Bluetooth

Bluetooth is a standard for short range, low power, low cost wireless communication that uses radio technology. Although originally envisioned as a cable-replacement technology. Bluetooth technology can be used at home, in the office, in the car, etc. This technology allows to the users instantaneous connections of voice and information between several devices in real time. The way of transmission used assures protection against interferences and safety in the sending of information.

The Bluetooth is a small microchip that operates in a band of available frequency throughout the world. Communications can realize point to point and pointmultipoint. The standard Bluetooth operates in the band of 2,4 GHz. Though worldwide, this band is available, the width of the band can differ in different countries. This is the frequency of band of the scientific and medical industries 2.45 GHz (ISM*). The ranges of the bandwidth in The United States and Europe are between 2.400 to 2.483,5 MHz and it covers part of France and Spain. The ranges of the bandwidth in Japan are between 2.471 to 2.497 MHz.

User scenarios

Many different user scenarios can be imagined for wireless piconets or WPANs:

- Connection of peripheral devices: Most of the devices are connected to a desktop computer via wires (e.g., keyboard, mouse, joystick, headset, speakers).This type of connection has several disadvantages: each device has its own type of cable, different plugs are needed, and wires block office space. In a wireless network, no wires are needed for data transmission. However, batteries now have to replace the power supply, as the wires not only transfer data but also supply the peripheral devices with power.
- Support of ad-hoc networking: Imagine several people coming together,

Wireless networks can support interactive exchange of data as a group. Small devices might not have WLAN adapters following the IEEE 802.11 standard, but cheaper Bluetooth chips built in.

- Bridging of networks: Using wireless piconets, a mobile phone can be connected to a PDA or laptop in a simple way. Mobile phones will not have full WLAN adapters built in, but could have a Bluetooth chip. The mobile phone can then act as a bridge between the local piconet and, e.g., the global GSM network.

ARCHITECTURE OVERVIEW

Bluetooth link control hardware, integrated as either one chip or a radio module and a baseband module, implements the RF, baseband, and link manager portions of the Bluetooth specification. This hardware handles radio transmission and reception as well asrequired digital signal processing for the baseband protocol. Its functions include establishing

connections, support for asynchronous (data) and synchronous (voice) links, error correction, and authentication. The link manager firmware provided with the

baseband CPU performs low-level device discovery, link setup, authentication, and link configuration.

Bluetooth operates on 79 channels in the 2.4 GHz band with 1 MHz carrier spacing. Eachdevice performs frequency hopping with1,600 hops/s in a pseudo random fashion. A piconet is a collection of Bluetooth devices which are synchronized to the same hopping sequence. One device in the piconet can act as master (M), all other devices connected to the master must act as slaves (S).

The master determines the hopping pattern in the piconet and the slaves have to synchronize to this pattern. Each piconet has a unique hopping pattern. If a device wants toparticipate it has to synchronize to this. Two additional types of devices are shown: parked devices (P) cannot actively participate in the piconet (i.e., they do not have a connection), but are known and can be reactivated within some milliseconds.

Devices in stand-by (SB) do not participate in the piconet. Each piconet has exactly one master and up to seven simultaneous slaves. More than 200 devices can be parked. The reason for the upper limit of eight active devices is the 3-bitaddress used in Bluetooth. If a parked device wants to communicate and there are already seven active slaves, one slave has to switch to park mode to allow the parked device to switch to active mode.

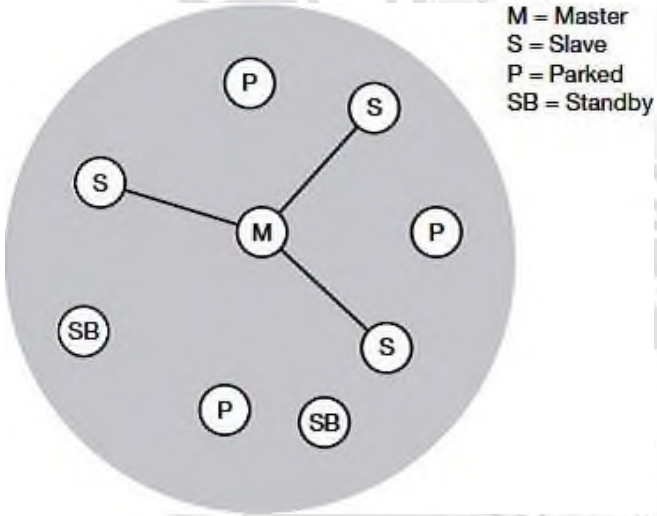

Fig. 1.25 Bluetooth piconet

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

The Piconet are several devices that are in the same radio of coverage where they share the same channel and that is constituted between two and eight of these units. Every device has the unique direction of 48 bits, based on the standard IEEE 802.11 for WLAN, whereas the Scatternet formed by the connection of a Piconet to other one, with a maximum of interconnections of ten Piconets.

