Advances in Engineering Science
Sect. C (2), April-June 2008, PP 25-30

BLUETOOTH: THE BUDDY COMMUNICATION TECHNOLOGY

Abdul Muqeet*

Lecturer, Tom Patrick Institute of Computer & IT, Dr. Rafiq Zakaria Campus,
Rouza Bagh, Aurangabad 431 001 (M.S.)

1.0 INTRODUCTION

The term Bluetooth refers to an open specification for a technology to enable short-range wireless voice and data communications anywhere in the world. Bluetooth is the name of a new short-range, low bandwidth wireless communication technology. Many people have heard of Bluetooth but few have experienced it hands-on. It is designed to be small enough to include in portable devices such as mobile phones and personal digital assistants (PDAs) but many usage scenarios also involve laptops, desktops, printers, cameras and other types of devices. Several consumer accessories featuring Bluetooth support are due to reach markets. As the rate of adoption grows so will the interest for including Bluetooth support in programs across many different hardware and software platforms. At present such efforts are initially hindered by a steep learning curve. This is the result of rapid pace of change in the field, which has led to several poorly documented protocol stacks.

Part of the design requirements for Bluetooth was to make it small enough to use in embedded devices. A complication arises because devices such as mobile phones and PDAs typically have limited processing capability yet increasingly complex capabilities are demanded from them. Rather than develop specialized hardware, field programmable gate arrays (FPGAs) offer the possibility for reconfiguration depending on the task at hand. They have successfully been used to accelerate a variety of applications such as multimedia processing and compression. As the target markets of Bluetooth and FPGAs overlap, a marriage between the two technologies should be inevitable.

The logo for Bluetooth is based on Runes surrounding the legend of Harald Bluetooth. Bluetooth the technology is based on communications central to man's own personal space. Fundamentally Bluetooth operates within the Industrial, Scientific and Medical (ISM) band at 2.4 GHz. It is a short-range wireless communication standard defined as cable replacement for a Personal Area Network (PAN).

The Bluetooth brand is now recognized worldwide on products with short range wireless communication capabilities. The brand is a label that is not a single company technology but is shared by many members of the Bluetooth SIG. The brand is applied to devices implementing the Bluetooth technology, even if it says little about the way the technology works.

Figure 1 : Bluetooth Logo

A cable replacement standard has been defined because cables limit mobility of the consumer; they are cumbersome to carry around, are easily lost or broken. Often connectors are prone to difficult to diagnose failures; or are proprietary. To counteract these limitations Bluetooth is designed to be light and portable. It can be embedded to take the riggers of physical knocks and shocks. It includes standards and protocols to make it mobile, robust, reliable and not limited to one manufacturer.

The operating band also fits the goals of Bluetooth, imposing requirements as a cable replacement. The cost needs to be comparable with cable. Reductions

*muqeetwaheed@gmail.com

can be achieved by operating in the licence free 2.4 GHz ISM band, keeping backward compatibility wherever possible lowers the cost of ownership by avoiding upgrades and having a relaxed radio specification enables single chip integrated circuit solutions. It also needs to be as reliable and resilient as cable and cope with errors and degradation caused by interference. For mobile devices it must be compact, lightweight, low power and easy to use.

2.0 FREQUENCY HOPPING

We have addressed the reasons for the Bluetooth without delving into the 'nuts and bolts' of the technology to discover how it operates. For the majority of countries the ISM band used by Bluetooth is available from 2.40-2.4835 GHz, although some countries impose restrictions. In this band Bluetooth uses Frequency Hopping Spread Spectrum (FHSS) techniques in order to improve its immunity from interference.

In unrestricted countries the radios hop in pseudo random sequences around all available channels, this equates to 79 RF channels with a channel spacing of 1 MHz. Starting at a base frequency of 2402 MHz then the frequency of the channels, f, can be expressed as:

$$f = 2402 + n \text{ MHz}$$

where, n, is the channel number with an integer value in the range of 0 to 78. In restricted countries a limited frequency hopping schemes with just 23 channels is used and is catered for in the Bluetooth specification. Both hopping schemes have a 1 MHz channel spacing making it possible to design a simple radio interface whereby the baseband only has to specify a channel number and the radio multiplies this up to the appropriate frequency offset.

