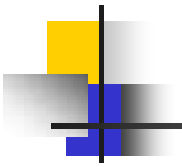
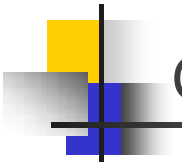


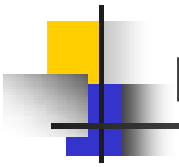
S-72.333 Postgraduate Course in Radio Communications
Spring 2004

Overview of Bluetooth

Mervi Berner 23.03.2004
mervi.berner@iki.fi

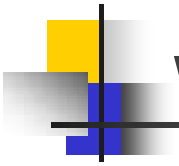


Contents



Bluetooth Overview

- short-range connectivity solution for personal, portable, and handheld devices
- asynchronous data flows and synchronous audio streams over links (1 Mb/s)
- operates in the 2.4 GHz ISM band utilizing low transmit power radios (0 dBm), using a frequency-hopping spread-spectrum technique
- an open industry specification, an ongoing process steered/ developed by the promoters of the Bluetooth SIG since May 1998
- provided license-free to the adopter members of the technology
- specification incl. protocols and application scenarios, and a qualification program designed to assure end-user value for Bluetooth products
- can interact with other devices and behave when executing any application conformant to the Bluetooth profiles



Why Bluetooth?

- advantages over other data transfer technologies, e.g. IrDA, HomeRF
- designed to be low cost ($10/unit)
- limited connection distance and transmission speeds: Bluetooth supports 780 kb/s; 721 kb/s unidirectional data transfer (57.6 kb/s return direction) or up to 432.6 kb/s symmetric data transfer
- ability to simultaneously handle both data and voice transmissions
- ad hoc device connection and automatic service discovery
- adequate e.g. for file transfer/printing applications, mobile Hands free headset for voice calls, and automatically synchronizing PDA, laptop, and cell phone address book applications

The History of the Bluetooth Wireless Technology

- invented in 1994 by L. M. Ericsson
- named after *Harald Blåtand* "Bluetooth" II, king of Denmark 940- 981A.D.
- Bluetooth SIG (Special Industry Group)
1998: Ericsson, IBM, Intel, Nokia, and Toshiba
1999: 3Com, Lucent (2001 Agere), Microsoft, and Motorola
app. 3000 adopter members (Dec.2001) have joined the SIG
- 1999: Bluetooth specification version 1.0A
- Bluetooth SIG license agreement: open 'short range wireless communication' specification, adopter members can look at the specification prior to its public availabity
- Bluetooth qualification program (BQP) incl. radio, protocol, and profile (when applicable) conformance testing, interoperability
- 1999 IEEE 802.15 standards working group, communication standards for WPANs (wireless personal area networks). Bluetooth specification chosen as baseline of the 802.15.1 standard (other IEEE group studies 802.15.2-4)

The Bluetooth Piconet

A group of Bluetooth devices (2-8) that can communicate with each other.
- formed in ad hoc manner
- a single ***master***, 1-7 ***slaves*** (the Bluetooth radio may serve either as master or slave)
- ***parked***, additional devices, may be registered with the master and be invited to become active whenever necessary, ***stand-by*** mode, Bluetooth devices not associated with any piconet
- to identify each slave, the master assigns a locally unique active member address (AM_ADDR) to the slaves. The master regulates and controls who transmits and when.
- ***scatternet***, a single device may be a member of several piconets

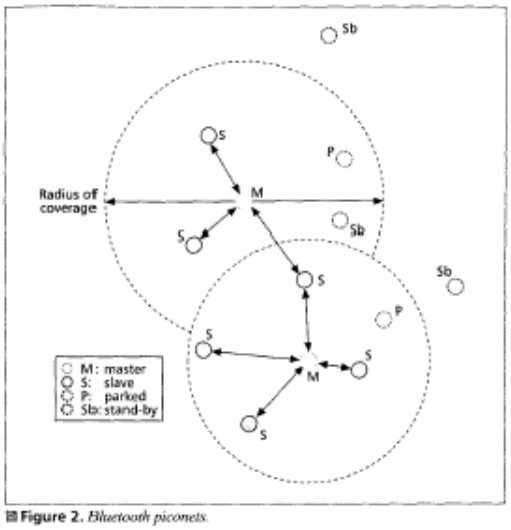


Figure 2. *Bluetooth piconets.*

Piconets may be static or formed dynamically

Communication in a piconet

To engage in communication in a piconet

- the master needs to know the identitities of the slaves
- the slaves need to know the BD_ADDR and Bluetooth clock of the master