As all active devices have to use the same hopping sequence they must be synchronized. The first step involves a master sending its clock and device ID. All Bluetooth devices have the same networking capabilities, i.e., they can be master or slave. There is no distinction between terminals and base stations, any two or more devices can forma piconet.

The unit establishing the piconet automatically becomes the master, all other devices will be slaves. The phase in the hopping pattern is determined by the master‘s clock. After adjusting the internal clock according to the master a device may participate in the piconet. All active devices are assigned a3-bit active member address (AMA). All parked devices use an 8-bit parked member address (PMA). Devices in stand-by do not need an address.

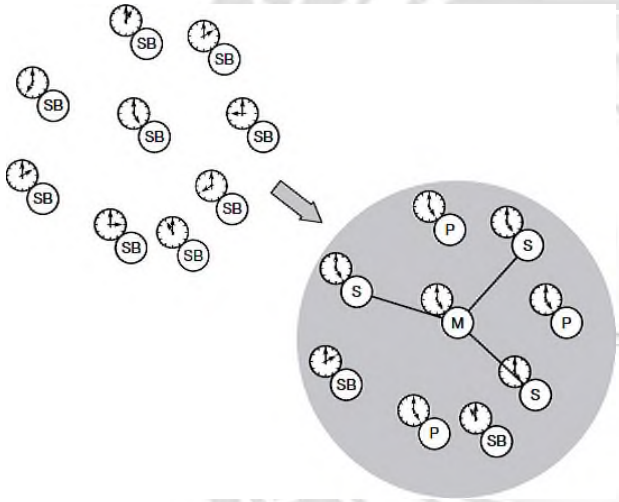

Fig. 1.26 Forming a Bluetooth piconet

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

All users within one piconet have the same hopping sequence and share the same 1 MHz channel. As more users join the piconet, the throughput per user drops quickly (a single piconet offers less than 1 Mbit/s gross data rate).This led to the idea of forming groups of piconets called scatternet. If a device wants to participate in more than one piconet, it has to synchronize to the hopping sequence of the piconet it wants to take part in.

If a device acts as slave in one piconet, it simply starts to synchronize with the hopping sequence of the piconet it wants to join. After synchronization, it acts as a slave in this piconet and no longer participates in its former piconet. To enable synchronization, a slave has to know the identity of the master that determines the hopping sequence of a piconet. Before leaving one piconet, a slave informs the current master that it will be unavailable for a certain amount of time. There maining devices in the piconet continue to communicate as usual.

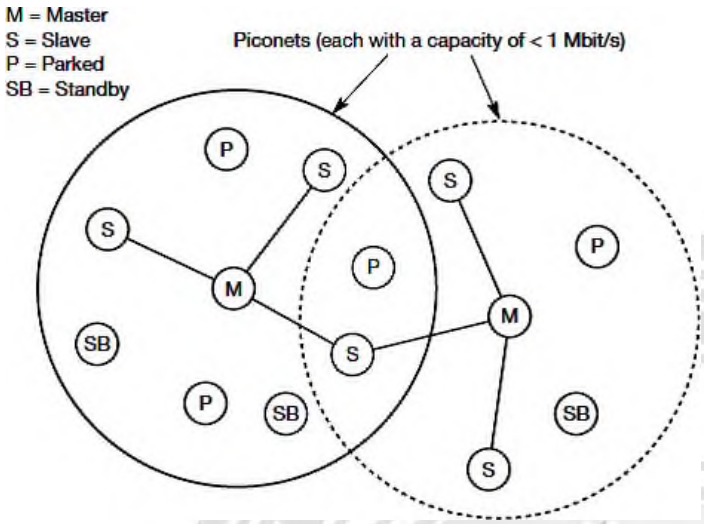

Fig. 1.27 Bluetooth scatternet

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

Protocols Stack

The protocol architecture of the Bluetooth consists of following in a Bluetooth protocol stack:

