

Bluetooth

(or IEEE 802.15.1)



WPAN Technologies

- HomeRF
- Bluetooth



2

Bluetooth



- A cable replacement technology
- 1 Mb/s symbol rate
- Range 10+ meters
- Single chip radio+baseband
 - at low power & low price
- Why not using WLANs?
 - power
 - cost
- Why not using IrDA?
 - Line of sight
 - Short distance range (1m)



3

The Bluetooth Idea

- Bluetooth has been named after a Scandinavian king, who lived in the X century A.D., called Harald Bluetooth
- Harald Bluetooth took over several tribes which had different cultures and habits
- The aim of the Bluetooth technology is to be "universal" and suitable for any kind of environment



4

Bluetooth Working Group History

- February 1998: The Bluetooth SIG is formed
 - promoter company groups: Ericsson, IBM, Intel, Nokia, Toshiba
- May 1998: Public announcement of the Bluetooth SIG
- July 1999: 1.0A spec (>1,500 pages) is published
- December 1999: v. 1.0B is released
- December 1999: The promoter group increases to 9 members
 - 3Com, Lucent, Microsoft, Motorola
- June 2002: There are 1,900+ adopters



5

The IEEE 802.15 Working Groups

Task Group	Goal
IEEE 802.15.1	Developing a standard for short range wireless communication referred as WPAN, and based on the Bluetooth Specifications
IEEE 802.15.2	Facilitating coexistence of WPAN and WLAN. The coexistence model tries to quantify the mutual interference of the two
IEEE 802.15.3	Drafting and publishing a new standard for high-rate (20 Mbit/s or greater) WPANs
IEEE 802.15.4	Providing a standard for low data-rate wireless connectivity (LR-WPAN)



IEEE 802.15.1

- In March 2002, the IEEE 802.15.1 WG has released the first version of the standard for WPANs

- The two lower layers of the protocol stack (Physical and MAC layers) are based on the Bluetooth v1.x Specifications



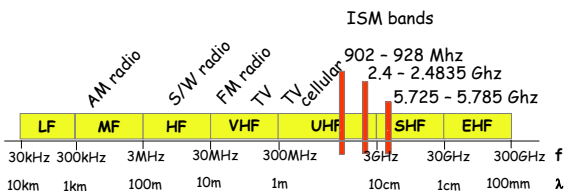
7

Basic Characteristics



8

EM Spectrum



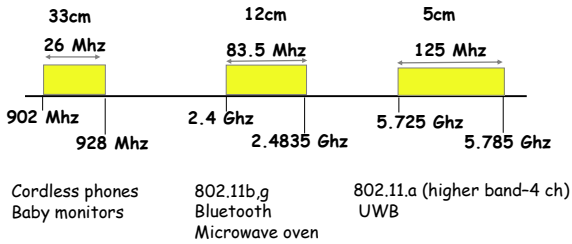
Propagation characteristics are different in each frequency band

(ISM: Industrial, Scientific and Medical)



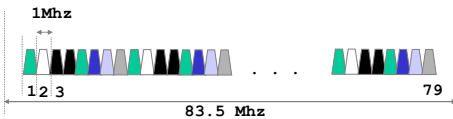
9

Unlicensed Radio Spectrum (U.S.)



10

Bluetooth Radio Link



- $2.402 \text{ GHz} + k \text{ MHz}$, $k=1, \dots, 79$
(79 channels spaced by 1 MHz)
- GFSK modulation: 1 Mb/s symbol rate
- transmit power: 0 dBm (up to 20 dBm with power control)



11

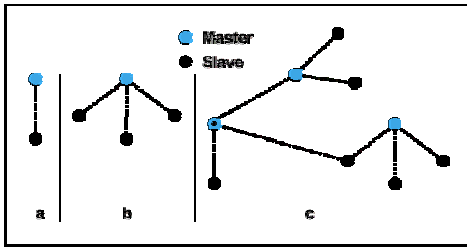
Network Architecture

- Dynamic reconfigurability for a very flexible system suited to many environments
 - **Piconet**: all ad hoc networks with at most 8 simultaneously active devices
 - 1 master: controls the channel access within the piconet and handles all the traffic within the piconet
 - up to 7 slaves
 - **Scatternet**: Many piconets coexisting in the same area (interconnected or not)
- Any device can be either a master or a slave in a piconet



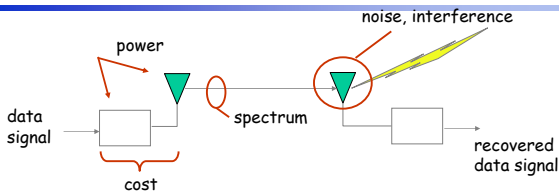
12

An Example



13

Design Considerations



Goals

- high bandwidth
- conserve battery power ←
- cost < \$10
- robust system

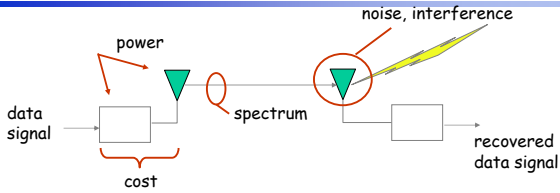
14

Bluetooth Radio

- **Low Power**
 - Low voltage RF
 - Standby modes (Sniff, Hold, Park)
- **Power Classes:** devices can be classified into 3 power classes
 - Power Class 1: long range (~100m) devices, max output power = 20dBm
 - Power Class 2: ordinary range devices (~10m), max output power = 4dBm
 - Power Class 3: short range devices (~10cm), max output power = 0dBm

15

Design Considerations



Goals

- high bandwidth
- conserve battery power
- cost < \$10 ←
- robust system

16

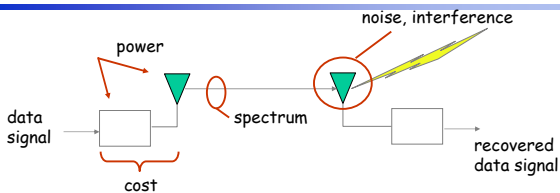
Bluetooth Radio

• Low Cost

- Single chip radio (minimize external components)
- Today's technology
- Time division duplex

17

Design Considerations



Goals

- high bandwidth
- conserve battery power
- cost < \$10
- robust system ←

18

Bluetooth Radio

- **Robust operation**

- Fast frequency hopping: 1600 hops/s
- Strong interference protection
 - Fast ARQ
 - Robust access code
 - Forward header correction



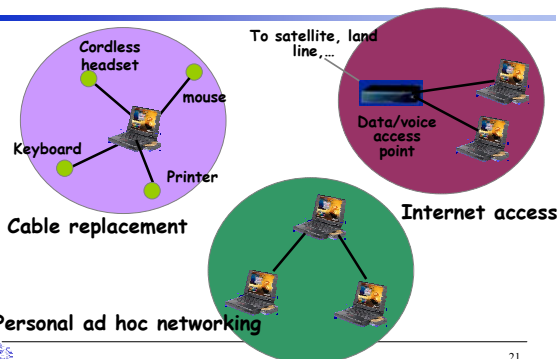
19

Applications



20

Application Scenarios



21

Synchronization



User benefits

- Automatic synchronization of calendars, address books, business cards
- ↑ Push button synchronization
- ↓ Proximity operation



22

Cordless Headset

User benefits

- Multiple device access
- Cordless phone benefits
- Hands free operation



23

Usage Scenarios Examples

- Data Access Points ✓
- Synchronization ✓
- Headset ✓
- Conference Table
- Cordless Computer
- Instant Postcard
- Computer Speakerphone
-



24

Technical Overview



The Bluetooth Technology

Bluetooth documentation is divided into two parts:

