ABSTRACT

The seemingly endless entanglement of data wires connecting today's electronic devices has become slightly less jumbled with the introduction of Bluetooth technology and the creation of a wireless data link. This article delves into the implementation and architecture of Bluetooth. It also describes the functional overview and applications of Bluetooth. It gives significant advantages of Bluetooth over other data transfer technologies such as IrDA and Home RF. It illustrates how a connection is made in Bluetooth between two environments. It mainly emphasizes the architecture of Bluetooth. It gives over all Bluetooth packet structure and different communication and data information protocols such as WAP, UDP, IP, TCP, RFCOMM, and L2CAP etc. It also explains Link Security by Data Encryption. Finally it narrates how Bluetooth will bring a new level of connectivity and convenience when operating electronic devices. These details in the article establish the growing need for Bluetooth technology.

INTRODUCTION

Bluetooth is a method for data communication that uses short-range radio links to replace cables between computers and their connected units. Bluetooth is a radio frequency technology utilizing the unlicensed 2.5GHz industrial, scientific and medical (ISM) band. **B**luetooth is an open standard for wireless connectivity with supporters mostly from the PC and cell phone industries. Not surprisingly, its primary market is for data and voice transfer between communication devices and L.M.Ericson of Sweden invented PCs. Bluetooth in 1994. The standard is named after Harald Blaatand"Bluetooth"2nd,king of Denmark.

WHY BLUETOOTH?

Bluetooth attempts to provide significant advantages over other data transfer technologies such as IrDA and HomeRF. IrDA is already popular in PC to peripherals,but is severely limited by the short connection distance of 1m and the line of sight requirement for communication. Due to its RF nature bluetooth is not subjected to such limitations. In addition to wireless device connections up to 10-100m, devices need not be within line of sight. Also it is designed to be low cost i.e under $10/unit.

Establishing a connection in Bluetooth:

Linking one Bluetoooth device to another to another involves a series of inquiry and paging procedures. The inquiry process entails the following steps:

- The Bluetooth device sends out an inquiry access code packet (inquiry packet) to search and locate these devices.
- The existing Bluetooth devices already within the area (and usually unware of any inquiring devices) will occasionally enter an inquiry scan state of their own to troll for any inquiring devices.
- when a device in the inquiry scan state receives an inquiry packet, it will respond with a frequency hop synchronization (FHS) packet that is sent back to the inquiring device.

Once the inquiry routine is completed, the paging process follows:

- the inquiring Bluetooth device now wants to establish a connection with another Bluetoooth device.
- To successfully locate and page a target Bluetooth device, the paging device estimates the hop frequency and clock of the target Bluetooth device using the FHS packet received during inquiry.
- the paging device "pages" the target device with the target device's device access code (DAC). The paging device transmits the DAC on several different hop frequencies that it thinks the target device is receiving (as calculated using the FHS packet) and continues to do so until a connection is made.
- while the paging device (the master) is paging, the target (slave) device may be involved in other piconets. Occasionally, it will enter the page scan state and listen for pages directed to it, scanning through 16 different frequencies. When it receives a page from the paging device, it will respond to the page by sending an update of its clock to the paging device.
- once the paging device receives a page response from the target device, information vital for a connection is exchanged between the two devices. Information exchanged includes the device address and clock of the paging device, which is used to determine the timing and frequency-hop sequence of the newly formed piconet. When all connection information has been communicated, the connection is complete, and the two devices can begin to exchange data with one another.

Bluetooth packet format:

Since Bluetooth is meant to be compatible with many different applications, it must be able to send data with different protocols quickly and efficiently. When data is transmitted at the lowest level, it is first broken down into smaller packets and sent serially with the least significant bit sent first. Each data packet (represented in Figure 2) contains three fields: an access code, a header, and a payload.

Access codes

At the beginning of each Bluetooth packet is an access code. The access code is used primarily for piconet identification and synchronization. The access code identifies the piconet to which

each data packet belong; all data packets having both a packet header and payload present will have a 72-b access code; otherwise, the access code is 68-b long. Access codes are also used extensively in Bluetooth with no header or payload present. The access code itself (Figure 3) is divided into three sections-preamble, sync word, and trailer-which are not present in inquiry or device access codes.

