Bluetooth, Seamless Connectivity

Author: Punit Ganshani
Email Address: punit@ganshani.com
Downloaded from http://www.ganshani.com
Published In: Mag 'IC 2004, Nirma University

Technology has always spread its tentacles wide in each and every direction, may it be the biological sciences or wireless communication. And today a broad pillar of seamless connectivity widens the horizons of vision. One such technology is Bluetooth!

Bluetooth is a specification for a **radio solution** that is small form-factor, low-cost, and low power, that provides ***seamless wireless connectivity*** between notebook computers, cellular phones and other portable handheld devices.

The Cry for Blue Tooth!

(What was the *need* to develop Blue Tooth?)

Bluetooth technology was developed to create a **short-range wireless voice** and data link between a broad range of devices such as PCs, notebook computers, handhelds and PDAs, Smart Phones, mobile phones and digital cameras.

Consistent with its aim of operating in even the **smallest battery-powered devices**, the Bluetooth specification calls for a small form factor, low power consumption and low cost.

The range and speed of the technology were kept intentionally low so as to ensure maximum battery life and **minimum incremental cost** for devices incorporating the technology.

At its heart, Bluetooth is about creating a ***Wireless* Personal Area Network (WPAN)** consisting of all the Bluetooth-enabled electronic devices immediately surrounding a user, wherever that user may be located.

How it pulled the skin!

(Benefits of Bluetooth v/s other technologies)

Through LAN:

With the advancement of technology and ideas such as IEEE 802.11 blooming up, a user with a notebook computer can move from place-to-place within a building or campus and maintains connection to the LAN, via an access point, at each stop.

This portability can even extend outside the bounds of the office to public areas such as airports, hotels and coffee shops.

In all cases, the user expects to be able to use her computer just as she would at the office – to connect to other computers on the LAN, such as servers, to connect to peripherals on the LAN, such as printers and to access the Internet.

Through WPAN:
(Or PAN)

Bluetooth, on the other hand, supports a much wider variety of usage scenarios, including:

- Device *inter operability*

  The wireless technology gives interconnection of multiple Bluetooth-enabled devices, elimating the need for cables to connect the devices. This is not possible in LAN!

  PC connected wirelessly to all of its peripheral devices which eliminates the need of cables and space to accommodate it.

- Peer-to-peer collaboration between multiple PDAs and/or notebooks

  WPAN can accomodate up to 8 Bluetooth-enabled devices simultaneously to allow exchange of data, voice, or any other objects.

- Notebook and PDA *internet access* via mobile phone

  It opens up a new gate to access Internet through notebook computers, PDAs and mobile phones. In fact emailing, chatting, downloading all can be doped in a small palm sized-device.

- Direct Network Access

  Bluetooth access points (AP) can be used to allow Bluetooth-enabled devices that are in range of the AP to access the Internet or an intranet directly.

  This AP is physically connected to an Ethernet using modem (in case of public location) or cable. Thus multiple devices can simultaneously use the same AP to connect to a LAN or the Internet.

Inside Outs of Bluetooth!

Protocol:

All of the parties in an electronic discussion need to know what the bits mean and whether the message they receive is the same message that was sent. In most cases, this means developing a language of commands and responses known as a **protocol**.

Some types of products have a standard protocol used by virtually all companies so that the commands for one product will tend to have the same effect on another. Modems fall into this category.

Other product types each speak their own language, which means that commands intended for one specific product will seem *gibberish* if received by another. Printers are like this, with multiple standards like PCL and PostScript

There are already a couple of ways to get around using wires.

1. Using Infrared rays
2. Cable Synchronization

Infrared Rays

Infrared refers to light waves of a lower frequency than human eyes can receive and interpret. Infrared is used in most television remote control systems, and with a standard called IrDA (Infrared Data Association) it's used to connect some computers with peripheral devices. For most of these computer and entertainment purposes, infrared is used in a digital mode -- the signal is pulsed on and off very quickly to send data from one point to another.

Infrared communications are fairly reliable and don't cost very much to build into a device, but there are a couple of drawbacks.

- **Infrared is a "line of sight" technology.**
  You have to point the remote control at the television to make things happen.

- **The second drawback is that infrared is almost always a "one to one" technology.**
  You can send data between your desktop computer and your laptop computer, but not your laptop computer and your PDA at the same time.

These two qualities of infrared are actually advantageous in some regards. Because infrared transmitters and receivers have to be lined up with each other, interference between devices is uncommon. The one-to-one nature of infrared communications is useful in that you can make sure a message goes only to the intended recipient, even in a room full of infrared receivers.