In this FHSS scheme there are 1600 hops per second, which is a hop every 625 µs. Part of this hop timing is taken up by the guard time of 220 µs allowing the synthesizer time to settle. The frequency hopping implements time division multiplexing as shown in Figure 2. The basis of the scheme has the Master device transmitting in the first 625 us slot, k, and here the Slave receives. In the next slot k = 1 the Slave is permitted to transmit and the master listens.

The radio must be able to retune and stabilise on a new frequency within tight time constraints. This is

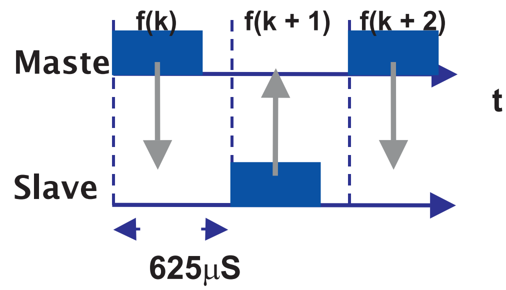

Figure 2 : Frequency Hopping, master and slave interact on corresponding slots

pushed further when establishing a connection; the hop rate can be shortened to every 312.5 us. As the radios are constantly hopping to different radio channels, this ensures that packets affected by interference on one channel can be retransmitted on a different frequency channel. To further enhance resilience both ARQ (Automatic Repeat reQuest) and FEC (Forward Error Correction) form part of the specification.

One drawback with the normal hop sequence is the time taken for production testing. Bluetooth ensures adequate frequency coverage with a test sequence allowing the radios to be tested at a faster rate.

2.1 The Protocol Stack

The Bluetooth specifications define not only a radio system but cover the underlying structure. The Core Specification contains a software protocol stack similar to the more familiar Open Systems Interconnect (OSI) standard reference model for communication protocol stacks. It permits applications to discover devices, the services they offer and permission to use these services. The stack is a sequence of layers with features crossing single or multiple layered boundaries. Figure 4 outlines the stack with each block corresponding to a Core Specification chapter. Other remaining chapters relate to compliance requirements, test modes and test control interface.

If we ascend the stack, we first come across the fundamental component, the radio. The radio modulates and demodulates data for transmitting and receiving over the air. The operating band of the radio is divided into 1 MHz spaced channels with a chosen modulation scheme of Gaussian Frequency Shift Keying (GFSK). Each channel is specified to signal at 1mega symbols per second, equivalent to 1 Mb/s. Above the radio are the Baseband and Link Controller, they are responsible for controlling the physical links via the radio, assembling the packets and controlling the frequency hopping.

Progressing through the layers, the Link Manager (LM) controls and configures links to other devices. The Host Controller Interface (HCI) is above the LM layer and is probably one of the most important layers to consider as a designer. It handles communication between host and the module. The standard defines the HCI command packets that the host uses to control the module, the event packets used by the host to inform lower protocol layers of changes, the data packets for voice and data traffic between host and module and the transport layer used by the HCI packets. The transport layer can be USB (H2), RS232 (H3), UART (4) or a robust proprietary standard such as BCSP (BlueCore Serial Protocol).

The Logical Link Control and Adaptation (L2CAP) is a multiplexor, adapting data from higher layers and converting between different packet sizes. The next 4 layers could be loosely grouped as communication interfaces. These are RFCOMM (Radio Frequency COMMunication port) which provides an RS232 like serial interface. Wireless Application Protocol (WAP) and OBject EXchange (OBEX) are responsible for providing interfaces to other Communications Protocols. The final member of this rough grouping is the Telephony Control protocol Specification (TCS) providing telephony services. Service Discovery Protocol (SDP) lets devices discover the services available on another Bluetooth device.

