Bluetooth Vs. 802.11

Pravin Bhagwat

ReefEdge, Inc.
pravin@acm.org
http://www.cs.umd.edu/~pravin

Hot Interconnects
Aug 24, 2001

Bluetooth

- A cable replacement technology
- 1 Mb/s symbol rate
- Range 10+ meters
- Single chip radio + baseband
  ‣ at low power & low price point ($5)

Why not use Wireless LANs?
 - power
  - cost

802.11
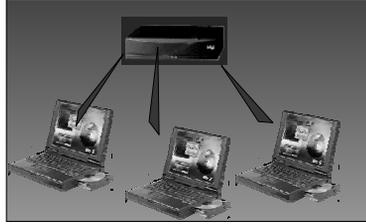
- Replacement for Ethernet
- Supported data rates
  - Current: 11, 5.5, 2, 1 Mbps
  - Future: 20+ Mbps in 2.4 GHz and up to 54 Mbps in 5.7 GHz band
- Range
  - Indoor 20 - 25 meters
  - Outdoor: 50 – 100 meters
- Transmit power up to 100 mW
- Cost:
  - Chipsets $ 35 – 50
  - AP $200 - $1000
  - PCMCIA cards $100 - $150

Emerging Landscape

802.11
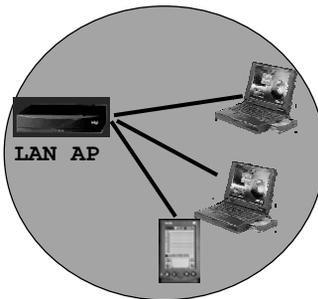
Bluetooth

New developments are blurring the distinction

- 802.11b for PDAs
- Bluetooth for LAN access

Cordless headset

LAN AP
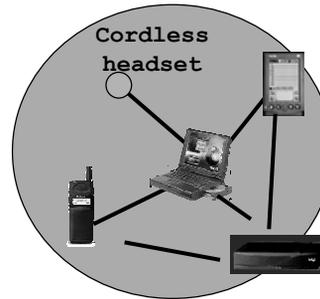
- Which option is technically superior ?
- What market forces are at play ?
- What can be said about the future ?

Questions I hope to answer

- What are the key design differences between Bluetooth and 802.11 ?
    - ▸ At PHY, MAC, and System level
- How do Bluetooth and 802.11 compare ?
    - ▸ Cost, Range of communication, performance
- Why is Bluetooth supposed to be low cost and low power ? Can 802.11 achieve the same price and performance target ?
- Is Bluetooth more secure than 802.11 ?
- What is the reality behind the hype ?
- Can the two systems co-exist ?

Tutorial Overview

1:30 – 2:00 pm	Introduction, Bluetooth history, basic radio concepts, Bluetooth RF
2:00 - 2:30 pm	Bluetooth Baseband
2:30 - 3:00 pm	LMP, Security
3:00 - 3:30 pm	SDP, Scatternets
3:30 - 4:00 pm	802.11 specifications overview, PHY
4:00 - 4:30 pm	MAC, WEP
4:30 - 5:00 pm	Comparison, Conclusion

Bluetooth working group history

- February 1998: The Bluetooth SIG is formed
  - ‣ promoter company group: 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: ver. 1.0B is released
- December 1999: The promoter group increases to 9
  - ‣ 3Com, Lucent, Microsoft, Motorola
- March 2001: ver. 1.1 is released
- Aug 2001: There are 2,491+ adopter companies

New Applications

Synchronization

User benefits

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

Cordless Headset

Cordless headset

User benefits

- **Multiple device access**
- **Cordless phone benefits**
- **Hands free operation**
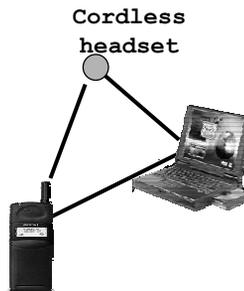
Usage scenarios examples

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

Bluetooth Specifications

Bluetooth Specifications

Applications

IP

SDP

RFCOMM

Data

HCI

Audio

L2CAP

Link Manager

Baseband

RF

Single chip with RS-232, USB, or PC card interface
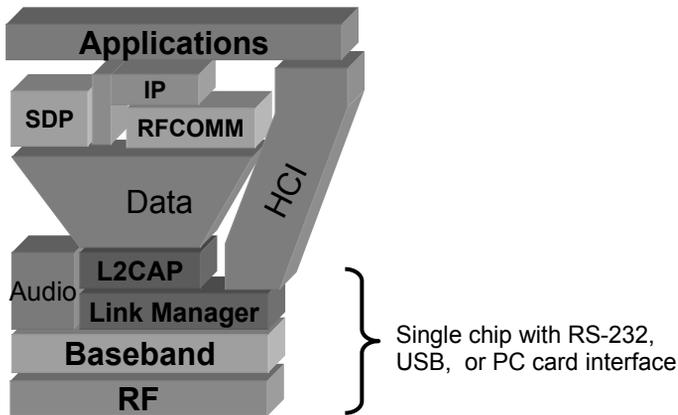
- A hardware/software/protocol description
- An application framework

P. Bhagwat   13

Interoperability & Profiles

- Represents default solution for a usage model
- Vertical slice through the protocol stack
- Basis for interoperability and logo requirements
- Each Bluetooth device supports one or more profiles

Applications

Protocols

Profiles

P. Bhagwat   14
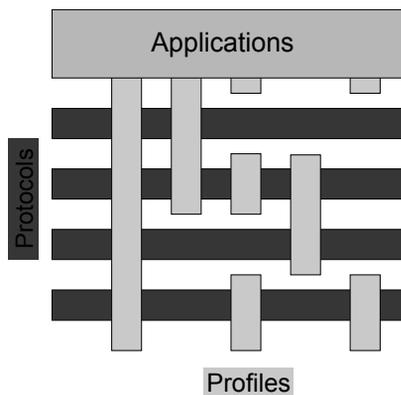
Technical Overview

Bluetooth Radio Specification

Design considerations

Noise, interference

power

Data signal x(t)

spectrum

Recovered data signal
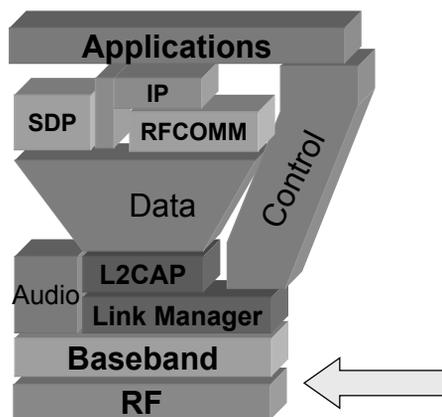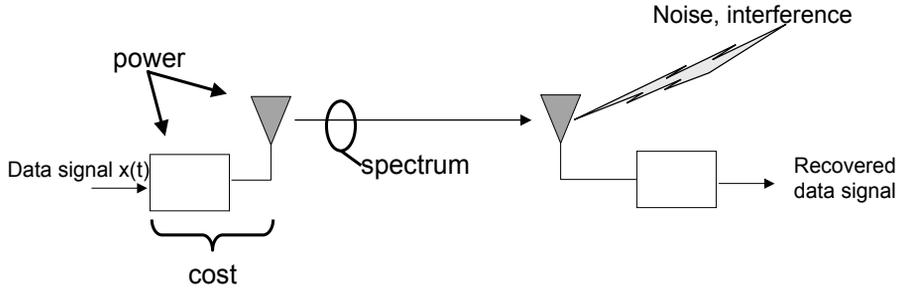
cost

Goal

- high bandwidth
- conserve battery power
- cost < $10

EM Spectrum

ISM band
902 - 928 Mhz

2.4 - 2.4835 Ghz

5.725 - 5.785 Ghz

AM radio

S/W radio

FM radio

TV   TV   cellular

| LF | MF | HF | VHF | UHF | SHF | EHF |

ν

30kHz   300kHz   3MHz   30MHz   300MHz   3GHz   30GHz   300GHz

10km   1km   100m   10m   1m   10cm   1cm   100mm   λ

ν

X rays

Gamma rays

infrared visible UV

1 kHz   1 MHz   1 GHz   1 THz   1 PHz   1 EHz
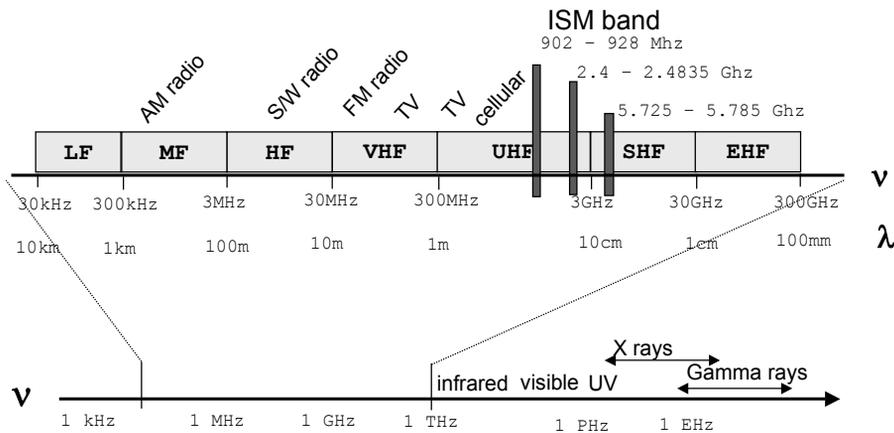
Propagation characteristics are different in each frequency band

