure Simple Pairing uses a form of public key cryptography, and some types can help protect against man in the middle, or MITM attacks. SSP has the following characteristics:
  - *Just works*: As the name implies, this method just works, with no user interaction. However, a device may prompt the user to confirm the pairing process. This method is typically used by headsets with very limited IO capabilities, and is more secure than the fixed PIN

mechanism this limited set of devices uses for legacy pairing. This method provides no man-in-the-middle (MITM) protection.

- *Numeric comparison*: If both devices have a display, and at least one can accept a binary yes/no user input, they may use Numeric Comparison. This method displays a 6-digit numeric code on each device. The user should compare the numbers to ensure they are identical. If the comparison succeeds, the user(s) should confirm pairing on the device(s) that can accept an input. This method provides MITM protection, assuming the user confirms on both devices and actually performs the comparison properly.
- *Passkey Entry*: This method may be used between a device with a display and a device with numeric keypad entry (such as a keyboard), or two devices with numeric keypad entry. In the first case, the display is used to show a 6-digit numeric code to the user, who then enters the code on the keypad. In the second case, the user of each device enters the same 6-digit number. Both of these cases provide MITM protection.
- *Out of band* (OOB): This method uses an external means of communication, such as Near Field Communication (NFC) to exchange some information used in the pairing process. Pairing is completed using the Bluetooth radio, but requires information from the OOB mechanism. This provides only the level of MITM protection that is present in the OOB mechanism.

SSP is considered simple for the following reasons:

- In most cases, it does not require a user to generate a passkey.
- For use-cases not requiring MITM protection, user interaction can be eliminated.
- For *numeric comparison*, MITM protection can be achieved with a simple equality comparison by the user.
- Using OOB with NFC enables pairing when devices simply get close, rather than requiring a lengthy discovery process.

Security concerns

Prior to Bluetooth v2.1, encryption is not required and can be turned off at any time. Moreover, the encryption key is only good for approximately 23.5 hours; using a single encryption key longer than this time allows simple XOR attacks to retrieve the encryption key.

- Turning off encryption is required for several normal operations, so it is problematic to detect if encryption is disabled for a valid reason or for a security attack.

Bluetooth v2.1 addresses this in the following ways:

- Encryption is required for all non-SDP (Service Discovery Protocol) connections
- A new Encryption Pause and Resume feature is used for all normal operations that require that encryption be disabled. This enables easy identification of normal operation from security attacks.
- The encryption key must be refreshed before it expires.

Link keys may be stored on the device file system, not on the Bluetooth chip itself. Many Bluetooth chip manufacturers let link keys be stored on the device—however, if the device is removable, this means that the link key moves with the device.

Air interface

The protocol operates in the license-free ISM band at 2.402–2.480 GHz.[76] To avoid interfering with other protocols that use the 2.45 GHz band, the Bluetooth protocol divides the band into 79 channels (each 1 MHz wide) and changes channels, generally 1600 times per second. Implementations with versions 1.1 and 1.2 reach speeds of 723.1 kbit/s. Version 2.0 implementations feature Bluetooth Enhanced Data Rate (EDR) and reach 2.1 Mbit/s; this comes with a concomitant higher power consumption. In some cases, the higher data rate is expected to offset this increased drain.

Security

Overview

See also: Mobile security § Attacks based on communication networks

Bluetooth implements confidentiality, authentication and key derivation with custom algorithms based on the SAFER+ block cipher. Bluetooth key generation is generally based on a Bluetooth PIN, which must be entered into both devices. This procedure might be modified if one of the devices has a fixed PIN (e.g., for headsets or similar devices with a restricted user interface). During pairing, an initialization key or master key is generated, using the E22 algorithm.[77] The E0 stream cipher is used for encrypting packets, granting confidentiality, and is based on a shared cryptographic secret, namely a previously generated link key or master key. Those keys, used for subsequent encryption of data sent via the air interface, rely on the Bluetooth PIN, which has been entered into one or both devices.