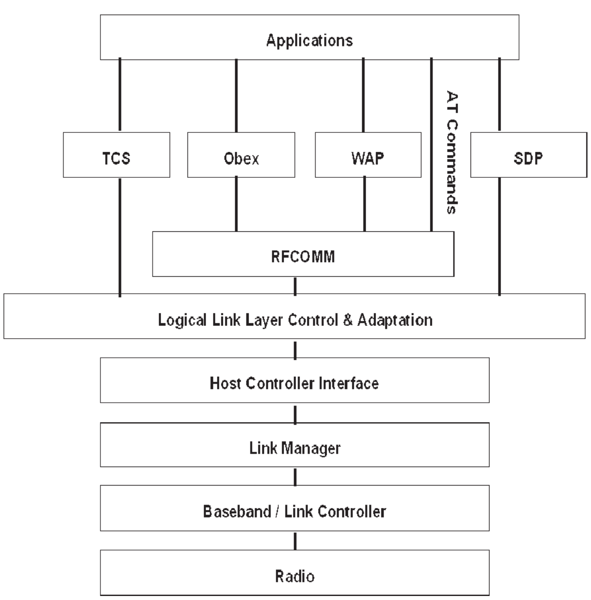

Figure 4 : The Bluetooth Protocol Stack

The application layer is probably obvious, but the standard provides Profiles laying out rules for how applications use the protocol stack, ensuring interoperability at application level.

2.1.1 Master and Slave Operation

Bluetooth devices exist in small ad-hoc network configuration with the ability to operate as either master or the slave; the specification also allows a mechanism for master and slave to switch their roles. The configurations can be single point, which is the simplest configuration with one master and one slave. Multipoint, called a Piconet, based on up to 7 slaves clustered around a single Master. And a third type called a Scatternet, this is a group of Piconets effectively hubbed via a single Bluetooth device acting as a master in one Piconet and a slave in the other Piconet. The Scatternet permits either larger coverage areas or number of devices than a single Piconet can offer. Figure 5 outlines the different master and slave topologies permitted for networks in the standard.

The role of the master is to control the available bandwidth between the slaves, it calculates and allocates how often to communicate with each slave and locks them into the appropriate frequency hopping sequence. The specification describes an algorithm that calculates the hop sequence, the seed being based on the master's device address and clock. In addition to hop sequence control, the master is responsible for transmit control by dividing the network into a series of time slots amongst the net members, as part of a Time Division Multiplexing (TDM) scheme. These time slots can consist of data and potentially additional voice traffic i.e. you will always need a data channel before you can add a voice channel. The time slot is defined as 625 μs and all packet traffic is allocated 1, 3 or 5 slots, grouped together in transmit and receive pairs. Prior to connection some operations such as inquiry, paging and scanning operations may sometimes occur on half slots.

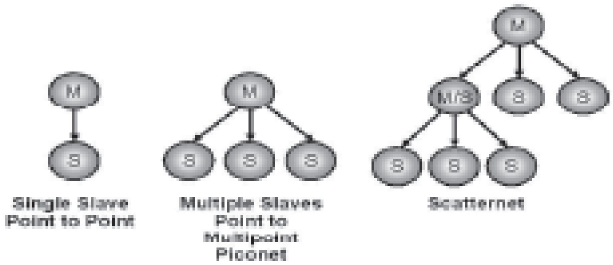

Figure 5 : Point to point, Piconet and Scatternet

2.1.2 Voice and Data Links

Bluetooth carries communication traffic over two types of air interface links defined as Asynchronous ConnectionLess (ACL) or Synchronous Connection Oriented (SCO). During a connection the links carry voice and data traffic in the time slots and are categorised as either time critical, as used for voice and audio, or high speed non-time critical data with a mechanism for acknowledgement and re-transmission. The first link established between master and slave is the ACL link and carries high speed data that is insensitive to time. It is packet switched, as the data is sporadic in nature, asynchronous, contains asymmetric and symmetric services and uses a polling access scheme. A master may be permitted to have a number of ACL links up to the maximum number of slaves permitted by the specification but only one link is allowed between any two devices.

- Once an ACL has been established a SCO link can be created on top of the ACL link. The SCO link is circuit switched; it has symmetric synchronous services and has slot reservation at fixed intervals, making it suitable for time critical data such as voice. The specification restricts the number of SCO links that a master can support to three.

3.0 FUNCTIONS AND PROFILES

Undeniably the ideal candidate for the first wave of applications will inevitably be based on mobile cellular technology, but what other applications can be realised using Bluetooth technology? The specifications outline a wireless technology that is as cost effective as the cable it replaces and aim to balance reliability, resilience, convenience and low power. The short-range connections of data and voice could mean the emergence of applications suitable for:

- Access points allowing mobile devices connection to services e.g. telephone network (PSTN) or LAN services.
- Mobile phone link to Laptop PCs
- Mobile phone connections to wireless headsets
- PDA, palmtop and desktop PC inter accessibility for file and data synchronisation.