Unlicensed Radio Spectrum

λ

| 33cm | 12cm | 5cm |

26 Mhz

83.5 Mhz

125 Mhz

902 Mhz

928 Mhz

2.4 Ghz

2.4835 Ghz

5.725 Ghz

5.785 Ghz

cordless phones
baby monitors
Wireless LANs

802.11
Bluetooth
Microwave oven

unused

Bluetooth radio link

1Mhz

1 2 3

79

83.5 Mhz

- frequency hopping spread spectrum
  - 2.402 GHz + k MHz, k=0, …, 78
  - 1,600 hops per second
- GFSK modulation
  - 1 Mb/s symbol rate
- transmit power
  - 0 dbm (up to 20dbm with power control)

Review of basic concepts

---

dB (relative measure)

10^{11} \$ 100B

dB = 10 log (times)

Net worth

10,000 times
40 dB

10,000 * 1,000 times
= 10,000,000 times

10^7 \$ 10M

40 dB + 30 dB
= 70dB

1,000 times
30 dB

10^4 \$ 10K

Bill   Steve   Grad

Path loss in dB

10 W

10^1

$dB = 10 \log (\frac{P_1}{P_2})$

Power

Path loss from source to d2 = 70dB

10^{-3}

1 mW

10^{-6}

10,000 times
40 dB

1,000 times
30 dB

1 μW

source   d1   d2

P. Bhagwat   23

---

dBm (absolute measure of power)

10 W   = 40 dBm

10^1

$dBm = 10 \log (\frac{P_1}{1mW})$

+ 10,000 times

Power

10^{-3}

1 mW   = 0 dBm

- 1,000 times

10^{-6}

1 μW   = -30 dBm

source   d1   d2

P. Bhagwat   24

Radio propagation: path loss

near field

P_r

P_t

r

P_r
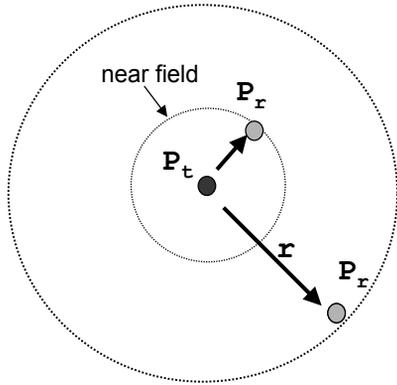
path loss in 2.4 Ghz band

$r \leq 8m$ $r > 8m$

near field   far field

$\propto r^2$ $\propto r^{3.3}$

path loss $= 10 \log (4\pi r^2/\lambda)$ $r \leq 8m$

$= 58.3 + 10 \log (r^{3.3}/8)$ $r > 8m$

Transmit power & receiver sensitivity

0 dBm ⊤ Tx power

-20 ┼ Rx power @ 10 cm

-70 ┼ Rx power @ 10m

-91 ┼   Noise floor   C/I = 21 dB
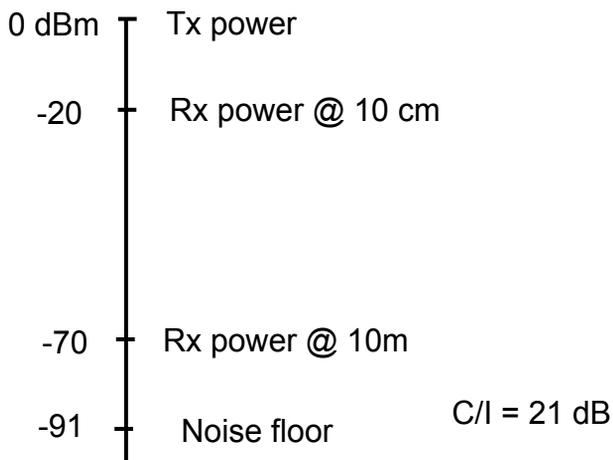
Bluetooth Radio

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

- Low Power
  - ▸ Standby modes   Sniff, Hold, Park
  - ▸ Low voltage RF

- Robust operation
  - ▸ Fast frequency hopping   1600 hops/sec
  - ▸ Strong interference protection
    - ● Fast ARQ
    - ● Robust access code
    - ● Forward header correction

Radio: design rationale

- Allow low cost low IF
- Trade sensitivity for integration
- One chip radio is possible

Baseband
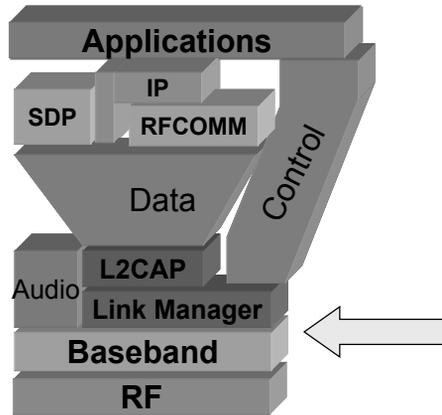
Bluetooth Physical link

■ Point to point link
  ‣ master - slave relationship
  ‣ radios can function as masters or slaves

■ Piconet
  ‣ Master can connect to 7 slaves
  ‣ Each piconet has max capacity (1 Mbps)
  ‣ hopping pattern is determined by the master
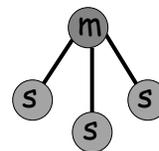
Connection Setup

- Inquiry - scan protocol
  - ‣ to lean about the clock offset and device address of other nodes in proximity

P. Bhagwat   31

Inquiry on time axis

Slave1   f1   f2

Master   Inquiry hopping sequence

Slave2

P. Bhagwat   32
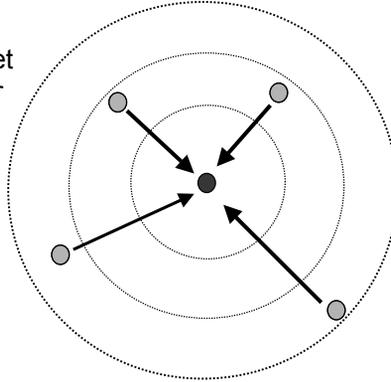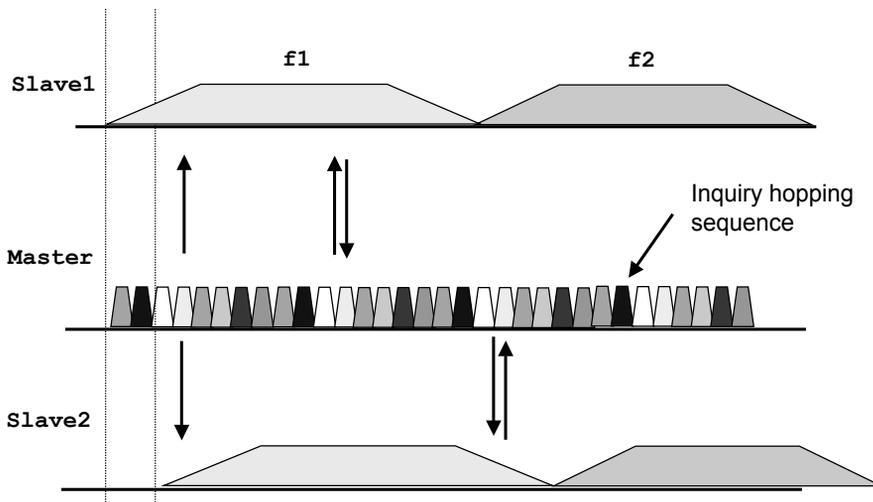
Piconet formation

- Page - scan protocol
  - to establish links with nodes in proximity

● **Master**

◯ **Active Slave**

◯ **Parked Slave**

◯ **Standby**

P. Bhagwat   33
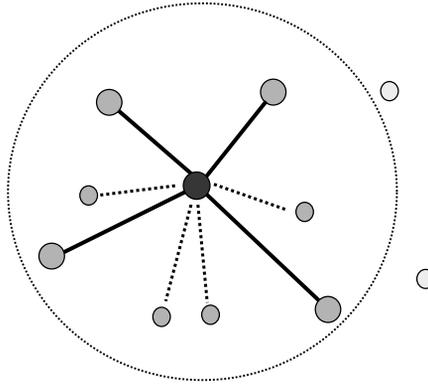
Addressing

- Bluetooth device address (BD_ADDR)
  - 48 bit IEEE MAC address

- Active Member address (AM_ADDR)
  - 3 bits active slave address
  - all zero broadcast address

