
Introduction to Wireless Networks

Chapter 3: Introduction to Bluetooth

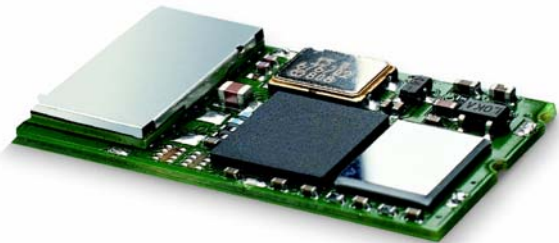
Prof. Yuh-Shyan Chen
Department of CSIE
National Taipei University

Chapter 3: Introduction to Bluetooth

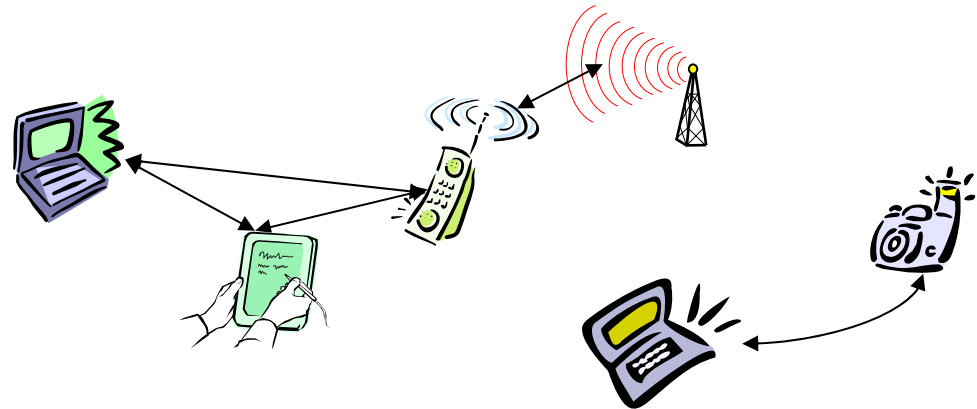
Bluetooth

Idea

- ❑ Universal radio interface for ad-hoc wireless connectivity
- ❑ Interconnecting computer and peripherals, handheld devices, PDAs, cell phones – replacement of IrDA
- ❑ Embedded in other devices, goal: 5€/device (2002: 50€/USB bluetooth)
- ❑ Short range (10 m), low power consumption, license-free 2.45 GHz ISM
- ❑ Voice and data transmission, approx. 1 Mbit/s gross data rate




One of the first modules (Ericsson).



Bluetooth

History

- ❑ 1994: Ericsson (Mattison/Haartsen), “MC-link” project
- ❑ Renaming of the project: Bluetooth according to Harald “Blåtand” Gormsen [son of Gorm], King of Denmark in the 10th century
- ❑ 1998: foundation of Bluetooth SIG (Special Interest Group), (was:  **Bluetooth**)
www.bluetooth.org
- ❑ 1999: erection of a rune stone at Ericsson/Lund ;-)
- ❑ 2001: first consumer products for mass market, spec. version 1.1 released

Special Interest Group

- ❑ Original founding members: Ericsson, Intel, IBM, Nokia, Toshiba
- ❑ Added promoters: 3Com, Agere (was: Lucent), Microsoft, Motorola
- ❑ > 2500 members
- ❑ Common specification and certification of products





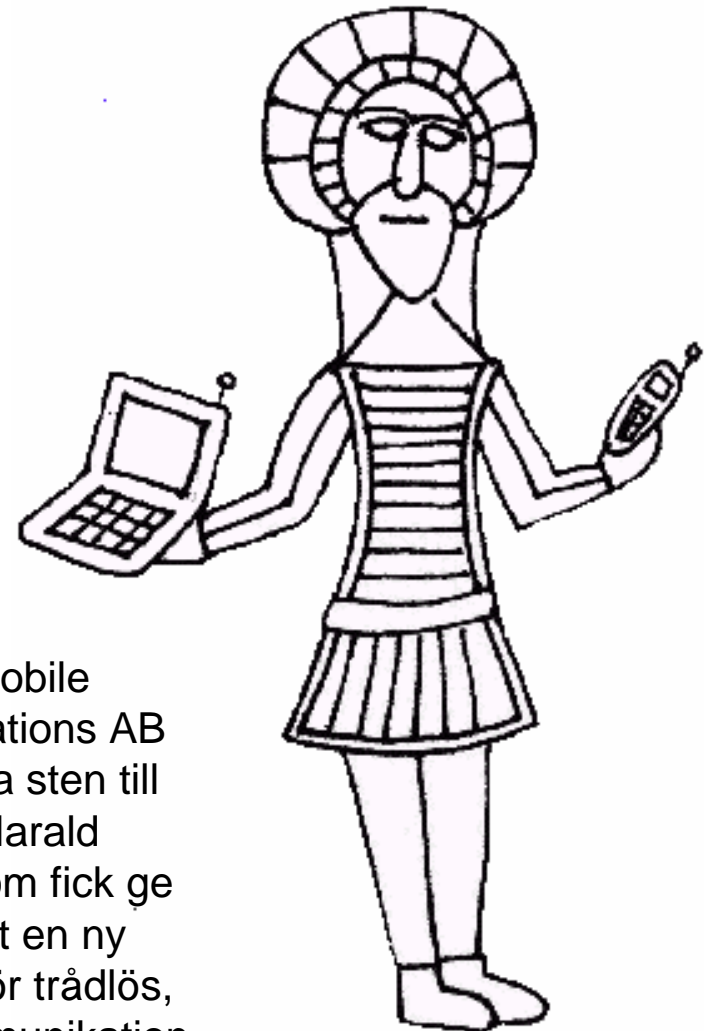
一．藍牙歷史和應用

在很久很久以前，丹麥一個叫哈拉爾德（Harald Gormsson）的海盜，通過自己的力量統一了北歐四分五裂的國家，後來成為國王（有點像秦始皇）。這個國王喜歡吃藍梅，牙齒常常被染成藍色，由此人們都叫他“藍牙”（Bluetooth）（他的名字也可能來源於丹麥文“bla”，意思是黑色皮膚的，或“棕褐色的”，象徵著偉大的人物。）。公元1998年，還是在北歐，一個叫愛立信的公司提出一種無線通信技術，為了使這種技術“一統天下”，取名“藍牙”。“藍牙”技術正是取自10世紀丹麥國王哈拉爾德的別名。

History and hi-tech...



1999:
Ericsson mobile
communications AB
reste denna sten till
minne av Harald
Blåtand, som fick ge
sitt namn åt en ny
teknologi för trådlös,
mobil kommunikation.



...and the real rune stone



Located in Jelling, Denmark,
erected by King Harald “Blåtand”
in memory of his parents.
The stone has three sides – one side
showing a picture of Christ.

Inscription:

"Harald king executes these sepulchral
monuments after Gorm, his father and
Thyra, his mother. The Harald who won the
whole of Denmark and Norway and turned
the Danes to Christianity."

Btw: Blåtand means “of dark complexion”
(not having a blue tooth...)



This could be the “original” colors
of the stone.

Inscription:

“auk tani karthi kristna” (and
made the Danes Christians)

Characteristics

2.4 GHz ISM band, 79 (23) RF channels, 1 MHz carrier spacing

- ❑ Channel 0: 2402 MHz ... channel 78: 2480 MHz
- ❑ G-FSK modulation, 1-100 mW transmit power

FHSS and TDD

- ❑ Frequency hopping with 1600 hops/s
- ❑ Hopping sequence in a pseudo random fashion, determined by a master
- ❑ Time division duplex for send/receive separation

Voice link – SCO (Synchronous Connection Oriented)

- ❑ FEC (forward error correction), no retransmission, 64 kbit/s duplex, point-to-point, circuit switched

Data link – ACL (Asynchronous ConnectionLess)

- ❑ Asynchronous, fast acknowledge, point-to-multipoint, up to 433.9 kbit/s symmetric or 723.2/57.6 kbit/s asymmetric, packet switched

Topology

- ❑ Overlapping piconets (stars) forming a scatternet

Piconet

Collection of devices connected in an ad hoc fashion

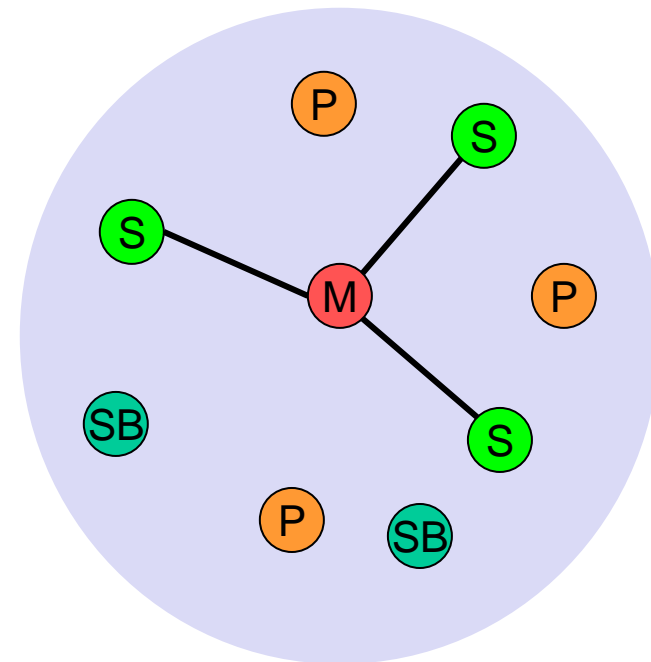
One unit acts as master and the others as slaves for the lifetime of the piconet

Master determines hopping pattern, slaves have to synchronize

Each piconet has a unique hopping pattern

Participation in a piconet = synchronization to hopping sequence

Each piconet has **one master** and up to 7 simultaneous slaves (> 200 could be parked)