- The **Specifications** describe **how the technology works** (i.e., the Bluetooth protocol architecture)
- The **Profiles** describe **how the technology is used** (i.e., how different parts of the specification can be used to fulfill a desired function for a Bluetooth device)

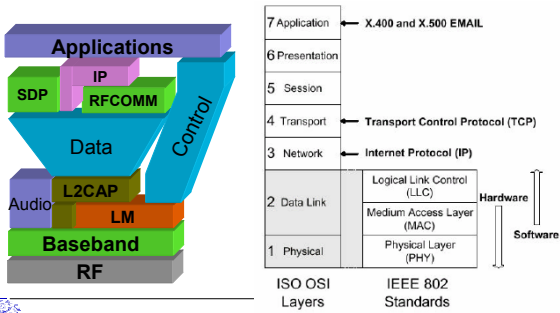


Bluetooth Specifications

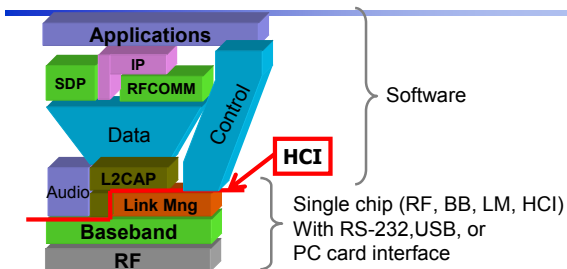
Bluetooth Protocol Stack



Protocol Stack Comparison

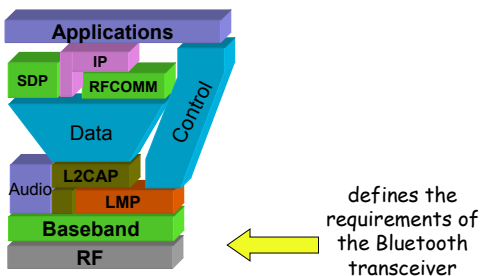


Bluetooth Protocol Stack



- A hardware/software/protocol description
- An application framework

Bluetooth Radio Specification



Spread Spectrum

- **Idea**
 - spread signal over all the available bandwidth
 - originally designed to thwart jamming
- **Direct Sequence**
- **Frequency Hopping**
 - transmit over pseudo-random sequence of frequencies
 - sender and receiver share:
 - seed
 - pseudo-random number generator



--

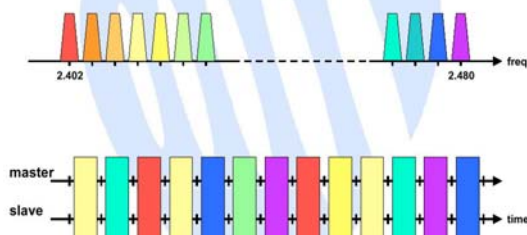
Radio Channel

- Uses an FHSS technique to minimize power waste and guarantee robustness to interference
- Bandwidth: 79 MHz divided into 79 frequency channels with width equal to 1 MHz
 - In the U.S., hopping is performed over all the 79 channels
 - In Europe, hopping uses only 23 channels out of the 79



33

FREQUENCY HOPPING



34

Piconet Synchronization

- Each BT device has a free-running clock that is the heart-beat of the tranceiver
- Slaves synchronize with the master by adding an offset to their native clock; offsets have to be updated regularly



35

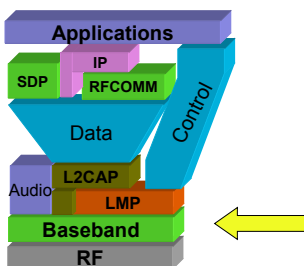
Piconet Synchronization

- Once created, each piconet uses its own frequency hopping sequence which is derived from the master node address
 - Interference between neighboring piconets is reduced
 - The hopping sequence is defined so that there is equal probability to hop on any of the available frequency channels (pseudo-random sequence)
 - in the U.S.: channel hopping prob.=1/79
 - in Europe: channel hopping prob.= 1/23



36

Baseband



37

Bluetooth Physical Link

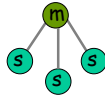
- **Point to point link**

- master - slave relationship
- radios can function as masters or slaves



- **Piconet**

- Master can connect up to 7 active slaves
- Each piconet has max gross capacity of 1 Mbps
- hopping pattern is determined by the master

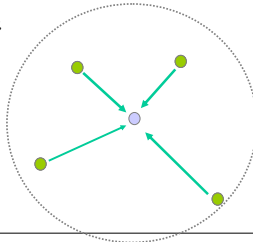


38

Piconet Formation

- **Inquiry - scan protocol**

- to learn about the clock offset and device address of other nodes in proximity

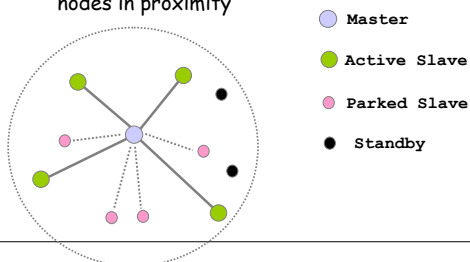


39

Piconet Formation

- **Page - scan protocol**

- to establish links with nodes in proximity



40

Addressing

- Bluetooth device address (**BD_ADDR**)
 - 48 bit IEEE MAC address
- Active Member address (**AM_ADDR**)
 - 3 bits active slave address
 - all zeros: broadcast address
- Parked Member address (**PM_ADDR**)
 - 8 bit parked slave address

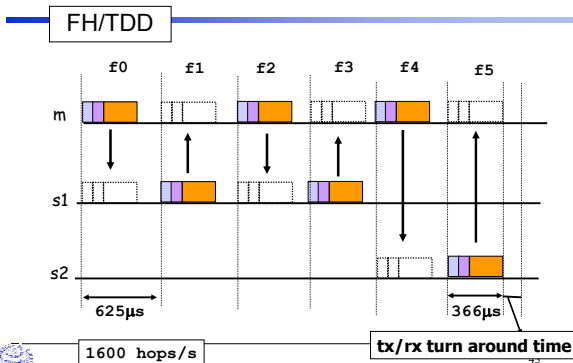


Physical Channel

- A **Hopping Sequence** is used to select the next radio channel
 - It is only related to master's hardware address
 - The phase in the hopping sequence is determined by the master's BT clock
- Channel is temporally slotted (slot duration= 625 μ s)
- A packet is transmitted within a single radio channel



Piconet Channel



Channel Access

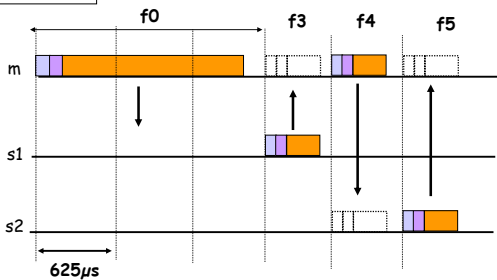
- Slaves can transmit only if polled by the master
 - The packet header indicates the intended recipient
- Master always starts transmitting on even slots
- Slaves always start transmitting on odd slots



44

Multi-Slot Packets

FH/TDD

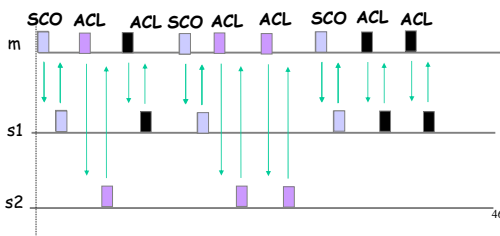


Data rate depends on the packet type



Physical Link Types

- **Synchronous Connection Oriented (SCO) Link**
 - slot reservation at fixed intervals
- **Asynchronous Connection-less (ACL) Link**
 - Polling access method



