

Overview of Blue tooth

Addicam.V.Sanjay

Abstract

This paper attempts to present an analysis of the Blue tooth standard. This paper will Describe how Blue tooth standard works and also the various situations in which this standard can be used. This paper looks into the various components and various definitions, which goes into making a Blue tooth network. This paper will describe the protocol architecture of the Blue tooth standard. This paper will look into the future of Blue tooth standard. This paper will also describe the pros and cons of this standard. It will suggest ways in which the limitations of this standard can be overcome.

What is Blue tooth???

Bluetooth is the name given to a new technology using short-range radio links, intended to replace the cable(s) connecting portable and/or fixed electronic devices. It is envisaged that it will allow for the replacement of the many propriety cables that connect one device to another with one universal radio link. Its key features are robustness, low complexity, low power and low cost. Designed to operate in noisy frequency environments, the Bluetooth radio uses a fast acknowledgement and frequency-hopping scheme to make the link robust. [Palowireless]

What goes into making a Blue tooth network??

A Blue tooth Network is a true Ad-Hoc system. In a truly ad hoc system, there is no difference between radio units; that is, there are no distinctive base stations or terminals. Ad hoc connectivity is based on peer communications.

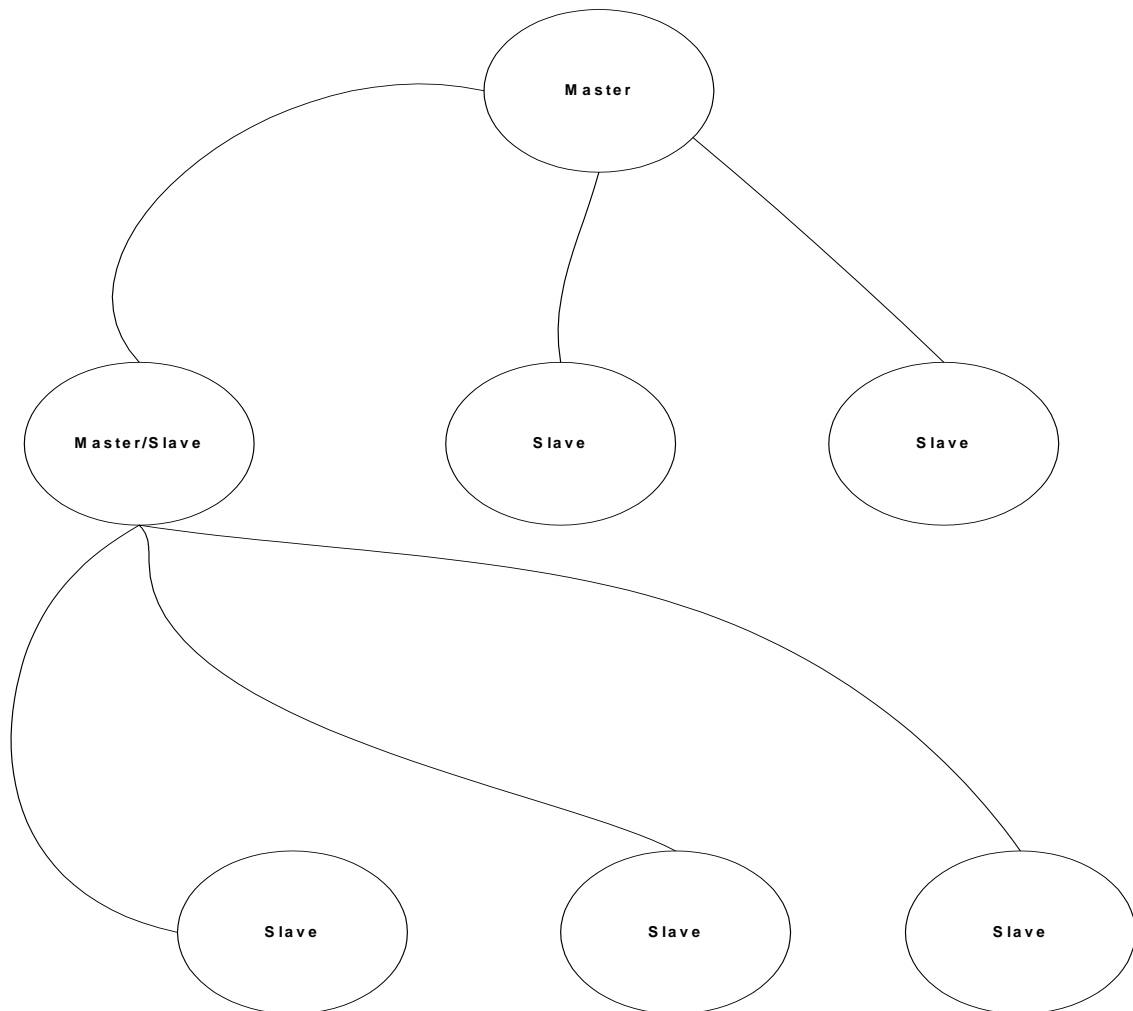
There is no wired infrastructure to support connectivity b/w portable units, there is no central controller for the units to rely on for making interconnections; nor is there support for coordination of communications.