M=Master P=Parked
S=Slave SB=Standby

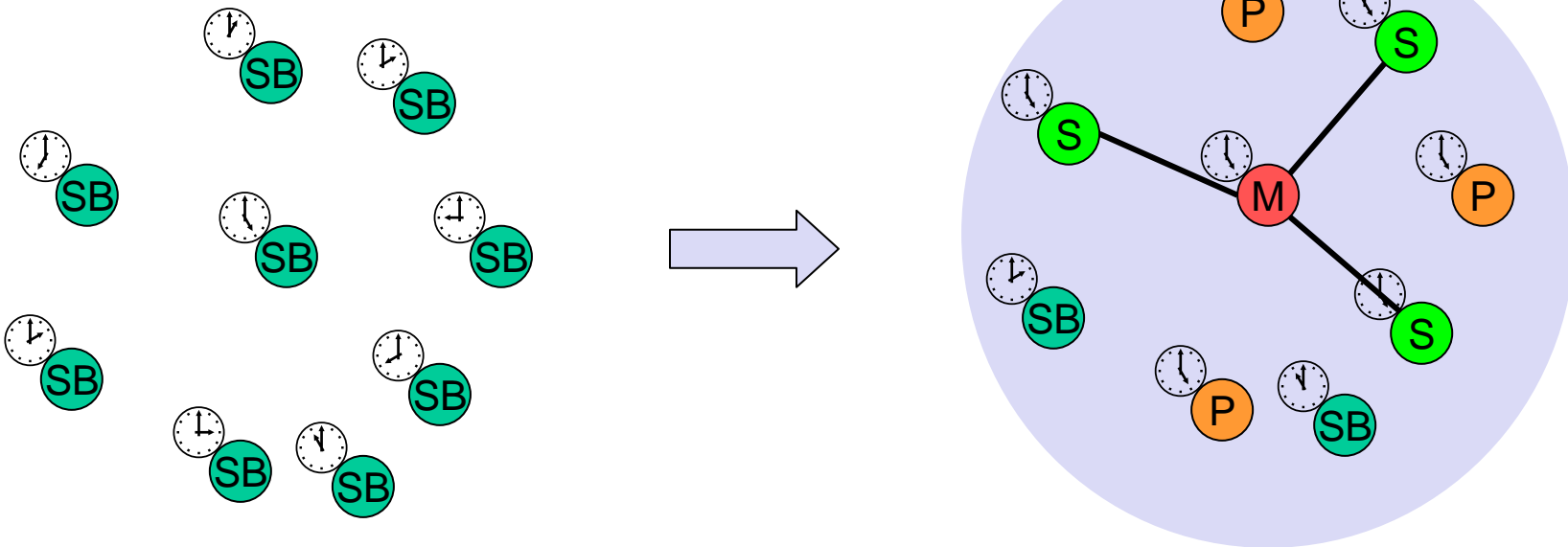
Forming a piconet

All devices in a piconet hop together

- ❑ Master gives slaves its clock and device ID
 - Hopping pattern: determined by device ID (48 bit, unique worldwide)
 - Phase in hopping pattern determined by clock

Addressing

- ❑ Active Member Address (AMA, 3 bit)
- ❑ Parked Member Address (PMA, 8 bit)



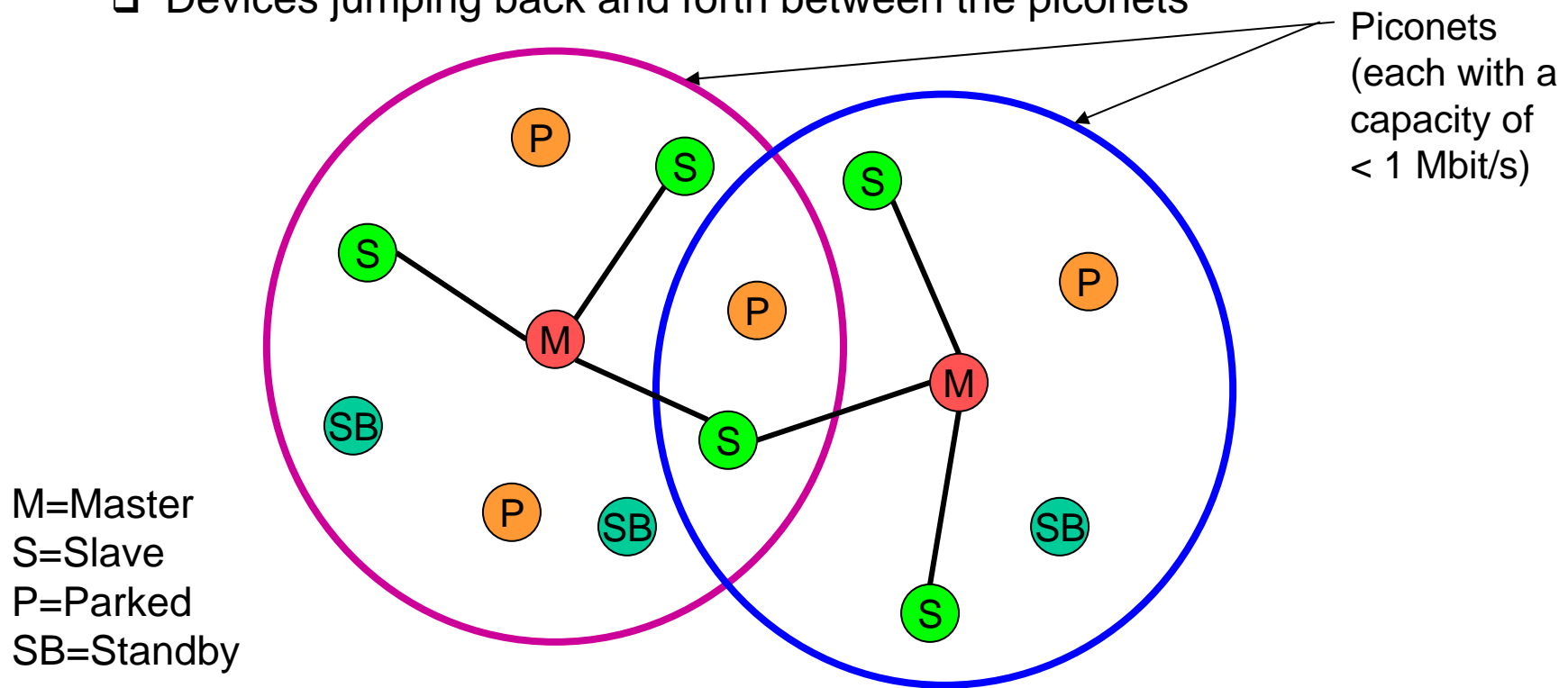
Scatternet

Linking of multiple co-located piconets through the sharing of common master or slave devices

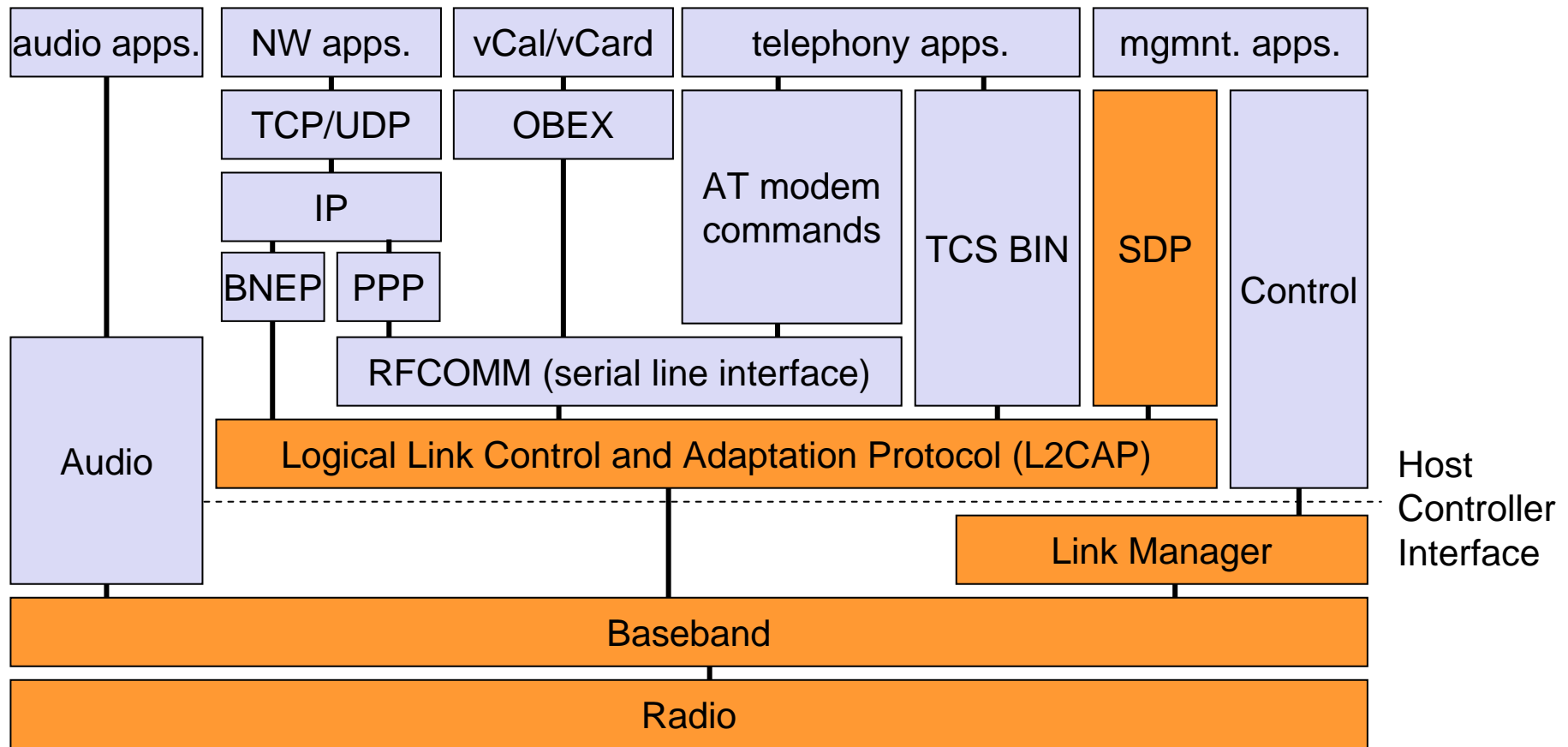
- ❑ Devices can be slave in one piconet and master of another