- Parked Member address (PM_ADDR)
  - 8 bit parked slave address

P. Bhagwat   34

Piconet channel

FH/TDD

f1 f2 f3 f4 f5 f6

m

s1

s2

625 λsec

1600 hops/sec

P. Bhagwat 35

Multi slot packets

FH/TDD

f1 f4 f5 f6

m

s1

s2

625 μsec

Data rate depends on type of packet

P. Bhagwat 36
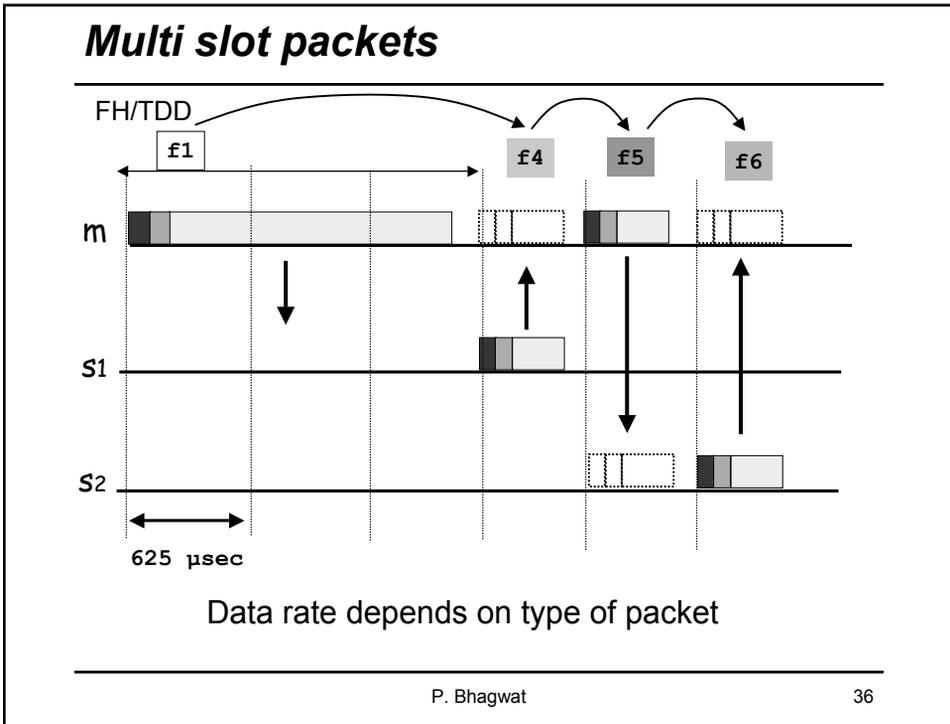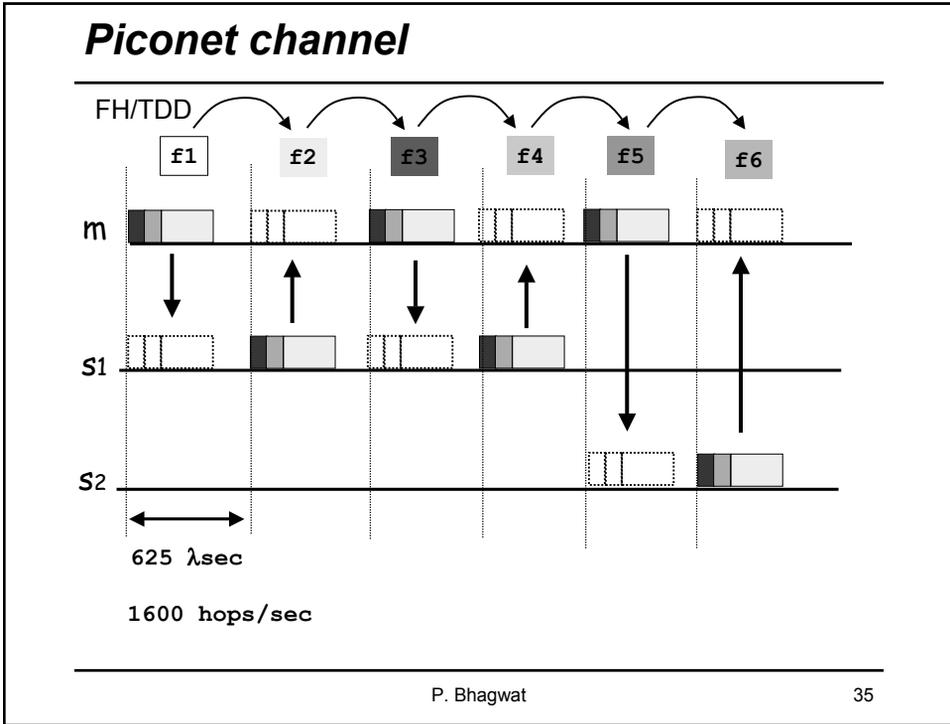
Physical Link Types

- Synchronous Connection Oriented (SCO) Link
  - ▸ slot reservation at fixed intervals

- Asynchronous Connection-less (ACL) Link
  - ▸ Polling access method

Packet Types

Control packets	Data/voice packets

Voice

data

ID*
Null
Poll
FHS
DM1

HV1
HV2
HV3
DV

DM1
DM3
DM5

DH1
DH3
DH5

Packet Format

Access code	Header	Payload
72 bits	54 bits	0 - 2744 bits

Voice

No CRC
No retries
FEC (optional)

header	Data	CRC

ARQ

FEC (optional)

625 µs

master

slave

P. Bhagwat   39

Access Code

72 bits

Access code	Header	Payload

Purpose

- Synchronization
- DC offset compensation
- Identification
- Signaling

Types

- Channel Access Code (CAC)
- Device Access Code (DAC)
- Inquiry Access Code (IAC)

X

P. Bhagwat   40

Packet Header

54 bits

```
Access │ Header │    Payload
code   │        │
```

```
      m
     /|\
    s s
     s
```

Purpose

■ Addressing   (3) ──────→ Max 7 active slaves
■ Packet type   (4) ──────→ 16 packet types (some unused)
■ Flow control   (1)
■ 1-bit ARQ   (1) ──────→ Broadcast packets are not ACKed
■ Sequencing   (1) ──────→ For filtering retransmitted packets
■ HEC   (8) ──────→ Verify header integrity

────────────────────────────
  total   18 bits

Encode with 1/3 FEC to get 54 bits

P. Bhagwat   41

Voice Packets (HV1, HV2, HV3)

72 bits 54 bits   240 bits   = 366 bits

```
Access │ Header │      30 bytes
code   │        │
```

                              Payload

HV1   │ 10 bytes │ + 1/3 FEC │

HV2   │   20 bytes   │ + 2/3 FEC │

HV3   │   30 bytes   │

              3.75ms   (HV3)
         2.5ms   (HV2)
    1.25ms (HV1)

P. Bhagwat   42
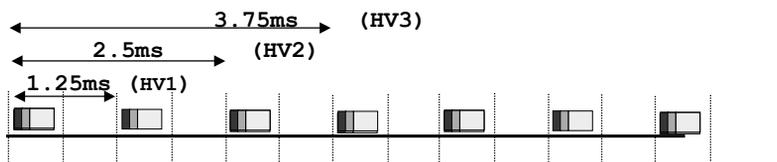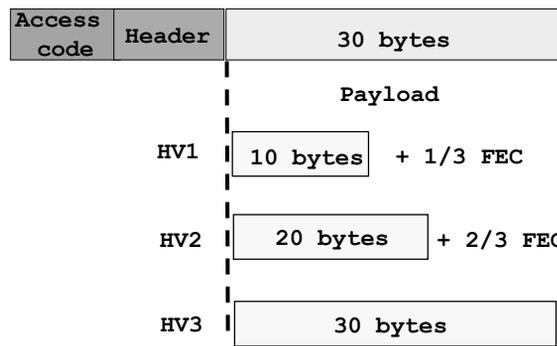
Data rate calculation: DM1 and DH1

