2011

Bluetooth

[A SHORT REPORT ON BLUETOOTH TECHNOLOGY]

By Ram Kumar Bhandari

Bluetooth Technology

A Technical Report

1. Introduction

Bluetooth is a short-ranged wire-less communication technology implementing the radio waves for the communication between the fixed or portable devices without the need of cable wire while maintaining the high level of security. Unlike the **infrareds**, Bluetooth doesn’t need the ‘line of sight’ for transmission. Hence it is much more flexible. Originally it was considered as the wireless alternative for RS-232 standard cable transmission.

The name ‘Bluetooth’ was named honoring the king ***Harald I Bluetooth*** who ruled over the united Denmark and Norway by uniting the Danish tribes into a single kingdom during the 10th century. Similarly the main objective of Bluetooth as protocol is to unify all the data transmission technology among the mobile devices and the static electronic devices without the need of any cable medium. The symbol of Bluetooth is design in such a way that it contains both the initials of the king Harald Bluetooth i.e. ᚼ which means H (for Harald) and ᛒ which means B (for Bluetooth).

Bluetooth Symbol

Logo of Bluetooth

2. How Bluetooth Technology Works

The Bluetooth core architecture consists of Radio Frequency (RF) transceiver, baseband and protocol stack. The system enables the connection between the different varieties of devices. The Bluetooth radio (physical layer) operates in the unlicensed ISM (Industrial, Scientific and Medical) band at the 2.4GHz. The system operates on the radio technology called *frequency-hopping spread spectrum*. In this technology the data being sent are chopped up and chunks of it are transmitted up to 79 frequencies. This helps in overcoming the interference and fading of the signal and uses the binary frequency modulation in order to minimize the transceiver complexities. In its basic mode, it supports the bit rate of 1 megabits per second (1Mbps) and with Enhanced Data Rate (EDR) mode it supports the bit rate of 2 to 3 Mbps.

2.1 *General Architecture*

2.1.1 Piconet/Scatternet

The Bluetooth network is termed as **Piconet.** During the typical connection, number of devices shares the common radio channel. The device that initiates the connection or synchronization is called the **master** and all the other devices in the Piconet are called **slaves**. Bluetooth implies the ad hoc networking i.e. the network will be established only when the data has to be transmitted and dismantle after the task has been accomplished.

A master device can have connections up to seven slaves simultaneously. But this will cause to reduce the data transmission rate. Also one device can have connection with other more Piconet. This type of multi-connection with different piconets is called Scatternet. However, a device can only master to one Piconet at a time. Functions such as hold, park or sniff mode is needed for a device to participate in the Scatternet.

Note: The point to multipoint connection depends on the implementation as most of the current devices support only piconets.