An overview of Bluetooth vulnerabilities exploits was published in 2007 by Andreas Becker.[78]

In September 2008, the National Institute of Standards and Technology (NIST) published a Guide to Bluetooth Security as a reference for organizations. It describes Bluetooth security capabilities and how to secure Bluetooth technologies effectively. While Bluetooth has its benefits, it is susceptible to denial-of-service attacks, eavesdropping, man-in-the-middle attacks, message modification, and resource misappropriation. Users and organizations must evaluate their acceptable level of risk and incorporate security into the lifecycle of Bluetooth devices. To help mitigate risks, included in the NIST document are security checklists with guidelines and recommendations for creating and maintaining secure Bluetooth piconets, headsets, and smart card readers.[79]

Bluetooth v2.1 – finalized in 2007 with consumer devices first appearing in 2009 – makes significant changes to Bluetooth's security, including pairing. See the pairing mechanisms section for more about these changes.

Bluejacking

Main article: Bluejacking

Bluejacking is the sending of either a picture or a message from one user to an unsuspecting user through *Bluetooth* wireless technology. Common applications include short messages, *e.g.*, "You've just been bluejacked!".[80] Bluejacking does not involve the removal or alteration of any data from the device. Bluejacking can also involve taking control of a mobile device wirelessly and phoning a premium rate line, owned by the bluejacker. Security advances have alleviated this issue.

History of security concerns

2001–2004

In 2001, Jakobsson and Wetzel from Bell Laboratories discovered flaws in the Bluetooth pairing protocol and also pointed to vulnerabilities in the encryption scheme.[81] In 2003, Ben and Adam Laurie from A.L. Digital Ltd. discovered that serious flaws in some poor implementations of Bluetooth security may lead to disclosure of personal data.[82] In a subsequent experiment, Martin Herfurt from the trifinite.group was able to do a field-trial at the CeBIT fairgrounds, showing the importance of the problem to the world. A new attack called BlueBug was used for this experiment.[83] In 2004 the first purported virus using Bluetooth to spread itself among mobile phones appeared on the Symbian OS.[84] The virus was first described by Kaspersky Lab and requires users to confirm the installation of unknown software before it can propagate. The virus was written as a proof-of-concept by a group of virus writers known as "29A" and sent to anti-virus groups. Thus, it should be regarded as a potential (but not real) security threat to Bluetooth technology or Symbian OS since the virus has never spread outside of this system. In August 2004, a world-record-setting experiment (see also Bluetooth sniping) showed that the range of Class 2 Bluetooth radios could be extended to 1.78 km (1.11 mi) with directional antennas and signal amplifiers.[85] This poses a potential security threat because it enables attackers to access vulnerable Bluetooth devices from a distance beyond expectation. The attacker must also be able to receive information from the victim to set up a connection. No attack can be made against a Bluetooth device unless the attacker knows its Bluetooth address and which channels to transmit on, although these can be deduced within a few minutes if the device is in use.[86]

2005

In January 2005, a mobile malware worm known as *Lasco.A* began targeting mobile phones using Symbian OS (Series 60 platform) using Bluetooth enabled devices to replicate itself and spread to other devices. The worm is self-installing and begins once the mobile user approves the transfer of the file (velasco.sis) from another device. Once installed, the worm begins looking for other Bluetooth enabled devices to infect. Additionally, the worm infects other .SIS files on the device, allowing replication to another device through use of removable media (Secure Digital, Compact Flash, etc.). The worm can render the mobile device unstable.[87]

In April 2005, Cambridge University security researchers published results of their actual implementation of passive attacks against the PIN-based pairing between commercial Bluetooth devices. They confirmed that attacks are practicably fast, and the Bluetooth symmetric key establishment method is vulnerable. To rectify this vulnerability, they designed an implementation that showed that stronger, asymmetric key establishment is feasible for certain classes of devices, such as mobile phones.[88]

In June 2005, Yaniv Shaked[89] and Avishai Wool[90] published a paper describing both passive and active methods for obtaining the PIN for a Bluetooth link. The passive attack allows a suitably equipped attacker to eavesdrop on communications and spoof, if the attacker was present at the time of initial pairing. The active method makes use of a specially constructed message that must be inserted at a specific point in the protocol, to make the master and slave repeat the pairing process. After that, the first method can be used to crack the PIN. This attack's major weakness is that it requires the user of the devices under attack to re-enter the PIN during the attack when the device prompts them to. Also, this active attack probably requires custom hardware, since most commercially available Bluetooth devices are not capable of the timing necessary.[91]