625 µs

72 bits	54 bits	240 bits	= 366 bits

Access code	Header	30 bytes

Payload

DM1 | 1 | 17 | 2 | 2/3 FEC

Dir	Size	Freq	Rate
↑	17	1600/2	108.8
↓	17		108.8

DH1 | 1 | 27 | 2 |

Dir	Size	Freq	Rate
↑	27		172.8
↓	27		172.8

625 µs

1 | 2

P. Bhagwat   43
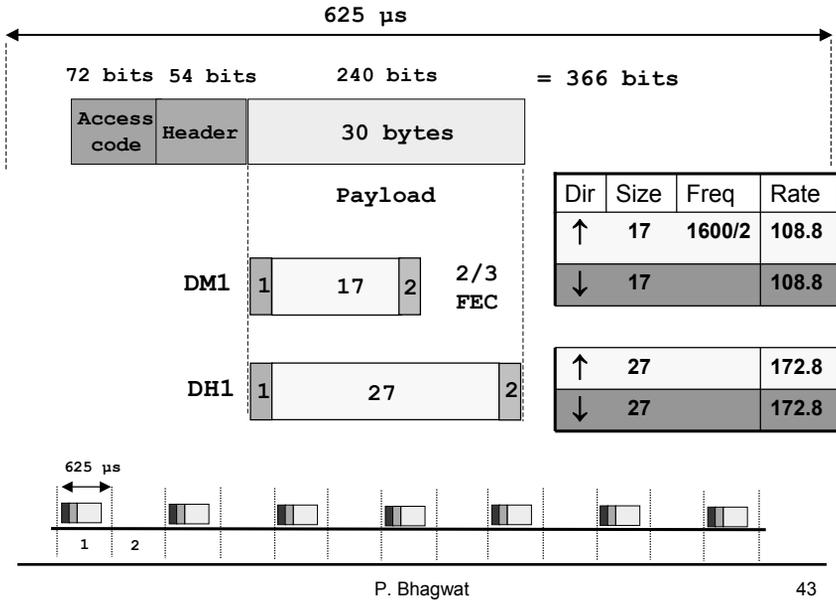
Data rate calculation: DM3 and DH3

1875 µs

72 bits	54 bits	1500 bits	= 1626 bits

Access code	Header	187 bytes

Payload

DM3 | 2 | 121 | 2 | 2/3 FEC

Dir	Size	Freq	Rate
↑	121	1600/4	387.2
↓	17		54.4

DH3 | 2 | 183 | 2 |

Dir	Size	Freq	Rate
↑	183		585.6
↓	27		86.4

1875 µs

1 | 2 | 3 | 4

P. Bhagwat   44
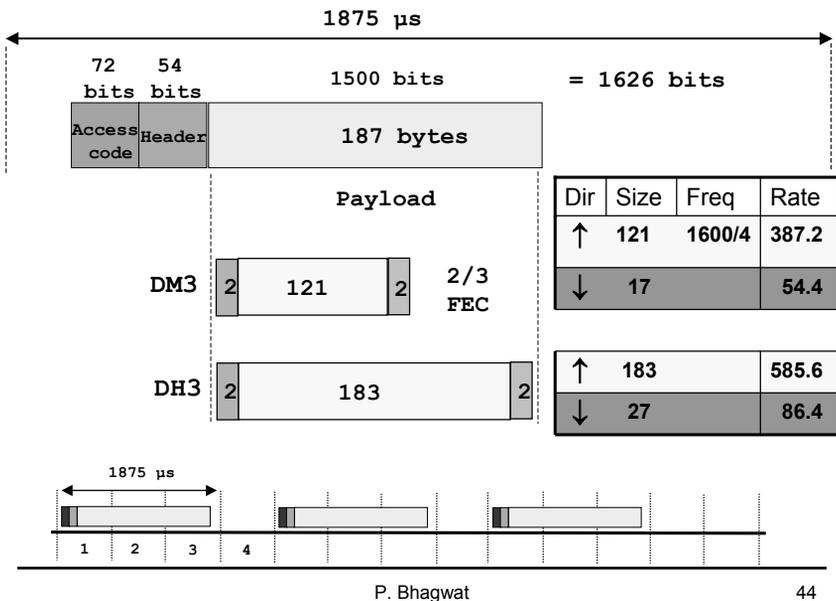
Data rate calculation: DM5 and DH5

3125 µs

72 bits	54 bits

2744 bits   = 2870 bits

Access Code | Header | 343 bytes

Payload

Dir	Size	Freq	Rate
↑	224	1600/6	477.8
↓	17		36.3

DM5   2 | 224 | 2   2/3 FEC

Dir	Size	Freq	Rate
↑	339		(723.2)
↓	27		57.6

DH5   2 | 339 | 2

3125 µs   625 µs

| 1 | 2 | 3 | 4 | 5 | 6 | | | |

P. Bhagwat   45

Data Packet Types

DM1

DM3

2/3 FEC

DM5

Symmetric	Asymmetric	
108.8	108.8	108.8
258.1	387.2	54.4
286.7	477.8	36.3

No FEC

DH1

DH3

DH5

Symmetric	Asymmetric	
172.8	172.8	172.8
390.4	585.6	86.4
433.9	723.2	57.6

P. Bhagwat   46

Inter piconet communication

Cordless
headset

mouse

Cordless
headset

Cell phone

Cell phone

Cell phone   Cordless
headset

P. Bhagwat   47

Scatternet

P. Bhagwat   48
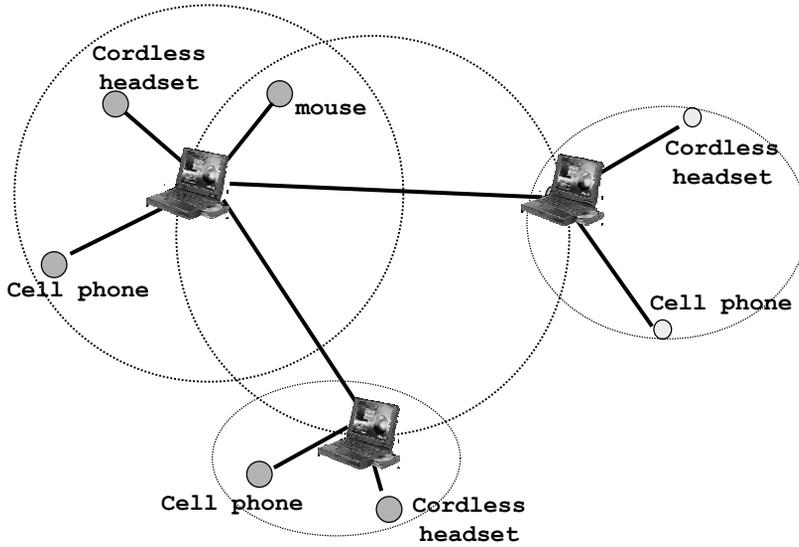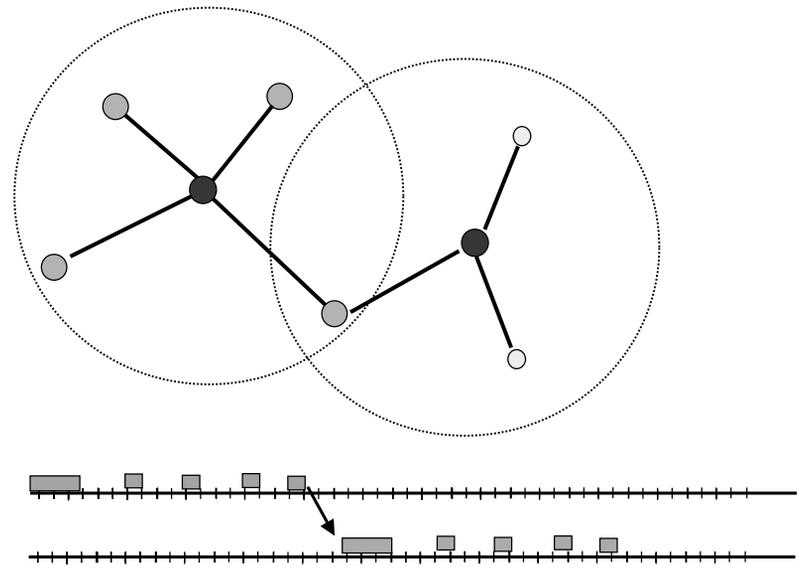
Scatternet, scenario 2
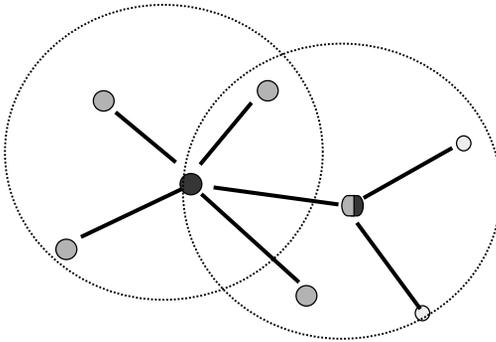
How to schedule presence in two piconets?

Forwarding delay ?

Missed traffic?

Baseband: Summary

Device 1   Device 2

L2CAP ⟷ L2CAP
Data link

LMP   LMP
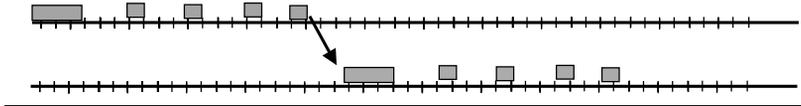
Baseband ⟷ Baseband
Physical
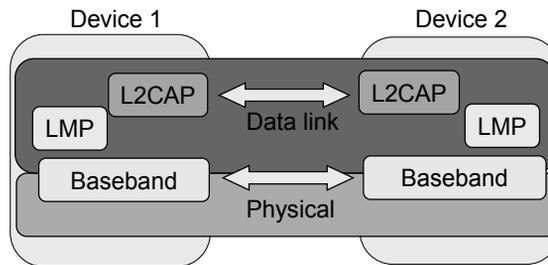
- TDD, frequency hopping physical layer
- Device inquiry and paging
- Two types of links SCO and ACL links
- Multiple packet types (multiple data rates with and without FEC)

Link Manager Protocol

Applications

IP

SDP   **RFCOMM**

Control

Data

L2CAP

Audio   **Link Manager**   ← **LMP**

Baseband

RF
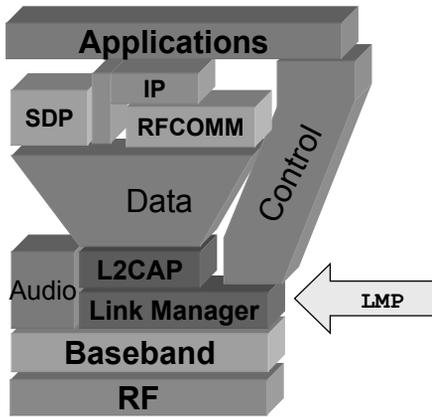
Setup and management
of Baseband connections

- Piconet Management
- Link Configuration
- Security

Piconet Management

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

Paging

m

s   s

s

Master   **req** →   **Slave**

← **response**

Low power mode (hold)

Hold offset

Slave

Hold duration

Master

Low power mode (Sniff)