46

SCO

- Point-to-point connection
- Two duplex slots are allocated periodically
- All packets are 1-slot long
- Packets are never retransmitted



47

SCO

- A master can support up to 3 SCO links with the same slave or with different slaves
- A slave can support up to 3 SCO links with the same master and up to 2 SCO links if they originate from different piconets
- The SCO link is established by the master sending the SCO period T_{SCO} and the SCO offset D_{SCO}
- Even if a slave fails in decoding the slave address in the SCO packet header, it can access the channel in the following slot



48

ACL

- Point-to-multipoint link between the master and the slaves within the piconet and point-to-point link between a slave and the master
- Can use all the slots not allocated to SCO traffic
- ACL traffic is scheduled by the master
- Multi-slot packets can be used
- Packets can be retransmitted



49

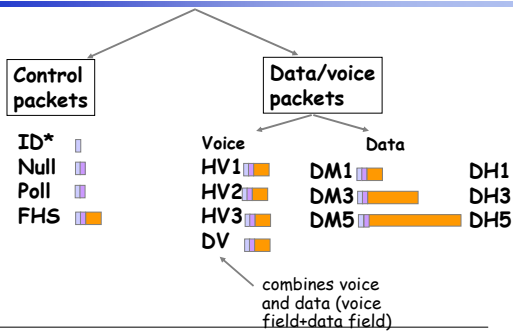
ACL

- Between a master and a slave one ACL link only can exist
- An ACL link is always established between a master and a slave since it must be used to exchange LMP messages
- If a slave fails in decoding the slave address in the packet header, it cannot access the channel in the following slot



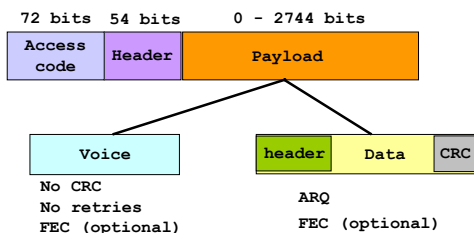
50

Packet Types



51

Packet Format



52

Access Code

Access Code (72 bits), three different access codes exist:

- **Channel Access Code (CAC)**: used for synchronization and to identify a piconet (used in *SCO* and *ACL* packets). If the piconet cannot be identified by the receiver, the packet is discarded
- **Device Access Code (DAC)**: used in paging and response to paging
- **Inquiry Access Code (IAC)**: 64 possible access codes used in the inquiry procedure
 - 1 General Inquiry Access Code (**GIAC**)
 - 63 Dedicated Inquiry Access Codes (**DIAC**)

Header

Header (54 bits): Encoded with a 1/3 FEC;
if not correctly received, the packet is discarded

- **AM_ADDR**: 3 bit active member address
- **TYPE**: 4-bit packet type (*SCO*, *ACL*, **duration**)
- **FLOW**: 1-bit flow control (=0 if rx buffer is full)
- **ARQN**: 1-bit ack indication
- **SEQN**: 1-bit sequence number (inverted at each packet tx so that 2 correct tx of the same packet can be distinguished)
- **HEC**: 8-bit header error check

Payload

- **Payload (0-2744 bits):**
 - For *ACL* packets, it's covered by a 16 bit *CRC*
 - Payload header only for *ACL*: indicates how many bytes are transmitted, some flow control information and the logical channel used



Control Packets

- **ID:** consists of the DAC or IAC (68 bits), used in inquiry, paging and response routines
- **NULL:** CAC+Header only, used to return information to the source such as ARQN and FLOW
- **POLL:** CAC+Header only, used by the master to poll a slave which must respond. Not a part of the ARQ scheme
- **FHS:** control packet revealing the sender's address and clock (144 bits+16-bit CRC)



56

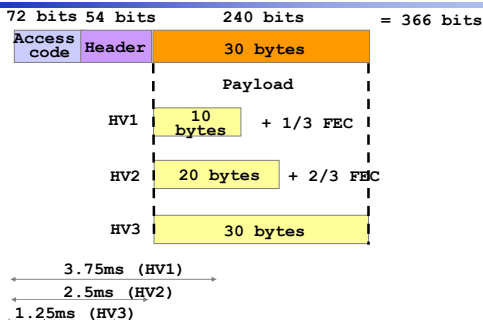
HV Packets

- **HV (High quality Voice):**
 - Used for SCO links
 - Bit-rate=64 Kbps
 - 2 packets every Tsc0 slots are sent
 - ♦ HV1: with 1/3 FEC; (6 slots over 6)
 - ♦ HV2: with 2/3 FEC; (4 slots over 6)
 - ♦ HV3: with no FEC; (2 slots over 6)



57

HV Packets



58

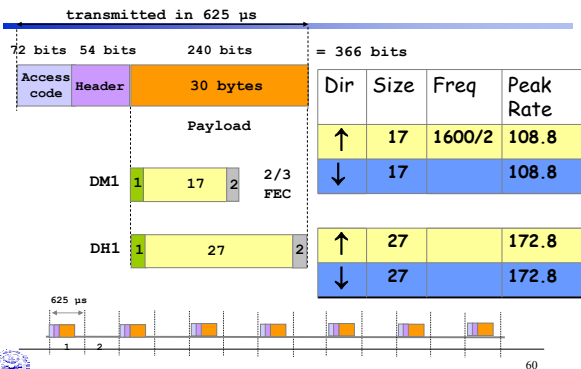
DH and DM Packets

- **DH/M (Data High/Medium rate):**
 - Used for ACL links
 - ♦ DM: with 2/3 FEC
 - ♦ DH: no FEC
 - Possible packet duration: 1, 3, 5 slots
 - ♦ DM1, DM3, DM5
 - ♦ DH1, DH3, DH5