Cable Synchronizing

If you have a Palm Pilot, a Windows CE device or a Pocket PC, you know about synchronizing data. In synchronizing, you attach the PDA to your computer (usually with a cable), press a button and make sure that the data on the PDA and the data on the computer match. It's a technique that makes the PDA a valuable tool for many people, but synchronizing the PDA with the computer and making sure you have the correct cable or cradle to connect the two can be a real hassle.

The Solution!

Bluetooth is intended to get around the problems that come with both infrared and cable synchronizing systems. The hardware vendors like Siemens, Motorola, Ericsson and many more have developed a specification for a ***very small radio module*** to be built into computer, telephone and entertainment equipment.

From the user's point of view, there are three important features to Bluetooth:

- **It's wireless.**
  There are no cables needed to empower the data transfer.
- **It's inexpensive.**
  It's the least expensive device giving maximum utility with great speed.
- **You don't have to think about it.**
  Bluetooth doesn't require you to do anything special to make it work. The devices find one another and strike up a conversation without any user input at all.

How it Works!

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

A number of devices including Baby monitors, garage-door openers, cordless phones, mobiles that you may already use take advantage of this same radio-frequency band.

Making sure that Bluetooth and these other devices don't interfere with one another has been a crucial part of the design process.

One of the ways Bluetooth devices avoid interfering with other systems is by sending out very weak signals of 1 milliwatt, the maximum of which can reach up to a signal of 3 watts. And as the signal wattage increases, so does the range of a Bluetooth device increase. The average range of a low power limit Bluetooth device is 10 meters which discards the idea of interferance between your computer system and your portable telephone or television.

The Cordless Phone – Bluetooth Speaks!

Let's say we've got a modern living room with an entertainment system with a stereo, a DVD player, a satellite TV receiver and a television; there's a cordless telephone and a personal computer.

Let's assume that each of these systems uses Bluetooth, and each forms its own piconet to talk between main unit and peripheral.

> The cordless telephone has one Bluetooth transmitter in the base and another in the handset.
>
> The manufacturer has programmed each unit with **an address** that falls into a range of addresses it has established for a particular type of device.
>
> When the base is first turned on, it **sends radio signals** asking for a response from any units with an address in a particular range.
>
> Since the **handset** has an address in the range, **it responds**, and a tiny network is formed.
>
> Now, even if one of these devices should receive a signal from another system, it will ignore it since it's not from within the network.

The computer and entertainment systems go through similar routines, establishing networks among addresses in ranges established by manufacturers. Once the networks are established, the systems begin talking among themselves.

Now the living room has three separate networks established, each one made up of devices that know the address of transmitters it should listen to and the address of receivers it should talk to.

Since each network is changing the frequency of its operation thousands of times a second, it's unlikely that any two networks will be on the same frequency at the same time.

If it turns out that they are, then the resulting confusion will only cover a tiny fraction of a second, and software designed to correct for such errors weeds out the confusing information and gets on with the network's business.

Most of the time, a network or communications method either works in one direction at a time, called **half-duplex communication**, or in both directions simultaneously, called **full-duplex communication**.

A speakerphone that lets you either listen or talk, but not both, is an example of half-duplex communication, while a regular telephone handset is a full-duplex device.

Bluetooth can send data at more than 64,000 bits per second in a full-duplex link -- a rate high enough to support several human voice conversations.

Spread Spectrum Frequency Hopping

It may be the case that there may be many Bluetooth devices in a room and with many different Bluetooth devices in a room, you might think they'd interfere with one another.

But it's unlikely that several devices will be on the same frequency at the same time, because Bluetooth uses a technique called **spread-spectrum frequency hopping**.

A device will use about 79 individual randomly chosen frequencies within a designated range changing from one to another on a regular basis.

In the case of Bluetooth, the transmitters change frequencies ***1,600 times every second***, meaning that more devices can make full use of a limited slice of the radio spectrum.

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 will disrupt Bluetooth devices, as any interference on a particular frequency will last only a tiny fraction of a second (1/1600 second).

THE INGREDIENTS...!

A typical implementation of Bluetooth includes the RF, baseband, HCI interface, and host stack software.

RF

- Bluetooth operates in the license-free 2.4-2.4835GHz ISM band by frequency hopping at a rate of 1600 hops/s within 79 1MHz channels. Japan, France and Spain have a smaller band but these issues are being resolved.

- Bluetooth supports 10-meter range and 1Mbps rate and a 100-meter range with improved transmission power and receiving sensitivity.

  There are three classes of transmit power for Bluetooth:

- Class 3 at 0 dBm (1 mW),
- Class 2 at 4 dBm (2.5 mW) and
- Class 1 at 20 dBm (100 mW).

BASEBAND

A wireless PAN, more often referred to as a Piconet, provides the cable replacement for connectivity among various devices such as a notebook PC to a cell phone, a cell phone to a headset, a PDA to a notebook, a cell phone to PSTN, a notebook/PDA to Internet and LAN, and other ad-hoc networking applications.