This information is acquired in two phases:

- the **inquiry** phase, for locating devices
- the **paging** phase, for inviting specific devices to join a piconet

Three lower power slave states: ***sniff***, ***hold***, **and** ***park***.

Bluetooth specification and protocol stack

Bluetooth Specification version 1.1.

- *core specification*: defines the radio characteristics and the communication protocols for exchanging data between devices over Bluetooth radio links
- *profile specification*: defines how the Bluetooth protocols are to be used to realize a number of selected applications

Transport and Middleware Protocols

- transport protocols: developed exclusively for Bluetooth, protocols are involved in all data communications between Bluetooth devices
- middleware protocols: both Bluetooth-specific protocols and other adopted protocols, used selectively to enable different applications to exchange data using Bluetooth

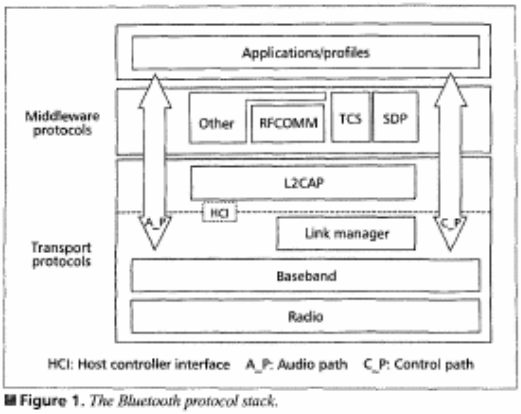


Figure 1. *The Bluetooth protocol stack.*

The Transport Protocols

The Radio
- 2.4GHz ISM band (license-free)
- fast (1,600 hops/s) FHSS technique
- modulation technique: GFSK
- baud rate: 1Msymbol/s
- three power classes depending on their transmit power: Class1: 20dBm (100mW), Class2: 4dBm (2.5mW), Class3: 0dBm (1mW)

The Baseband – key procedures that enable devices to communicate with each other using Bluetooth
Defines: the Bluetooth piconets, how they are created; Bluetooth links; how the transmit resources are to be shared among several devices in a piconet; low-level packet types

The Bluetooth Address and Clock
Bluetooth devices can communicate with each other by acquiring each other's Bluetooth addresses and clocks.

Parameters involved Bluetooth communications:
- unique IEEE-type 48-bit address assigned to each Bluetooth radio at manufacture time. The BD_ADDR (Bluetooth device address) is engraved on the Bluetooth HW and it cannot be modified.
- free-running 28-bit clock that ticks every 312.5μs, which corresponds to half the residence time in a frequency when the radio hops at the nominal rate of 1,600 hops/s.

The Bluetooth Links and Baseband Packets

Asynchronous connectionless (ACL)
- single best-effort link appropriate for asynchronous *data* transmission
- transmissions on a per-slot basis
- point to-multipoint transfers
- after an ACL transmission from the master, only the addressed slave device may respond during the next time slot, or if no device is addressed, the packet is considered a broadcast message
- packet retransmission, FEC (forward error correction)

Synchronous connection oriented (SCO)
- Up to three links, periodic *audio* transmissions at 64kb/s in each direction
- point-to-point symmetric connections that reserve time slots to guarantee timely transmission
- the slave device is always allowed to respond during the time slot immediately following an SCO transmission from the master
- a master can support up to three SCO links to a single or multiple slaves, but a single slave can support only two SCO links to different masters
- SCO packets are never retransmitted, FEC mechanisms to recover from transmission errors