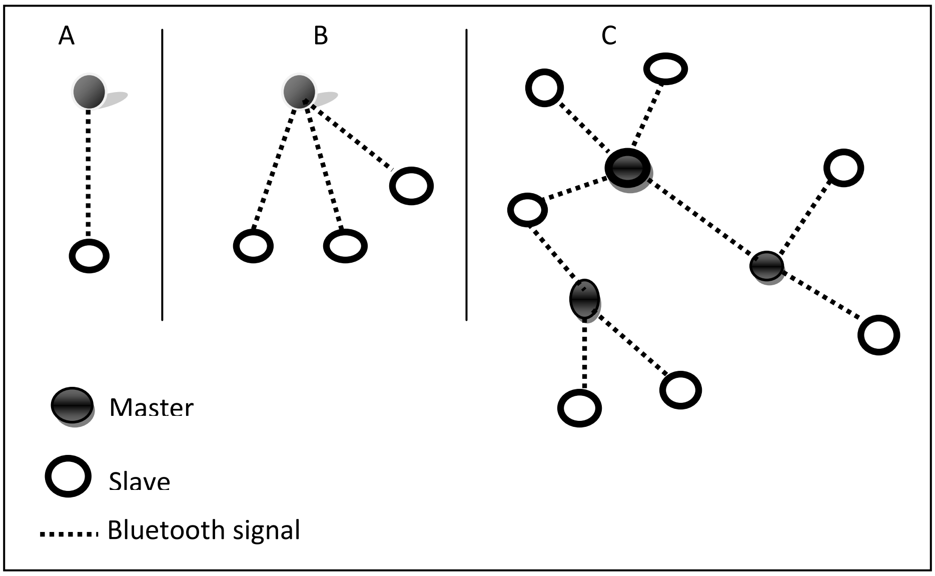


Fig: Piconet and Scatternet

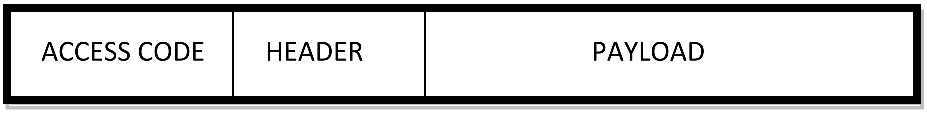
A: Point to point connection between two devices (a master and a slave)

B: Point to multipoint connection between a master and three slave devices.

C: Scenario showing the Scatternet containing three piconets.

2.1.2 Packets

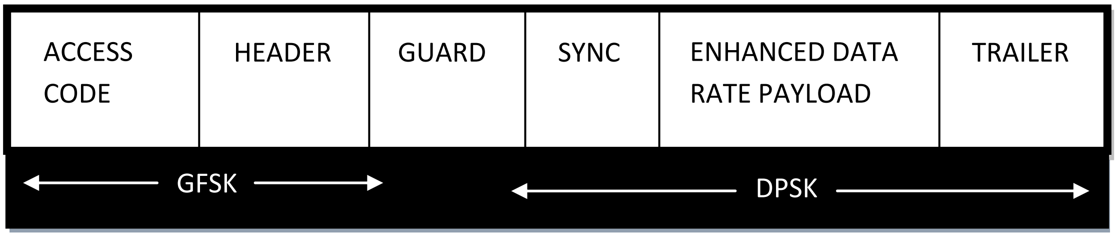
In Bluetooth technology, data are sent as packets over the air medium. The symbol rate for all type of mode is 1 Ms/s. The data rate for basic mode is 1 mbps.



ACCESS CODE	HEADER	PAYLOAD

Standard packet format for Basic rate

Enhanced Data Rate (EDR) has two modulation modes one is primary modulation mode which provides the data rate of 2Mbps and the other one is secondary modulation mode which provides the data rate of 3Mbs.



ACCESS CODE	HEADER	GUARD	SYNC	ENHANCED DATA RATE PAYLOAD	TRAILER

Standard packet format for Enhanced Data Rate

2.1.3 Bluetooth clock

For the synchronization with the other devices, every *Bluetooth* device has a native clock derived from the system clock. Such type of Bluetooth clock is temporary and is only added to for mutual synchronization.

2.1.4 Addressing of Bluetooth devices

Provided by IEEE Registration Authority, each Bluetooth device is given a unique 48-bit Bluetooth device address (BD_ADDR).

2.1.5 Access Codes

All transmission in a Bluetooth System begins with an access code. There are three defined access codes.

- Device access code
- Inquiry access code
- Channel access code

2.1.6 Frequency Hopping

As discussed earlier, Bluetooth implies the frequency hopping technique for transmission of packets which means that different frequencies are used to transmit the packets. Hopping is decided by the clock of the master device and the Bluetooth specification addresses. The fundamental hopping model is to divide the ISM band to 79 different frequencies. This hopping pattern may be adapted to prohibit the part of frequency that may be in use by other interfering devices. Such type of frequency hopping techniques is called **Adaptive Frequency Hopping (AFH).** This adaptive hopping technique helps in the co-existence of other non-hopping static ISM devices with the Bluetooth devices.

A good protection from the interference can be obtained with a fast hop rate (1600 hops per second). The other advantage is that the packets are of short length. So whenever there is blocking or interference in the frequency, the packets can be resent in any other frequency provided by the frequency scheme of the master.