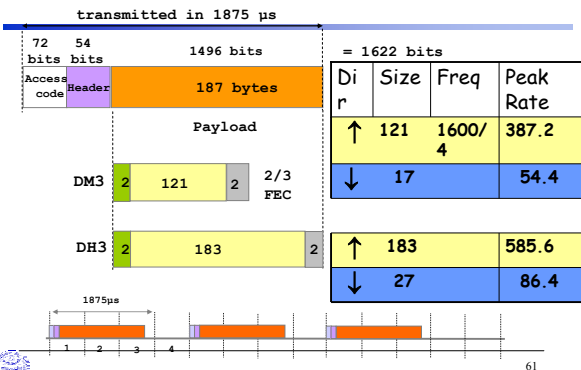


59

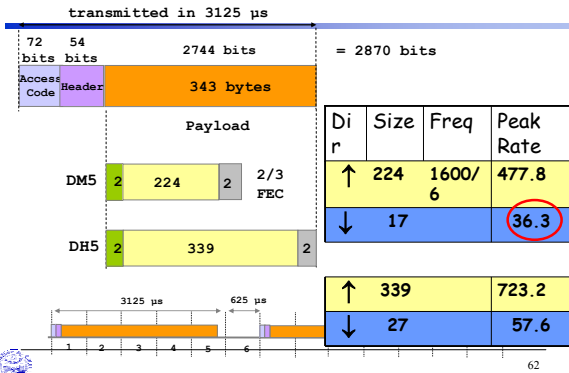
Rate Calculation: DM/H1



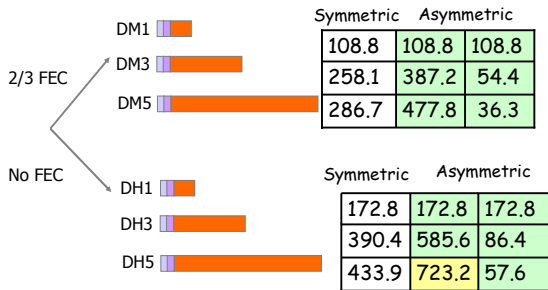
Rate Calculation: DM/H3



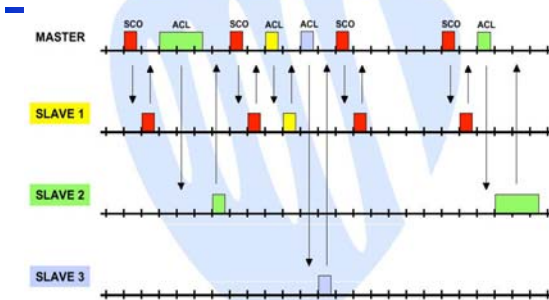
Rate calculation: DM/H5



Data Packet Types



MIXED LINK EXAMPLE



Traffic Scheduling

- **SCO** traffic always has priority due to delay requirements
- **ACL** link: a round-robin scheduling has been proposed by Ericsson
 - Not the most efficient solution in the case of asymmetric traffic
 - For asymmetric traffic, it's better to transmit to the same slave (or let the slave transmit) for a longer time
 - DH/M-3 and DH/M-5 packets can be used to reduce the overhead



65

Link Control

- **Stop-and-Wait**
 - Applied to DH and DM packets only
 - If the master is receiving, it can send the **ACK** in the slot next to the received packet even if the master transmission is toward a different slave (fast Stop&Wait)
 - the time latency is reduced
 - in this case the **ACK** is sent by setting the **ARQN** bit to 1



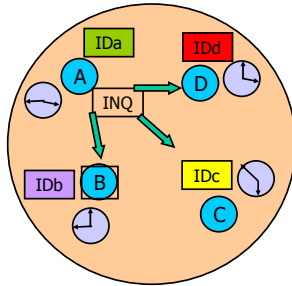
66

Inquiry and Paging



67

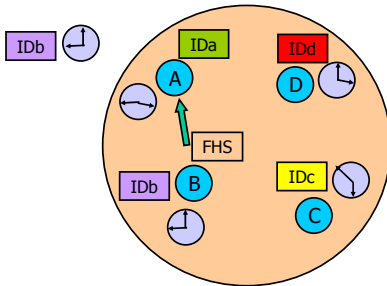
Example (1)



- B,C,D are in Inquire Scan

8

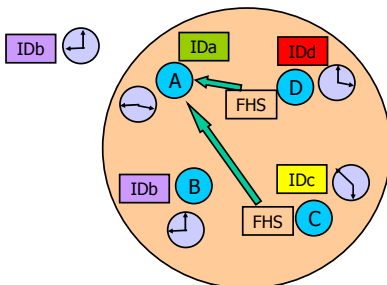
Example (2)



- B,C,D are in Inquire Scan

9

Example (3)



- C and D respond simultaneously:
their FHSs are lost

0



- 1

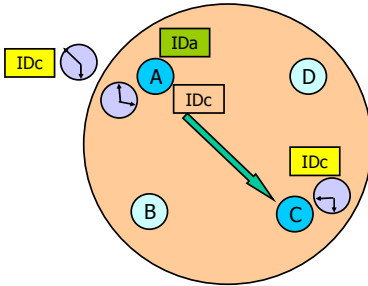


- 2



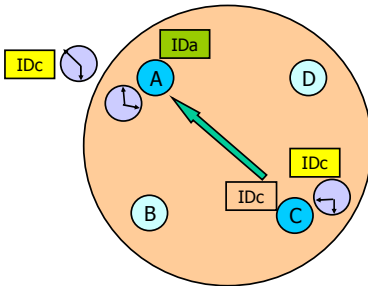
- no

Example (1)

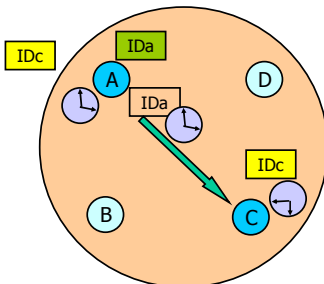


- A knows C's ID and has an idea of its clock

Example (2)

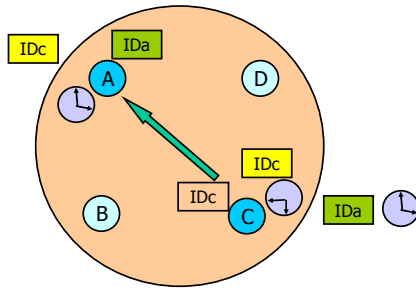


Example (3)



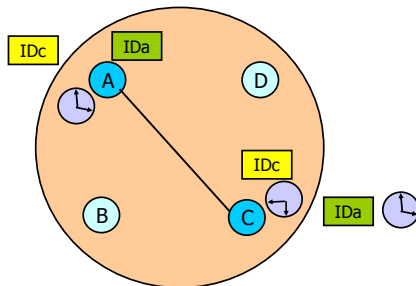
- A replies with its ID and clock (FHS packet)

Example (4)



77

Example (5)



• Then, A connects as a master to C

8

Inquiry

- Used to discover other devices and exchange synchronization information (HW address and clock)
 - This allows two nodes to agree on a common channel-hopping sequence:
 - ♦ Address used to select the sequence
 - ♦ Clock used to select the sequence phase
- Asymmetric procedure
 - Listener and sender hop using the same sequence but the sender hops faster than the listener



79

Inquiry Procedure

- The interval between two consecutive inquiry procedures is a random variable so that synchronization between two or more entities performing the procedure is avoided
- Typically, **the sender** repeats the procedure for about 10 s every minute
- **The sender** stops repeating the procedure when it has contacted a sufficient number of nodes



80

Inquiry Transmission

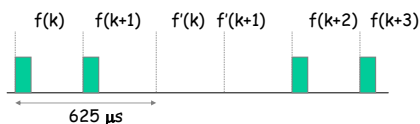
- **The sender** uses a known-to-all inquiry hopping sequence and IAC
- **The sender** can specify the class of devices to contact by using a *dedicated* instead of a *general inquiry access code*



81

Inquiry Timing

- **The sender:**
 - Keeps transmitting the IAC on different frequencies
 - Every 1.25 ms transmits on two hops and listens whether there is a response from neighboring units



82

Inquiry Transmission

- **The sequence** comprises 32 frequency hops:
 - It is divided into 2 sub-sequences of 16 hops, each lasting 10 ms ($625 \text{ ms} \cdot 16 = 10 \text{ ms}$)
 - The single sub-sequence is repeated 256 times, i.e., for 2.56 s
- To discover neighbors, 4 trains of sub-sequences have to be transmitted
 - Inquiry may have to last 10.24 s ($4 \cdot 2.56 = 10.24$)
 - It may finish earlier if many responses have been collected



83

Inquiry Scan

- A **listener**, i.e., a unit that wants to be discovered, periodically enters the **inquiry scan state** and listens to one frequency only for a while
- When it detects an inquiry message, it has the option to not reply
- If it replies, it uses a FHS packet with the same access code and the common sequence, called **inquiry response**
- Interval between two consecutive inquiry scans equal to 2.56 s. Each time the unit listens to a different frequency for 10 ms



84

Inquiry Procedure

Further observations

- **Listeners:**
 - when more than one listener is present, their replies may collide
 - to avoid collisions, listeners defer their replies until expiration of a random back-off timer
 - the FHS packet is retransmitted at other times and frequencies as long as the master is probing with inquiry messages