Communication between piconets

- ❑ Devices jumping back and forth between the piconets



Bluetooth protocol stack



AT: attention sequence

OBEX: object exchange

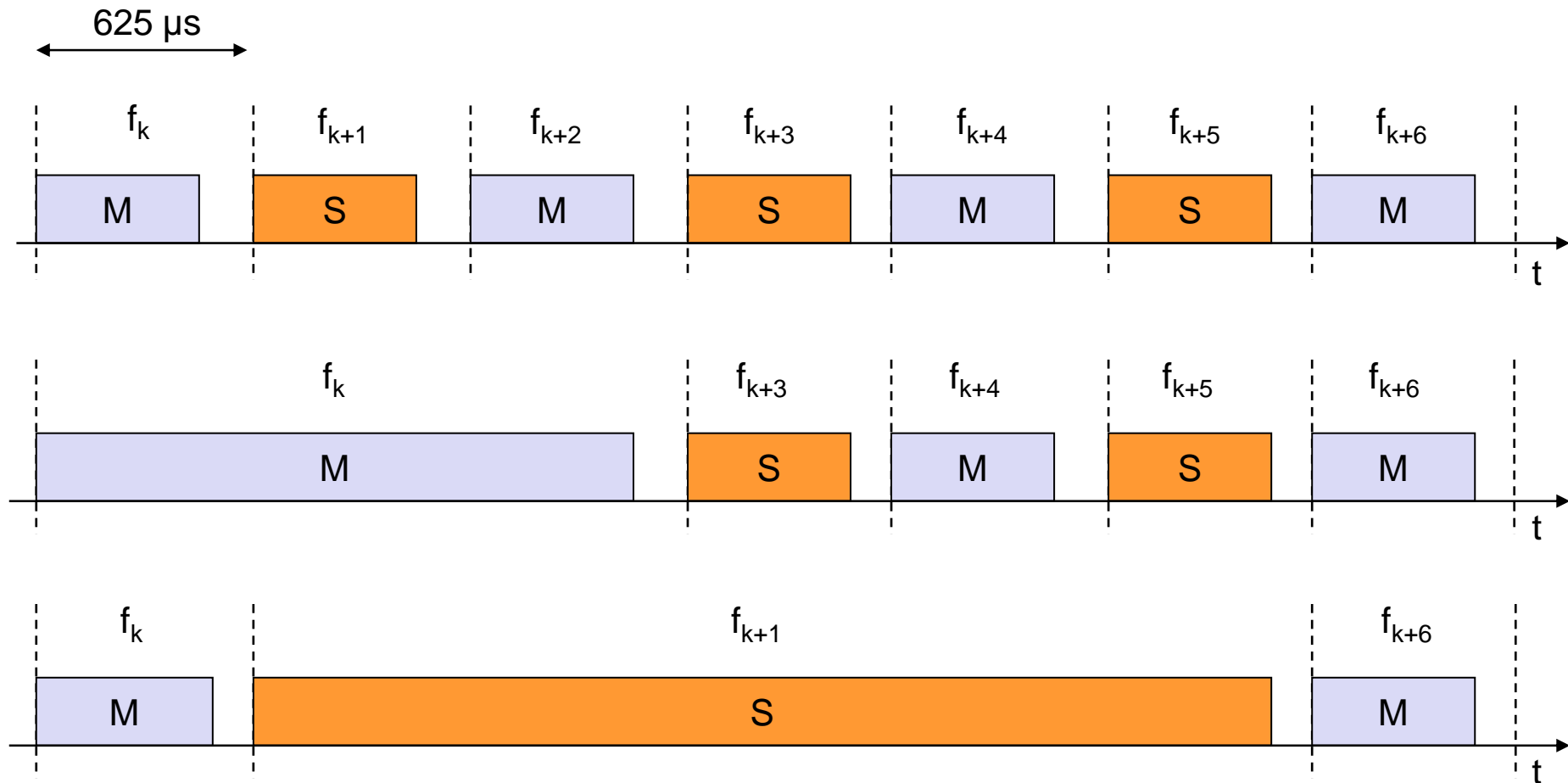
TCS BIN: telephony control protocol specification – binary

BNEP: Bluetooth network encapsulation protocol

SDP: service discovery protocol

RFCOMM: radio frequency comm.

Frequency selection during data transmission



Property

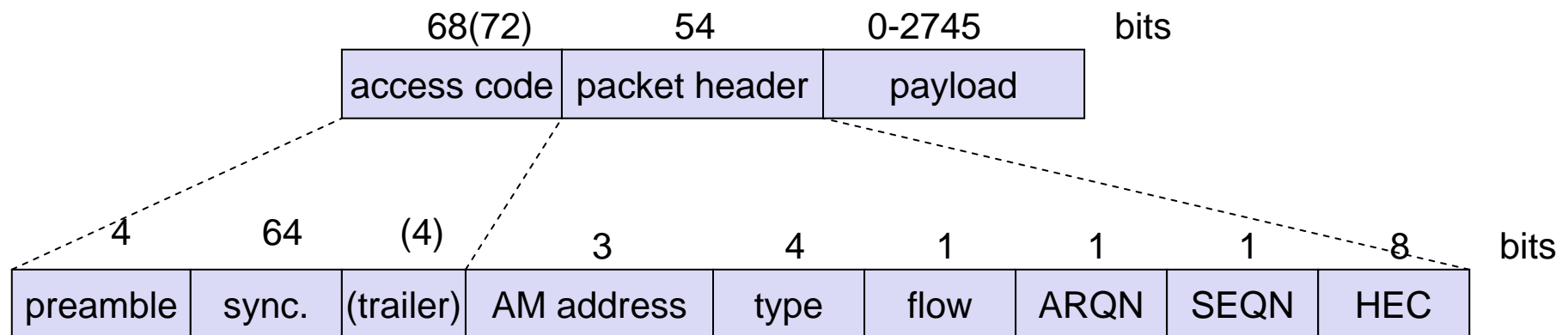
The master always uses the **even** frequency slots, and **odd** slots are for the slaves.

Baseband

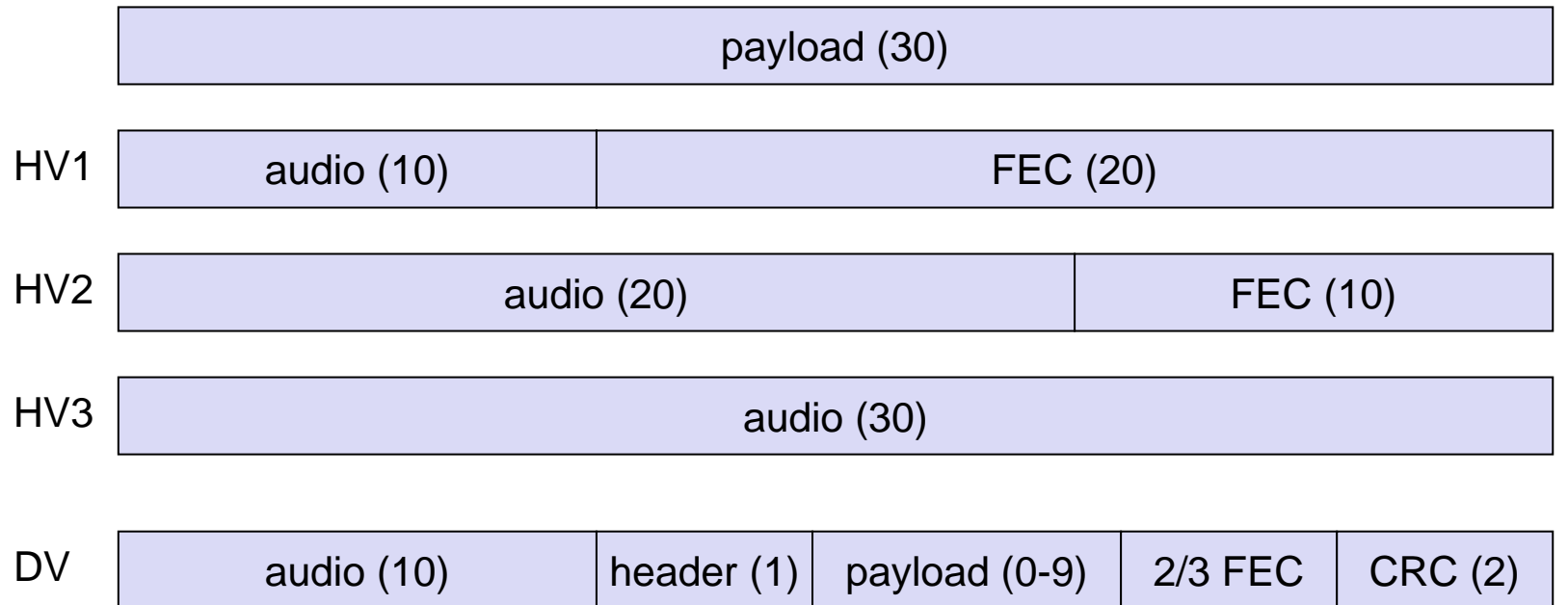
Piconet/channel definition

Low-level packet definition

- ❑ Access code
 - Channel, device access, e.g., derived from master
- ❑ Packet header
 - 1/3-FEC, active member address (broadcast + 7 slaves), link type, alternating bit ARQ/SEQ, checksum

