T.E.I. PIRAEUS

Faculty of Engineering

Departments of Electronics and Automation

MSc in DATA COMMUNICATIONS

COURSEWORK

MODULE:

Wireless Networks

CSESM00: CIM228

Module Coordinator:

Mr. Stylianos Savaidis

Date of Module:

2nd Term (Spring 2005)

Name of Student:

Vasileios Balafas

An overview for Bluetooth Network Architecture and Protocol Stack

Vasileios Balafas, *MSc in DCOM student*,(xwing@otenet.gr)

Abstract

In this coursework the Bluetooth technology and its protocol stack will be discussed as part of the DCOM module of Wireless Networks. Network technologies have already brought revolution in the way we work, we use devices and even we think. One of these technologies is Bluetooth which came to solve the problem of the cables in a LAN environment. Bluetooth seems ideal also for house use, especially in our country where no regulations are implemented when a house is built concerning the creation of a data cable network in the house. In every house in Greece several cables are laying on the floor serving the telephone network, the TV-Radio network and of course a small PC network. And if we think about peripheral devices, then the problem becomes huge with all the usb cables connecting the printer, the scanner, the PDA, our mobile phone and other useful devices with the PC unit. So, Bluetooth gives the solution offering a low cost way of interconnecting. In technical terms Bluetooth offers a radio wave system which provides short range wireless communication of data and voice. It is obvious that Bluetooth is a member of the wireless LANs family and is a killer application especially in PDAs and mobile phones. When you see someone walking in the street talking to himself, before deciding that he is a crazy man, look for a small device at his ear. If he has one it is his Bluetooth hands-free device connecting him with his cell phone without wires or other annoying cable things!

This coursework is an outline of the Bluetooth Core Specification version 1.1 dated on February 22 2001 concentrated on the architecture and the protocol stack of this technology which is attached to the coursework's CD-ROM and can be also found at the website www.bluetooth.com.

1. Introduction

Wireless LANs are the evolution of traditional networks and a new concept of interconnecting devices and computers. The high cost and low data rates didn't allow to these technologies to grow and become as popular as they should be. But, each year wireless technologies become more user friendly not only by their high data rates but by their price also. Bluetooth as a member of those technologies is now the outstanding and leading commercial technology of wireless networks, thanks to its low cost and its easiness in use. Bluetooth succeeded in establishing and consolidating the concepts of the PANs (Personal Area Networks) and ad-hoc networks (Bluetooth FAQs, No date, http://www.comsol.com.au/bluetooth.asp, [Online], viewed 23 May 2005).

By not needing any server unit scheme or special knowledge in order to create device connections, Bluetooth is now widely accepted in the consumers' consciousness and tends to become a must-have technology.

Bluetooth began from Ericsson Mobile Communications in 1994, but today, it is the result of the joint effort of many large companies. Ericsson, Intel, IBM, Toshiba, Nokia founded in February 1998 the SIG (Special Interest Group) as the core promoters. Later in 1999 more core promoters were added and today SIG has more than 2500 members. A very great factor of its success is the excellent marketing policy that has been followed which begins from its name. Bluetooth is named after Harald Blatand, a tenth-century Danish Viking king, who united Denmark and Norway during his rule from 940 to 985 AD. His fancy for blackberries and the lack of toothpastes offered him exactly the meaning of this technology; the Bluetooth!

This king's achievement is the goal of Bluetooth technology; to allow devices from lots of different manufacturers to work with one another and to unify telecommunication and computing devices. Various technologies try to implement this concept but Bluetooth achieved in the same time to be widely available, inexpensive, convenient, easy to use, reliable, small, and low power consumption. The last characteristic is extremely important because portable devices must have low power consumption and large time of autonomy because they have to work with batteries.

Bluetooth with a 1mW (0 dBm) consumption offers a communication range of 10 meters that can be increased to 100 meters amplifying the power to 20 dBm.

It does not need a *line of sight*, but it has limited tolerance to physical obstacles.

As we can already concur Bluetooth is a radio system optimized for mobility and has the characteristics that set it adequate for various applications. The general concept of its operation is a master-slave communication between devices which can be either the master or the slave thanks to the symmetric radio system. When two or more devices meet and form an ad-hoc network, they create a piconet. Each piconet must have only one master and there can be more than 7 active slaves at a time. The group implemented by those devices can be connected to another group creating a scatternet by setting the master of one group as slave to the other. In that case the data rate is lower and decreases significantly when the scatternet increases (Schiller 2003, pp. 272-3).