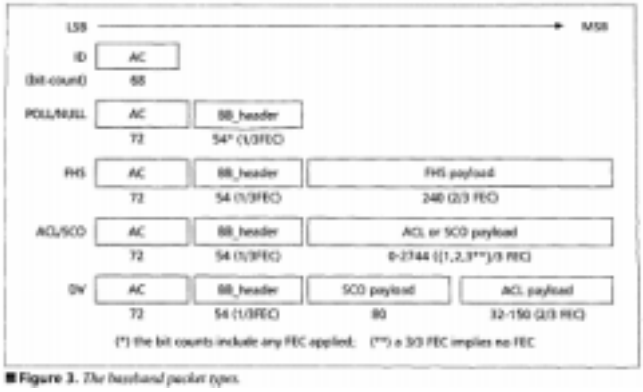
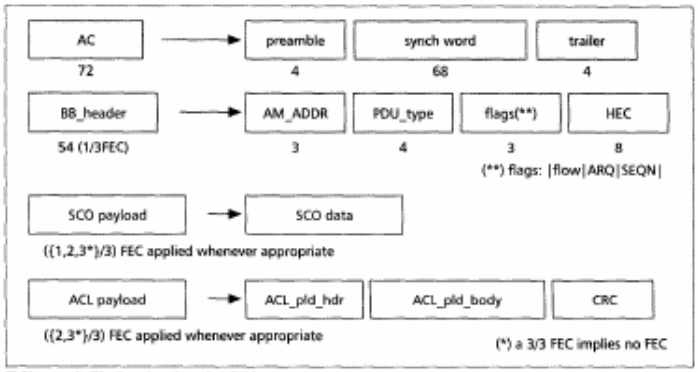
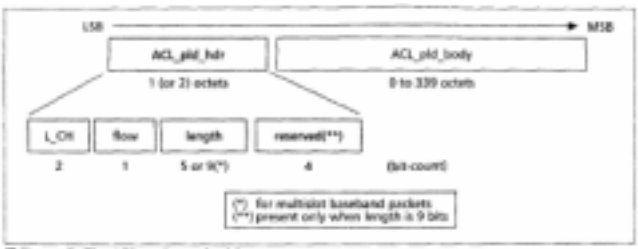


Figure 3. *The baseband packet types.*

Header and the payload of a baseband packet



■ **Figure 4.** *The baseband packet fields.*



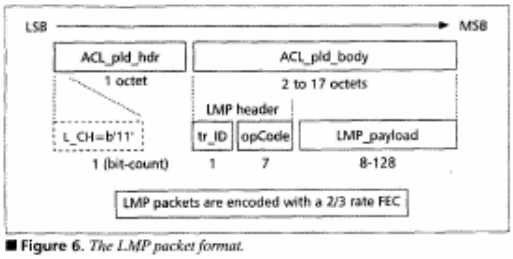
■ **Figure 5.** *The ACL packet payload format.*

The Link Manager Protocol

Link control HW: handles link setup, security (authentication: *Challenge Response mechanism*), and control (quality of service monitoring, baseband state control).

Link manager: controls paging, changing slave modes, handling required changes in master/slave roles, supervises the link and controls handling of multislot packets. Link managers communicate with each other using the *Link Management Protocol* (LMP), which uses the underlying baseband services. LMP packets are sent in the ACL payload. They are differentiated from logical link control and adaptation protocol (L2CAP) packets by a bit in the ACL header. They are always sent as single-slot packets and have higher priority than L2CAP packets.

Two link managers may learn each other's features, e.g. whether the devices support SCO link, what size of packet transmission do they support, or whether they support any of the low power consumption modes. SCO connections are established using LMP transactions; polling intervals and agreed upon packet sizes are also set up through LMP transactions.