In August 2005, police in Cambridgeshire, England, issued warnings about thieves using Bluetooth enabled phones to track other devices left in cars. Police are advising users to ensure that any mobile networking connections are de-activated if laptops and other devices are left in this way.[92]

2006

In April 2006, researchers from Secure Network and F-Secure published a report that warns of the large number of devices left in a visible state, and issued statistics on the spread of various Bluetooth services and the ease of spread of an eventual Bluetooth worm.[93]

2007

In October 2007, at the Luxemburgish Hack.lu Security Conference, Kevin Finistere and Thierry Zoller demonstrated and released a remote root shell via Bluetooth on Mac OS X v10.3.9 and v10.4. They also demonstrated the first Bluetooth PIN and Linkkeys cracker, which is based on the research of Wool and Shaked.

Mitigation

Options to mitigate against Bluetooth security attacks include:[94][95]

- Enable Bluetooth only when required
- Enable Bluetooth discovery only when necessary, and disable discovery when finished
- Do not enter link keys or PINs when unexpectedly prompted to do so
- Remove paired devices when not in use

- Regularly update firmware on Bluetooth-enabled devices

Health concerns

Main article: Wireless electronic devices and health

Bluetooth uses the microwave radio frequency spectrum in the 2.402 GHz to 2.480 GHz range.[76] Maximum power output from a Bluetooth radio is 100 mW for class 1, 2.5 mW for class 2, and 1 mW for class 3 devices. Even the maximum power output of class 1 is a lower level than the lowest powered mobile phones.[96] UMTS & W-CDMA outputs 250 mW, GSM1800/1900 outputs 1000 mW, and GSM850/900 outputs 2000 mW.

Interference caused by USB 3.0

USB 3.0 devices, ports and cables have been proven to interfere with Bluetooth devices due to the electronic noise they release falling over the same operating band as Bluetooth. The close proximity of Bluetooth and USB 3.0 devices can result in a drop in throughput or complete connection loss of the Bluetooth device/s connected to a computer.[97]

Various strategies can be applied to resolve the problem, ranging from simple solutions such as increasing the distance of USB 3.0 devices from any Bluetooth devices or purchasing better shielded USB cables. Other solutions include applying additional shielding to the internal Bluetooth components of a computer.[98]

Bluetooth award programs

The Bluetooth Innovation World Cup, a marketing initiative of the Bluetooth Special Interest Group (SIG), was an international competition that encouraged the development of innovations for applications leveraging Bluetooth technology in sports, fitness and health care products. The aim of the competition was to stimulate new markets.[99]

The Bluetooth Innovation World Cup morphed into the Bluetooth Breakthrough Awards in 2013. The Breakthrough Awards[100] Bluetooth program highlights the most innovative products and applications available today, prototypes coming soon, and student-led projects in the making.

See also

- Bluesniping

- BlueSoleil – proprietary driver
- Bluetooth wireless headsets
- Continua Health Alliance
- DASH7
- iBeacon
- Java APIs for Bluetooth
- Li-Fi
- MyriaNed
- Near field communication
- RuBee – secure wireless protocol alternative
- Tethering
- ZigBee – low-power lightweight wireless protocol in the ISM band