- Core protocols consisting 5 layer protocol stack viz. radio, baseband, link managerprotocol, logical link control and adaptation protocol, service discovery protocol.
- Cable replacement protocol, RFCOMM
- Telephony Control Protocols
- Adopted protocols viz. PPP,TCP/UDP/IP,OBEX and WAE/WAPCore protocols

Radio: This protocol specification defines air interface, frequency bands, frequency hopping specifications, modulation technique used and transmits power classes. Baseband: Addressing scheme, packet frame format, timing and power control algorithms rquired for establishing connection between Bluetooth devices within piconet defined in this part of protocol specification.

Link Manager Protocol: It is responsible to establish link between Bluetooth devices and to maintain the link between them. This protocol also includes authentication and encryption specifications. Negotiation of packet sizes between devices can be taken care by this.
Logical link control and adaptation protocol: This L2CAP protocol adapts upper layer frame to baseband layer frame format and vice versa. L2CAP take care of both connections oriented and connectionless services.
Service discovery protocol: Service related queries including device information can be taken care at this protocol so that connection can be established between Bluetoothdevices.

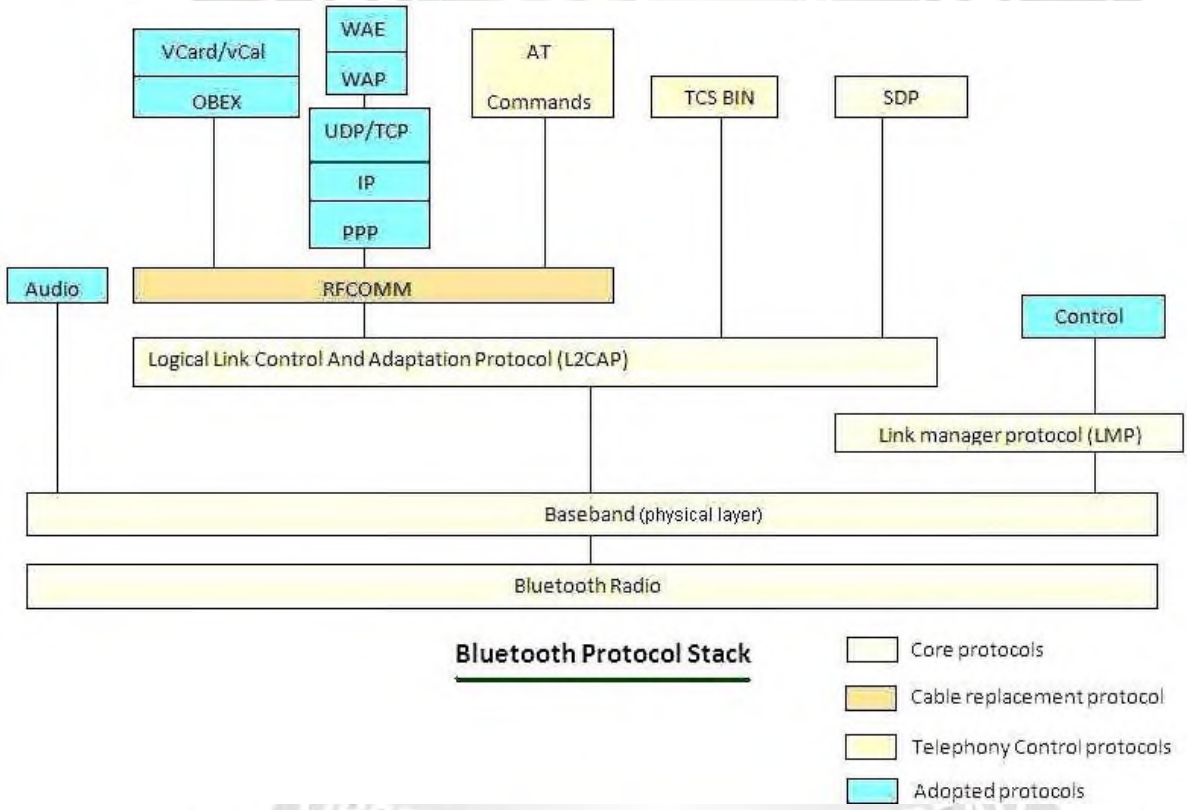

Fig.1.28 Bluetooth Protocol Stack

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

Radio Layer

• The Bluetooth radio layer corresponds to the physical layer of OSI model. It deals with radio transmission and modulation. The radio layer moves data from master to slave or vice versa. It is a low power system that uses 2.4 GHz ISM band in a range of 10 meters.