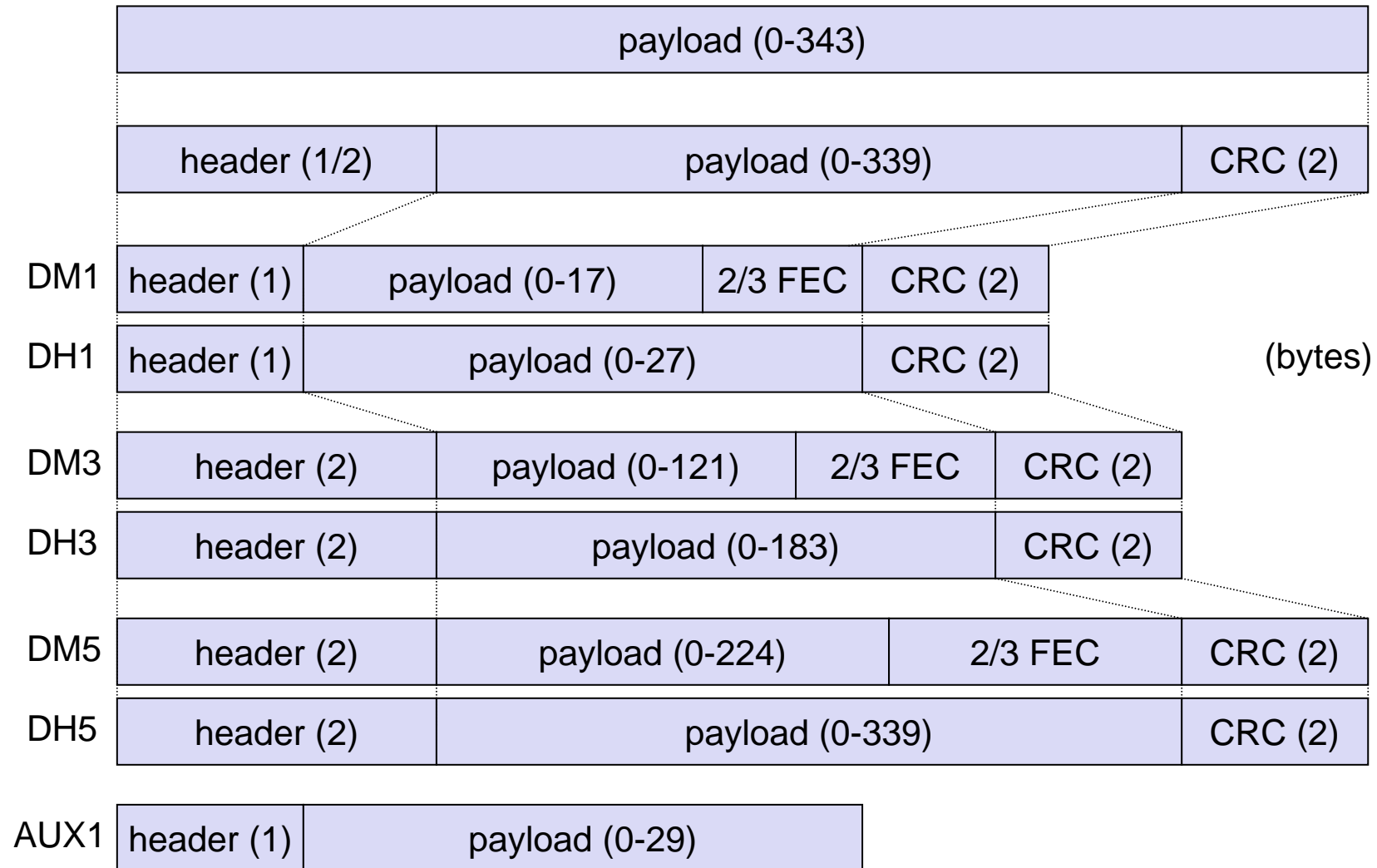


SCO payload types



(bytes)

ACL Payload types

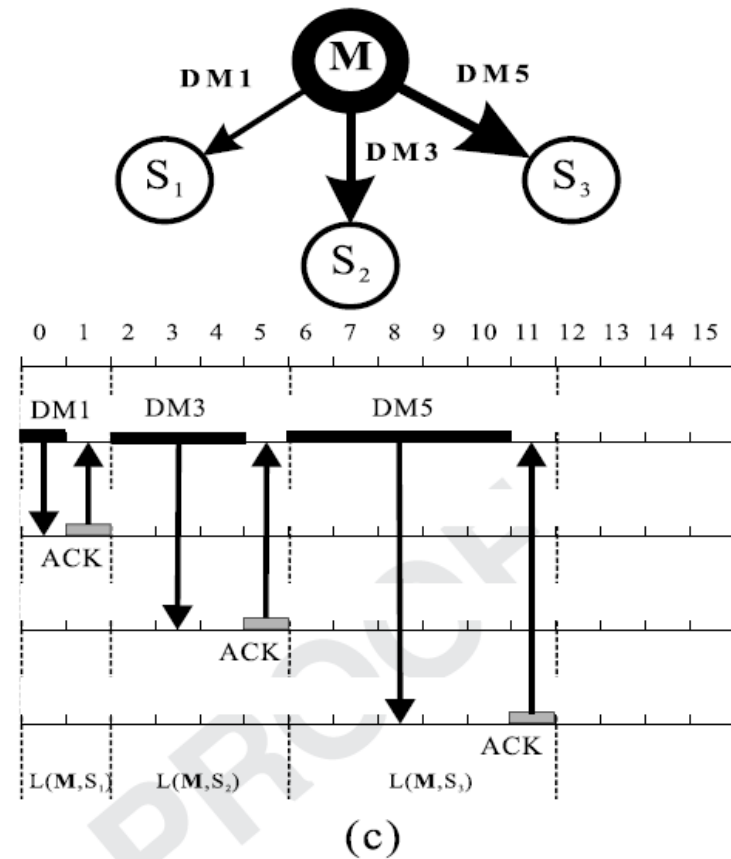
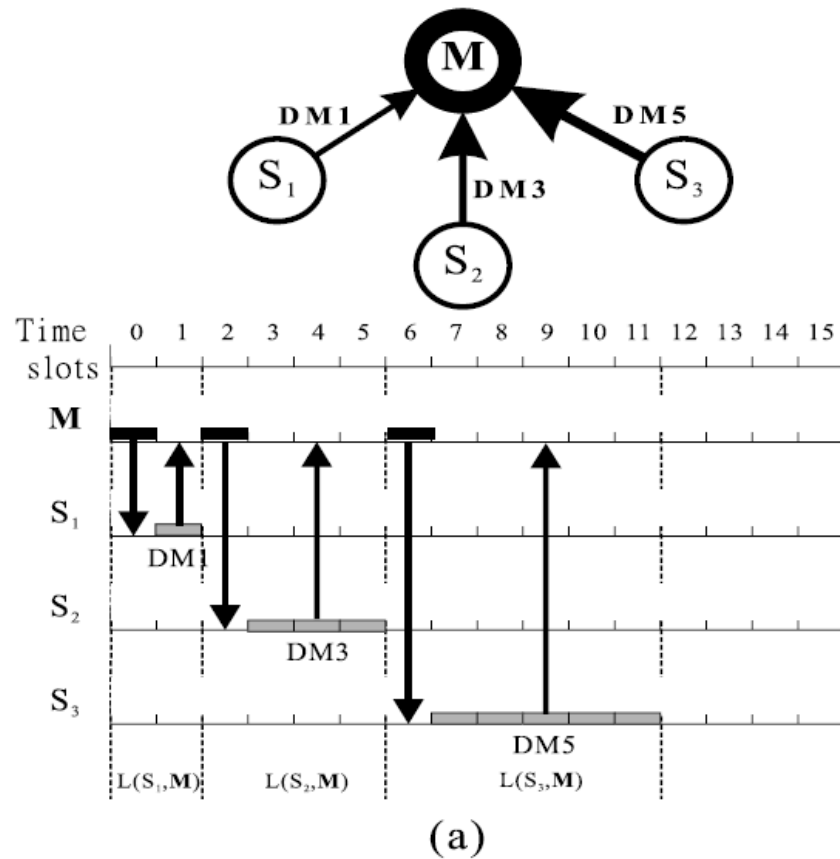


Baseband data rates

ACL	Type	Payload Header	User Payload	FEC	CRC	Symmetric	Asymmetric	
		[byte]	[byte]			max. Rate [kbit/s]	max. Rate Forward	max. Rate Reverse
1 slot	DM1	1	0-17	2/3	yes	108.8	108.8	108.8
	DH1	1	0-27	no	yes	172.8	172.8	172.8
3 slot	DM3	2	0-121	2/3	yes	258.1	387.2	54.4
	DH3	2	0-183	no	yes	390.4	585.6	86.4
5 slot	DM5	2	0-224	2/3	yes	286.7	477.8	36.3
	DH5	2	0-339	no	yes	433.9	723.2	57.6
SCO	AUX1	1	0-29	no	no	185.6	185.6	185.6
	HV1	na	10	1/3	no	64.0		
	HV2	na	20	2/3	no	64.0		
	HV3	na	30	no	no	64.0		
	DV	1 D	10+(0-9) D	2/3 D	yes D	64.0+57.6 D		