2.1.7 Time slots and Full Duplex Transmission of the Packets

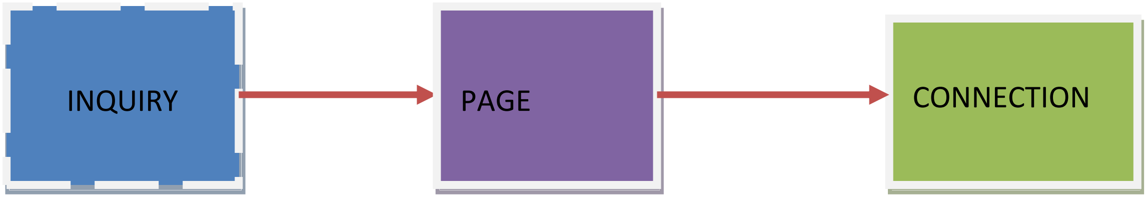
The physical channel is sub-divided into many units on the basis of time known as time slots. For the transmission of the data between the Bluetooth enabled devices, packets are positioned into these time slots. A single packet may be assigned a number of time slots if needed. The Bluetooth technology provides the full duplex transmission by implying the time-division duplex (TDD) scheme.

2.2 *Establishment of Connection and Inquiry*

To initialize the connection, the device sends the **page message.** An inquiry message is essential before paging if the address of the recipient is not clear. Initially all units are in **standby** mode before the connection is set up. While in standby mode, the unit wakes up in every 1.28 seconds to listen to page or inquiry messages. There are 32 defined hop frequencies for the page message of which one frequency is listened to by the unit each times it wakes up.

The 32 different frequencies are used by the page message. At first the page message is sent for 128 times through the first 16 frequencies. When there is no response, the master sends the page message on the remaining 16 frequencies again for 128 times. The maximum connection time is considered to be of 2.56 seconds, i.e. 1.28 seconds for each connection attempt.

The inquiry process helps the master to know the slave’s Bluetooth address and system clock which is needed to calculate the access code properly and manage the wake up sequence phase. For this process, the master sends the inquiry access code and other devices respond to it by sending back their identity i.e. Bluetooth access code and system clock.



A general process of connection

There are several modes of operations in which the units can be in their connection state.

- Active mode

  When the Bluetooth units are actively participating on the channel, they are said to be in active mode.

- Sniff mode

  In this mode, the master can only start the transmission in the specified time slots.

- Hold mode

  The Asynchronous Connectionless Link can be put into hold while still at the connection state. The slave can do scanning, inquiring, paging or attending the other piconets.

- Park mode

  Whenever a slave does not need to actively participate in the piconet but wants to remain synchronized with the channel, it gives up its active member address and enters the park mode.

3. Bluetooth profiles

On the basis of the nature of the Bluetooth application, the Bluetooth Special Interest Group (SIG) has number of models profile for the usage of Bluetooth technology in a device. In other words, it is a wireless specification for the device that communicates using Bluetooth technology. To provide the services based on the Bluetooth technology a device must incorporate the terms of Bluetooth profiles for the desired services.

3.1 *The Four General profiles in the Bluetooth Specification v1.1*

3.1.1 General Access Profile

This profile defines the general aspects of the Bluetooth devices and the procedures of the link management while connecting the Bluetooth devices. In addition to this it also includes the common formats required for the user interface on the device.

3.1.2 Service Discovery Application Profile

It defines the procedure for an application of a device to discover the services in the other Bluetooth device.

3.1.3 Serial Port Profile

It defines the requirements for a Bluetooth device which is essential for setting up the serial cable connections between two peer devices using RFCOMM.

3.1.4 Generic Object Exchange Profile

It defines the procedures that will be needed for the applications that exchange objects for example the situation like file transfer, synchronization etc.

Besides these four general profiles there are other additional profiles for the smooth operations for the Bluetooth technology incorporate devices.