• This band is divided into 79 channels of 1MHz each. Bluetooth uses the Frequency Hopping Spread Spectrum (FHSS) method in the physical layer to avoid interference from other devices or networks.

The radio specification defines the carrier frequencies and output power. Bluetooth devices will be integrated into typical mobile devices and rely on battery power. This requires small, low power chips which can be built into handheld devices. The combined use for data and voice transmission has to be reflected in the design, i.e., Bluetooth has to support multi-media data.

Bluetooth uses the license-free frequency band at 2.4 GHz allowing for worldwide operation with some minor adaptations to national restrictions. A frequency-hopping/time- division duplex scheme is used for transmission, with a fast hopping rate of 1,600 hops per second. The time between two hops is called a slot, which is an interval of 625 μs. Each slot uses a different frequency. In order to change bits into a signal, it uses a FSK with Gaussian bandwidth filtering.

Bluetooth transceivers use Gaussian FSK for modulation and are available inthree classes:

- Power class 1: Maximum power is 100 mW and minimum is 1 mW (typ. 100 m range without obstacles). Power control is mandatory.
- Power class 2: Maximum power is 2.5 mW, nominal power is 1 mW, and minimumpower is 0.25 mW (typ. 10 m range without obstacles). Power control is optional.
- Power class 3: Maximum power is 1 mW.

Baseband Layer

Baseband layer is equivalent to the MAC sublayer in LANs.

The baseband layer controls transmission of frames in association with frequency hopping. Master and slave stations communicate with each other using time slots. The master in a piconet takes the channel to transmit in even-numbered hops, and slaves transmit in odd-numbered hops, reflecting a time-division duplex for all devices in apiconet.

A single frame can be transmitted in the duration of one, three, or five hops. Depending on the nature of the logical link between a slave and the master, two types of links are offered. Bluetooth uses a form of TDMA called TDD-TDMA (time division duplex TDMA).The master in each piconet defines the time slot of 625 μsec.

In TDD- TDMA, communication is half duplex in which receiver can send and receive data but not at the same time. If the piconet has only no slave; the master uses even numbered slots (0, 2, 4, ...) and the slave uses odd-numbered slots (1, 3, 5,). Both master and slave communicate in half duplex mode. In slot 0, master sends & secondary receives; in slot 1, secondary sends and primary receives. If piconet has more than one slave, the master uses even numbered slots. The slave sends in the next odd-numbered slotif the packet in the previous slot was addressed to it.

The baseband layer has defined some types of frames that correspond to various purposes of the baseband frames. Different types of frames can carry different sizes of payload data and error-correction schemes. In particular, the access code field in a baseband frame indicates the purpose of the frame in a special state. For example, a frame with the inquiry access code (IAC) will be sent when a device elects to scan for other devices within the radio range in a series of 32 frequency hops.

Bluetooth devices can be configured to periodically hop according to the inquiry scan hopping sequence to scan inquires. When an inquiry is detected, the device, now the slave, will reply with its address and timing information to the master, and then the master and the slave begin the paging process to determine a common hopping sequence to establish a connection. Eventually, both the master and the slave will hop on the same sequence of channels for the duration of the connection.