References

1. DualShock#DualShock 4, Wikipedia
2. bluAir. "Bluetooth Range: 100m, 1km, or 10km?" (http://www.bluair.pl/bluetooth-range). *bluair.pl*. Retrieved 4 June 2015.
3. "Basics | Bluetooth Technology Website" (http://www.bluetooth.com/Pages/Basics.aspx). Bluetooth.com. 23 May 2010.
4. "Fast Facts" (http://www.bluetooth.com/Pages/Fast-Facts.aspx). Bluetooth.com. Retrieved 10 December 2013.
5. "Bluetooth traveler" (http://www.hoovers.com/business-information/--pageid__13751--/global-hoov-index.xhtml). hoovers.com. Retrieved 9 April 2010.
6. Newton, Harold. (2007). *Newton's telecom dictionary.* New York: Flatiron Publishing.
7. "Bluetooth.org" (https://www.bluetooth.org/About/bluetooth_sig.htm). Bluetooth.org. Retrieved 3 May 2011.
8. "Brand Enforcement Program" (https://www.bluetooth.org/en-us/bluetooth-brand/brand-enforcement-program). Bluetooth.org. Retrieved 2 November 2013.
9. Kardach, Jim (3 April 2008). "Tech History: How Bluetooth got its name" (http://www.eetimes.com/electronics-news/4182202/Tech-History-How-Bluetooth-got-its-name). Retrieved 11 June 2013.
10. Mark Forsyth. The etymologicon. // Icon Books Ltd. London N79DP, 2011. p. 139.
11. Monson, Heidi (14 December 1999). "Bluetooth Technology and Implications" (http://www.sysopt.com/features/network/article.php/3532506). SysOpt.com. Retrieved 17 February 2009.
12. "About the Bluetooth SIG" (http://www.bluetooth.com/Bluetooth/SIG/). Bluetooth SIG. Retrieved 1 February 2008.
13. "Milestones in the Bluetooth advance" (http://web.archive.org/web/20040620150507/http://www.ericsson.com/bluetooth/companyove/history-bl/). Ericsson Technology Licensing. 22 March 2004. Archived from the original (http://www.ericsson.com/bluetooth/companyove/history-bl/) on 20 June 2004.
14. "Bluetooth Radio Interface, Modulation & Channels" (http://www.radio-electronics.com/info/wireless/bluetooth/radio-interface-modulation.php). Radio-Electronics.com.
15. "How Bluetooth Technology Works" (http://web.archive.org/web/20080117000828/http://bluetooth.com/Bluetooth/Technology/Works/). Bluetooth SIG. Archived from the original (http://www.bluetooth.com/Bluetooth/Technology/Works/) on 17 January 2008. Retrieved 1 February 2008.
16. "Class 1 Bluetooth Dongle Test" (http://www.amperordirect.com/pc/r-electronic-resource/z-reference-bluetooth-class1-myth.html). Amperordirect.com. Retrieved 4 September 2010.