But Bluetooth didn't developed by the way it was expected and that happened because of its complexity. The Bluetooth *specification* defines basic connectivity, but specific uses require separate *profiles*. Not all Bluetooth-enabled devices support all of the profiles, and that can lead to confusion for buyers who may expect a Bluetooth PC adapter, for example, to do things it isn't set up for.

Bluetooth was reasonably easy to use between two products from the same vendor and for some simple functions, such as getting a headset to work with a phone. But an application such as synchronizing a phone or handheld device with a PC is still too complicated for the average person, who is needed in order to achieve Bluetooth's wide adoption. Another factor was its cost which was more expensive than 27-MHz technology. Bluetooth Specification version 1.2 came to solve lots of similar problems. It is of course backward compatible and includes new features that address security, co-existence with 802.11 systems, enhanced voice processing, user setup and improved quality of service. An analysis will follow for all the above during this coursework.

It is important here to refer to two keywords that were mentioned; specification and profiles. Specification describes how the technology works, i.e., the Bluetooth protocol architecture and the protocol stack and profiles describe how the technology is used, i.e., how different parts of the specification can be used to fulfil a desired function for a Bluetooth device which means user friendliness and easy connectivity between several different devices.

Finally, Bluetooth is the base for the 802.15 wireless personal area network (WPAN) standard offering the elements for the link and physical layers (Kurose 2005, p.528).

2. The Bluetooth Architecture

As mentioned before, Bluetooth communication occurs between a master and a slave radio. Bluetooth radios are symmetric in that the same device may operate as a master and also as a slave. Each radio has a 48-bit unique device address that is fixed.

Two or more radio devices together form ad-hoc networks called piconets. All units within a piconet share the same channel. Each active device within a piconet is identifiable by a 3 bit active device address. Inactive slaves in unconnected modes may continue to reside within the piconet. A master is the only one that may initiate a Bluetooth communication link. However, once a link is established, the slave may request a master/slave switch to become the master. Slaves are not allowed to talk to each other directly. All communication occurs between the slave and the master. Slaves within a piconet must also synchronize their internal clocks and frequency hops with those of the master in order to follow the same pattern. Each piconet uses a different frequency hopping sequence and this reduces interference possibilities.

Bluetooth devices operate at 2.4GHz, in the globally available, license-free, ISM band. That is the bandwidth reserved for general use by Industrial, Scientific and Medical applications worldwide. Since this radio band is free to be used by any radio transmitter as long as it satisfies the regulations, the intensity and the nature of interference can't be predicted. It uses 79 channels between 2.402 GHz to 2.480 GHz (23 channels in some countries).

Bluetooth supports three kinds of links; the Asynchronous Connection-less (ACL) links for data transmission and the Synchronous Connection Oriented (SCO) for audio/voice transmission. The third type is a combination of ACL and SCO, the Data Voice (DV) which has no flow Control or CRC but the data part supports flow control and retransmission.

Bluetooth devices use a Frequency Hopping Spread Spectrum (FHSS) instead of Direct Sequence Spread Spectrum (DSSS). The FHSS scheme provides 1600 hops / second and every hop is 625μs. A master device in a piconet transmits on even numbered slots and the slaves may transmit on odd numbered slots.

The master also controls the traffic on the piconet and takes care of access control. The time slots are alternatively used for master and slaves transmission. In order to prevent collisions on the channel due to multiple slave transmissions, the master applies a polling technique, for each slave-to-master slot the master decides which slave is allowed to transmit. If the master has no information to send, it still has to poll the slave explicitly with a short poll packet. This master control effectively prevents collisions between the participants in the piconet, but independent collocated piconets may interfere with one another when they occasionally use the same hop carrier. This can happen because units don't check for a clear carrier (no listen-before-talk). If the collision occurs, data are retransmitted at the next transmission opportunity.

Multiple piconets with overlapping coverage areas form a scatternet. Each piconet may have only one master, but slaves may participate in different piconets on a time-division multiplex basis. A device may be a master in one piconet and a slave in another or a slave in more than one piconet.

Fig.1 shows the network topologies that can be created by this concept and form three network types corresponding to the above logic; the point-to-point piconet which can be a Bluetooth hands free an a cell phone, the multipoint piconet which can be a PC and its peripheral devices and the scatternet which can be a combination of bluetooth networks.