85

Inquiry Procedure

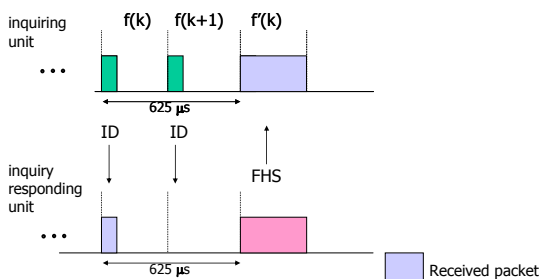
Further observations

- **Sender:**
 - collects device address and clock offset from the listeners
 - this information is subsequently used to page the selected listener



87

Inquiry Message Exchange



88

Paging

- Used to establish connections and define roles
- Steps similar to Inquiry, **BUT**
 - Paging message is unicast to a selected listener (ID packet uses the DAC) $\Rightarrow$ listener does not need to back-off
 - The sender has also an estimate of the listener's clock $\Rightarrow$ it is enabled to communicate with the listener almost instantaneously



90

Paging Transmission

The paging unit:

- Knows the address (DAC) of the unit to page (X)
- Derives the hopping frequency to be used for paging from X's address
- However, usually the pager and X are not perfectly sync. Thus, the pager does not know exactly:
 - ♦ when X will listen to the channel
 - ♦ on which frequency (i.e., X's phase)



92

Paging Transmission

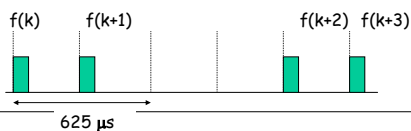
- **The paging sequence** is 32-hop long and is divided into two sub-sequences of 16 hops each (in U.S.)
- **The paging unit** periodically repeats the paging sequence



93

Paging Timing

- **The paging unit:**
 - keeps transmitting X's access code on different frequencies
 - every 1.25 ms transmits on two hops and listens whether there is a response from X



94

Paging Transmission

- In a 10 ms interval, the pager transmits X's access code on 16 frequency hops ($625\mu\text{s} \cdot 16 = 10\text{ms}$)
- Repeats the single sub-seq. for a period equal to the sleep time between two consecutive paging scans of X
 - 128 times (i.e., for 1.28 s) if it's using the R1 mode
 - 256 times (i.e., for 2.56 s) if it's using the R2 mode
- If X doesn't reply, the pager repeats the procedure using the other 16 freq. out of the 32-hop sequence
- The whole procedure is repeated until the paged unit replies or the timeout *pageTO* expires



95

Paging Scan

- There isn't a paging channel (it's an ad hoc environment)
 - X has to periodically listens to the channel to detect whether there is a paging message for itself
- X listens to the channel to detect whether the access code derived from its own address is being transmitted
- X scans the channel at least every 1.28 s (R1 mode) or 2.56 s (R2 mode), and each time listens to a different frequency for 10 ms



96

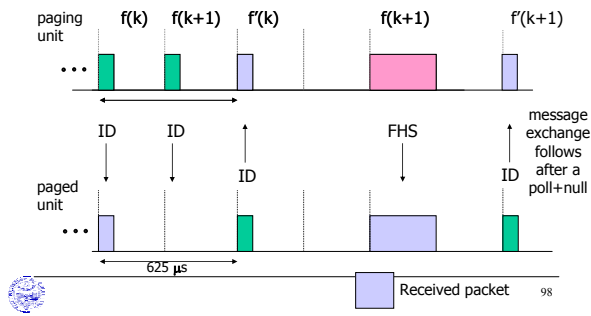
Connection Establishment

- When X receives the paging msg, it replies back with an ID packet using a sequence called **paging response**, derived from its address
- The pager replies by sending its own address and clock information (FHS packet) and using the same hopping frequency and access code employed by X
- X sends an acknowledgment with the same hopping frequency and access code
- After that, the paging unit (i.e., the master) starts the data exchange by using the hopping sequence of the piconet, derived by its own address and clock



97

Paging Message Exchange



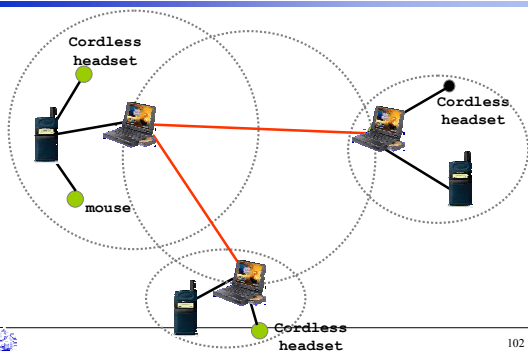
Paging

- Upon receiving a response for the paging message, the **sender** becomes the **master** and the **listener** the **slave** of a newly formed piconet
- Both nodes switch to the **piconet channel-hopping sequence**

Master and Slave

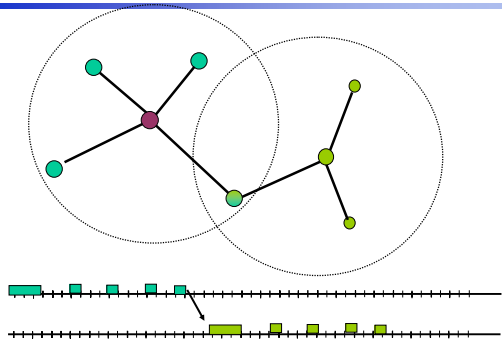
- Typically, masters have a much higher computational and communication load, thus experiencing higher energy consumption than slaves do
- Master and slave can switch role within the piconet through an appropriate procedure

Inter-Piconet Communication



102

Scatternet - Scenario 1



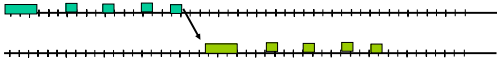
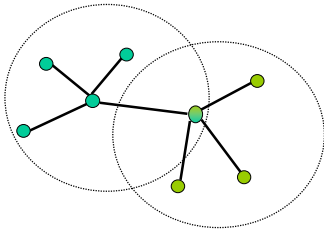
Scatternet - Scenario 1

- A slave can belong to two or more piconets, but cannot communicate with more than one at the same time
- It must use time multiplexing by being in "suspend" (i.e., hold, park, or sniff mode) in a piconet and active in another
- A slave can leave its current piconet (after informing its current master about the duration of the leave) and join another piconet



104

Scatternet - Scenario 2



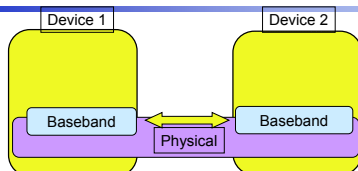
Scatternet - Scenario 2

- A master in one piconet can also act as a slave in another piconet (but not as a master)
- How to schedule presence in two piconets?
- Forwarding delay?
- Missed traffic?