17. "WT41 Long Range Bluetooth Module" (http://www.bluegiga.com/WT41_Long_Range_Bluetooth_Module).
18. "BluBear Industrial Long Range Bluetooth 2.1 Module with EDR" (http://www.lesswire.com/en/products/embedded-wireless-modules/bluetooth/bluebear/overview/).
19. "OEM Bluetooth Serial Port Module OBS433" (http://www.connectblue.com/products/classic-bluetooth-products/classic-bluetooth-modules/bluetooth-serial-port-module-obs433/).
20. "Profiles Overview" (http://developer.bluetooth.org/TechnologyOverview/Pages/Profiles.aspx). Bluetooth.com. Retrieved 3 June 2013.
21. Ian, Paul. "Wi-Fi Direct vs. Bluetooth 4.0: A Battle for Supremacy" (http://www.pcworld.com/article/208778/Wi_Fi_Direct_vs_Bluetooth_4_0_A_Battle_for_Supremacy.html). PC World. Retrieved 27 December 2013.
22. "History of the Bluetooth Special Interest Group" (http://www.bluetooth.com/Pages/History-of-Bluetooth.aspx). Bluetooth.com.
23. "Bluetooth Headphones" (http://www.pricenfees.com/best-bluetooth-headphones-for-running.html). PricenFees.com.
24. "Headphones Unboxed" (http://www.headphonesunboxed.com/best-bluetooth-headphones-for-running/). headphonesunboxed.com. Retrieved 9 January 2015.
25. "Bluetooth Technology" (http://www.mobileinfo.com/Bluetooth/applic.htm). mobileinfo.com.
26. John Fuller. "How Bluetooth Surveillance Works" (http://electronics.howstuffworks.com/bluetooth-surveillance1.htm). howstuffworks. Retrieved 26 May 2015.
27. "Wii Controller" (http://web.archive.org/web/20080220080315/http://bluetooth.com/Bluetooth/Products/Products/Product_Details.htm?ProductID=2951). Bluetooth SIG. Archived from the original (http://bluetooth.com/Bluetooth/Products/Products/Product_Details.htm?ProductID=2951) on 20 February 2008. Retrieved 1 February 2008.
28. "Telemedicine.jp" (http://www.telemedicine.jp/). Telemedicine.jp. Retrieved 4 September 2010.
29. "Real Time Location Systems" (http://www.clarinox.com/docs/whitepapers/RealTime_main.pdf) (PDF). clarinox. Retrieved 4 August 2010.
30. "Tenbu's nio Is Kind Of Like A Car Alarm For Your Cellphone" (http://www.ohgizmo.com/2009/03/30/tenbu-nio-is-kind-of-like-a-car-alarm-for-your-cellphone/). *OhGizmo!*. Retrieved 4 June 2015.
31. "Wireless waves used to track travel times | CTV Calgary News" (http://calgary.ctvnews.ca/wireless-waves-used-to-track-travel-times-1.1054731). Calgary.ctvnews.ca. 26 November 2012. Retrieved 11 July 2013.
32. "Bluetooth Technology for Running Headphones" (http://www.runnerwave.com/bluetooth-headphone-technologies/). runnerwave.com. Retrieved 18 February 2015.
33. "Watch" (http://www.bluetooth.com/English/Products/Pages/Watch.aspx). Bluetooth.com. Retrieved 4 September 2010.
34. "How Bluetooth Works" (http://www.howstuffworks.com/bluetooth.htm). How Stuff Works. 30 June 2010.
35. "Specification Documents" (http://www.bluetooth.com/Specification%20Documents/AssignedNumbersServiceDiscovery.pdf) (PDF). Bluetooth.com. 30 June 2010.
36. "Bluetooth for Programmers" (http://people.csail.mit.edu/rudolph/Teaching/Articles/PartOfBTBook.pdf) (PDF). MIT Computer Science And Artificial Intelligence Laboratory.
37. "Apple Introduces "Jaguar," the Next Major Release of Mac OS X" (http://www.apple.com/pr/library/2002/jul/17jaguar.html) (Press release). Apple. 17 July 2002. Retrieved 4 February 2008.
38. "Bluetooth Wireless Technology FAQ – 2010" (http://download.microsoft.com/download/9/c/5/9c5b2167-8017-4bae-9fde-d599bac8184a/Bth_FAQ.docx). Retrieved 4 September 2010.
39. "Network Protection Technologie" (http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/sp2netwk.mspx). *Changes to Functionality in Microsoft Windows XP Service Pack 2*. Microsoft Technet. Retrieved 1 February 2008.
40. "Official Linux Bluetooth protocol stack" (http://www.bluez.org/). BlueZ. Retrieved 4 September 2010.
41. "The Bluetooth Blues" (http://web.archive.org/web/20071222231740/http://www.information-age.com/article/2001/may/the_bluetooth_blues). Information Age. 24 May 2001. Archived from the original (http://www.information-age.com/article/2001/may/the_bluetooth_blues) on 22 December 2007. Retrieved 1 February 2008.
42. "English Introduction to Membership" (https://www.bluetooth.org/en-us/members/introduction-to-membership). Bluetooth.org. Retrieved 2014-05-13.
43. "IEEE Std 802.15.1–2002 – IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan

area networks – Specific requirements Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs)" (http://ieeexplore.ieee.org/servlet/opac?punumber=7932). Ieeexplore.ieee.org. doi:10.1109/IEEESTD.2002.93621 (https://dx.doi.org/10.1109%2FIEEESTD.2002.93621). Retrieved 4 September 2010.
44. Guy Kewney (16 November 2004). "High speed Bluetooth comes a step closer: enhanced data rate approved" (http://www.newswireless.net/index.cfm/article/629). Newswireless.net. Retrieved 4 February 2008.
45. "IEEE Std 802.15.1–2005 – IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (W Pans)" (http://ieeexplore.ieee.org/servlet/opac?punumber=9980). Ieeexplore.ieee.org. doi:10.1109/IEEESTD.2005.96290 (https://dx.doi.org/10.1109%2FIEEESTD.2005.96290). Retrieved 4 September 2010.
46. "Specification Documents" (http://www.bluetooth.org/docman/handlers/DownloadDoc.ashx?doc_id=40560&ei=25GiT8L3CuTa0QGnmqDVDA&usg=AFQjCNGXY5pm4Tkju1KGs4dYRJLtd03FEg). Bluetooth SIG. Retrieved 3 May 2012.
47. "HTC TyTN Specification" (http://www.europe.htc.com/z/pdf/products/1766_TyTN_LFLT_OUT.PDF) (PDF). HTC. Retrieved 4 February 2008.
48. "Simple Pairing Whitepaper" (http://web.archive.org/web/20061018032605/http://www.bluetooth.com/NR/rdonlyres/0A0B3F36-D15F-4470-85A6-F2CCFA26F70F/0/SimplePairing_WP_V10r00.pdf) (PDF). Version V10r00. Bluetooth SIG. 3 August 2006. Archived from the original (http://bluetooth.com/NR/rdonlyres/0A0B3F36-D15F-4470-85A6-F2CCFA26F70F/0/SimplePairing_WP_V10r00.pdf) (PDF) on 18 October 2006. Retrieved 1 February 2007.
49. "Bluetooth Core Version 3.0 + HS specification" (https://www.bluetooth.org/docman/handlers/DownloadDoc.ashx?doc_id=40560).
50. "Bluetooth Core Specification Addendum (CSA) 1" (https://www.bluetooth.org/DocMan/handlers/DownloadDoc.ashx?doc_id=119993).
51. David Meyer (22 April 2009). "Bluetooth 3.0 released without ultrawideband" (http://news.zdnet.co.uk/communications/0,1000000085,39643174,00.htm). zdnet.co.uk. Retrieved 22 April 2009.
52. "Wimedia.org" (http://www.wimedia.org/). Wimedia.org. 4 January 2010. Retrieved 4 September 2010.
53. "Wimedia.org" (http://www.wimedia.org/imwp/download.asp?ContentID=15508). Wimedia.org. Retrieved 4 September 2010.
54. "Wimedia.org" (http://www.wimedia.org/imwp/download.asp?ContentID=15506). Retrieved 4 September 2010.
55. "bluetooth.com" (http://www.bluetooth.com/Pages/Press-Releases-Detail.aspx?ItemID=4). Retrieved 29 January 2015.
56. "USB.org" (http://www.usb.org/press/WiMedia_Tech_Transfer/). USB.org. 16 March 2009. Retrieved 4 September 2010.
57. "Incisor.tv" (http://www.incisor.tv/2009/03/what-to-make-of-bluetooth-sig-wimedia.html). Incisor.tv. 16 March 2009. Retrieved 4 September 2010.
58. "Bluetooth group drops ultrawideband, eyes 60 GHz" (http://www.eetimes.com/showArticle.jhtml;jsessionid=J5E0PN3NQ5BNLQE1GHPSKH4ATMY32JVN?articleID=221100170). *EETimes*. Retrieved 4 June 2015.
59. "Report: Ultrawideband dies by 2013" (http://www.eetimes.com/showArticle.jhtml;jsessionid=J5E0PN3NQ5BNLQE1GHPSKH4ATMY32JVN?articleID=217201265). *EETimes*. Retrieved 4 June 2015.
60. "Simon Stenhouse - Leech Attempt" (http://www.incisor.tv/download.php?file=140november2009.pdf) (PDF). *incisor.tv*. Retrieved 4 June 2015.
61. "Wibree forum merges with Bluetooth SIG" (http://www.wibree.com/press/Wibree_pressrelease_final_1206.pdf) (PDF) (Press release). Nokia. 12 June 2007. Retrieved 4 February 2008.
62. "Bluetooth.com" (http://www.bluetooth.com/Bluetooth/Press/SIG/SIG_INTRODUCES_BLUETOOTH_LOW_ENERGY_WIRELESS_TECHNOLOGY_THE_NEXT_GENERATION_OF_BLUETOOTH_WIRELESS_TE.htm). Bluetooth.com. Retrieved 4 September 2010.
63. "Bluetooth SIG unveils Smart Marks, explains v4.0 compatibility with unnecessary complexity" (http://www.engadget.com/2011/10/25/bluetooth-sig-unveils-smart-marks-explains-v4-0-compatibility-w/). Engadget.
64. "BlueNRG Bluetooth® low energy wireless network processor - STMicroelectronics"