■ **Figure 6.** *The LMP packet format.*

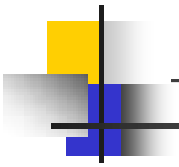
The Host Controller Interface (HCI)

- an interface for host devices to access the lower layers of the Bluetooth stack through a standardized interface.
- through the HCI:
  - a host device passes and receives data destined to or coming from another Bluetooth device
  - a host may instruct its baseband to create a link to a specific Bluetooth device, execute inquiries, request authentication, pass a link key to the baseband, request activation of a lower power mode, etc.
- link controller HW may include an HCI layer above the link manager
  - used to isolate the Bluetooth baseband and link manager from a transport protocol such as USB or RS-232 (-> a standard host processor interface to Bluetooth HW).
- an HCI driver on the host is used to interface a Bluetooth application with the transport protocol. Currently three transport mechanisms are supported: USB, RS-232, and UART.
- using HCI, a Bluetooth application can access Bluetooth HW without knowledge of the transport layer or other HW implementation details.

Middleware Protocols

The Logical Link Control and Adaptation Protocol (L2CAP)

- interface to the link controller, allows for interoperability between Bluetooth devices
- provides protocol multiplexing, which allows support for many third-party upper level protocols such as TCP/IP and group management mapping upper protocol groups to Bluetooth piconets, segmentation and reassembly of packets between layers, and negotiation and monitoring quality of service between devices
- operates over an ACL link provided by the baseband. A single ACL link, set up by the link manager using LMP, is always available between the master and any active slave. This provides a point-to-multipoint link supporting both asynchronous and isochronous data transfer. L2CAP packets can be much larger that the baseband packets and they may need to be segmented prior to transmission over the air, and reassembled following the receipt.
- Three types of L2CAP channels exist: ***bidirectional signaling channels*** that carry commands; ***connection-oriented channels*** for bidirectional point to-point connections; and ***unidirectional connectionless channels*** that support point-to multipoint connections, allowing a local L2CAP entity to be connected to a group of remote devices.
- Every L2CAP channel includes two endpoints referred to by a (two-octet) logical **channel identifier (CID)**.

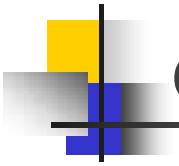


The Logical Link Control and Adaptation Protocol (L2CAP)

A **bi-directional signaling channel** is required between any two L2CAP entities before communication can take place. Every L2CAP entity will have one signaling channel endpoint with a reserved CID of 0x0001. All signal channels between the local L2CAP entity and any remote entities use this one endpoint.

Each **connection-oriented channel** in an L2CAP entity will have a local CID that is dynamically allocated. All connection-oriented CIDs must be connected to a single channel, and that channel must be configured before data transfer can take place. In addition, a quality of service(QoS) agreement for the channel will be established.

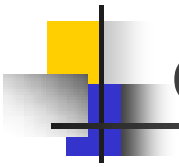
Connectionless channels are unidirectional and used to form groups. A single outgoing connectionless CID on a local device may be logically connected to multiple remote devices. The devices connected to this outgoing endpoint form a logical group. These outgoing CIDs are dynamically allocated. The incoming connectionless CID is fixed at 0x0002. Although multiple outgoing CIDs may be created to form multiple logical groups, only one incoming connectionless CID is provided on each L2CAP entity. All incoming connectionless data arrives via this endpoint. These channels do not require connection or configuration.



Other Middleware Protocols (1)

The Service Discovery Protocol (SDP)

- provides a means to determine what Bluetooth services are available on a particular device. A Bluetooth device may act as an SDP client querying services, an SDP server providing services, or both.
- two processes are supported: searching and browsing. Searching is based on UUIDs. Universally unique identifiers (UUIDs) are used to describe services and attributes of these services in a manner that may not require a central registration authority for registering services. Typically the UUIDs are 128 bits long; for known services 16-bit and 32 bit UUIDs may be used.
- packet-based protocol utilizing a request-response architecture. The SDP packet is referred to as a protocol data unit (PDU), which includes a header followed by a variable number of parameters.

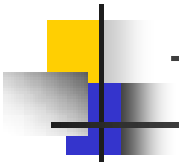


Other Middleware Protocols (2)

The RFCOMM Protocol
- used to expose a serial interface to the packet-based Bluetooth transport layers
- layer emulates the signals on the nine wires of an RS-232 interconnect cable. Based on the ETSI standard 07.10, which permits the emulation and multiplexing of several serial ports over a single transport.
- enables legacy applications that have been written to operate over serial cables to run on top of a Bluetooth link without modification. Several of the applications developed for Bluetooth use the RFCOMM as part of their implementation stack.