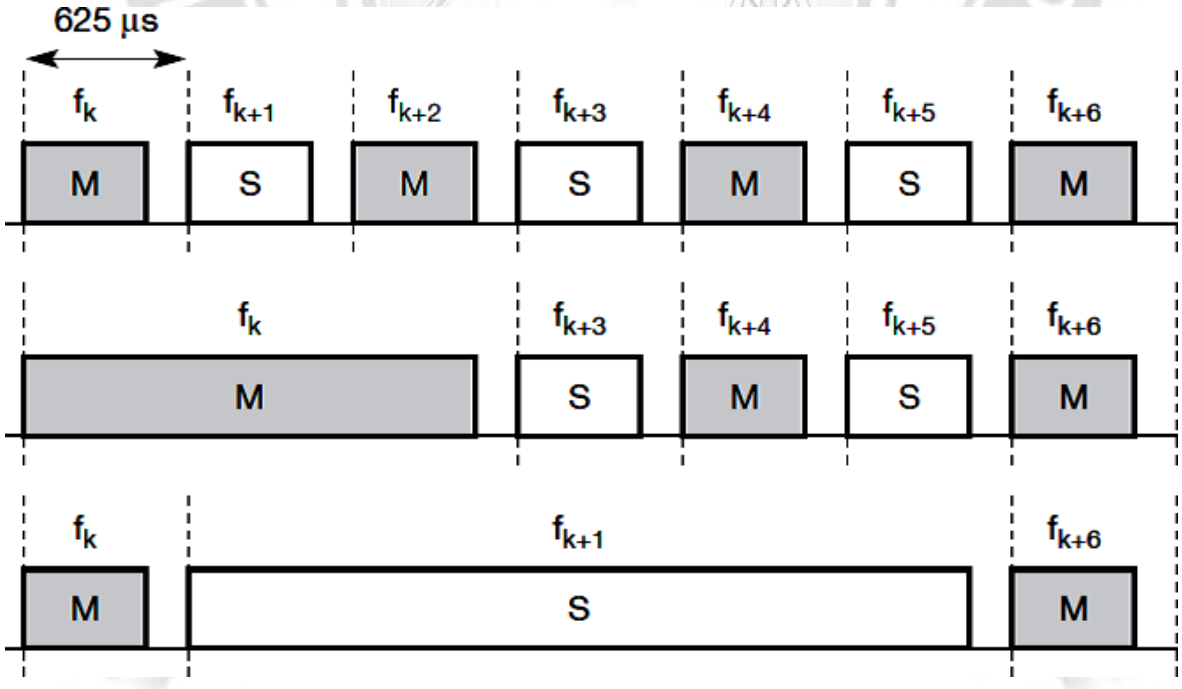

Fig. 1.29 Frequency selection during data transmission using 1, 3, 5 packet slots

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

Link manager protocol

The Link Manager (LM) translates the commands into operations at the Baseband level, managing the following operations.

1) Attaching slaves to piconets, and allocating their active member addresses.
2) Breaking connections to detach Slaves from a piconet.
3) Configuring the link including Master/Slave switches
4) Establishing ACL and SCO links.
5) Putting connections into Low Power modes: Hold, Sniff and Park.
6) Controlling test modes.

A bluetooth Link Manager communicates with Link Managers on other Bluetooth devices using the Link Management protocol (LMP).

The link can be configured at any time, including at mode changes, quality of service changes, packet type changes and any power level changes. Finally, information about an active link can be retrieved at any time. When the connection is no longer required, LMP can cause disconnection.

The link manager protocol (LMP) manages various aspects of the radio link between a master and a slave and the current parameter setting of the devices. LMP enhances baseband functionality, but higher layers can still directly access the baseband. The following groups of functions are covered by the LMP:

• Authentication, pairing, and encryption: Although basic authentication is handled in the baseband, LMP has to control the exchange of random numbers and signed responses. The pairing service is needed to establish an initial trust relationship between two devices that have never communicated before.

The result of pairing is a link key. This may be changed, accepted or rejected. LMP is not directly involved in the encryption process, but sets the encryption mode (no encryption, point-to-point, or broadcast), key size, and random speed.

• Synchronization: Precise synchronization is of major importance within a Bluetooth network. The clock offset is updated each time a packet is received from the master. Additionally, special synchronization packets can be received. Devices can also exchange timing information related to the time differences (slot boundaries) between two adjacent piconets.

• Capability negotiation: Not only the version of the LMP can be exchanged but also information about the supported features. Not all Bluetoothdevices will support all features that are described in the standard, so devices have to agree the usage of, e.g., multi-slot packets, encryption, SCO links, voice encoding, park/sniff/hold mode, HV2/HV3packets etc.

• Quality of service negotiation: Different parameters control the QoS of a Bluetooth device at these lower layers. The poll interval, i.e., the maximum time between transmissions from a master to a particular slave, controls the latency and transfer capacity.Depending on the quality of the channel, DMor DH packets may be used (i.e., 2/3 FEC protection or no protection). The number of repetitions for broadcast packets can be controlled. A master can also limit the number of slots available for slaves‘ answers to increase its own bandwidth.

• Power control: A Bluetooth device can measure the received signal strength. Dependingon this signal level the device can direct the sender of the measured signal to increase or decrease its transmitting power.