Packet header

The packet header, which follows the access code and contains link control information, co9ntain six fields: AM_ADDR, TYPE, FLOW, ARON, SEQN, and HEC (Figure 4).

- AM_ADDR, a 3-b active member address, is used to indicate where the packet is destined. When a slave receives a data packet, it checks the packet header's AM_ADDR. If it matches its own assigned AM_ADDR, the packet will be decoded; otherwise, it is discarded.
- the 4-b TYPE field indicates the type of packet that has been sent. There are up to 16 different types of Bluetooth packets.
- The FLOW bit is used for flow control. For example, if the receive (RX) buffer of a recipient device is full, it will indicate in its response to the master that it cannot accept any data at that moment. Once it can receive more data, the FLOW bit is changed from 0 to 1.
- ARQN is the acknowledge bit that informs the source whether the previous transaction was successful.
- The sequence (SEQN) bit allows the source and the recipient to keep track of the packets that have been sent. The bit is inverted on each packet transmission and used to prevent the reception of packets that may have been sent twice. Repeat transmission of a packet occurs when the acknowledgement signal of a successful data transaction to the master fails to transmit. The receiving device can simply compare the SEQN bit of the packet that was previously processed to determine whether to discard or accept the packet.
- The header error check, HEC, is used to check the integrity and accuracy of the header during each packet transaction. If the HEC is incorrect, the packet is discard. While the header comprises 18 b, the fact that it is encoded at a rate of one-third the forward error correction (FEC) rate, extends the total bit length to 54 b.
- The payload , which follows the header, can range from 0 to 2,745 b, and contains the actual data of interest. With a packet capable of being sent during every 625 micro second time slot, a maximum bit rate of 723.2 kb/s can be achieved for an ACL, and 64 kb/s can be achieved for an ACL, and 64 kb/s for an SCO.

Bluetooth can handle the transmission of many different applications. This entails dealing with different architectural layers to decompose the application data into a form suitable for transmission over a Bluetooth link, as well as to reassemble the data into its original form at the receiving end.

GENERAL BLUETOOTH ARCHITECHTURE

Facilitating this data transmission is a series of protocols within the Bluetooth system that processes the data for suitable transmission and receipt.

The general structure of a Bluetooth system consists of a microprocessor that handles all the base band specifications, and several software layers that structure the data so that it may be sent properly over a Bluetooth link. Figure 5 provides a good representation of the architecture.

At the highest architecture level lies the different communication and data information protocols that can communicate over the Bluetooth link, including wireless application protocol (WAP), user datagram protocol (UDP), transport control protocol (TCP), internet protocol (IP), and point-to-point protocol (PPP). While all of these are standalone communication protocols, they can be adapted for transmission over a Bluetooth link. To support these different types of communication protocols, the Bluetooth system architecture must be capable of capable of differentiating and converting data associated with these protocols into data packets that the Bluetooth base band controller and RF transceiver can send.

One of the protocols within the Bluetooth architecture that is responsible for this adaptation is RFCOMM, which emulates a serial port and can be used by applications that use the serial ports on a Bluetooth device. RFCOMM can take the data from some of the higher level protocols mentioned previously and adapt it so it can be sent down to the baseband and converted into Bluetooth data packets and subsequently sent over a Bluetooth link.

Below RFCOMM lies the logical link control and adaptation protocol (L2CAP) that further supports the adaptation of other communication protocols, such as telephony control specification binary (TCS-binary) and the Bluetooth-established service discovery protocol (SDP), as well as performing the multiplexing between all incoming upper-level protocols (RFCOMM, TCS, SDP), as well as performing the multiplexing between all incoming upper-level protocols (RFCOMM, TCS, SDP). In addition to protocol multiplexing, L2CAP is responsible for the segmentation of outgoing data packets so they may be transferred to the baseband processor cannot handle data packets of great size. L2CAP is also responsible for the

reassembly of received data packets, which are subsequently sent to one of the higher-level protocols designated to receive this data.