Sniff offset

Sniff duration

Slave

Sniff period

Master
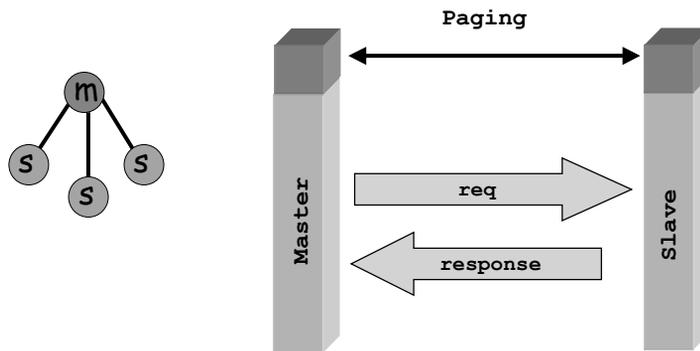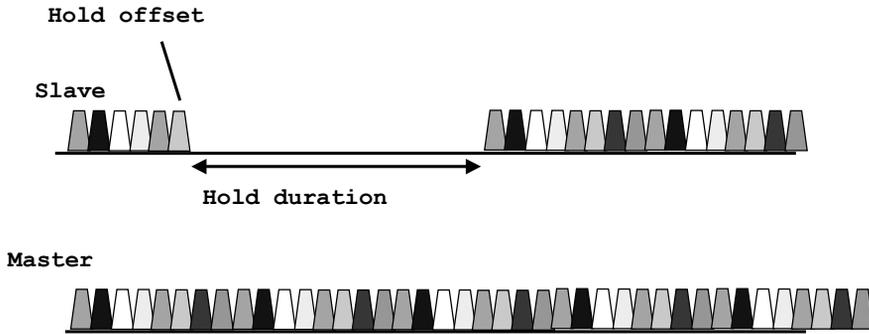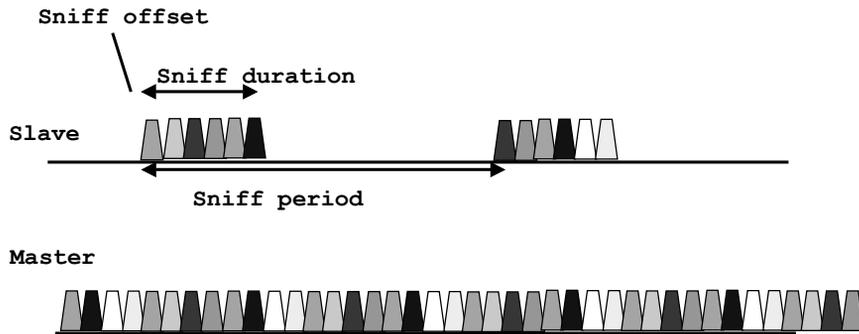
■ Traffic reduced to periodic sniff slots

Low power mode (Park)

Slave

Beacon instant

Master

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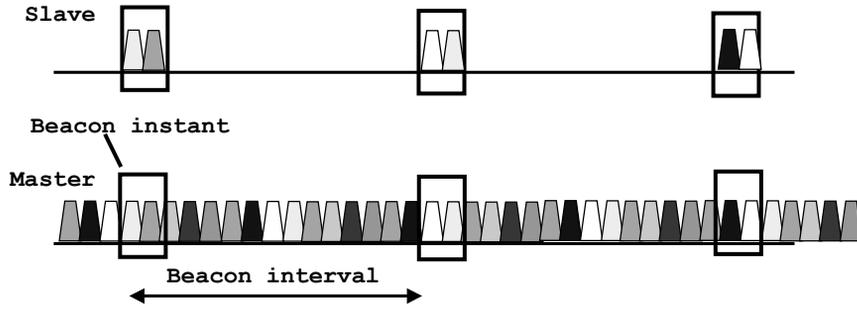
- Power saving + keep more than 7 slaves in a piconet
- Give up active member address, yet maintain synchronization
- Communication via broadcast LMP messages

P. Bhagwat   55

Link Configuration

- Quality of service
  - ▸ Polling interval
  - ▸ Broadcast repetition
- Power control
- Packet type negotiation
- Multi-slot packets

Master

Slave

Paging

LMP_quality_of_service

LMP_not_Accepted

P. Bhagwat   56
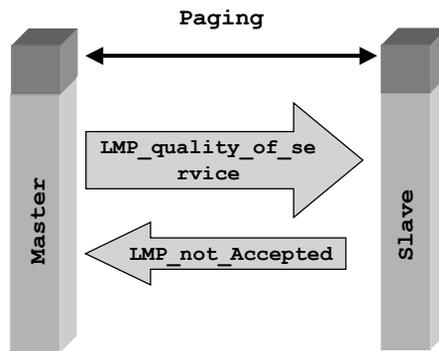
Connection establishment & Security

- Goals
  - ▸ Authenticated access
    - ● Only accept connections from trusted devices
  - ▸ Privacy of communication
    - ● prevent eavesdropping

- Constraints
  - ▸ Processing and memory limitations
    - ● $10 headsets, joysticks
  - ▸ Cannot rely on PKI
  - ▸ Simple user experience

Paging

LMP_host_conn_req

LMP Accepted

Master   **Security procedure**   **Slave**

LMP_setup_complete

LMP_setup_complete

P. Bhagwat   57
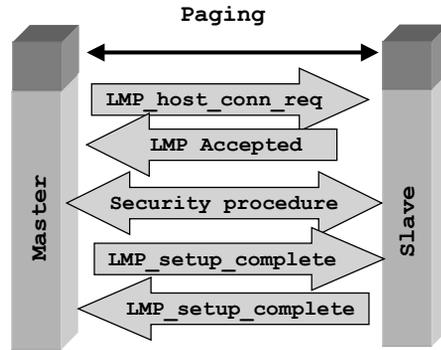
Authentication

- Authentication is based on link key (128 bit shared secret between two devices)
- How can link keys be distributed securely ?

Verifier   **challenge** ➡   **Claimant**

             ⬅ **response**

accepted ➡

● **Link key**   ● **Link key**

P. Bhagwat   58
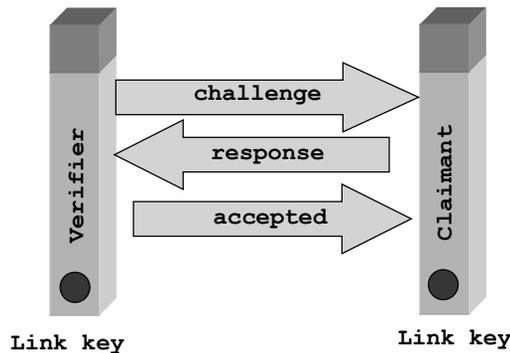
Pairing (key distribution)

- Pairing is a process of establishing a trusted secret channel between two devices (construction of initialization key K_{init})
- K_{init} is then used to distribute unit keys or combination keys

PIN +
Claimant
address

Verifier

Random
number

Kinit ⬤

Random number → Verifier →

challenge →

← response

accepted →

Claimant

PIN +
Claimant
address

Random
number

⬤ **Kinit**
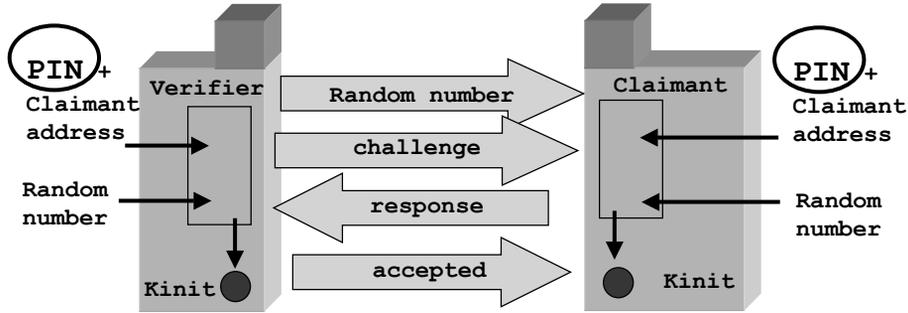
Encryption

- Encryption Key (8 – 128 bits)
- Derived from the Link key

Encryption mode

Key size

Start encryption

Encrypted traffic
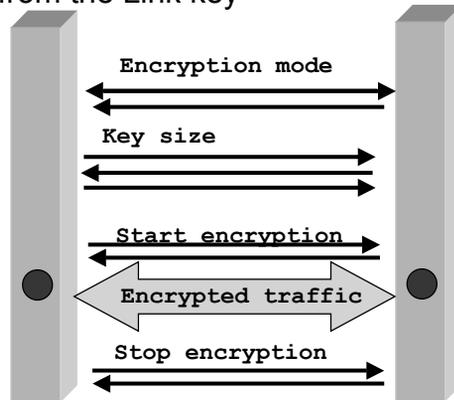
Stop encryption

Link Manager Protocol Summary

Device 1   Device 2

L2CAP ⟷ L2CAP

LMP   Data link   LMP

Baseband ⟷ Baseband

Physical
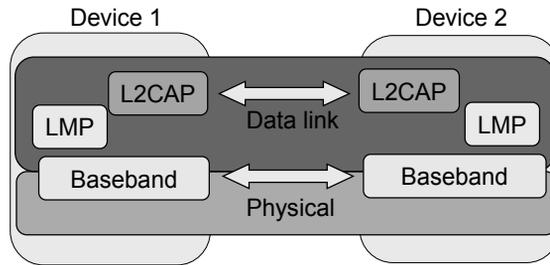
- Piconet management
- Link configuration
  - ▸ Low power modes
  - ▸ QoS
  - ▸ Packet type selection
- Security: authentication and encryption

P. Bhagwat   61

L2CAP

Applications

IP

SDP   **RFCOMM**

Data

L2CAP

Audio   **Link Manager**

Baseband

RF
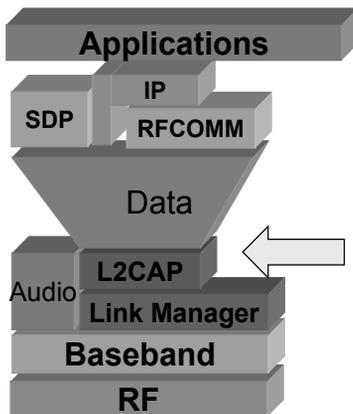
Logical Link Control and Adaptation Protocol