In addition, there is no intervention of operators. For the scenarios envisioned by blue tooth, it is highly likely that a large number of Ad hoc connections will co exist in the same area without any mutual coordination, that is tens of ad hoc links must share the same medium at the same location in an uncoordinated fashion. [Haartsen]

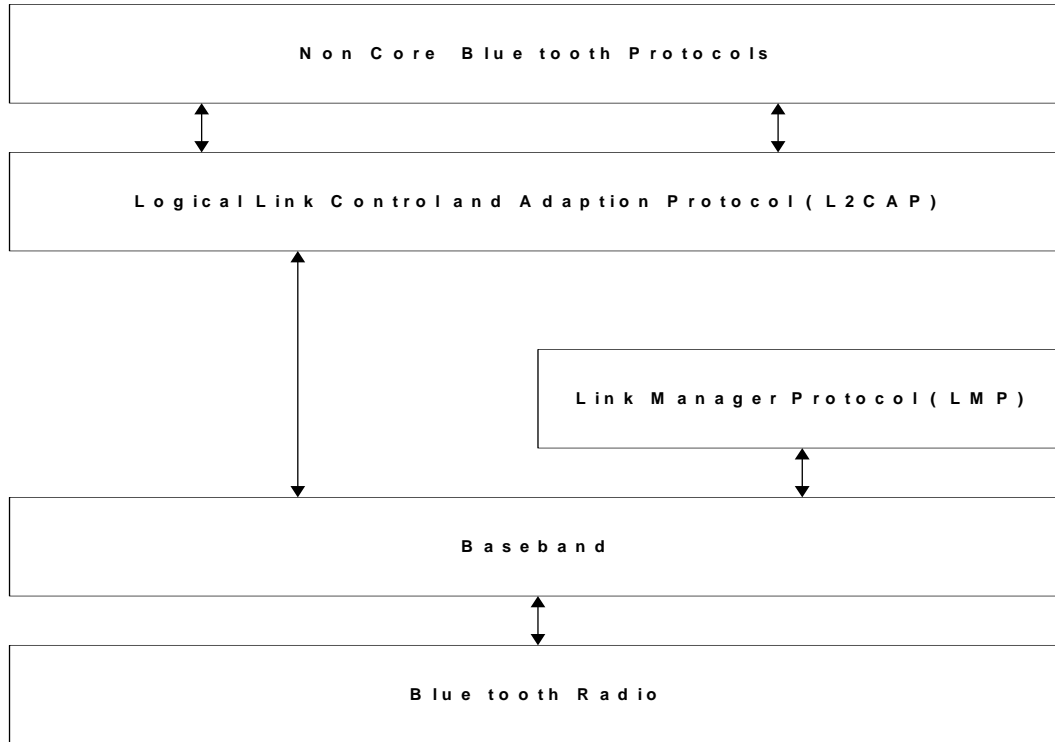
Blue tooth is designed to operate in an environment of many users. Up to eight devices can communicate in a small network called a *piconet*. A *piconet* consists of a master and from one to seven active slave devices. The radio designated as the master makes the determination of the channel that shall be used by all devices on this *piconet*.