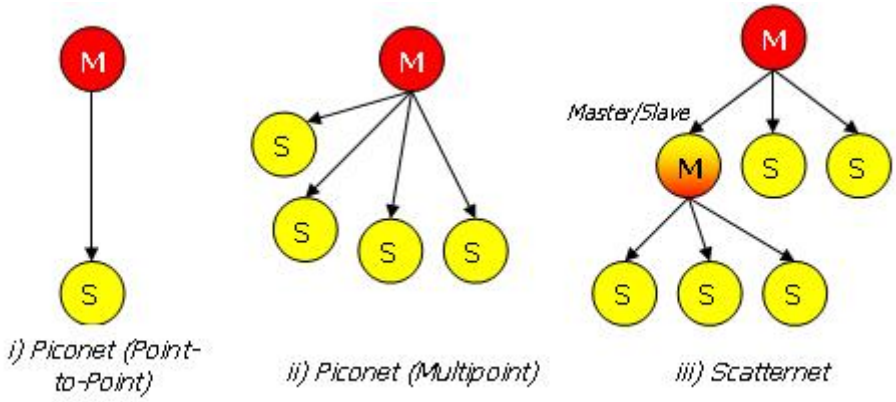

Fig. 1 Bluetooth Network Topologies

Bluetooth uses Gaussian-shaped frequency shift keying (GFSK) modulation with a nominal modulation index of k=0.3. This binary modulation was chosen for its robustness, and, with the accepted bandwidth restrictions, it could provide data rates to about 1Mbps. This simple modulation scheme allows the implementation of low-cost radio units, which is one of the main aims of the Bluetooth system.

The Bluetooth devices can have four connection states determining their comportment in a piconet. They can be in active, sniff, hold and park state as it is shown in Fig. 2.

In active state both master and slave participate actively on the channel by transmitting or receiving the packets (A,B,E,F,H).

In sniff state, slave rather than listening on every slot for master's message for that slave and it sniffs on specified time slots for its messages. Hence the slave can go to sleep in the free slots thus saving power (C).

In hold state, device can temporarily not support ACL (Asynchronous Connection-Less) packets and go to low power sleep mode to make the channel available for things like paging, scanning etc (G).

Finally, in park state, the slave stays synchronized but not participating in the piconet, then the device is given a Parking Member Address (PMA) and it loses its Active Member Address (AMA) (D,I).

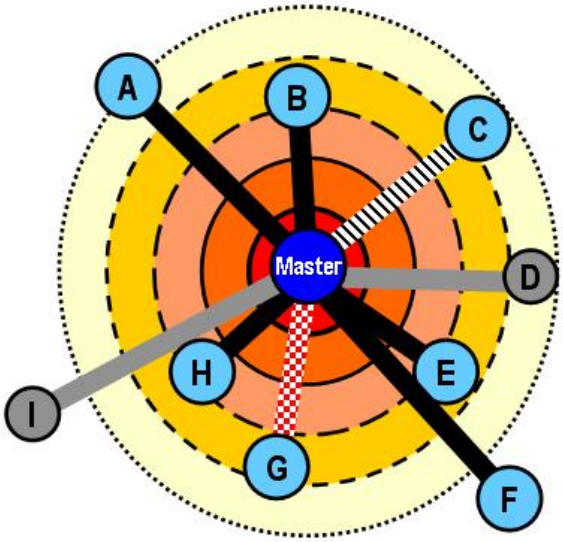

Fig. 2 Bluetooth devices states

Finishing the reference to the architecture of Bluetooth it is useful to offer an image of its supported distances which vary following the changes of power and form three classes of power and range covering (Fig. 3).

Power Class	Max Output Power	Max Output Power	Expected Range	Range in Free Space
Class 1	100mW	20dBm	42m	300m
Class 2	2.5mW	4dBm	16m	50m
Class 3	1mW	0dBm	10m	30m