Data Medium/High rate, High-quality Voice, Data and Voice

Example



Baseband link types

Polling-based TDD packet transmission

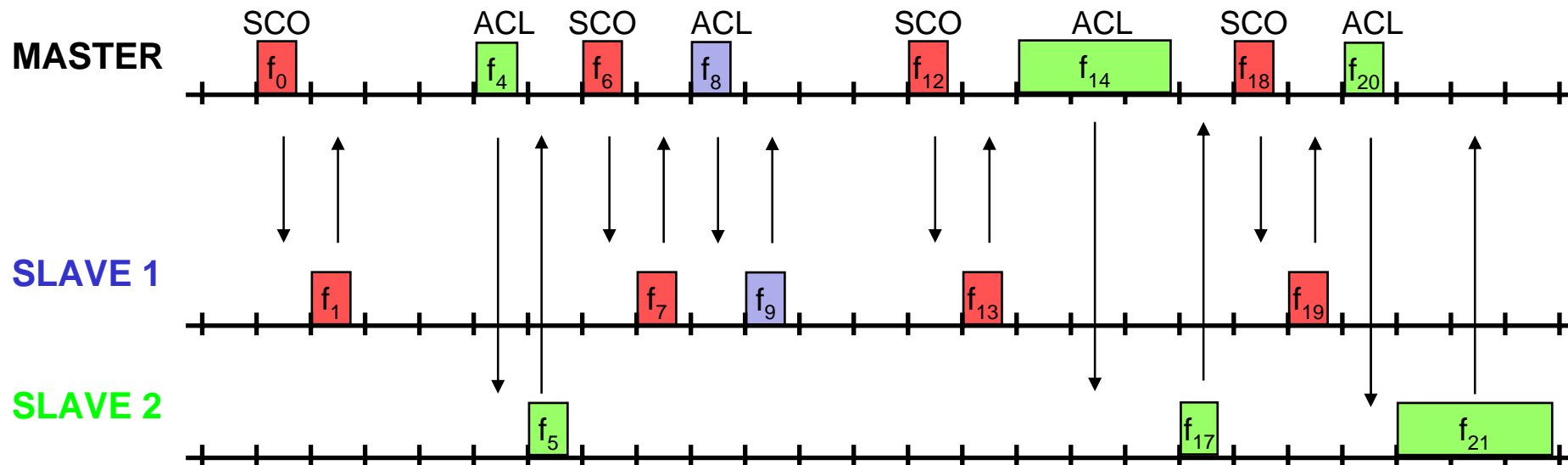
- 625μs slots, master polls slaves

SCO (Synchronous Connection Oriented) – Voice

- Periodic single slot packet assignment, 64 kbit/s full-duplex, point-to-point

ACL (Asynchronous ConnectionLess) – Data

- Variable packet size (1,3,5 slots), asymmetric bandwidth, point-to-multipoint



Robustness

Slow frequency hopping with hopping patterns determined by a master

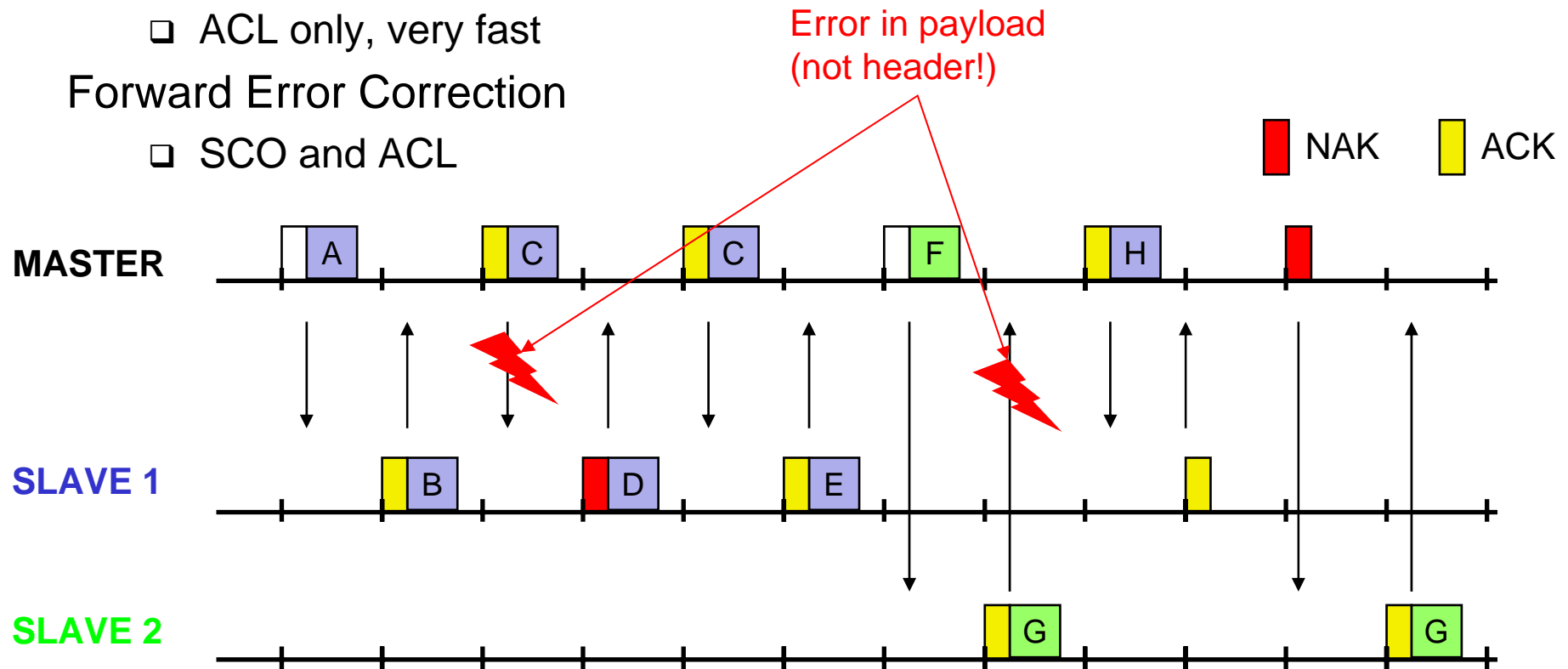
- ❑ Protection from interference on certain frequencies
- ❑ Separation from other piconets (FH-CDMA)

Retransmission

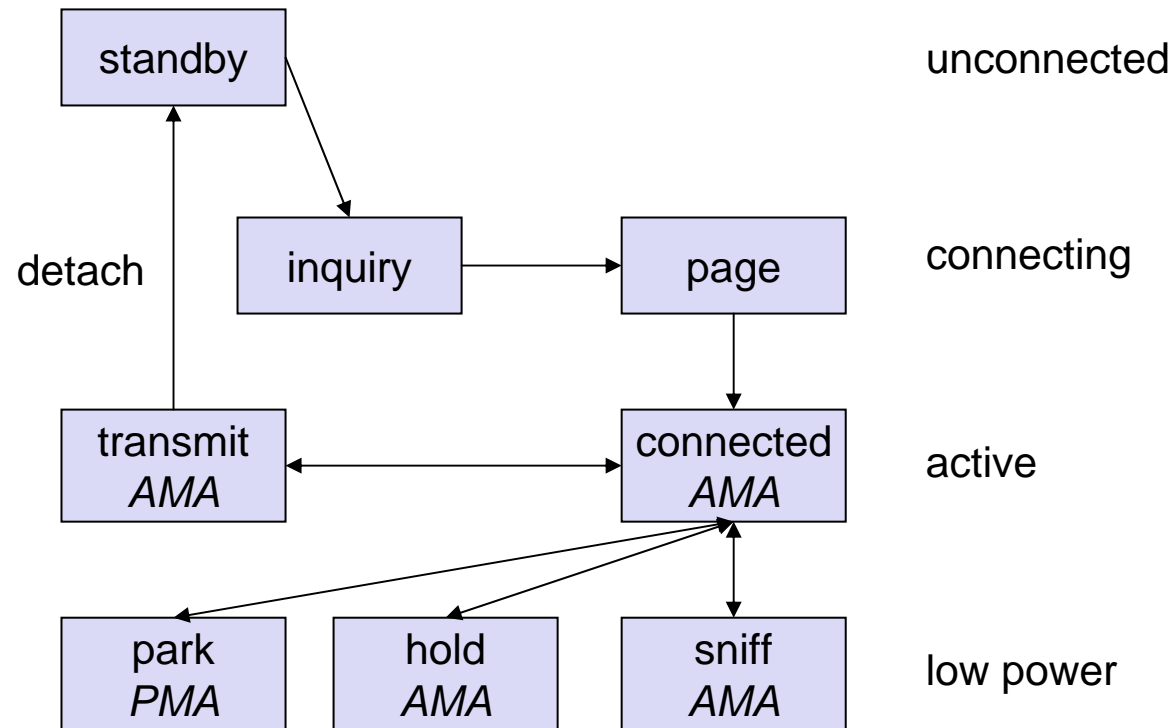
- ❑ ACL only, very fast

Forward Error Correction

- ❑ SCO and ACL



Baseband states of a Bluetooth device



Standby: do nothing

Inquire: search for other devices

Page: connect to a specific device

Connected: participate in a piconet

Park: release *AMA*, get *PMA*

Sniff: listen periodically, not each slot

Hold: stop ACL, SCO still possible, possibly participate in another piconet

Example: Power consumption/CSR BlueCore2

Typical Average Current Consumption (1)

VDD=1.8V Temperature = 20°C

Mode

SCO connection HV3 (1s interval Sniff Mode) (Slave)	26.0 mA
SCO connection HV3 (1s interval Sniff Mode) (Master)	26.0 mA
SCO connection HV1 (Slave)	53.0 mA
SCO connection HV1 (Master)	53.0 mA
ACL data transfer 115.2kbps UART (Master)	15.5 mA
ACL data transfer 720kbps USB (Slave)	53.0 mA
ACL data transfer 720kbps USB (Master)	53.0 mA
ACL connection, Sniff Mode 40ms interval, 38.4kbps UART	4.0 mA
ACL connection, Sniff Mode 1.28s interval, 38.4kbps UART	0.5 mA
Parked Slave, 1.28s beacon interval, 38.4kbps UART	0.6 mA
Standby Mode (Connected to host, no RF activity)	47.0 µA
Deep Sleep Mode(2)	20.0 µA