Overview of Blue tooth 4

A slave may only communicate with the master and may only communicate when granted permission by the master. A device in one *piconet* may also exist as a part of another *piconet* and may function as either a slave or master in each *piconet*. This form of overlapping is called a *scatternet*. This relationship is shown in the following figure:



What are the various components, which make up a blue tooth stack??



Can you give an explanation of each of these layers ???? Sure !!!!

Here is a description of the Blue tooth Radio layer.....

The Blue tooth radio layer is a specification that gives the basic details of radio transmission for Blue tooth devices.

It specifies the Transmission characteristics, when a blue tooth device transmits data. All blue tooth devices can be categorized into one of three possible classes. Class 1 is for long-range devices with a maximum output power of 20dbm. Class 2 is for ordinary range devices with a maximum output power of 4dbm. Class 3 is for short-range devices with a maximum output power of 0dbm. It also specifies the modulation characteristics, radio frequency tolerance level and spurious emission levels of a blue tooth transmitter.

It also specifies the Receiver characteristics in terms of sensitivity of a receiver, interference performance of a receiver, out of band blocking capability of a receiver, inter modulation characteristics of a receiver and the maximum usable level of a receiver.

The radio layer also specifies the frequencies used in a blue tooth network. Blue tooth makes use of the 2.4-Ghz band within the ISM (industrial, scientific and medical) band. In most countries, the bandwidth is sufficient to define 79-1Mhz physical channels. Power control is used to keep the devices from emitting any more RF power than necessary. The power control algorithm is implemented using the link management protocol between a master and the slaves in a piconet. Blue tooth makes use of Gaussian Frequency shift keying, with a binary one represented by a positive frequency deviation and binary zero represented by a negative frequency deviation from the center frequency. [stallings]

A description of the Blue tooth Baseband layer...

The Base band layer in a blue tooth stack specifies the following characteristics

1. Multiple access scheme in a blue tooth network : Multiple access scheme as the name suggests allows multiple devices the communicate simultaneously in a blue tooth network The selection of the multiple access scheme for ad hoc radio system is driven by the lack of coordination and the regulations in the ISM band.

Multiple access is achieved in a blue tooth network by frequency hopping. Frequency hopping in Blue tooth serves two purpose: It provides resistance to interference and multi path effects. It also provides a form of multiple access

among co-located devices in different piconets. The frequency Hopping scheme works as follows. The total bandwidth is divided into 79 physical channels, each of bandwidth 1 MHz. Frequency Hopping occurs by jumping from one physical channel to another in a pseudorandom sequence. The same hopping sequence is shared by all of the devices on a single piconet; we will refer to this as an Frequency Hopping channel. The hop rate is 1600 hops per second, so that each physical channel is occupied for a duration of .625 milliseconds. Each .625 millisecond time period is referred to as a slot, and these are numbered sequentially.[stallings]

2. Physical links: Two types of links can be established between a Master and a Slave.

Synchronous connection oriented (SCO): Allocates a fixed bandwidth between a point-to-point connection involving the master and single slave. The master maintains the SCO link by using reserved slots at regular intervals. The basic unit of reservation is two consecutive slots (one in each transmission direction). The master can support up to three simultaneous SCO links while a slave can support two or three SCO links. SCO packets are never retransmitted.

Asynchronous Connectionless (ACL): A point to multipoint link between the master and all the slaves in the piconet. In slots not reserved for SCO links, the master can exchange packets with any slave on a per-slot basis, including a slave already engaged in an SCO link. Only a single ACL link can exist. For most ACL packets, packet retransmission is applied.[stallings]

3. Packet specification: 13 different packet types are defined for the baseband layer of the Bluetooth system. All higher layers use these packets to compose higher level Protocol Data Unit's. The packets are ID, NULL, POLL, FHS, DM1; these packets are defined for both SCO and ACL links. DH1, AUX1, DM3, DH3, DM5, DH5 are defined for ACL links only. HV1, HV2, HV3, DV are defined for SCO links. [palowireless]
4. Error correction: Blue tooth includes both FEC (Forward Error correction) and packet retransmission scheme. For FEC, a 1/3-rate code and a 2/3-rate FEC code are supported. The 1/3 rate code merely uses a 3 bit repeat coding with majority decision at the recipient. With the repeat coding, extra gain is obtained due to the reduction of the instantaneous bandwidth.