Fig. 3 Bluetooth Power Class Table

3. The Bluetooth Protocol Stack

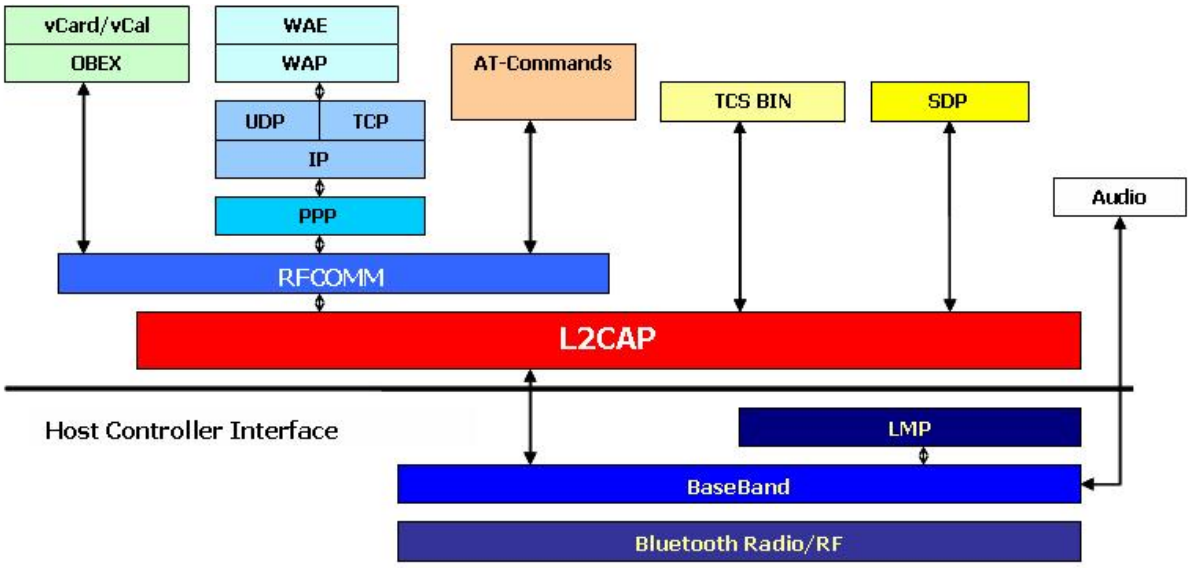

Fig.4 Bluetooth Protocol Stack

In Fig.4 the Bluetooth Protocol Stack is represented in an understanding and fundamental way. Examining the stack, we first come across the fundamental component, the *radio* that was explained earlier. Remember that the radio modulates and demodulates data for transmitting and receiving over the air. Above the radio are the *Baseband* and the Link Controller that 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 Protocol (LMP)* controls and configures links to other devices. Peers communicate each other via LMP messages that are very important because they determine the roles between the peers. Every LMP message begins with a flag bit which is 0 if a master initiates the transaction and 1 if the slave initiates the transaction. That bit is followed by a 7-bit Operation Code, and by the message's parameters. LMP also provides a mechanism for negotiating encryption modes and coordinating encryption keys used by devices on both ends of the link. Additionally, LMP supports messages for configuration of the quality of service on a connection. Packet types can automatically change according to the channel quality, so that the data can be transferred at a higher rate when the channel quality is good and on lower rates with more error protection if the channel quality deteriorates. Another responsibility of LMP is the determination of power modes and connection states that form the communication.

The *Host Controller Interface (HCI)* is above the LMP layer and is probably one of the most important layers to be considered from designers. 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, RS232, UART or a robust proprietary standard such as BCSP (BlueCore Serial Protocol). In simple words the HCI abstracts away transport dependencies and provides a common device driver interface to various interfaces working like the glue between devices.

Above HCI we find the *Logical Link Control and Adaptation (L2CAP)*, which is a multiplexer, adapting data from higher layers and converting between different packet sizes.

That means that it offers segmentation and reassembly to allow transfer of larger packets than lower layers support. Additionally it performs Quality of service management for higher layer protocols. All applications must use the L2CAP layer to send data. Bluetooth's higher layers such as RFCOMM, SDP and TCS also use it, so L2CAP is a compulsory part of every Bluetooth system.

RFCOMM (Radio Frequency COMMunication port) is responsible for the implementation of functionalities of a virtual RS232 link. Most of the application profiles use RFCOMM as a means of transmitting and receiving data. Up to 30 data channels can be set up, so RFCOMM can theoretically support 30 different services at once. RFCOMM is based on GSM TS 07.10 standard, which is an asymmetric protocol used by GSM cellular phones to multiplex several streams of data onto one physical serial cable.

SDP (Service Discovery Protocol) provides a means for applications to discover which services are provided by or are available through a Bluetooth device. It also allows applications to determine the characteristics of those available services. Information about services is maintained in SDP databases. There is no centralized database, so each SDP server maintains its own database. The SDP database is simply a set of records describing all the services that a Bluetooth device can offer to another Bluetooth device, and service discovery protocol provides a means for another device to look at these records. To make it easier to find the service you want, services are arranged in a hierarchy structure as a tree that can be browsed. Clients begin by examining the root of the tree, and then follow the hierarchy out to the leaf nodes where individual services are described.
To browse service classes, or get information about a specific service, SDP clients and servers exchange messages that are carried in SDP Protocol Data Units (PDUs). The first byte of PDU is an ID, identifying the message in the PDU. Services have Universally Unique Identifiers (UUIDs) that describe them. The services defined by the Bluetooth profiles have UUIDs assigned by the standard, but service providers can define their own services and assign their own UUIDs to those services. It is clear that SDP is essential for all bluetooth models and can be used in conjunction with other protocols such as Jini and UpnP extending bluetooth capabilities.