The Telephony Control Signalling (TCS) Protocol
- provided for voice and data call control, providing group management capabilities; connectionless TCS, which allows for signaling unrelated to an ongoing call
- Telephony control can be performed using the AT command set. Since AT commands have been designed to be passed over serial lines, Bluetooth devices use the RFCOMM to send and receive control signaling based on the AT command set.
- AT command set well established, used for supporting legacy applications (e.g. dialer application)
- control protocol TCS-AT, an additional packet-based telephony control signaling protocol TCS BIN (BIN, binary coding of information) that runs directly on top of L2CAP. Protocol supports normal telephony control functions such as placing and terminating a call, sensing ringing tones, accepting incoming calls, etc. Unlike TCS-AT, TCS-BIN supports point-to-multipoint communications.

Other Protocols
- a number of industry standards have been adopted to support various applications: PPP, OBEX, IrMC. Run on top of RFCOMM.



The Bluetooth Profiles

The specification for building interoperable applications are called **profiles**.

All profiles depend on the Generic Access Profile (GAP), which defines:

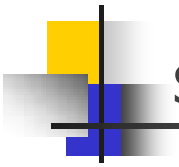
- the basic rules and conditions for connecting devices with each other and establishing Bluetooth links and L2CAP channels
- security levels and conditions necessary to establish trust relationships between devices.

Two protocol profiles:

- ***serial port profile*** defines how RFCOMM runs on top of the Bluetooth transport protocols
- ***generic object exchange profile*** defines how objects can be exchanged using the OBEX protocol running on top RFCOMM as defined in the serial port profile

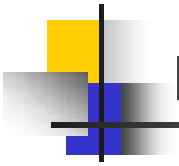
Service discovery application profile shows:

- how a service discovery application uses the service discovery protocol
- how the protocol uses the Bluetooth transports for carrying the service discovery packets between a service discovery client and a server.



SUMMARY: Bluetooth today and tomorrow

- Bluetooth movement started in May 1998, products introduced into the market at an increasing rate, but the deployment of the technology has moved slower than originally anticipated.
- the Bluetooth SIG investigates improvements in speed, security, noise immunity, and so on, and continues to develop Bluetooth profiles.
- as more and more manufacturers adopt Bluetooth and create devices that support it, developers will find new, previously unimagined ways of applying its power.
- Bluetooth is one of the key technologies that can make the mobile information society possible, blurring the boundaries between home, office, and outside world.
- 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. Many possibilities (new innovative applications, value added services, end-to-end solutions) opened, and because the radio frequency used is globally available, Bluetooth can offer fast and secure access to wireless connectivity all over the world.



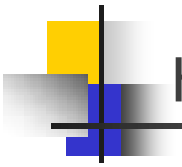
References

An overview of the Bluetooth wireless technology *Chatschik, B. IEEE Communications Magazine,* Page(s): 86-94, December 2001. [1]

Bluetooth in wireless communication *Sairam, K.V.S.S.S.S.; Gunasekaran, N.; Redd, S.R., IEEE Communications Magazine,* Page(s): 90-96, June 2002. [2]

More information available at:
https://www.bluetooth.org/ ; http://www.bluetooth.com/

Note: Acc. to the Bluetooth brand requirements, the term "Bluetooth" must always be used as an adjective. Furthermore, when the term "Bluetooth" is used to denote the corresponding technology, the term "wireless" must be inserted between Bluetooth and technology. The terminology is not followed here, the term "Bluetooth" has grown to represent both the technology and the whole industry behind it.



Homework

a) With both Infrared networks and Bluetooth, it is principally possible to bridge PAN with the wider network. What advantages does Bluetooth have in comparison with IrDA?

b) Investigate the security strengths and weaknesses of Bluetooth.

(Hint: Consult e.g. the Bluetooth security white paper at: http://www.bluetooth.com/upload/24Security_Paper.PDF.)