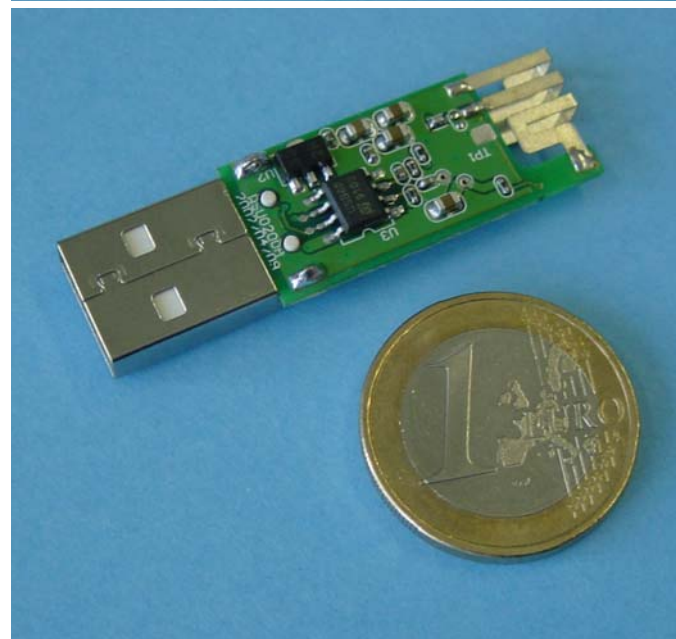
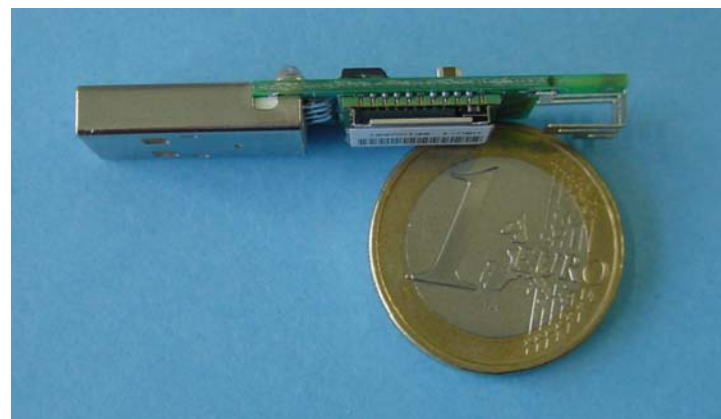
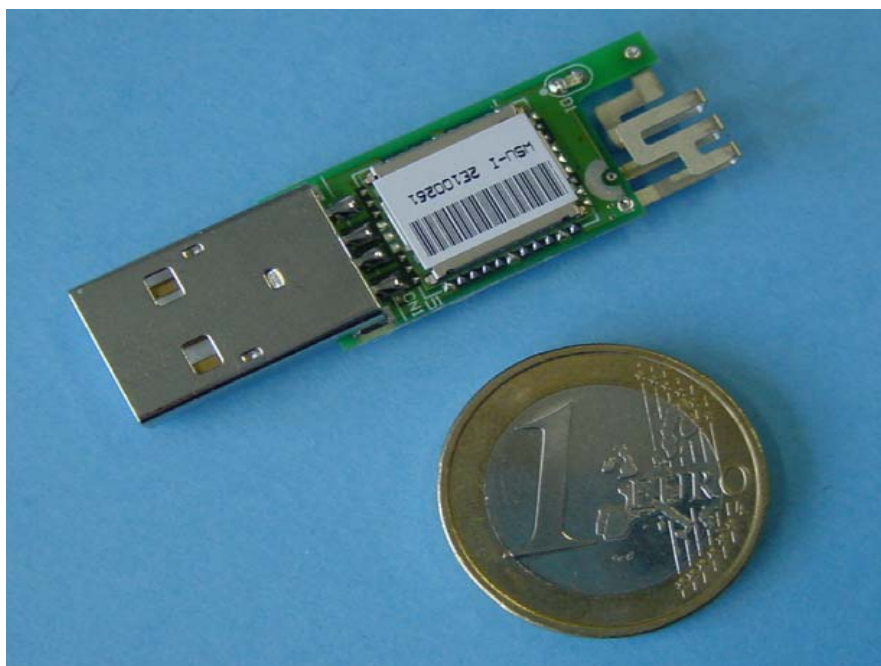
Notes:

(1) Current consumption is the sum of both BC212015A and the flash.

(2) Current consumption is for the BC212015A device only.

(More: www.csr.com)

Example: Bluetooth/USB adapter (2002: 50€)