106

Baseband Summary

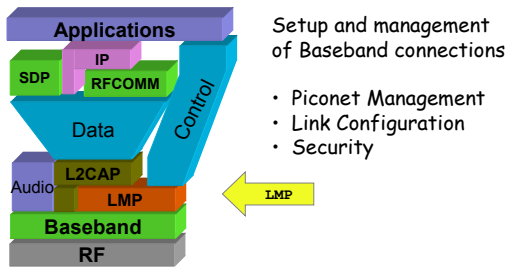


- FH/TDD physical layer
- Two types of links: SCO and ACL links
- Multiple packet types (i.e., data rates with/without FEC)
- Device inquiry and paging
- Scatternet



107

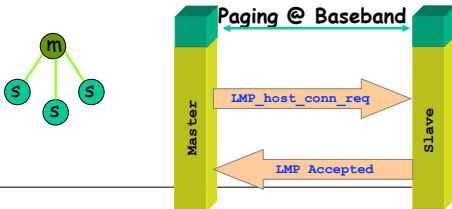
Link Manager Protocol



108

Piconet Management

- Attach and detach slaves
- Master-slave switch
- Establishing ACL and SCO links
- Handling of low power modes (Sniff, Hold, Park)



109

Detach/Reset

- Detach:
 - The connection between 2 units can be closed anytime either by the master or the slave
 - A reason parameter is included in the message to inform the other party of why the connection is closed
- A Reset procedure occurs in the case of an abrupt link failure



110

Master-Slave Switch (1)

- The pager becomes the master, but a switch between slave and master may occur if both agree on it
- First, a TDD switch is performed between the old and the new master
- A piconet switch for all the piconet participants follows



111

Master-Slave Switch (2)

- The piconet switch is done with one piconet participant at a time: The new master sends a time alignment command and an FHS packet and waits for an ack (ID packet) from the slave
- From then on, that slave uses the new master parameters for its communications
- Information on the piconet participants may be transferred from the old to the new master



112

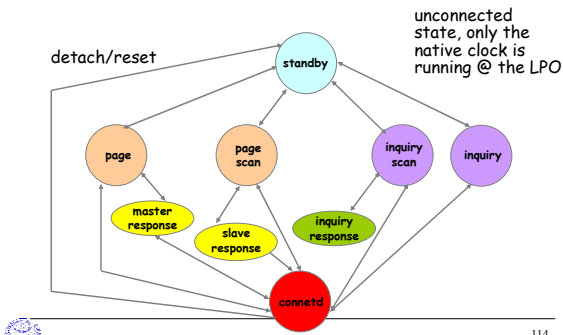
Node Operational State

- **Standby:**
 - The node is not connected to anyone through a traffic link
 - However it listens to the channel checking every 1.28 s (or 2.56 s) over 32 frequency hops if there are msgs from the master sent to him
- **Page/Inquiry-scan**
- **Connected:**
 - The node is connected to another node through a traffic link

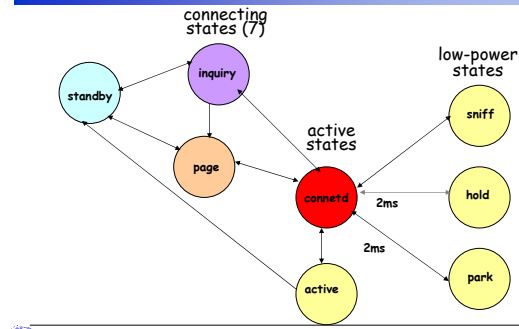


113

Link Controller State Transitions



Link Controller State Transitions



Connected States: Active

- The node transmit and/or receive traffic

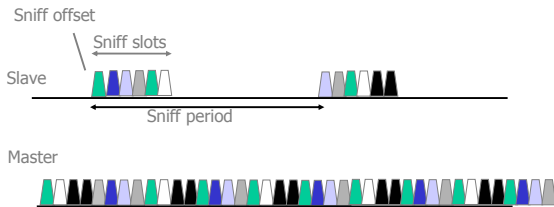
Connected States: Sniff

- Defined for slaves only, the slave listens for D_{sniff} slots every T_{sniff} and for a N_{sniff} number of times
- The master issues a sniff command indicating the T_{sniff} period, the D_{sniff} , and N_{sniff}
- The slave remains synchronized to the piconet and maintains its MAC address
- Listens to the channel while consuming little energy
- The master can force the slave in sniff mode; both the slave and the master can request to put the connection in sniff mode or to move back to active mode



117

Sniff Mode



- Traffic reduced to periodic sniff slots



118

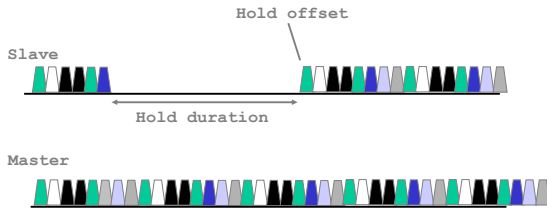
Connected States: Hold

- Master and slave agree on the hold time duration. Both of them can request hold mode
- Tx/rx in one piconet/inquiry/paging/scanning and in hold state in the other
- ACL link can be put into hold mode also to save energy (if so, the unit in hold turns off its receiver)
- Maintains its MAC address
- Returning from hold, it must listen for the master and resync its clock offset



119

Hold Mode



120

Connected States: Park

- The master can force a slave in park mode; either the slave or the master can require to put the connection into park mode
- The master can force the park mode to one slave at a time
- The node does not participate in piconet activity and does not have a MAC address (PM_ADDR for the unpark master initiated procedure, AR_ADDR for the unpark slave initiated-procedure)



121

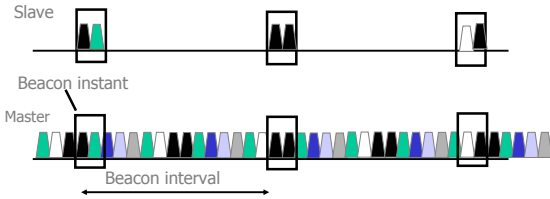
Connected States: Park

- Remains synchronized to the piconet waking up periodically for listening to the beacons from the master
- Returning from park, it must listen for the master and resync its clock offset
- A slave can send an unpark request in a proper half-slot after a broadcast packet sent by the master to poll parked slaves. The slave can unpark when it receives an ack by the master



122

Park Mode



- Power saving + keep more than 7 slaves in a piconet
- Give up active member address, yet maintain synchronization
- Communication via broadcast LMP messages



Battery Life

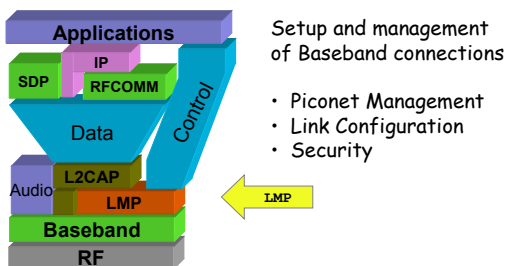
- **Low power consumption***
 - Standby current < 0.3 mA $\Rightarrow$ 3 months
 - Voice mode 8-30 mA $\Rightarrow$ 75 hours
 - Data mode average 5 mA (0.3-30mA, 20 kbit/s, 25%) $\Rightarrow$ 120 hours
- **Low Power Architecture**
 - Programmable data length (else radio sleeps)
 - Hold and Park modes 60 μ A
 - Devices connected but not participating
 - Device can participate within 2 ms

*Estimates calculated with 0.6 Ah battery



124

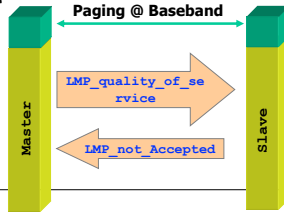
Link Manager Protocol



125

Link Configuration

- Power control
- Quality of service
 - Polling interval for ACL traffic
 - Packet type negotiation (multi-slot packets)
 - Broadcast repetition



Power Control

- Mandatory for class 1 devices and optional otherwise
- In the practice, most devices are class 2 and most support power control
- A device can send increase or decrease link manager commands to another device based on the RSSI



127

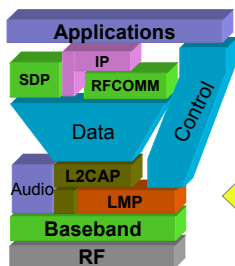
Power Control

- The specification defines a 20dB golden window with the lower limit at least 6dB above the receiver sensitivity. If the RSSI falls within this window, no power adjustment is requested
- Typically, the power control scheme tends to drive the output power to somewhere in the range of -50 to -70 dBm



