RTIG

UK Real Time Information Group

Communications Briefing Paper: Bluetooth

RTIG Library Reference: ***RTIGT015-1.0***

15 July 2005

Price:

Foundation Members:	Free
Full Members:	Free
Associate Members:	£25
Non-members:	£25

List of contents

1 Bluetooth

1.1 Introduction

1.1.1 The Bluetooth Special Interest Group was formed in September 1998 by Ericsson, IBM, Intel, Nokia, Toshiba, 3Com, Lucent, Microsoft and Motorola and is a trade association comprised of telecommunications, computing, automotive, industrial automation and network industries that is driving the development of Bluetooth wireless technology, a low cost short-range wireless specification for connecting mobile devices and bringing them to market.

1.1.2 Bluetooth is a royalty-free, open specification, and is also called the IEEE 802.15.1 standard.

1.1.3 The first devices start to appear during 2000 with a slow start, but are now widespread across mobile phones, headsets, laptop computers, PDAs and small peripheral devices.

1.1.4 It is called Bluetooth after a Harald Blatand (English translation - Bluetooth) who was king of Denmark in the late 900s. He was known for his love of blueberries, hence his name. More importantly though he managed to unite parts of what are now Denmark, Sweden and Norway into a single kingdom. He left a large monument, the Jelling rune stone, in memory of his parents. He was killed in 986 during a battle with his son, Svend Forkbeard. Choosing this name for the standard indicates how important companies from the Nordic region are to the communications industry, even if it says little about the way the technology works!

1.2 Technical Detail

1.2.1 Bluetooth communicates on a frequency of 2.45 gigahertz, which has been set aside by international agreement for the use of industrial, scientific and medical devices (ISM).

1.2.2 In the United States and Europe, the frequency range is 2,400 to 2,483.5 MHz, with 79 1-MHz radio frequency (RF) channels. In practice, the range is 2,402 MHz to 2,480 MHz. In Japan, the frequency range is 2,472 to 2,497 MHz with 23 1-MHz RF channels

1.2.3 Each Transceiver has a unique 48 Bit Address.

1.2.4 There are two specifications, one for modules with a range of 10m, the second with a range of 100m in open space.

1.2.5 Most devices are the short range devices. and transmit very weak signals of a maximum of 1 milliwatt. (by comparison, the most powerful cell phones can transmit a signal of 3 watts). A a result of the low radio signal powers devices are very efficient and use little battery power.

1.2.6 This low power limits the range of a Bluetooth device to about 10 meters, cutting the chances of interference with other devices, but severely limiting range. Signals will pass through relatively radio transparent materials such as plasterboard walls etc.

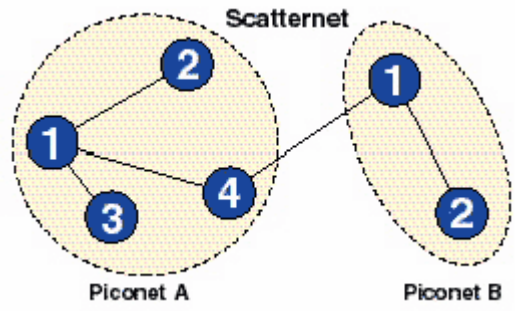
1.2.7 To assist with security and reduce interference Bluetooth uses spread-spectrum frequency hopping. There are 79 individual frequencies that devices use within the allocated spectum, randomly changing frequencies 1,600 times every second. In full duplex mode time division multiplexing is used.

1.2.8 Since every Bluetooth transmitter uses spread-spectrum transmitting automatically, it's unlikely that two transmitters will be on the same frequency at the same time. This same technique minimizes the risk that portable phones or baby monitors will disrupt Bluetooth devices, since any interference on a particular frequency will last only a tiny fraction of a second

1.2.9 When Bluetooth-capable devices come within range of one another they automatically initiate handshaking (also called discovery) to determine whether they have data to share or whether one needs to control the other.

1.2.10 Once the handshaking has completed conversation has occurred, the devices -- whether they're part of a computer system or an audio device - form a network. Bluetooth systems create a personal-area network (PAN), or piconet, that may fill a room or may encompass no more distance than that between the cell phone on a belt-clip and the headset on your head. Once a piconet is established, the members randomly hop frequencies in unison so they stay in touch with one another and avoid other piconets that may be operating in the same room.

1.2.11 Piconets can be linked by a common device to form a scatternet.



1.2.12 A piconet has a master and up to seven slaves. The master transmits in even time slots, slaves in odd time slots.

1.2.13 Most current devices, such as laptops, mobile phones, headsets etc only currently support piconets of two devices.

1.2.14 Devices are capable of operating in either half or full duplex mode or both if required.

1.2.15 The devices in a piconet share a common communication data channel. The channel has a total capacity of 1 megabit per second (Mbps). Headers and handshaking information consume about 20 percent of this capacity.

1.2.16 There are currently two supported types of data transfer between devices: SCO (synchronous connection oriented) and ACL (asynchronous connectionless).

1.2.17 Data rates of 400 kbps of data under SCO or 700 to 150 kbps of data as ACL are supported per piconet.

1.2.18 In a piconet, there can be up to three SCO links. To avoid timing and collision problems, the SCO links use reserved slots set up by the master.

- Masters can support up to three SCO links with one, two or three slaves.

- Slots not reserved for SCO links can be used for ACL links.
- One master and slave can have a single ACL link.
- ACL is either point-to-point (master to one slave) or broadcast to all the slaves.
- ACL slaves can only transmit when requested by the master.
- All data transfer is passed through the master.

1.3 Security

1.3.1 Supports unidirectional or mutual encryption based on a secret link key shared between two devices

1.3.2 Security Defined In 3 modes:

- Mode1- No Security
- Mode 2 - Service Level Security: Not Established Before Channel is Established
- Mode 3 - Link Level Security: Device Initiates Security Before Link is Setup

1.3.3 Devices and services can be set for different levels of security. Two trust levels are supported for devices

- Trusted Device: Fixed Relationship and Unrestricted Access to All Services
- Untrusted: No Permanent relationship and Restricted Services

1.3.4 There are 3 Levels of Service Access supported:

- Require Authorization and Authentication
- Require Authentication Only
- Default Security for Legacy Applications

1.3.5 Most devices in common use such as mobile phones linking to headsets or laptops require authorisation (yes, this device can connect), authentication (normally pin number) and as a result are trusted (once connected no further authorisation required to access a service – e.g. once connected the laptop can dial a number on the mobile phone without further permission having to be given).

1.3.6 The Bluetooth network is susceptible to denial of service attacks by any device constantly requesting a response from another device, if the device under attack is the master then this stops the whole network.

1.4 RTIG Uses

1.4.1 Bluetooth could be used on vehicle for short range low bandwidth communication between multiple devices.

1.4.2 Communications from an onboard computer to internal displays or audio functions are possible uses

1.4.3 Like many short range radio systems that use high frequencies the metallic superstructure of a vehicle is likely to cause problems, so testing would be advised before specifying.

1.5 Related RTIG Strategy Information

1.5.1 Currently there is no RTIG Strategy for BlueTooth

1.6 Conclusion

1.6.1 Bluetooth has the potential to be used on vehicle in applications that are not time or safety critical.

1.7 Additional Information and Links

1.7.1.1	Bluetooth commercial information site	http://www.bluetooth.com/
1.7.1.2	Bluetooth SIG site	https://www.bluetooth.org/
1.7.1.3	The Wireless Directory	http://www.thewirelessdirectory.com/