The Bluetooth core specification describes the protocol, but the Profiles document enhances this by setting out a number of profiles for applications and defining the way a number of services operate e.g. a file transfer profile defines how devices exchange data files. The profile document aids applications development, describing implementation schemes and highlights parts of the core Bluetooth protocol supporting the profile. Profiles supported are outlined in Figure 6; they are depicted grouped together. Each profile is built upon the one underneath, attaining their features from the lower profiles. The result of this approach gives the profiles a similar look and feel for user recognition. Plus developers can recycle modules for speeding up development time and reducing costs.

A wireless headset for a mobile phone is an application example using the profiles. It uses the Headset profile as its core specification. In Figure 6 the Headset profile is built from the Serial Port Profile (SPP) and the Generic Access Profile (GAP). The GAP being the base of all profiles, it defines the generic procedures related to device discovery and link management.

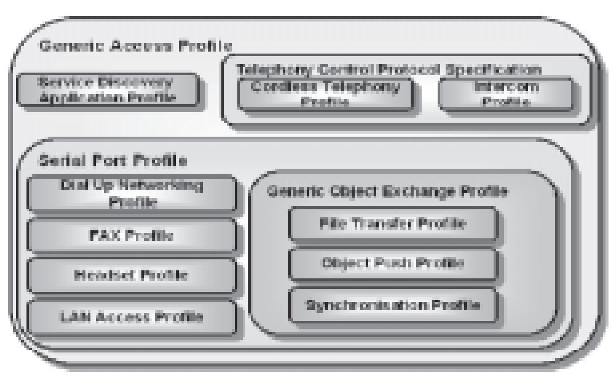

Figure 6 : Bluetooth Profiles

3.1 Connections

As applications need to connect to one another it is probably appropriate to introduce how devices connect to each other. Unlike the wired technology it is designed to replace, a Bluetooth device does not have to be aware of the devices and capabilities they are attaching to. There is a built in mechanism to inquire for devices, connect to them and once connected discover the services they possess in their database. In its simplest form the devices needing to connect proceed as follows:

1) The master enters inquiry mode and sends out an inquiry to discover devices available to connect to.

2) Potential slaves make themselves discoverable by entering inquiry scan mode and listen for an inquiry from a master.

3) On receiving an inquiry, the slave responds to the master with a Frequency Hop Synchronisation packet (FHS). The FHS contains information that is needed to create a connection to the device; this information includes its Bluetooth address and class of device.

4) The master collects the FHS information from each device discovered. To connect to one of these devices the master goes into page mode and will page the device using the corresponding Bluetooth address.

5) The slave being paged by a master will need to be in page scan mode to be able to connect to a master

This is a simplified overview of steps the link controller uses to make a connection. The specification describes various parameters that can be set, examples being the number of inquiry responses from slaves to the master, the length and number of inquiry scans the master issues. Devices do not need to carry out the full set of inquiry, inquiry scan, page and page scan. For instance some devices may not scan for inquiries, thus making them invisible, or they may be set up to only page scan so they can be connected to only one specific master. Perhaps a master device may not go into page scan mode, as it may only need to page or inquire. As entering any mode necessitates the turning on of RF circuitry then limiting options reduces power consumption as this is a major influence on power consumption, so missing out a few of these modes has an advantage.

Once a connection is created between two devices, the application can use the Service Discovery Protocol (SDP) to find out what particular services a device supports. This is done via a L2CAP channel to the service discovery server. The potential Bluetooth Services available sit on top of the Bluetooth protocol stack. In real terms, before the service can be accessed and used, the lower levels must be connected, i.e. an ACL must be connected and configured.

3.2 Results

In the previous section the importance of profiles in the development of applications and how these applications get access to the service running on top of the Bluetooth protocol stack was explored. To truly appreciate the products that could be realised with Bluetooth technology, then a trip to the Bluetooth website is a good starting point. Look at the products that have been qualified already. As the technology matures more applications will emerge within the Personal Area Network using profiles as their building blocks. We will certainly see the PDA that is placed in the vicinity of your desktop computer and files synchronised between them. This latter concept extending to your digital stills camera when downloading your holiday photos without the palaver of connecting the inevitable miniature cable.