L2CAP - Logical Link Control and Adaptation Protocol

Simple data link protocol on top of baseband

Connection oriented, connectionless, and signalling channels

Protocol multiplexing

- ❑ RFCOMM, SDP, telephony control

Segmentation & reassembly

- ❑ Up to 64kbyte user data, 16 bit CRC used from baseband

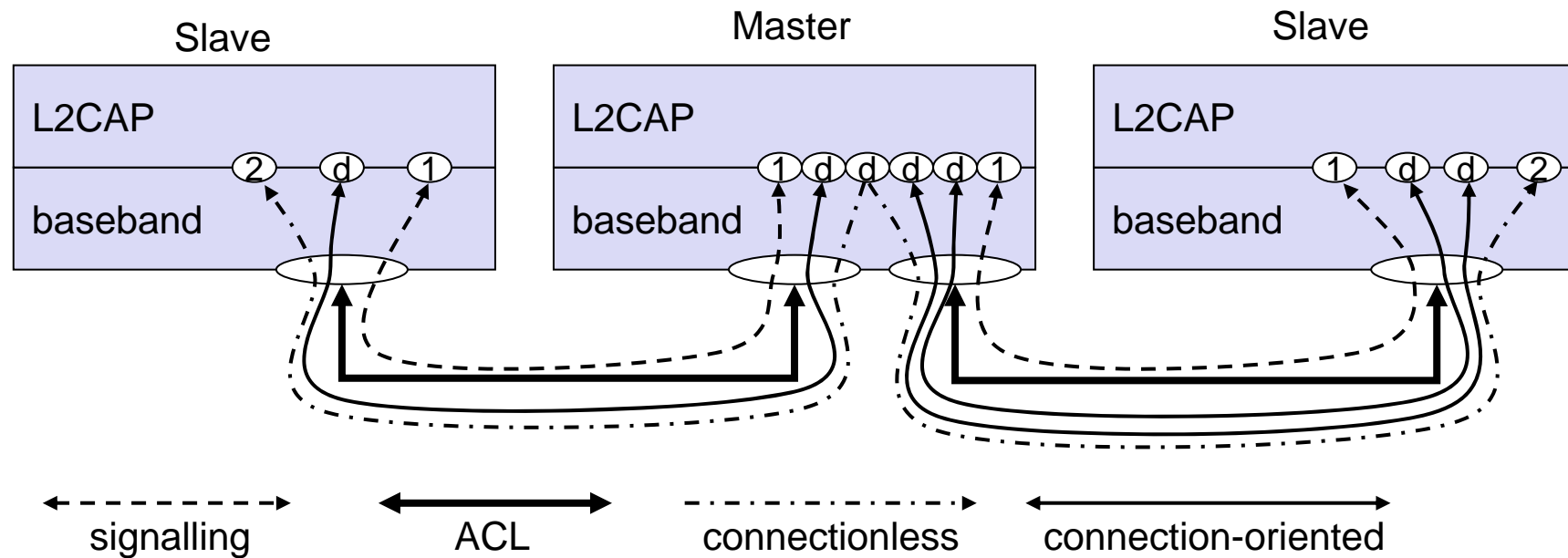
QoS flow specification per channel

- ❑ Follows RFC 1363, specifies delay, jitter, bursts, bandwidth

Group abstraction

- ❑ Create/close group, add/remove member

L2CAP logical channels



L2CAP packet formats

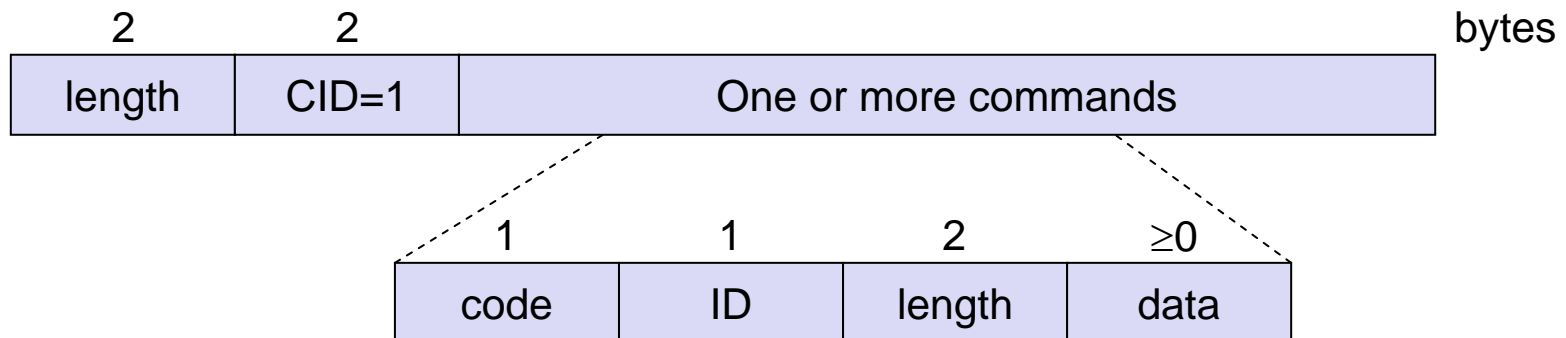
Connectionless PDU



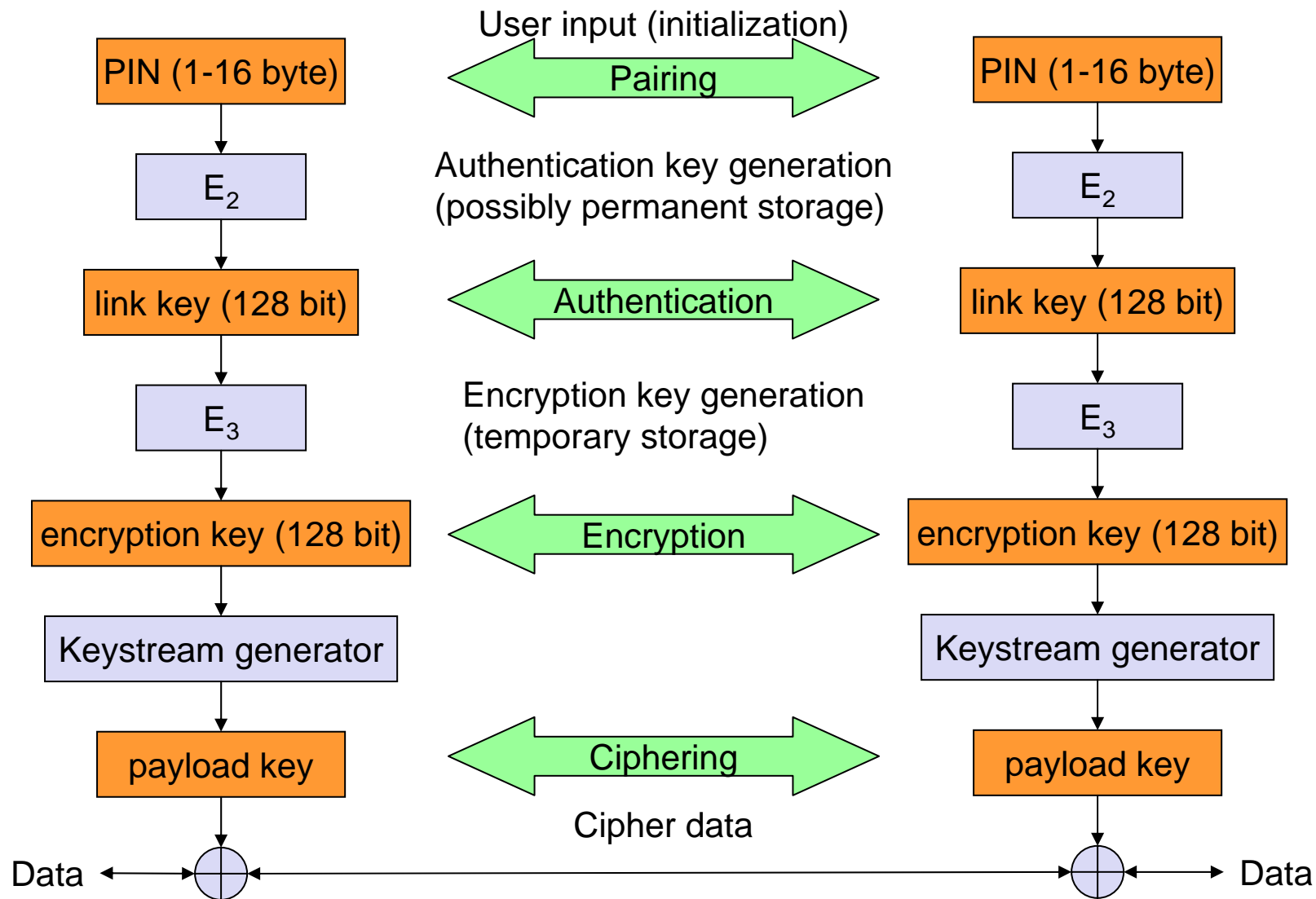
Connection-oriented PDU



Signalling command PDU



Security



SDP – Service Discovery Protocol

Inquiry/response protocol for discovering services

- ❑ Searching for and browsing services in radio proximity
- ❑ Adapted to the highly dynamic environment
- ❑ Can be complemented by others like SLP, Jini, Salutation, ...
- ❑ Defines discovery only, not the usage of services
- ❑ Caching of discovered services
- ❑ Gradual discovery

Service record format

- ❑ Information about services provided by attributes
- ❑ Attributes are composed of an 16 bit ID (name) and a value
- ❑ values may be derived from 128 bit Universally Unique Identifiers (UUID)

Additional protocols to support legacy protocols/apps.

RFCOMM

- ❑ Emulation of a serial port (supports a large base of legacy applications)
- ❑ Allows multiple ports over a single physical channel

Telephony Control Protocol Specification (TCS)

- ❑ Call control (setup, release)
- ❑ Group management

OBEX

- ❑ Exchange of objects, IrDA replacement

WAP

- ❑ Interacting with applications on cellular phones

Profiles

Represent default solutions for a certain usage model

- ❑ Vertical slice through the protocol stack
- ❑ Basis for interoperability

Generic Access Profile

Service Discovery Application Profile

Cordless Telephony Profile

Intercom Profile

Serial Port Profile

Headset Profile

Dial-up Networking Profile

Fax Profile

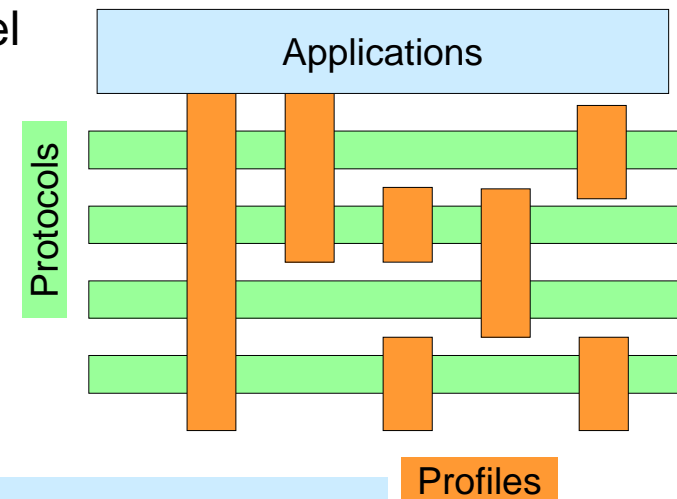
LAN Access Profile

Generic Object Exchange Profile

Object Push Profile

File Transfer Profile

Synchronization Profile



Additional Profiles

Advanced Audio Distribution
PAN

Audio Video Remote Control

Basic Printing

Basic Imaging

Extended Service Discovery

Generic Audio Video Distribution

Hands Free

Hardcopy Cable Replacement

WPAN: IEEE 802.15-1 – Bluetooth

Data rate

- ❑ Synchronous, connection-oriented: 64 kbit/s
- ❑ Asynchronous, connectionless
 - 433.9 kbit/s symmetric
 - 723.2 / 57.6 kbit/s asymmetric

Transmission range

- ❑ POS (Personal Operating Space) up to 10 m
- ❑ with special transceivers up to 100 m

Frequency

- ❑ Free 2.4 GHz ISM-band

Security

- ❑ Challenge/response (SAFER+), hopping sequence

Cost

- ❑ 50€ adapter, drop to 5€ if integrated

Availability

- ❑ Integrated into some products, several vendors

Connection set-up time

- ❑ Depends on power-mode
- ❑ Max. 2.56s, avg. 0.64s

Quality of Service

- ❑ Guarantees, ARQ/FEC

Manageability

- ❑ Public/private keys needed, key management not specified, simple system integration

Special Advantages/Disadvantages

- ❑ Advantage: already integrated into several products, available worldwide, free ISM-band, several vendors, simple system, simple ad-hoc networking, peer to peer, scatternets
- ❑ Disadvantage: interference on ISM-band, limited range, max. 8 devices/network&master, high set-up latency

WPAN: IEEE 802.15 – future developments 1

802.15-2: Coexistence

- ❑ Coexistence of Wireless Personal Area Networks (802.15) and Wireless Local Area Networks (802.11), quantify the mutual interference

802.15-3: High-Rate

- ❑ Standard for high-rate (20Mbit/s or greater) WPANs, while still low-power/low-cost
- ❑ Data Rates: 11, 22, 33, 44, 55 Mbit/s
- ❑ Quality of Service isochronous protocol
- ❑ Ad hoc peer-to-peer networking
- ❑ Security
- ❑ Low power consumption
- ❑ Low cost
- ❑ Designed to meet the demanding requirements of portable consumer imaging and multimedia applications

WPAN: IEEE 802.15 – future developments 2

802.15-4: Low-Rate, Very Low-Power

- ❑ Low data rate solution with multi-month to multi-year battery life and very low complexity
- ❑ Potential applications are sensors, interactive toys, smart badges, remote controls, and home automation
- ❑ Data rates of 20-250 kbit/s, latency down to 15 ms
- ❑ Master-Slave or Peer-to-Peer operation
- ❑ Support for critical latency devices, such as joysticks
- ❑ CSMA/CA channel access (data centric), slotted (beacon) or unslotted
- ❑ Automatic network establishment by the PAN coordinator
- ❑ Dynamic device addressing, flexible addressing format
- ❑ Fully handshaked protocol for transfer reliability
- ❑ Power management to ensure low power consumption
- ❑ 16 channels in the 2.4 GHz ISM band, 10 channels in the 915 MHz US ISM band and one channel in the European 868 MHz band

WLAN: Home RF

Data rate

- ❑ 0.8, 1.6, 5, 10 Mbit/s

Transmission range

- ❑ 300m outdoor, 30m indoor

Frequency

- ❑ 2.4 GHz ISM

Security

- ❑ Strong encryption, no open access

Cost

- ❑ Adapter 130€, base station 230€

Availability

- ❑ Several products from different vendors

Connection set-up time

- ❑ 10 ms bounded latency

Quality of Service

- ❑ Up to 8 streams A/V, up to 8 voice streams, priorities, best-effort

Manageability

- ❑ Like DECT & 802-LANs

Special Advantages/Disadvantages

- ❑ Advantage: extended QoS support, host/client and peer/peer, power saving, security
- ❑ Disadvantage: future uncertain due to DECT-only devices plus 802.11a/b for data

RF Controllers – ISM bands

Data rate

- ❑ Typ. up to 115 kbit/s (serial interface)

Transmission range

- ❑ 5-100 m, depending on power (typ. 10-500 mW)

Frequency

- ❑ Typ. 27 (EU, US), 315 (US), 418 (EU), 426 (Japan), 433 (EU), 868 (EU), 915 (US) MHz (depending on regulations)

Security

- ❑ Some products with added processors

Cost

- ❑ Cheap: 10€-50€

Availability

- ❑ Many products, many vendors

Connection set-up time

- ❑ N/A

Quality of Service

- ❑ none

Manageability

- ❑ Very simple, same as serial interface

Special Advantages/Disadvantages

- ❑ Advantage: very low cost, large experience, high volume available
- ❑ Disadvantage: no QoS, crowded ISM bands (particularly 27 and 433 MHz), typ. no Medium Access Control, 418 MHz experiences interference with TETRA