As a result, inter symbol interference (ISI) introduced by the receive filtering is decreased. The 1/3 rate code is used for the packet header, and can additionally be applied on the payload of the synchronous packets on the SCO link. For the 2/3 rate FEC code, a shortened Hamming code is used. Error trapping can be applied for decoding. This code can be applied on both the payload of the synchronous packets on the SCO link and the payload of the asynchronous packets on the ACL link.

The applied FEC codes are very simple and fast in encoding and decoding applications, which is requirement because of the limited processing time between the receiver and the transmitter. On the ACL link, an ARQ scheme can be applied. In this scheme, a packet retransmission is carried out i.e the reception of

the packet is not acknowledged. Each pay load contains a CRC to check out errors. Several ARQ schemes have been considered.[Haartsen]

- Blue tooth Security : The blue tooth base band specification defines a facility for link security between any two blue tooth devices, consisting of the following elements: Authentication, Encryption, Key management and usage.

The security algorithms make use of four parameters

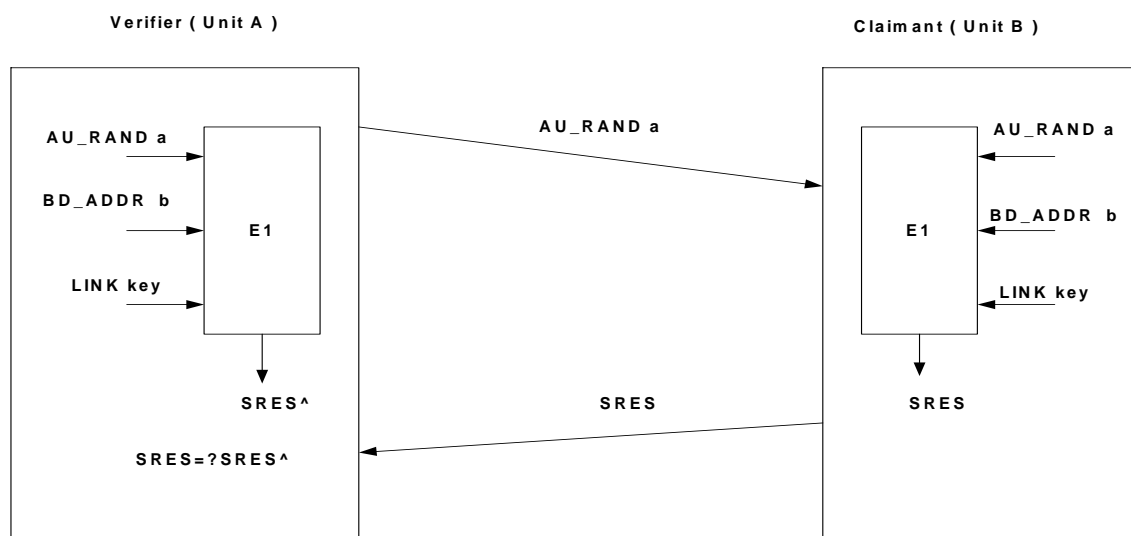
Unit Address : The 48-bit device address, which is publicly known.

Secret authentication key : A secret 128-bit key

Secret Privacy key: A secret key of length from 4 to 128 bits

Random number: A 128-bit random number derived from a pseudorandom generation algorithm executed in the bluetooth unit.

The two secret keys are generated and configured with the unit and not disclosed. The purpose of authentication is to verify the claimed identity of one of the two blue tooth devices involved in an exchange. The following picture shows the procedure in which unit A is authenticating unit B



Authentication is performed by verifying that the two devices share the same preconfigured authentication key. To begin, A generates a random number AU_RAND a and transmits this value to B. Both sides use the authentication algorithm E1 to generate a 32-bit signed response SRES. E1 takes as input the value AU_RAND a, the 48 –bit device address of B, and the shared secret key, and produce a 128-bit output; 32 bits of this output form SRES. The algorithm E1 is based on the encryption algorithm SAFER, and generates a message authentication code (MAC), which is a hash code of the input based on the secret key. After B has generated SRES, it returns this value to A. A compares the incoming value of SRES with the value that it has generated. If the two match B is authenticated. The above picture shows authentication in one direction only. Mutual authentication is achieved by performing the same exchange with B initiating the challenge.[stallings]

6. Channel control: Bluetooth controller operates in two major states: **Standby** and **Connection** . There are seven substates which are used to add slaves or make connections in the piconet. These are **page, page scan, inquiry, inquiry scan, master response, slave response and inquiry response** .