The wireless headset to mobile phone contains a speaker and microphone and connects over a Bluetooth link permitting voice and data communications. The RF power for this link is significantly lower than the power required by the mobile phone to connect to its base station. Therefore from a health hazard, it is preferable to have the Bluetooth headset with its small RF power next to your head than the phone.

4.0 COMPATIBILITY

Compatibility covers various issues, whether it is compatibility with other Bluetooth devices, the specification or other systems that share the same frequency band. We will examine some of these aspects here.

4.1 Interference

Bluetooth is subject to interference from two types of emitters, as well as environmental problems. The emitters break down to intentional emitters and accidental emitters. Intentional emitters occupy the ISM band and are systems based on IEEE 802.11b (Wi-Fi), Home RF, DECT variants, proprietary systems and of course other Bluetooth devices. Accidental emitters include microwave ovens and lighting. The third source of interference could be the environment, signals can fade due to distance or being blocked by walls, furniture and human bodies; device positioning could be critical.

How is the affect of these forms of interference minimised? With respect to the intentional emitters, Bluetooth has a clear advantage over systems based on Direct Sequence Spread Spectrum (DSSS) systems such as IEEE802.11b as it is based on a FHSS system. What makes the DSSS poor in comparison is that transmission power is often low in any specified band. The FHSS signal may have high enough power in its narrower band to effectively ‘punch through’ the parts of the wider band occupied by the DSSS system. Otherwise, if there is strong interference from the DSSS system on Bluetooth, its ability to hop utilises the rest of the band more effectively. Bluetooth allows for retries meaning data will eventually get through, so users will see a decrease in the throughput of the network but it will continue to operate. The major degradation is in audio quality as voice data transmitted on a SCO channel is not retransmitted, as it is time critical.

HomeRF is another FHSS system and you could be lucky that both systems could hop around and miss each other. But HomeRF with greater data rates has larger channel sizes and therefore Bluetooth has a greater chance of hitting these on a hop. HomeRF covers a larger distance potentially over powering the Bluetooth on the channels where they clash. With retry available eventually data will get through, although performance degrades. HomeRF on the other hand has built features in its higher layers of protocol and it has MAC level retry mechanism both for data and isochronous voice connections. This although comes at a cost, whereas Bluetooth radio is designed for simplicity.

Against other intentional emitters and accidental emitters the techniques for co-existence with IEEE 802.11b and HomeRF are just as applicable i.e. the ability to hop away from offending channels and retry are Bluetooth’s natural defence.

5.0 CONCLUSION

This was an overview of Bluetooth giving insight to the key features and potential challenges of the technology. The technology occupies the 2.4 GHz ISM band sharing the bandwidth with potential competing standards. It defines a Personal Area Network (PAN) whereas others advocate a Wide Area Network (WAN) approach. It is best positioned as a short-range wireless standard designed with the same cost goals and similar or greater reliability and performance as the cable it replaces. Based on a frequency agile FHSS scheme it leverages hopping to avoid interference and it was not intended as a replacement for wireless LAN in a WAN scenario, because as yet it does not fully specify a hand over mechanism.

The importance of the Bluetooth SIG and how its specifications aid development of applications was highlighted, especially through the profiles, and their interoperability is assured through the qualification process. A flavour of the applications was explored through the functionality and where particular attention must be paid to the protocol stack for system segmentation. But to thoroughly investigate Bluetooth a list of further reading and applicable websites is given in the reference section. The latest specifications including the profiles are available from the Bluetooth SIG website. Reading specifications can seem a little ‘one dimensional’ but read in conjunction with a good book, whilst using a development tool from one of the Bluetooth silicon vendors, then the jigsaw pieces to really start to fit.

In conclusion, if we allow PCs a cornucopia of competing, serial cable standards hanging from them surely there must be room for differing wireless standards to co-exist to cover various functionalities.

REFERENCES

- http://www.bluetooth.com
- http://www.nokia-asia.com
- http://www.bluecellworld.com
- J. Bray and C.F. Sturman, “Bluetooth: Connect Without Cables”, Prentice Hall.