TCS BIN (Telephony Control protocol Specification – TCS BINary) defines as it can be understood by its name the call control signaling for the establishment of speech and data calls between bluetooth devices. It is based on the OUT-T Q.931 recommendation and it is an oriented protocol providing also group management.

The last grouped layer of the Bluetooth protocol stack over RFCOMM defines the adopted and supported protocols of the bluetooth system. IP and WAP protocols are known and there is not any reason to be explained.

Some attention needs to be focused at the *OBEX (Object Exchange)* which is designed to allow a variety of devices to exchange data simply and spontaneously. Bluetooth has adopted this protocol from the Infrared Data Association (IrDA) specifications. OBEX has a client/server architecture and allows a client to push data to a server or pull data from the server. For example, a PDA might pull a file from a laptop, or a phone synchronizing an address book might push it to a PDA. The similarities between the two communications protocols' lower layers mean that IrDA's OBEX protocol is ideally suited to transferring objects between Bluetooth devices. It is largely accepted and extremely highlighted by companies that provide bluetooth adapters such as the one which is demonstrated at the next section. They consider it as a "catchy" implementation and surely it is but in my opinion the reference to its functions by its name brings confusion to the large target market group that bluetooth aims. It is very useful and it should be referred by the services and applications that it can offer.

Finally, the *vCard/vCal (VCARD & VCalendar)* layer represents a supported format of data, very popular in synchronization situations from users and it is not a protocol or a mechanism. For example once a VCard is received, we can easily add the user to our contacts. The same is happening using VCal to schedule an appointment.

At this point ends the presentation of the Bluetooth protocol stack that I hope that can help understanding the Bluetooth operation and functionality.

4. Bluetooth in real life

Bluetooth is not something scientific or a theory case anymore. Day by day more and more people use bluetooth devices which are very useful, easy to use and very affordable. Towards this wireless revolution cell phones helped very much as the killer application-device of this new technology was the hands-free sets that gave cables freedom to cell phone users. Now it is very easy and safe to drive talking to mobile phone and very convenient to connect a peripheral device to a PC without using usb cables.

In this section some bluetooth devices are shown which came to make our life easier, and integrated technological evolution in the life of simple people who don't have to be computer experts or future "freaks" in order to use those devices and create their own PANs!

Mobile Phone and Bluetooth Hands Free HBH - 600

Bluetooth USB Adapter Level One

Laptop and PDA connected via Bluetooth

5. Conclusion

The Bluetooth system is a universal interface developed to enable electronic devices to communicate wirelessly via short-range ad hoc radio connections. This coursework presents general overview of the Bluetooth radio system architecture and it focuses on a description of the Bluetooth protocol stack, which is designed to achieve better interoperability for data communication between devices.

It is a common consensus that Bluetooth is successful and brings the new era of PAN networks in every home with a low cost and a simple way. Its applications can be enormous and very interesting like Mobile phones headsets and communication, Laptops desktops and PDAs interconnection, home networking, Data access points, Office equipment etc.

During this coursework some Bluetooth devices were examined and tested and it was a great experience concluding that Bluetooth is indeed a fresh hi-tech puff of wind and a wonderful low-budget proposition for our deliverance from cables spaghetti situations on our desks and generally in our living with devices that are becoming more and more essential and necessary.

Figures that are included here where designed with Smart Draw Suite Edition version 7, determined by the study of books, web sites and the specification document.

6. Reference List – Bibliography

Bluetooth Core Specification version 1.1, February 22 2001

Bluetooth FAQs, No date, <http://www.comsol.com.au/bluetooth.asp>, [Online], viewed 23 May 2005

Bluetooth Protocol Stack, No date, <www.thewirelessdirectory.com/Bluetooth-Software/Bluetooth-Protocol-Stack.htm>, [Online], viewed 25 May 2005

Kardach J. (2000), *Bluetooth* Architecture Overview*, Journal, Available: <http://www.intel.com/technology/itj/q22000/articles/art_1a.htm>, viewed 8 June 2005

Kurose J. and Ross K. (2005), *Computer Networking*, 3rd ed., Addison Wesley, pp.528-530

Schiller Jochen (2003), *Mobile Communications*, 3rd ed., Addison Wesley, pp.269-292

Balafas Vasileios

Digitally signed by Balafas Vasileios
DN: CN = Balafas Vasileios, C = GR, O = DCOM, OU = DCOM
Reason: I am the author of this document
Date: 2005.06.14 23:28:23 +03'00'