(http://www.st.com/web/catalog/sense_power/FM1968/CL1976/SC1898/PF258646?s_searchtype=partnumber). *st.com*. Retrieved 4 June 2015.
65. http://www.amiccom.com.tw/
66. "CSR.com" (http://www.csr.com/products/45/csr-energy). CSR. Retrieved 7 April 2011.
67. "Nordicsemi.com" (http://www.nordicsemi.com/eng/Products/Bluetooth-R-low-energy/nRF8001). Nordic Semiconductor. Retrieved 7 April 2011.
68. "TI.com" (http://focus.ti.com/docs/prod/folders/print/cc2540.html). Texas Instruments. Retrieved 7 April 2011.
69. "iFixit MacBook Air 13" Mid 2011 Teardown" (http://www.ifixit.com/Teardown/MacBook-Air-13-Inch-Mid-2011-Teardown/6130/1). iFixit.com. Retrieved 27 July 2011.
70. "Broadcom.com – BCM20702 – Single-Chip Bluetooth® 4.0 HCI Solution with Bluetooth Low Energy (BLE) Support" (http://www.broadcom.com/products/Bluetooth/Bluetooth-RF-Silicon-and-Software-Solutions/BCM20702). Broadcom. Retrieved 27 July 2011.
71. "Press Releases Detail | Bluetooth Technology Website" (http://www.bluetooth.com/Pages/Press-Releases-Detail.aspx?ItemID=197). Bluetooth.com. 2013-12-04. Retrieved 2014-05-13.
72. "Adopted Specification; Bluetooth Technology Website" (https://www.bluetooth.org/en-us/specification/adopted-specifications). Bluetooth.com. 2013-12-04. Retrieved 2014-05-14.
73. "Redmondpie" (http://www.redmondpie.com/bluetooth-4.2-announced-heres-what-is-new/).
74. "DailyTech" (http://www.dailytech.com/Bluetooth+42+Promises+Faster+Connections+Better+Security+to+Stop+Snooping/article36960.htm).
75. Stallings, William. (2005). *Wireless communications & networks.'=' Upper Saddle River, NJ: Pearson Prentice Hall.*
76. D. Chomienne, M. Eftimakis (20 October 2010). "Bluetooth Tutorial" (http://www.newlogic.com/products/Bluetooth-Tutorial-2001.pdf) (PDF). Retrieved 11 December 2009.
77. Juha T. Vainio (25 May 2000). "Bluetooth Security" (http://www.iki.fi/jiitv/bluesec.pdf) (PDF). Helsinki University of Technology. Retrieved 1 January 2009.
78. Andreas Becker (16 August 2007). "Bluetooth Security & Hacks" (http://gsyc.es/~anto/ubicuos2/bluetooth_security_and_hacks.pdf) (PDF). Ruhr-Universität Bochum. Retrieved 10 October 2007.
79. Scarfone, K., and Padgette, J. (September 2008). "Guide to Bluetooth Security" (http://csrc.nist.gov/publications/nistpubs/800-121-rev1/sp800-121_rev1.pdf) (PDF). National Institute of Standards and Technology. Retrieved 3 July 2013.
80. John Fuller. "What is bluejacking?" (http://electronics.howstuffworks.com/bluejacking.htm). howstuffworks. Retrieved 26 May 2015.
81. "Security Weaknesses in Bluetooth". RSA Security Conf. – Cryptographer's Track. CiteSeerX: 10.1.1.23.7357 (http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.23.7357).
82. "Bluetooth" (http://web.archive.org/web/20070126012417/http://www.thebunker.net/resources/bluetooth). The Bunker. Archived from the original (http://www.thebunker.net/resources/bluetooth) on 26 January 2007. Retrieved 1 February 2007.
83. "BlueBug" (http://trifinite.org/trifinite_stuff_bluebug.html). Trifinite.org. Retrieved 1 February 2007.
84. John Oates (15 June 2004). "Virus attacks mobiles via Bluetooth" (http://www.theregister.co.uk/2004/06/15/symbian_virus/). The Register. Retrieved 1 February 2007.
85. "Long Distance Snarf" (http://trifinite.org/trifinite_stuff_lds.html). Trifinite.org. Retrieved 1 February 2007.
86. "Dispelling Common Bluetooth Misconceptions" (http://www.sans.edu/research/security-laboratory/article/bluetooth). SANS. Retrieved 9 July 2014.
87. "F-Secure Malware Information Pages: Lasco.A" (http://www.f-secure.com/v-descs/lasco_a.shtml). F-Secure.com. Retrieved 5 May 2008.
88. Ford-Long Wong, Frank Stajano, Jolyon Clulow (April 2005). "Repairing the Bluetooth pairing protocol" (http://web.archive.org/web/20070616082657/http://www.cl.cam.ac.uk/~fw242/publications/2005-WongStaClu-bluetooth.pdf) (PDF). University of Cambridge Computer Laboratory. Archived from the original (http://www.cl.cam.ac.uk/~fw242/publications/2005-WongStaClu-bluetooth.pdf) (PDF) on 16 June 2007. Retrieved 1 February 2007.
89. http://www.eng.tau.ac.il/~shakedy