RFID – Radio Frequency Identification (1)

Data rate

- ❑ Transmission of ID only (e.g., 48 bit, 64kbit, 1 Mbit)
- ❑ 9.6 – 115 kbit/s

Transmission range

- ❑ Passive: up to 3 m
- ❑ Active: up to 30-100 m
- ❑ Simultaneous detection of up to, e.g., 256 tags, scanning of, e.g., 40 tags/s

Frequency

- ❑ 125 kHz, 13.56 MHz, 433 MHz, 2.4 GHz, 5.8 GHz and many others

Security

- ❑ Application dependent, typ. no crypt. on RFID device

Cost

- ❑ Very cheap tags, down to 1€ (passive)

Availability

- ❑ Many products, many vendors

Connection set-up time

- ❑ Depends on product/medium access scheme (typ. 2 ms per device)

Quality of Service

- ❑ none

Manageability

- ❑ Very simple, same as serial interface

Special Advantages/Disadvantages

- ❑ Advantage: extremely low cost, large experience, high volume available, no power for passive RFIDs needed, large variety of products, relative speeds up to 300 km/h, broad temp. range
- ❑ Disadvantage: no QoS, simple denial of service, crowded ISM bands, typ. one-way (activation/ transmission of ID)

RFID – Radio Frequency Identification (2)

Function

- ❑ Standard: In response to a radio interrogation signal from a reader (base station) the RFID tags transmit their ID
- ❑ Enhanced: additionally data can be sent to the tags, different media access schemes (collision avoidance)

Features

- ❑ No line-of sight required (compared to, e.g., laser scanners)
- ❑ RFID tags withstand difficult environmental conditions (sunlight, cold, frost, dirt etc.)
- ❑ Products available with read/write memory, smart-card capabilities

Categories

- ❑ Passive RFID: operating power comes from the reader over the air which is feasible up to distances of 3 m, low price (1€)
- ❑ Active RFID: battery powered, distances up to 100 m

RFID – Radio Frequency Identification (3)

Applications

- ❑ Total asset visibility: tracking of goods during manufacturing, localization of pallets, goods etc.
- ❑ Loyalty cards: customers use RFID tags for payment at, e.g., gas stations, collection of buying patterns
- ❑ Automated toll collection: RFIDs mounted in windshields allow commuters to drive through toll plazas without stopping
- ❑ Others: access control, animal identification, tracking of hazardous material, inventory control, warehouse management, ...

Local Positioning Systems

- ❑ GPS useless indoors or underground, problematic in cities with high buildings
- ❑ RFID tags transmit signals, receivers estimate the tag location by measuring the signal's time of flight

RFID – Radio Frequency Identification (4)

Security

- ❑ Denial-of-Service attacks are always possible
 - Interference of the wireless transmission, shielding of transceivers
- ❑ IDs via manufacturing or one time programming
- ❑ Key exchange via, e.g., RSA possible, encryption via, e.g., AES

Future Trends

- ❑ RTLS: Real-Time Locating System – big efforts to make total asset visibility come true
- ❑ Integration of RFID technology into the manufacturing, distribution and logistics chain
- ❑ Creation of „electronic manifests“ at item or package level (embedded inexpensive passive RFID tags)
- ❑ 3D tracking of children, patients

RFID – Radio Frequency Identification (5)

Devices and Companies

- ❑ AXCESS Inc., www.axcessinc.com
- ❑ Checkpoint Systems Group, www.checkpointsystems.com
- ❑ GEMPLUS, www.gemplus.com/app/smart_tracking
- ❑ Intermec/Intellitag, www.intermec.com
- ❑ I-Ray Technologies, www.i-ray.com
- ❑ RF Code, www.rfcode.com
- ❑ Texas Instruments, www.ti-rfid.com/id
- ❑ WhereNet, www.wherenet.com
- ❑ Wireless Mountain, www.wirelessmountain.com
- ❑ XCI, www.xci-inc.com

Only a very small selection...

RFID – Radio Frequency Identification (6)

Example Product: Intermec RFID UHF OEM Reader

- ❑ Read range up to 7m
- ❑ Anticollision algorithm allows for scanning of 40 tags per second regardless of the number of tags within the reading zone
- ❑ US: unlicensed 915 MHz, Frequency Hopping
- ❑ Read: 8 byte < 32 ms
- ❑ Write: 1 byte < 100ms



Example Product: Wireless Mountain Spider

- ❑ Proprietary sparse code anti-collision algorithm
- ❑ Detection range 15 m indoor, 100 m line-of-sight
- ❑ > 1 billion distinct codes
- ❑ Read rate > 75 tags/s
- ❑ Operates at 308 MHz



RFID – Radio Frequency Identification (7)

Relevant Standards

- ❑ American National Standards Institute
 - ANSI, www.ansi.org, www.aimglobal.org/standards/rfidstds/ANSIT6.html
- ❑ Automatic Identification and Data Capture Techniques
 - JTC 1/SC 31, www.uc-council.com/sc31/home.htm,
www.aimglobal.org/standards/rfidstds/sc31.htm
- ❑ European Radiocommunications Office
 - ERO, www.ero.dk, www.aimglobal.org/standards/rfidstds/ERO.htm
- ❑ European Telecommunications Standards Institute
 - ETSI, www.etsi.org, www.aimglobal.org/standards/rfidstds/ETSI.htm
- ❑ Identification Cards and related devices
 - JTC 1/SC 17, www.sc17.com, www.aimglobal.org/standards/rfidstds/sc17.htm,
- ❑ Identification and communication
 - ISO TC 104 / SC 4, www.autoid.org/tc104_sc4_wg2.htm,
www.aimglobal.org/standards/rfidstds/TC104.htm
- ❑ Road Transport and Traffic Telematics
 - CEN TC 278, www.nni.nl, www.aimglobal.org/standards/rfidstds/CENTC278.htm
- ❑ Transport Information and Control Systems
 - ISO/TC204, www.sae.org/technicalcommittees/gits.htm,
www.aimglobal.org/standards/rfidstds/ISOTC204.htm

RFID – Radio Frequency Identification (8)

ISO Standards

- ❑ ISO 15418
 - MH10.8.2 Data Identifiers
 - EAN.UCC Application Identifiers
- ❑ ISO 15434 - Syntax for High Capacity ADC Media
- ❑ ISO 15962 - Transfer Syntax
- ❑ ISO 18000
 - Part 2, 125-135 kHz
 - Part 3, 13.56 MHz
 - Part 4, 2.45 GHz
 - Part 5, 5.8 GHz
 - Part 6, UHF (860-930 MHz, 433 MHz)
- ❑ ISO 18047 - RFID Device Conformance Test Methods
- ❑ ISO 18046 - RF Tag and Interrogator Performance Test Methods

ISM band interference

Many sources of interference

- ❑ Microwave ovens, microwave lightning
- ❑ 802.11, 802.11b, 802.11g, 802.15, Home RF
- ❑ Even analog TV transmission, surveillance
- ❑ Unlicensed metropolitan area networks
- ❑ ...

Levels of interference

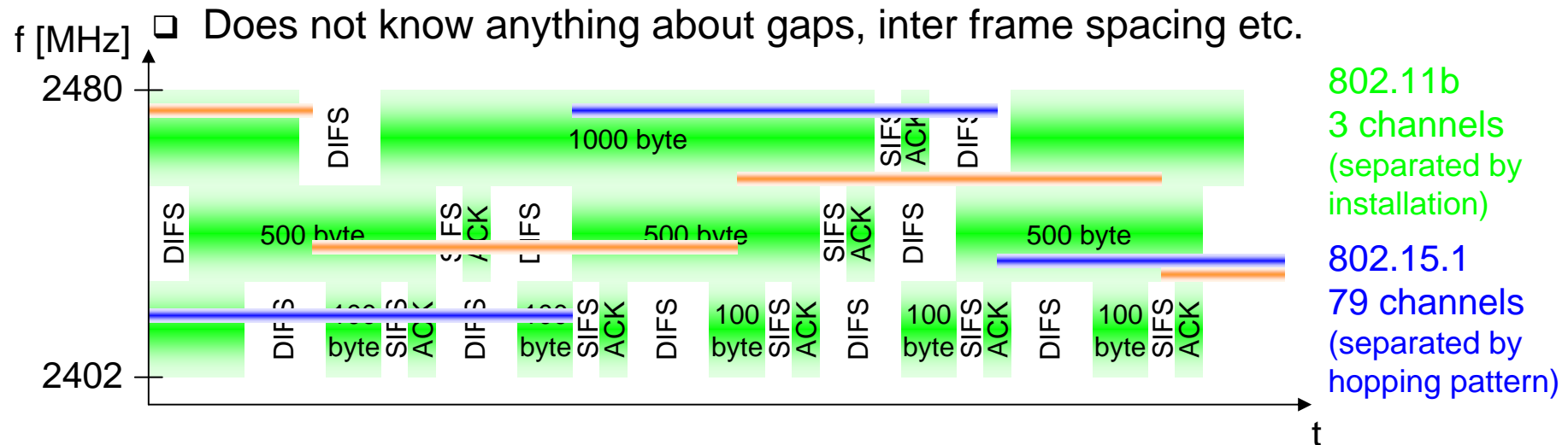
- ❑ Physical layer: interference acts like noise
 - Spread spectrum tries to minimize this
 - FEC/interleaving tries to correct
- ❑ MAC layer: algorithms not harmonized
 - E.g., Bluetooth might confuse 802.11



© Fusion Lighting, Inc.

802.11 vs.(?) 802.15/Bluetooth

Bluetooth may act like a rogue member of the 802.11 network



IEEE 802.15-2 discusses these problems

- Proposal: Adaptive Frequency Hopping
 - a non-collaborative Coexistence Mechanism

Real effects? Many different opinions, publications, tests, formulae, ...

- Results from complete breakdown to almost no effect
- Bluetooth (FHSS) seems more robust than 802.11b (DSSS)

Homework #3:

1. What's piconet and scatternet in Bluetooth networks ?
2. What's ACL and SCO in Bluetooth networks ?