Once the original data has been segmented by L2CAP into subsequent L2CAP packets, the packets are then sent to the host controller interface (HCI), which is responsible for sending data to and receiving data from the lower level Bluetooth hardware (baseband controller) through a physical bus (USB, RS232, PCI), HCI further alters the L2CAP packets so that the data may be transported over one of the physical buses. The link manager and baseband controller that assemble it into packets that are communicable using a Bluetooth link receive this data.

At the lowest level lie the link manager and baseband controller. The baseband controller performs all low level processing, such as Bluetooth packet composition for transmission and packet decomposition upon reception. Running on the baseband controller is firmware implementing the link manager protocol, which handles link control, is responsible for placing the device in low power states, and performs any encryption of the data transmitted.

LINK SECURITY

As with any communication link, there must be security surrounding the data transfer between two devices. With the frequency hopping and the timing involved in the hopping, is very difficult for an external device to eavesdrop on a Bluetooth link. However, there are some security risks from other Bluetooth devices already synchronized to an existing piconet and accessing sensitive information intended for another device on the piconet.

Data encryption is used to prevent other devices and the piconet from eavesdropping on data transactions. The basic security procedure used over a Bluetooth link is based on a challenge response scheme. The authenticity of a Bluetooth device is determined a challenge sent by a verifier to a claimant and response to that challenge by that claimant device. The response to the challenge is a function of the challenge, the claimant device's Bluetooth address, and a secret key. The secret key is known only by the verifier and the true claimant device and is not known to any other Bluetooth device. If the claimant contains the correct secret key, the correct response to the challenge will be calculated, and information between the verifier and claimant can begin, otherwise verifier will detach from the claimant device.

ADVANTAGES AND APPLICATIONS OF BLUETOOTH

Bluetooth can handle data and voice simultaneously. It is capable of supporting one between computers and their connected units. Bluetooth is an open standard for wireless connectivity with supporters mostly from the PC and cell phone industries. Its primary market is for data and voice transfer between communication devices and PCs. It is

capable of supporting one asynchronous data channel and up to three synchronous voice channels, or one channel for both voice and data. This capability combined with adhoc device connection and automatic service discovery make it a superior solution for mobile devices and Internet applications.

Bluetooth finds applications in PC and peripheral networking, hidden computing, data synchronization for address books and calendars, home networking and home appliances such a s heating systems and entertainment devices. Asynchronous data channel and up to three synchronous voice channels, or one channel for both voice and data. This capability combined with adhoc device connection and automatic service discovery make it a superior solution for mobile devices and Internet applications.

LIMITATIONS OF BLUETOOTH

The main drawback of Bluetooth is its limited connection distance and less transmission speeds. It supports data rates up to 780kb/s which may be used for unidirectional data transfer. It is perfectly adequate for file transfer and printing applications.

CONCLUSION

With its relatively low implementation costs, Bluetooth technology seems destined to dominate the electronic landscape, as humans worldwide will be able to form personal area networks with devices and completely simplify the way in which they interact with electronic tools and each other.

In the years to come, Bluetooth will become a worldwide connectivity among electronic devices, leading to applications unthinkable by today's technological standards. Because the radio frequency used is globally available, Bluetooth can offer fast and secure connectivity all over the world.

REFERENCES:

1. J.C. Haartsen et al. ,"The Bluetooth Radio System" IEEE pers. Commum.,Feb.2000 .

2. "Bluetooth in Wireless Communications" IEEE Communications Magazine June 2002

3. "Bluetooth" IEEE Microwave Magazine September 2002.

Overall Bluetooth Packet Structure

Figure 2. Overall Bluetooth packet structure.

Access code

Figure 3. Access Code.

Header

Bluetooth System Hierarchy

Device1 Device 2

Data Transfers Data Transfers

HCI HCI

Bluetooth Link