L2CAP provides
- Protocol multiplexing
- Segmentation and Re-assembly
- Quality of service negotiation

P. Bhagwat   62

Why baseband isn't sufficient

```
  IP      RFCOMM                    IP      RFCOMM
```

MTU | Multiplexing
    | demultiplexing

Baseband ◁━━━━━ **reliable*, flow controlled** ━━━━━▷
          in-sequence, asynchronous link
          with possible duplication
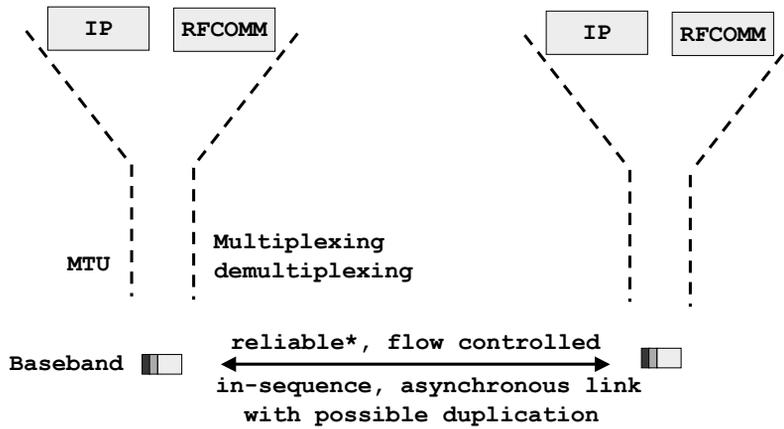
- Baseband packet size is very small (17min, 339 max)
- No protocol-id field in the baseband header

P. Bhagwat   63

Need a multiprotocol encapsulation layer

```
  IP   RFCOMM                       IP   RFCOMM
```

◁━━━━━ **unreliable, no integrity** ━━━━━▷

◁━━━━ **reliable*, in-order,** ━━━━▷
      flow controlled, ACL link
      with possible duplication
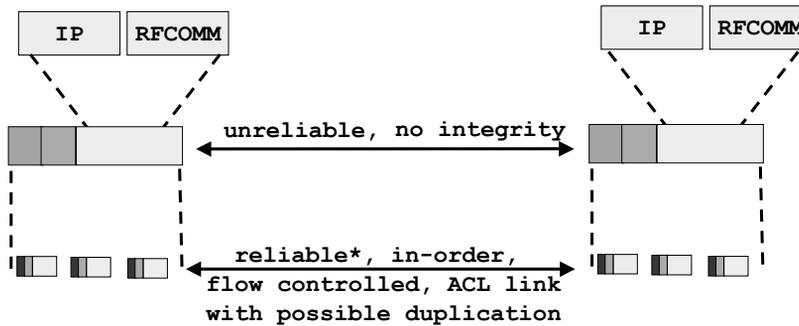
Desired features
- Protocol multiplexing
- Segmentation and re-assembly
- Quality of service

What about
- Reliability?
- Connection oriented or connectionless?
- integrity checks?

P. Bhagwat   64

Segmentation and reassembly

Length		Payload

Baseband packets

```
start of        continuation    continuation
L2CAP           of L2CAP        of L2CAP
```

CRC   CRC   CRC

• cannot cope with re-ordering or loss
• mixing of multiple L2CAP fragments not allowed
• If the start of L2CAP packet is not acked, the rest should be discarded

```
min MTU = 48
672 default
```

P. Bhagwat   65

Multiplexing and Demultiplexing

| IP | RFCOMM | | IP | RFCOMM |

Circuit or connection-less ?
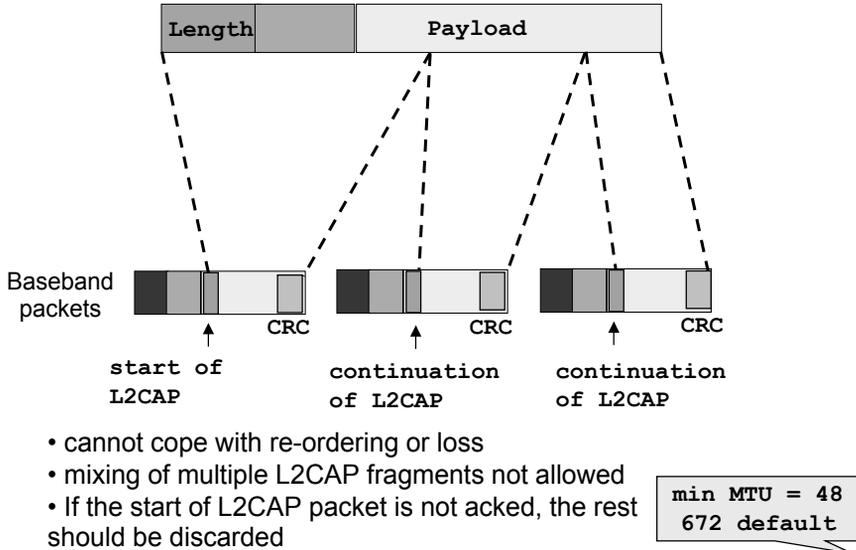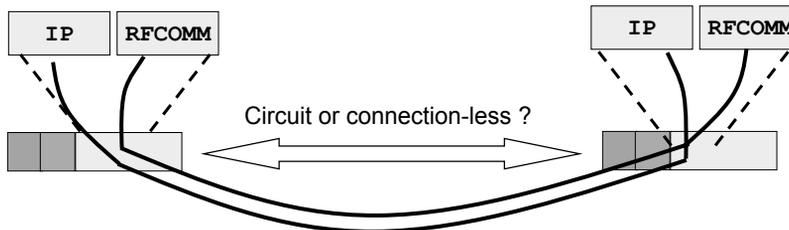
Why is L2CAP connection oriented ?

• Baseband is polling based
• Bandwidth efficiency
    - carry state in each packet Vs. maintain it at end-points
• Need ability for logical link configuration
    - MTU
    - reliability (Flush timeout option)
    - QoS   (token bucket parameter negotiation)

P. Bhagwat   66

L2CAP Channels

Length	CID	Payload

```
Slave #1  01          01  master
          CID    CID              01      signaling
          CID    CID              CID     channel      01   Slave #3
                       CID  01                         CID
                                           data
                                           channel
```

Signaling channel for
1) connection establishment
2) channel configuration
3) disconnection

```
                CID  01
                Slave #2
```

Signaling channel CID
does not uniquely
determine the identity
of the source L2CAP entity
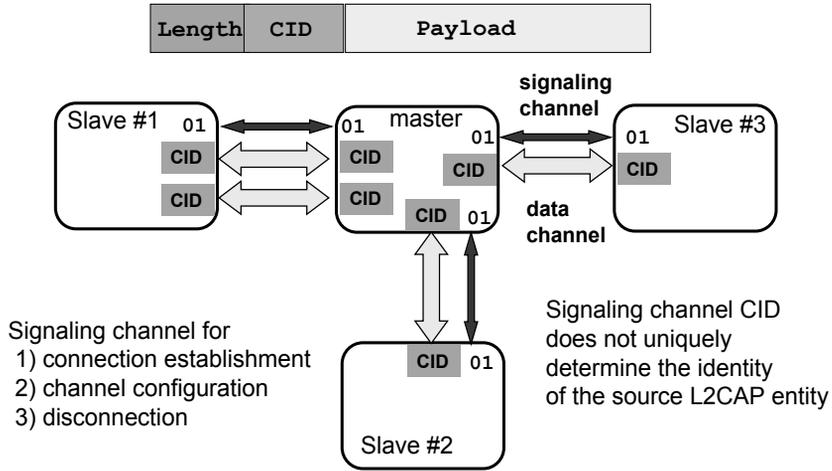
L2CAP connection: an example

```
                Initiator                         Target

                          L2CAP_ConnectReq
Establishment
                          L2CAP_ConnectRsp

                          L2CAP_ConfigReq
Configuration     L2CAP_ConfigRsp
MTU, QoS          L2CAP_ConfigReq
reliability
                          L2CAP_ConfigRsp

Data transfer


Termination               L2CAP_DisconnectReq

                  L2CAP_DisconnectRsp
```
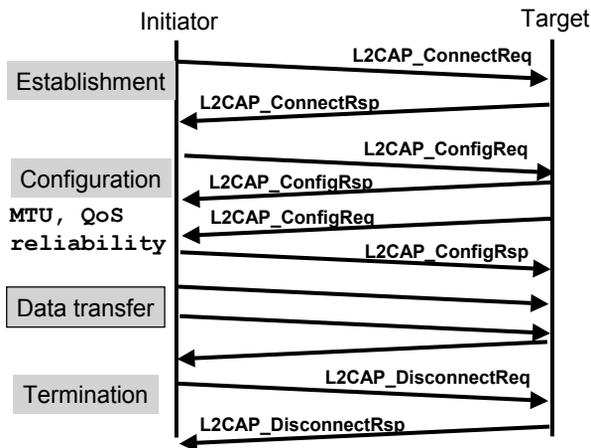
L2CAP Packet Format (Connectionless)
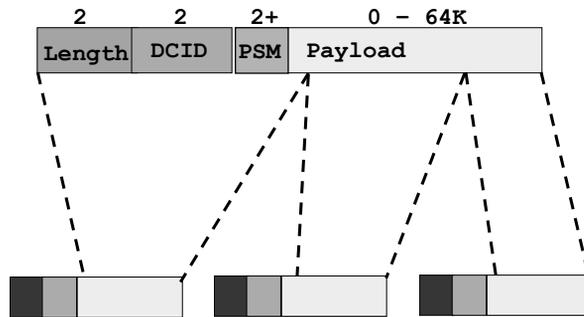
Not fully developed yet.