Bluetooth communications in a Piconet is based on a **master/slave relationship**, where one unit serves as a master and the rest serve as slaves.

The access is synchronized via **master identity** whose Bluetooth address determines the frequency hopping sequence and system clock determines the phase.

Each slave will **follow the hop sequence** and **add an offset** to its clock to follow the master. Each Bluetooth packet has a fixed format that starts with a **72-bit access code** that is based on the master identity and is unique to the Piconet.

Then a **54-bit header** containing error correction, retransmission and control information follows. Finally, a payload of 0 to 2745 bits ends a packet.

To provide full duplex operation, it uses **Time-Division Duplex (TDD)** scheme to divide the channel into a number of 625 us time slots with a 220 us TDD guard time. Master and slave alternatively transmit.

The master shall transmit in even-numbered time slot only while the slave shall start its transmission in odd numbered time slots.

The time slots are numbered based on the Bluetooth clock of the piconet master.
The numbering ranges from 0 to (227 –1) and is cyclic with a cycle length of 227.

Bluetooth protocol is a combination of circuit and packet switching. Reservation of slots can be made for **Synchronous Connection-Oriented (SCO)** links for circuit switching audio application.

It also supports an **Asynchronous Connection-Less (ACL)** link for packet data switching, based on a polling access scheme. Typical packet size is one slot but can span multiple slots as defined in the specification.

The master controls all traffic in a Piconet. It allocates capacity for SCO links and handles the polling scheme for ACL links among slaves. Slave may only send in the slave-to-master slot after being addressed in the preceding master-to-slave

slot.

Bluetooth supports authentication and encryption, combining with frequency hopping, to give the technology the robust security.

HOST CONTROLLER INTERFACE (HCI**) INTERFACE**

The Host Controller Interface, HCI, provides a uniform interface method for accessing the Bluetooth hardware capabilities.

It contains a command interface to the Basedband controller and link manager and access to hardware status. Typical connection w/standard interfaces include USB, UART, and PCMCIA.

HOST PROTOCOL STACK

The Link Manager Protocol, LMP, is responsible for link setup between Bluetooth devices. It manages master/slave switch, lower power mode (hold, sniff, park), clock offset, and packet size negotiation.

It handles generation, exchange and control of link and encryption key for authentication and encryption.

Earlier:
RFCOMM is a serial port emulation protocol
It emulates RS232 control and data signal over the Bluetooth baseband.

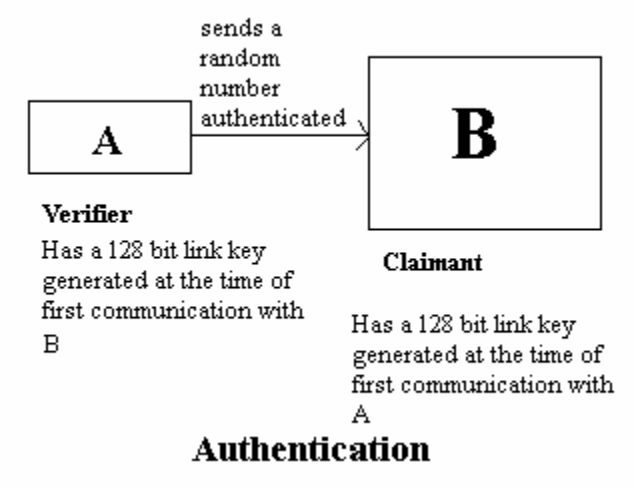
Now:
***PPP (point-to-point protocol)** is a widely deployed protocol to allow access to Internet. PPP provides authentication, encryption, data compression and multi-protocol support.*

PPP over RFCOMM has been chosen as means of providing LAN access for Bluetooth devices because of the **large installed base of devices equipped with PPP client software**.

SECURITY!

(The need of Encryption)

Used when two devices communicate (connected through Bluetooth Technology) for the first time., it requires that a PIN of 4 to 16 digits be entered into both devices. The result is the creation of a 128-bit link key that is never transmitted on air.



Device A (verifier) sends device B (claimant) a random number to be authenticated.

If devices do not share a secret 128-bit link key, the claimant will be unable to respond properly. No user intervention is required in this step. If a shared link key is successfully verified, an encryption key of up to 128 bits can be generated. The encryption key will be different for each session and is
not transmitted over the air.

If enabled, encryption is automated using a 40-bit or 128-bit WEP key that is shared by all users on the WLAN. Some vendors offer proprietary dynamic WEP session key capability.

When security procedures are fully implemented, the effort required to violate the security of these networks is substantial, but within the capabilities of a determined hacker.