90. "Avishai Wool - אבישי וול" (http://www.eng.tau.ac.il/~yash/). *tau.ac.il*. Retrieved 4 June 2015.
91. Yaniv Shaked, Avishai Wool (2 May 2005). "Cracking the Bluetooth PIN" (http://www.eng.tau.ac.il/~yash/shaked-wool-mobisys05/). School of Electrical Engineering Systems, Tel Aviv University. Retrieved 1 February 2007.
92. "Phone pirates in seek and steal mission" (http://web.archive.org/web/20070717035938/http://www.cambridge-news.co.uk/news/region_wide/2005/08/17/06967453-8002-45f8-b520-66b9bed6f29f.lpf). Cambridge Evening News. Archived from the original (http://www.cambridge-news.co.uk/news/region_wide/2005/08/17/06967453-8002-45f8-b520-66b9bed6f29f.lpf) on 17 July 2007. Retrieved 4 February 2008.
93. "Going Around with Bluetooth in Full Safety" (http://www.securenetwork.it/bluebag_brochure.pdf) (PDF). F-Secure. May 2006. Retrieved 4 February 2008.
94. Marsh, Jennifer. "Bluetooth Hacking – Understanding Risks" (https://blog.udemy.com/bluetooth-hacking/). Retrieved 26 April 2015.
95. Elaina Chai, Ben Deardorff, and Cathy Wu. "Hacking Bluetooth" (https://css.csail.mit.edu/6.858/2012/projects/echai-bendorff-cathywu.pdf) (PDF). Retrieved 26 April 2015.
96. M. Hietanen, T. Alanko (October 2005). "Occupational Exposure Related to Radiofrequency Fields from Wireless Communication Systems" (http://web.archive.org/web/20061006124651/http://www.ursi.org/Proceedings/ProcGA05/pdf/K03.7(01682).pdf) (PDF). *XXVIIIth General Assembly of URSI – Proceedings*. Union Radio-Scientifique Internationale. Archived from the original (http://www.ursi.org/Proceedings/ProcGA05/pdf/K03.7(01682).pdf) (PDF) on 6 October 2006. Retrieved 19 April 2007.
97. *USB 3.0* Radio Frequency Interference Impact on 2.4 GHz Wireless Devices* (http://www.usb.org/developers/whitepapers/327216.pdf) (PDF)
98. *A guide to resolving Bluetooth and USB 3.0 interference issues* (http://www.bluetoothandusb3.com)
99. "Bluetooth Innovation World Cup" (http://www.bluetooth.com/Bluetooth/Press/Bluetooth_World_Innovation_Cup.htm). Bluetooth.com. Retrieved 4 September 2010.
100. "Bluetooth Breakthrough Awards" (https://www.bluetooth.org/en-us/news-events/bluetooth-breakthrough-awards). *bluetooth.org*. Retrieved 4 June 2015.

External links

- Official website (http://www.bluetooth.org/)
- Specifications (https://www.bluetooth.org/en-us/specification/adopted-specifications) at Bluetooth SIG

Wikimedia Commons has media related to ***Bluetooth***.

Retrieved from "https://en.wikipedia.org/w/index.php?title=Bluetooth&oldid=681669535"

Categories: Channel access methods | Bluetooth | Mobile computers | Networking standards | Wireless | 1994 introductions | Dutch inventions | Swedish inventions

---