L2CAP: Summary

Design constraints:

- Simplicity
- Low overhead
- Limited computation and memory
- Power efficient

Assumptions about the lower layer

- Reliable, in-order delivery of fragments
- Integrity checks on each fragment
- Asynchronous, best effort point-to-point link
- No duplication
- Full duplex

Service provided to the higher layer

- Protocol multiplexing and demultiplexing
- Larger MTU than baseband
- Point to point communication

Bluetooth Service Discovery Protocol
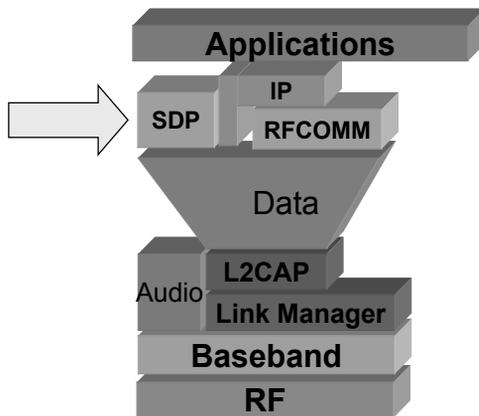
Example usage of SDP

- 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 user the service

Serial Port Emulation using RFCOMM

Applications

IP

SDP **RFCOMM** ⇐

Data

L2CAP

Audio **Link Manager**

Baseband

RF
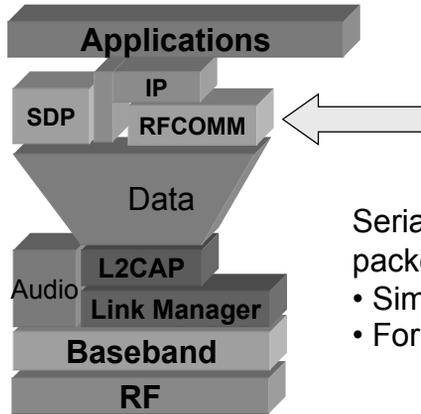
Serial Port emulation on top of a
packet oriented link
• Similar to HDLC
• For supporting legacy apps

Serial line emulation over packet based MAC

RFCOMM		RFCOMM
L2CAP		L2CAP

- Design considerations
  - framing: assemble bit stream into bytes and, subsequently, into packets
  - transport: in-sequence, reliable delivery of serial stream
  - control signals: RTS, CTS, DTR

IP over Bluetooth V 1.0

Applications

IP

SDP   **RFCOMM**

Data

L2CAP

Audio   **Link Manager**

Baseband

RF
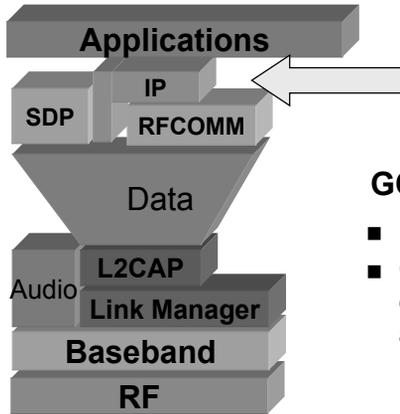
GOALS

- Internet access using cell phones
- Connect PDA devices & laptop computers to the Internet via LAN access points

---

LAN access point profile

Access Point

IP

↓

PPP

↓

RFCOMM

↓

L2CAP

↓

Baseband
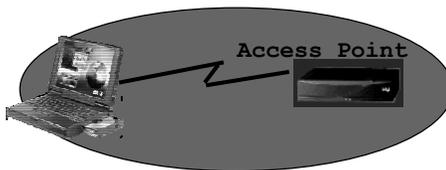
Why use PPP?

Security
    Authentication
    Access control
Efficiency
    header and data compression
Auto-configuration
Lower barrier for deployment
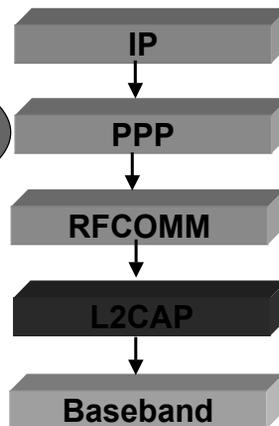
IP over Bluetooth v 1.1: BNEP

Access Point
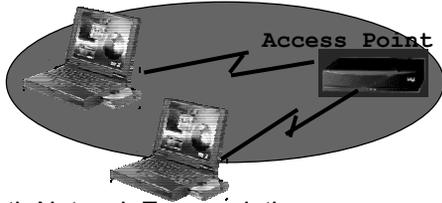
Bluetooth Network Encapsulation
Protocol (BNEP) provides emulation of
Ethernet over L2CAP

- BNEP defines
  - a frame format which includes IEEE
    48 bit MAC addresses
  - A method for encapsulating BNEP
    frames using L2CAP
- Option to compress header fields to
  conserve space
- Control messages to activate filtering of
  messages at Access Point

IP
↓
BNEP
↓
L2CAP
↓
Baseband
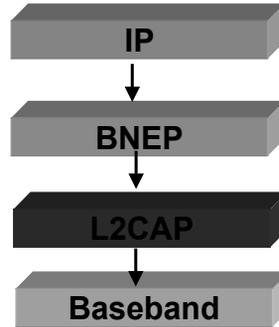
802.11 specifications overview

802.11 Specifications

Applications

Control

LLC

WEP

MAC   MAC Mgmt

PHY   MIB

DSSS   FH   IR   OFDM
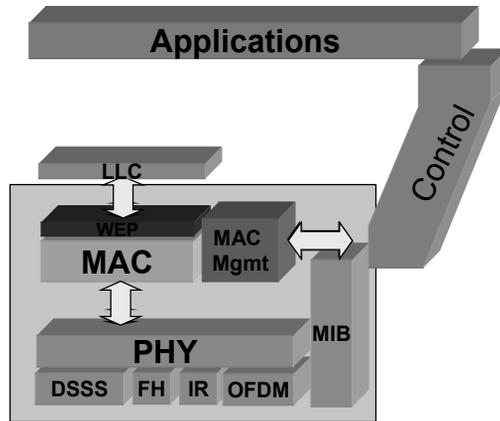
- Specification of layers below LLC
- Associated management/control interfaces

802.11 Specifications

LLC

WEP

MAC   MAC Mgmt

PHY   MIB

DSSS   FH   IR   OFDM

`LLC`		**MAC Mgmt Service Interface**
MAC Service Interface		
MAC sublayer	**MAC Layer Management**	
PHY Service Interface	**PHY Mgmt Service Interface**	
`PLCP Sublayer`	`PHY layer Management`	
`PMD Sublayer`		

802.11 Specifications

```
                        ┌─────────┐
                        │   LLC   │
                        └─────────┘
 MAC Service                 ↕                      MAC Mgmt Service
 Interface                                          Interface (clause 10)
 (clause 6)
           ┌──────────────────────┬──────────────────────────┐
           │ MAC sublayer         │ MAC Management            │
           │                      │                           │
           │ MAC framing (clause 7)│ Protocols (clause 11)    │
           │ MAC operation (clause 9)│ State Machines (Annex C)│
           │ WEP (clause 8)       │ MIBs (Annex D)            │
           │ State Machines (Annex C)│                        │
           └──────────────────────┴──────────────────────────┘
 PHY Service        ↕                       PHY Mgmt Service    ↕
 Interface (clause 12)                      Interface (clause 13)
           ┌──────────────────────┬──────────────────────────┐
           │ PHY Layer            │ PHY Management            │
           │ FH (clause 14)       │                           │
           │ DSSS (clause 15)     │                           │
           │ Infrared (clause 16) │   MIBs (Annex D)          │
           │ OFDM (clause 17)     │                           │
           │ High rate DSSS (clause 18)│                      │
           └──────────────────────┴──────────────────────────┘
```

P. Bhagwat   81

802.11 System Architecture

Basic Service Set (BSS): a set of stations which communicate
with one another

Independent Basic Service   Infrastructure Basic Service
Set (IBSS)   Set (BSS)
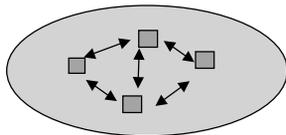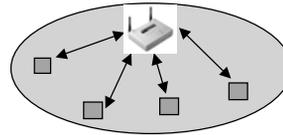
- only direct communication   • AP provides
  possible   • connection to wired network
- no relay function   • relay function
                                     • stations not allowed to
                                        communicate directly

P. Bhagwat   82

Extended Service Set

ESS: a set of BSSs interconnected by a distribution system (DS)
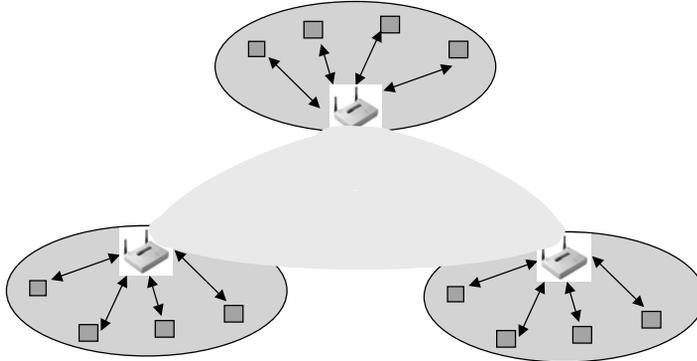
- ESS and all of its stations appear to be a single MAC layer
- AP communicate among themselves to forward traffic
- Station mobility within an ESS is invisible to the higher layers