128

Link Manager Protocol



Setup and management of Baseband connections

- Piconet Management
- Link Configuration
- Security



129

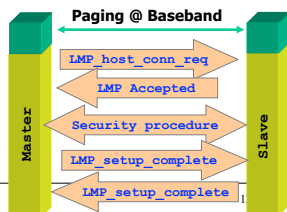
Baseband Connection Establishment & Security

Goals:

- Authenticated access
 - Only accept connections from trusted devices
- Privacy of communication
 - Prevent eavesdropping

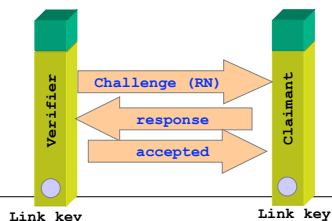
Constraints:

- Processing & memory limitations (e.g., \$10 headsets)



Authentication

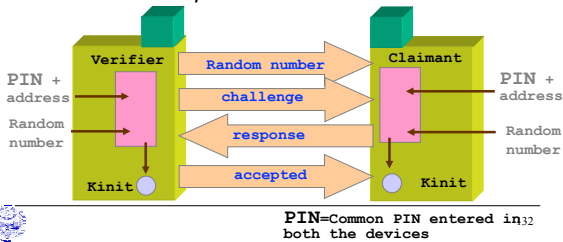
- It is a mandatory feature
- Authentication is based on a challenge/response mechanism using a **link key** (128 bit shared secret between two devices)
- How can link keys be distributed securely?



131

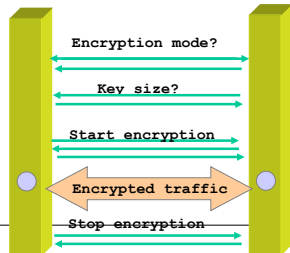
Pairing (Key Distribution)

- Pairing is a process of establishing a trusted secret channel between two devices (construction of initialization **symmetric key** K_{init})
- K_{init} is used for initial authentication and then to distribute link keys

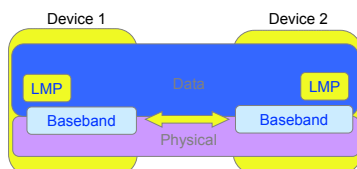


Encryption

- It is optional
- An **encryption key** (configurable key length 8 - 128 bits, derived from the link key) and the encryption algorithm are needed

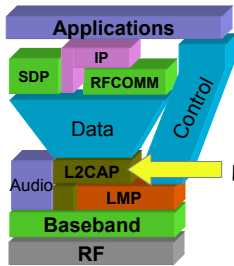


LMP Summary



- Piconet management
 - Low-power modes
- Link configuration
 - Power Control
 - QoS
- Security: authentication and encryption

L2CAP



Logical Link Control and Adaptation Protocol

L2CAP provides:

- Protocol multiplexing
- Segmentation and reassembly
- Quality of service negotiation



135

L2CAP

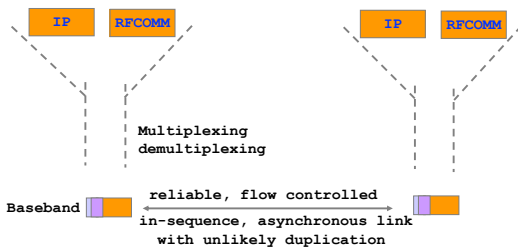
Goals

- Hides peculiarities of lower layer protocols from the upper layers thus providing great flexibility in supporting higher layer protocols
- Provides services to ACL traffic links



136

Why Is L2CAP Needed ?

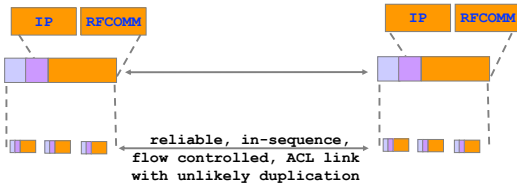


- Baseband pkt size is very small (17min, 339 max) cmp to HL pkts
- No protocol-ID field in the baseband header



137

Need for a Multi-protocol Encapsulation Layer



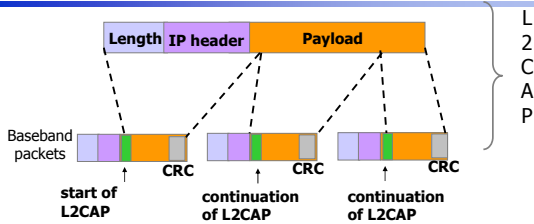
Desired features:

- Protocol multiplexing
- Segmentation and reassembly



138

Segmentation & Reassembly



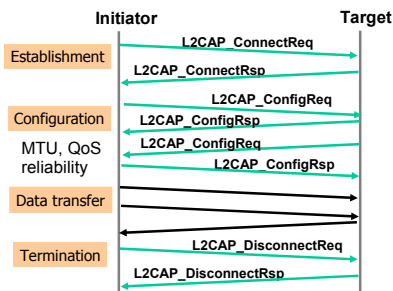
MTU (Maximum Transmission Unit): Max L2CAP PDU payload that a local device can accept

- min MTU = 48 B; max MTU = 65535 B
- default MTU = 672 B



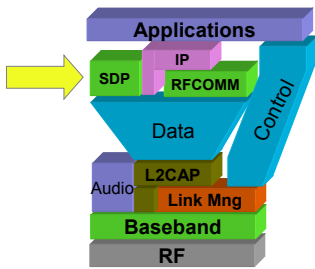
139

L2CAP Connection-oriented: Example



146

Bluetooth Service Discovery Protocol



149

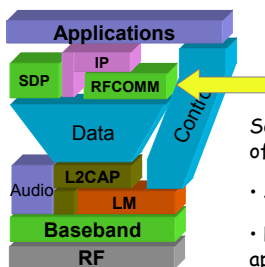
Example Usage of SDP

- Establish L2CAP connection to remote device
- Query for services
 - search for specific class of service, or
 - browse for services
- Retrieve attributes that detail how to connect to the service
- Establish a separate (non-SDP) connection to use the service



150

Serial Port Emulation Using RFCOMM



Serial Port emulation on top of a packet oriented link

- Similar to HDLC
- For supporting legacy applications



151

Serial Line Emulation over Packet Based MAC



- Functions:
 - **framing**: assemble bit stream into bytes and, subsequently, into packets
 - **transport**: in-sequence, reliable delivery of serial stream
 - **control signals**: emulate RTS, CTS, ...
- Options at the TX
 1. collect MTU bytes @ L2CAP and then send
 2. wait until a timeout
 3. send whatever is available



152

Bluetooth Profiles



153

Profiles and Usage Models

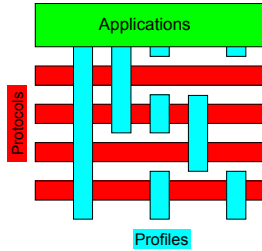
- Represent default solutions for usage models: They describe how implementations of usage models have to be accomplished
- The usage models describe a number of user scenarios where Bluetooth performs the radio transmission
- The profile concept is used to decrease the risk of interoperability problems between different manufacturers' products



154

Bluetooth Profiles

- A profile can be described as a vertical slice through the protocol stack
- It defines options in each protocol that are mandatory for the profile and parameter ranges for each protocol



155

Examples

- FTP (File Transfer Profile)
- CTP (Cordless TelePhony)
- HS (Headset)
- FP (Fax)
- LAN (Local Area Network Access)