The **Standby** state is the default low power state in the Bluetooth unit. Only the native clock is running and there is no interaction with any device whatsoever. In the **Connection** state, the master and slave can exchange packet , using the channel (master) access code and the master Bluetooth clock. The hopping scheme used is the channel hopping scheme. [palowireless]

The sub states are briefly explained below

Page : Device has issued a page. Used by the master to activate and connect a slave. Master sends page message by transmitting slave's device access code (DAC) in different hop channels.

Page scan : Device is listening for a page with its own DAC.

Master Response: A device acting as a master receives a page response from a slave. The device acting as a master receives a page response from a slave. The device can now enter the connection state or return to the page state to page for other slaves.

Slave Response: A device acting as a slave responds to a page from a master. If connection setup succeeds, the device enters the connection state; otherwise it returns to the page scan state.

Inquiry: Device has issued an inquiry, to find the identity of the devices within range.

Inquiry scan: Device is listening for an inquiry.

Inquiry response: A device that has issued an inquiry receives an inquiry response.[stallings]

A description of the Blue tooth Link manager specifications layer...

The Link Manager carries out link setup, authentication, link configuration and other protocols. It discovers other remote LM's and communicates with them via the Link Manager Protocol (LMP). [palowireless]The protocol involves the exchange of message in the form of LMP protocol data units between the LMP entities in the master and slave. Messages are always sent as single slot packets with a 1 byte payload header that identifies the message type and a payload body that contains additional information pertinent to the message.[stallings]

LMP supports various security services with mechanisms for managing authentication, encryption and key distribution. These services include the following Authentication, Pairing, Change link key, change current link key and Encryption.

A description of the Blue tooth Logical Link Control and Adaptation protocol (L2CAP)....

The Bluetooth logical link control and adaptation protocol (L2CAP) [3] adapts upper layer protocols over the baseband. It can be thought to work in parallel with LMP in difference that L2CAP provides services to the upper layer when the payload data is never sent at LMP messages.

L2CAP provides connection-oriented and connectionless data services to the upper layer protocols with protocol multiplexing capability, segmentation and reassembly operation, and group abstractions. L2CAP permits higher level protocols and applications to transmit and receive L2CAP data packets up to 64 kilobytes in length.

Although the Baseband protocol provides the SCO and ACL link types,

L2CAP is defined only for ACL links and no support for SCO links is specified in Bluetooth Specification 1.0. [Mettala]

L2CAP provides three types of logical channels:

Connectionless: Supports the connectionless service. Each channel is unidirectional. This channel type is typically used for broadcast from the master to multiple slaves.

Connection-oriented: Supports the connection-oriented service. Each channel is bi-directional (full duplex).A quality of service flow specification is assigned in each direction.

Signaling: Provides for the exchange of signaling messages between L2CAP entities.

[stallings]

Non-protocol features of Blue tooth.....

Some applications which make use of the bluetooth network.....

File transfer, Internet bridge, LAN access, Three-in –one phone, wireless head set etc ... are some of the applications which make use of Blue tooth.

Power management in blue tooth networks.....

In the blue tooth design, special attention has been paid to reduction of current consumption. In the idle mode, the unit only scans a little over 10ms every T_s , where T can range from 1.28 to 3.84 second. Thus, the duty cycle is well below 1 percent.

Additionally a PARK mode has been defined where the duty cycle can be reduced even more.

However, the PARK mode can only be applied after the piconet has been established.

The slave can then be parked; that is, it only listens to the channel at a very low duty cycle.

The slave only has to listen to the channel at a very low duty cycle. The slave only has to listen to the access code and the packet header (126 micro seconds excluding guard time to account for drift) to resynchronize its clock and decide whether it can return to sleep.

Since there is no uncertainty in time and frequency (the parked slave is located to the master, similar to how cordless and cellular phones are locked to their base stations), a much lower duty cycle is achievable. Another low power mode during connection is the SNIFF mode, in which the slave does not scan at every master slave slot, but has a larger interval between scans.