- Advanced Audio Distribution Profile (A2DP)
- Audio/Video Remote Control Profile (AVRCP)
- Basic Imaging Profile (BIP)
- Basic Printing Profile (BPP)
- Common ISDN Access Profile (CIP)
- Cordless Telephony Profile (CTP)
- Device ID Profile (DID)
- Dial-up Networking Profile (DUN)
- Fax Profile (FAX)
- File Transfer Profile (FTP)
- Generic Audio/Video Distribution Profile (GAVDP)
- Generic Access Profile (GAP)
- Generic Object Exchange Profile (GOEP)
- Hard Copy Cable Replacement Profile (HCRP)

- Hands-Free Profile (HFP)
- Human Interface Device Profile (HID)
- Headset Profile (HSP)
- Intercom Profile (ICP)
- LAN Access Profile (LAP)
- Object Push Profile (OPP)
- Personal Area Networking Profile (PAN)
- Phone Book Access Profile (PBAP, PBA)
- Serial Port Profile (SPP)
- Service Discovery Application Profile (SDAP)
- SIM Access Profile (SAP, SIM)
- Synchronization Profile (SYNCH)
- Video Distribution Profile (VDP)
- Wireless Application Protocol Bearer (WAPB)

4. Bluetooth protocols

In order to operates smoothly between different profiles, protocols acts as the guidance. Every profile uses more or less the part of the protocols. There core protocols defined by the Bluetooth SIG and the additional protocols adopted from the other standard organizations.

4.1 *Bluetooth core protocols*

Baseband and link control

These together enables the physical connections between the Bluetooth units via Radio Frequency and are responsible for the synchronizing the clocks and transmission hopping frequency.

Audio

It is directly routed from and to baseband. So the audio data can be transmitted between two Bluetooth enabled devices just by opening audio link.

Link Manager Protocol (LMP)

It is responsible for the link set up including the encryption authentication and the controls of the packets between the two Bluetooth devices.

Logical Link Control and Adaptation Protocol (L2CAP)

It is responsible of segmentation, multiplexing and reassembly of the packets.

Service Discovery Protocol (SDP)

It deals with the discovery of the services, information and the features of the other devices that supports the same service.

5. Bluetooth Security

When there is the transfer of data from one node to other node there is always the issue of security. The wireless technology of communication is more vulnerable to the security risk. Like other wireless technology Bluetooth is not isolated from the security risk. However the developers using the Bluetooth technology have several options for implementing security in their products. There are three modes of security between the two Bluetooth devices.

- Security Mode 1: non-secure
- Security Mode 2: service level enforced security
- Security Mode 3: link level enforced security

5.1 Bluejacking

Sending the clever and flirtatious business cards without any typical name and phone numbers by using the Bluetooth is called **bluejacking.** This is just like the email spam. For bluejacking the distance should be within 10 meters. Devices set to no-discoverable mode are not susceptible to the bluejacking.

5.2 Bluebugging

Getting the unauthorized access to the phone without allowing the user and controlling its command using Bluetooth is called bluebugging. The hackers can send or receive the text messages, set up a call, read and write phone contacts and also take control over the phone conversation.

6. Applications of Bluetooth Technology

On the basis of the power consumption, data rate and the range of transmission, there are three classes of Bluetooth devices.

Class	Maximum Permitted Power mW (dBm)	Appx. range
1	100mW (20dBm)	˜100 meters
2	2.5mW (4dBm)	˜10 meters
3	1mW (0dBm)	˜1 meters

List of applications

- Hands free wireless communication in mobile phone using the Bluetooth technology.
- Small area Network with limited bandwidth between the PCs.
- Wireless communication between the parts of the computer. For e.g. keyboard, mouse and printer.
- In the test equipment like bar code reader, scanner, traffic controller device etc.
- Applications transfer in mobile devices.
- In gaming consoles like playstations and gameboy.

References

Internet reference

1. http://www.bluetooth.com/Bluetooth/Technology/Works/Overview_of_Operation.htm

2. http://en.wikipedia.org/wiki/Bluetooth

3. http://www.bluetooth.com/NR/exeres/2F0D2E9A-295B-4D9E-ABDA-8E33BFA2E399,frameless.htm?NRMODE=Published