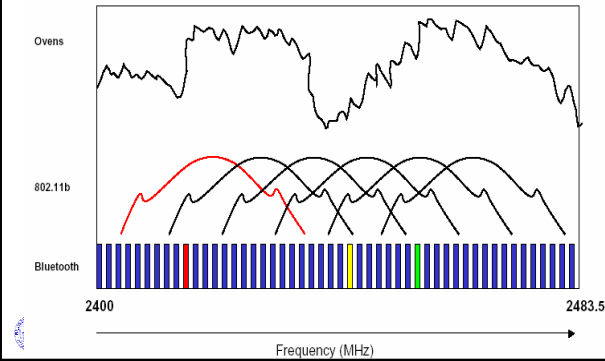


156

Coexistence between Different Wireless Technologies



The 2.4 GHz ISM Band



Coexistence

- Systems operating in the ISM bands and sharing the same environment may interfere
- Example: Bluetooth and 802.11b that are in the one another's transmission range
- The closer the interfering transmitter to the receiver, the greater the throughput decrease
- Coexistence is obtained when different technologies do not significantly degrade each other's performance



168

An Example of Coexistence Mechanisms: The OLA Schemes



IEEE 802.11 WLANs

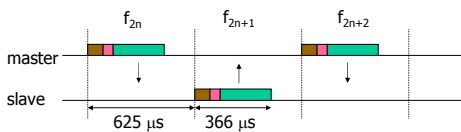
- Designed to cover areas as vast as offices or buildings
- The Basic Service Set (BSS) is the basic architectural block and is composed of one access point and several wireless stations
- DSSS WLANs at 11Mbps
- Bandwidth roughly equal to **22 MHz**
- DCF used at the MAC layer



170

Bluetooth (IEEE 802.15 WPANs)

- Interconnection of devices in a range of about 10 m
- FH/TDD channel with bandwidth equal to 79 MHz



171

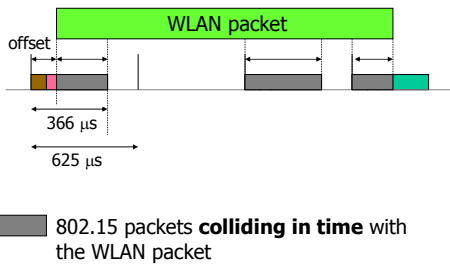
The Interference Model

- One 802.11 BSS and several 802.15 devices in the proximity of each other interfere when their transmissions overlap both in **time** and in **frequency**
- The probability that an 802.15 packet hops within the **802.11 frequency band** is equal to $22/79=0.278$



172

The Interference Model



173

Coexistence Mechanisms

- **Collaborative (e.g., META):**
 - Centralized controller at the MAC layer monitoring the 802.11 and the 802.15 traffic
 - Implemented between co-located interferers only
- **Non-collaborative (e.g., AFH):**
 - Counteract interference from both co-located and non co-located interferers
 - In the case of co-located devices, worse performance in terms of goodput with respect to collaborative mechanisms



174

The OLA Schemes

- **V-OLA (Voice OverLap Avoidance):**
 - Performed at the WLAN stations to avoid interference between 802.11 data traffic and 802.15 voice traffic
- **D-OLA (Data OverLap Avoidance):**
 - Performed at the 802.15 devices to avoid interference between 802.11 and 802.15 data traffic



Both schemes assume that 802.11 and 802.15 can detect interference due to other technologies



175

The V-OLA Scheme

- By listening to the channel, an 802.11 station becomes aware of which time slots are busy over the 802.15 voice link
- When a station has traffic to transmit, it checks on the channel status:
 - if **idle** and expected to be so for the next $(i-1)$ slots, a packet with length equal to $\min(i-500, 1500)$ bytes is sent
 - if **busy**, either refrain from transmitting (PT mode) or send a 500 bytes packet (ST mode)



178

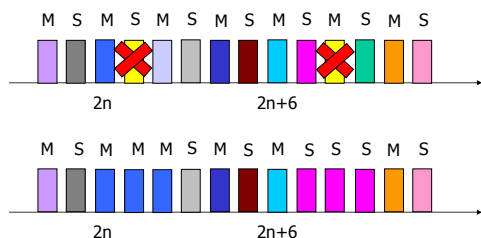
The D-OLA Scheme (1)

- 802.15 devices supporting data links become aware of the frequency band used by the interfering WLAN (e.g., through assessment of the RSS)
- Let $2n$ be the current time slot (master tx) and consider the case of 1-slot packets:
 - If f_{2n+1} hops on the 802.11 band, the master schedules a multi-slot packet so that f_{2n+1} is skipped
 - If f_{2n+2} hops on the 802.11 band, the master asks the next transmitting slave to send a multi-slot packet so that f_{2n+2} is skipped



179

The D-OLA Scheme (2)



M = Master transmission
S = Slave transmission



180

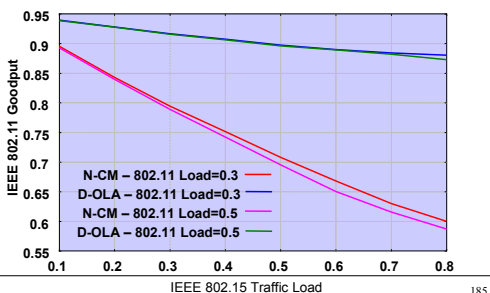
Advantages

- V-OLA and D-OLA do not require a centralized traffic scheduler
- Interference mitigation between collocated and non-collocated interfering devices
- Minor impact on the 802.11 and the 802.15 standard
 - V-OLA can be implemented through the CCA function specified in 802.11
 - In 802.15 the master can only indicate to a slave the maximum no. of slots to use. While in D-OLA the slave should interpret the indication as the suggested packet length

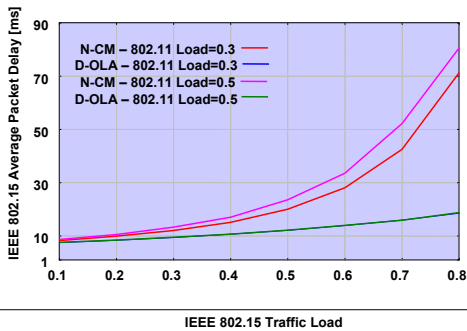
Simulation Scenario

- HV3-link for 802.15 voice traffic, DH1-link for 802.15 data traffic
- RTS/CTS mechanism always active
- Arrival of frames at the 802.11 and 802.15 MAC layers modeled with exponential inter-arrival times and a truncated geometric distribution for the frame length
- The OLA schemes performance are compared with the results obtained in the case where no coexistence mechanism is used (hereinafter indicated by label N-CM)

D-OLA: 802.11 Goodput vs. 802.15 Data Traffic



D-OLA: 802.15 Packet Delay vs. 802.15 Data Traffic



IEEE 802.15 Traffic Load

187

Microwave Ovens

- Operate in the ISM bands
- Residential transformer type is active for about 8 ms over a power cycle of 20 ms, when the supply frequency is equal to 60 MHz
- The impact on the WLAN performance varies depending on the distance between the oven and the WLAN receiver
- BER at the 802.11 receiver equal to 0.01 (i.e., distance from the oven equal to 3 m)



188

References

- A. Tanenbaum, "Computer networks," 4th ed., Prentice-Hall, 2002.
- J. Haartsen, "The Bluetooth Radio System," IEEE Personal Comm. Magazine, Feb. 2000.
- B.A. Miller and B. Bisdikian, *Bluetooth Revealed*, Prentice Hall, 2nd Ed., 2002.
- B. Chatschik, An Overview of the Bluetooth Wireless Technology, IEEE Communications Magazine, Vol. 39, Dec. 2001.
- Chiasserini and Rao, "Coexistence Mechanisms for Interference Mitigation between IEEE 802.11 WLANs and Bluetooth," IEEE Transactions on Wireless Communications