In the connection state, current consumption is minimized and wasteful interference prevented by only transmitting when data is available. If no useful information needs to be exchanged, no transmission takes place. If only link control information needs to be transferred (ex: ACK/NACK), a null packet without payload is sent.

In longer periods of silence, the master once in a while needs to send a packet on the channel such that all slaves can resynchronize their clocks and compensate for drift.

[Haartsen.]

Short comings of the blue tooth standard.....

The problems with managing mobile devices relate to the basics of network management: fault, configuration, inventory control, performance and security management. Some of these issues are special problems for Bluetooth. The problems you solve in the wired world will be multiplied by the proliferation of Bluetooth devices and users.

Security: Security is a stubborn problem. Bluetooth's discovery protocol lets devices automatically find and start interacting with each other, unintentionally exposing access and data to unauthorized users. Network managers must plan for users toting around instant access to their corporate networks wherever they travel.

The security scheme for authorizing communications between two Bluetooth devices (say, a PDA and a network hub) is weak. The Bluetooth spec provides for 4-digit PIN codes to be used for authentication. A 4-digit code allows for only 10,000 different possibilities. Add to this the propensity of users to adopt simple PIN codes (0000, 1111, 2222, 3333, and so on), and you see that the trustworthiness of a 4-digit code is low. A sophisticated intruder could quickly and unobtrusively spoof it. If this basic authentication is broken while the user is traveling with a Bluetooth device that contains sensitive data or, for that matter, provides access to voice services, the risk of a significant security breach is high.

Device conflict: Bluetooth operates in the same range as wireless LANs based on the IEEE 802.11b standard and microwave ovens. Devices can easily conflict. (Ironically, Bluetooth doesn't let users roam through different zones and stay connected.) This is an issue of interference and interoperability. Bluetooth is in a radio-frequency band reserved for use by industrial, scientific and medical devices (ISM). A number of common devices (garage-door openers and some cordless phones, for example) use this same band. And other networking specs (HomeRF and 802.11b) operate here, too. The Bluetooth spec was designed to avoid conflict with other devices using a technique called spread-spectrum frequency hopping. However, today Bluetooth is seriously compromised by a

lack of standard feature implementation. Because manufacturers have implemented certain Bluetooth capabilities differently, devices of different brands often can't communicate with each other. This leads to a number of problems, not the least of which is failure to negotiate spectrum use between devices from different manufacturers.

Potentially high-support costs: It is estimated that support costs for mobile users are 40% higher than those for desktop users.[Thurmond]

future of the blue tooth standard.....

In the future, Bluetooth is likely to be standard in tens of millions of mobile phones, PCs, laptops and a whole range of other electronic devices. As a result, the market is going to demand new innovative applications, value-added services, end-to-end solutions and much more. The possibilities opened up really are limitless, and because the radio frequency used is globally available, Bluetooth can offer fast and secure access to wireless connectivity all over the world. With potential like that, it's no wonder that Bluetooth is set to become the fastest adopted technology in history. [nokia]

Conclusion

Blue tooth is a very promising standard for ad –hoc short range networking. It work is a complimentary fashion with the current existing wireless LAN standards like 802.11 a, b etc. Blue tooth has a robust technological back ground and can support a number of applications. It has a excellent power management technology. Blue tooth has a very bright future in the future world of wireless networking.

References

Haartsen, Jaap. The Blue tooth Radio System. Ericsson Radio Systems, 2000.

Mettala, Riku. Blue tooth Protocol architecture version 1.0. Nokia Mobile Phones, 1999.

Nokia. What is Blue tooth. Retrieved April 22 2004 from the World Wide Web:
<http://www.nokia.com/bluetooth/whatis.html>

PaloWireless. Blue tooth tutorial – specifications. Retrieved April 22 2004 from the World Wide Web: <http://www.palowireless.com/infotooth/tutorial.asp>

Stallings William, Wireless Communications and Networks , Prentice Hall, New Jersey, 2002

Thurmond, Bob. (2002). 2001 Blue tooth Reigns ?. Retrieved April 22 2004 from the World Wide Web:
http://www.wsta.org/publications/articles/0601_article01.html