

Abdulaziz Asiry

Adel Alsihli

## Bluetooth

**Bluetooth** is an industrial specification for wireless personal area networks (PANs). Bluetooth provides a way to connect and exchange information between devices such as mobile phones, laptops, personal computers, printers, GPS receivers, digital cameras, and video game consoles over a secure, globally unlicensed short-range radio frequency. The Bluetooth specifications are developed and licensed by the Bluetooth Special Interest Group.

### Uses:

Bluetooth is a standard and communications protocol primarily designed for low power consumption, with a short range (power-class-dependent: 1 meter, 10 meters, 100 meters) based on low-cost transceiver microchips in each device.

Bluetooth enables these devices to communicate with each other when they are in range. The devices use a radio communications system, so they do not have to be in line of sight of each other, and can even be in other rooms, as long as the received transmission is powerful enough.

<b>Class</b>	<b>Maximum Permitted Power</b>	<b>Range</b>
<b>Class 1</b>	100 mW (20 dBm)	~100 meters
<b>Class 2</b>	2.5 mW (4 dBm)	~10 meters
<b>Class 3</b>	1 mW (0 dBm)	~1 meter

In most cases the effective range of class 2 devices is extended if they connect to a class 1 transceiver, compared to pure class 2 network. This is accomplished by the higher sensitivity and transmission power of Class 1 devices.

<b>Version</b>	<b>Data Rate</b>
<b>Version 1.2</b>	1 Mbit/s
<b>Version 2.0 + EDR</b>	3 Mbit/s
<b>WiMedia Alliance (proposed)</b>	53 - 480 Mbit/s

### List of applications

More prevalent applications of Bluetooth include:

- Wireless control of and communication between a mobile phone and a hands-free headset. This was one of the earliest applications to become popular.
- Wireless networking between PCs in a confined space and where little bandwidth is required.

## Computer requirements

A personal computer must have a Bluetooth adapter in order to be able to communicate with other Bluetooth devices (such as mobile phones, mice and keyboards). While some desktop computers and most recent laptops come with a built-in Bluetooth adapter, others will require an external one in the form of a dongle.

Unlike its predecessor, IrDA, which requires a separate adapter for each device, Bluetooth allows multiple devices to communicate with a computer over a single adapter.

## Specifications and features

The Bluetooth specification was developed in 1994 by Jaap Haartsen and Sven Mattisson, who were working for Ericsson Mobile Platforms in Lund, Sweden. The specification is based on frequency-hopping spread spectrum technology.

### Bluetooth 1.0 and 1.0B

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.

### Future of Bluetooth

- **Broadcast Channel:** enables Bluetooth information points. This will drive the adoption of Bluetooth into mobile phones, and enable advertising models based around users pulling information from the information points, and not based around the object push model that is used in a limited way today.
- **Topology Management:** enables the automatic configuration of the piconet topologies especially in scatternet situations that are becoming more common today. This should all be invisible to the users of the technology, while also making the technology just work.
- **Alternate MAC PHY:** enables the use of alternative MAC and PHY's for transporting Bluetooth profile data. The Bluetooth Radio will still be used for device discovery, initial connection and profile configuration, however when lots of data needs to be sent, the high speed alternate MAC PHY's will be used to transport the data. This means that the proven low power connection models of Bluetooth are used when the system is idle, and the low power per bit radios are used when lots of data needs to be sent.

## **High-speed Bluetooth**

On 28 March 2006, the Bluetooth Special Interest Group announced its selection of the WiMedia Alliance Multi-Band Orthogonal Frequency Division Multiplexing (MB-OFDM) version of UWB for integration with current Bluetooth wireless technology.

## **Ultra Low Power Bluetooth**

On June 12, 2007, Nokia and Bluetooth SIG announced that Wibree will be a part of the Bluetooth specification as an ultra low power Bluetooth technology. Expected use cases include watches displaying Caller ID information, sports sensors monitoring your heart rate during exercise, as well as medical devices. The Medical Devices Working Group is also creating a medical devices profile and associated protocols to enable this market.

# **Security**

## **Overview**

Bluetooth implements confidentiality, authentication and key derivation with custom algorithms based on the SAFER+ block cipher. In 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. 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 has been published by Andreas Becker.

## **Bluejacking**

Bluejacking allows phone users to send business cards anonymously using Bluetooth wireless technology. Bluejacking does NOT involve the removal or alteration of any data from the device. These business cards often have a clever or flirtatious message rather than the typical name and phone number.<sup>[citation needed]</sup> Bluejackers often look for the receiving phone to ping or the user to react. They then send another, more personal message to that device. Once again, in order to carry out a bluejacking, the sending and receiving devices must be within range of each other, which is typically 10 meters for most mobile devices. Devices that are set in non-discoverable mode are not susceptible to bluejacking. However, the Linux application Redfang claims to find non-discoverable Bluetooth devices.

## References:

[1] <http://www.answers.com/topic/bluetooth>

[2] WAP, Bluetooth, and 3G programming, 2202, 3rd, by Dr. K. V. K. K Prasad and others page: 129, 137, 139.

[3] Multimedia wireless networks: technologies standards, and Qos By Aura Ganz, September 18, 2003 Zvi Ganz, Kitti Wongthavarawat ch 8.

[4] Bluetooth technologies for short-range wireless application, by Pavin Bhagwat,IEEE Internet Computing, June 2001, pages: 96, 98 and 99.