802.11 PHY

Applications

Control

LLC

WEP

MAC   **MAC Mgmt**

PHY   MIB

DSSS   FH   IR   OFDM

802.11 PHY

Sender   Receiver

| MAC Protcol Data Unit (MPDU) | | MAC Protcol Data Unit (MPDU) |

MAC
- -
PHY

| PLCP header | MAC Protcol Data Unit (MPDU) | | PLCP header | MAC Protcol Data Unit (MPDU) |

Physical Media Dependent (PMD) layer   MWWWWWWWWWWWWW   PMD layer

Frequency Hopping Spread Spectrum (FHSS) PHY 1, 2 Mbps

Direct Sequence Spread Spectrum (DSSS) PHY 1,2 Mbps

Infrared (IR) PHY 1,2 Mbps

Orthogonal Frequency Division Multiplexing (OFDM) PHY 6,9,12,18,24,36,48,54 Mbps 802.11a

Higher rate (DSSS) PHY 20+ Mbps 802.11g

High rate (DSSS) PHY 11, 5.5 Mbps 802.11b

2.4 GHz   5.7 GHz

P. Bhagwat   85

DSSS PHY

| Preamble | Header | MPDU | | Preamble | Header | MPDU |
| 1 Mbps | 1, 2 Mbps | | 1 Mbps | 1, 2 Mbps |

DPSK modulation

Spread the signal using Barker word (11 bits) +1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1

DPSK de-modulation

Transmitter baseband signal

Transmitted signal after spreading

Received signal after despreading

- Baseband signal is spread using Barker word (10 dB processing gain)
- Spread signal occupies approximately 22 Mhz bandwidth
- Receiver recovers the signal by applying the same Barker word
- DSSS provides good immunity against narrowband interferer
- CDMA (multiple access) capability is not possible

P. Bhagwat   86

DSSS PHY

Ch 1   Ch 6   Ch 11

22 Mhz

83.5 Mhz

- ■ Direct sequence spread spectrum
  - ▸ Each channel is 22 Mhz wide
- ■ Symbol rate
  - ▸ 1 Mb/s with DBPSK modulatio
  - ▸ 2 Mbps with DQPSK modulation
  - ▸ 11, 5.5 Mb/ps with CCK modulation
- ■ Max transmit power
  - ▸ 100 Mw

FHSS PHY

Preamble	Header	MPDU

1 Mbps   1, 2 Mbps

Preamble	Header	MPDU

1 Mbps   1, 2 Mbps

GFSK
modulation

GFSK
de-modulation

1Mhz

1 2 3   . . .   79

83.5 Mhz
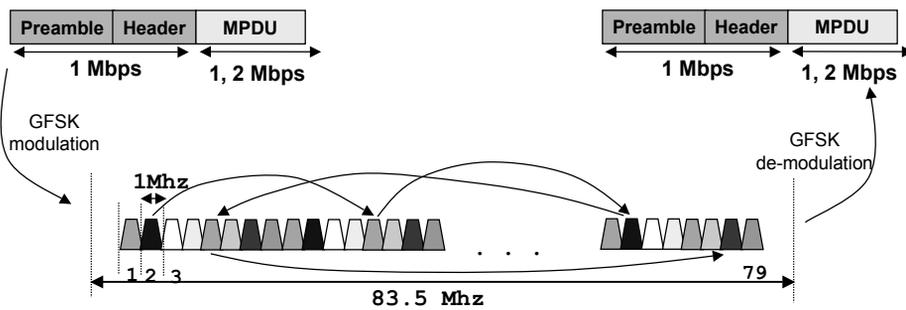
- ■ Hopping sequences are grouped into three sets
  - ▸ Each set contains 26 hopping sequences (North America)
  - ▸ 2.5 hops/sec, minimum hop distance = 6 Mhz
- ■ GFSK modulation
  - ▸ 1, 2 Mb/s symbol rate

802.11 MAC
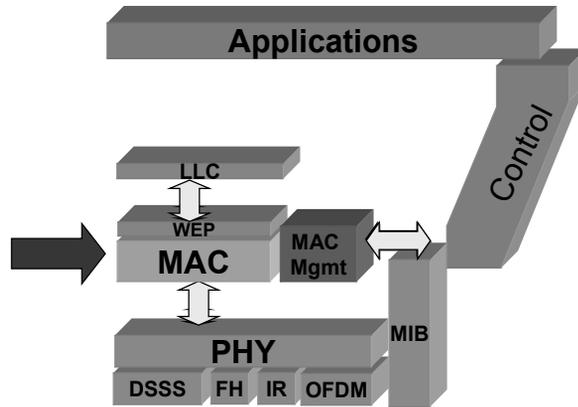
802.11 MAC : Design goals

- Single MAC to support multiple PHYs
  - ▸ Support multiple channel PHYs
- Robust against interference
- Cope with hidden nodes
- Support for time bounded service, QoS
- Should be scalable and stable at high loads
- Need provisions for Power Saving Modes
- Need provisions for Privacy and Access Control

802.11 MAC

- ■ Carrier sensing (CSMA)
  - ▸ Rules:
    - ● carrier   ==>   do not transmit
    - ● no carrier ==>   OK to transmit
  - ▸ But the above rules do not always apply to wireless.
   - ● Solution: RTS/CTS
- ■ Collision detection (CD)
  - ▸ Does not work over wireless
  - ▸ Therefore, use collision avoidance (CA)
    - ● random backoff
    - ● priority ack protocol

802.11 MAC protocol: CSMA/CA
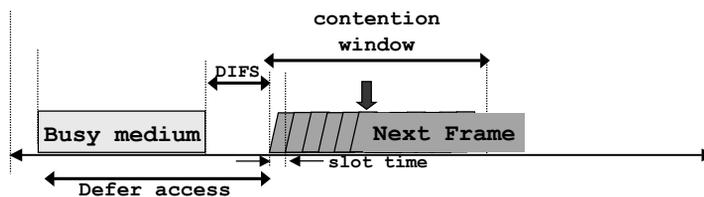
- ■ Use CSMA with collision Avoidance
  - ▸ Based on carrier sense function in PHY called Clear Channel Assessment (CCA)
- ■ Reduce collision probability where mostly needed
- ■ Efficient backoff algorithm stable at high loads
- ■ Possible to implement different fixed priority levels

802.11 MAC : Contention window

1023

CW max

For DSSS PHY
Slot time = 20 μs

511

255

127

63

CW min   31

Fifth retransmission
Fourth retransmission
Third retransmission
Second retransmission
First retransmission
Initial attempt

P. Bhagwat   93

CSMA/CA + ACK protocol

DIFS

Src   `Data`

SIFS

Dest   `ACK`

DIFS   contention
window

**Other**   Next Frame
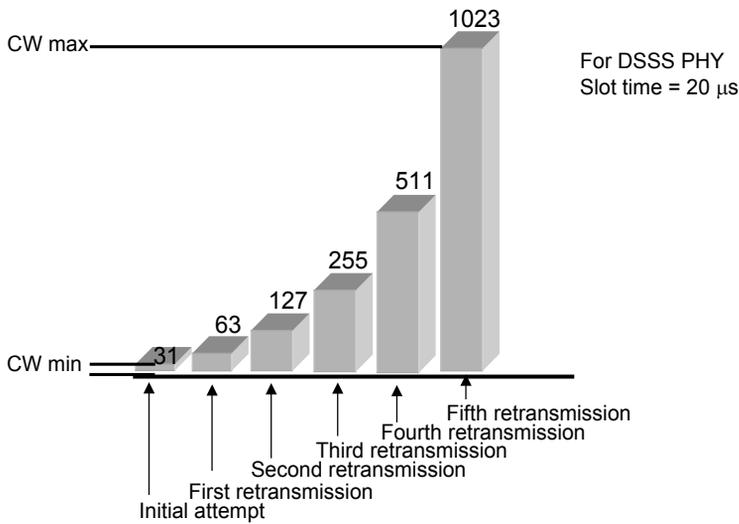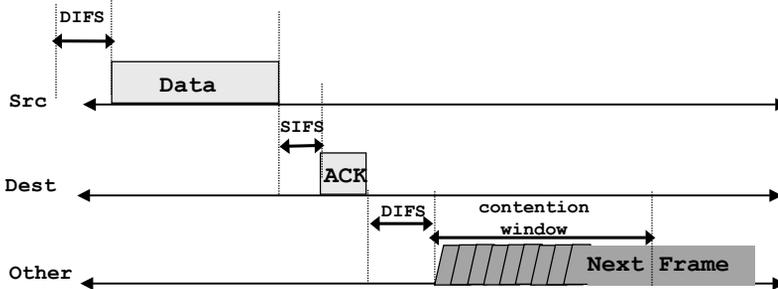
- Defer access based on carrier sense
- Direct access when medium is sensed free longer than DIFS
- Receiver of directed frames to return an ACK immediately when CRC is correct
  - When no ACK received then retransmit frame after a random backoff

P. Bhagwat   94

Problems with carrier sensing

Exposed terminal problem

W

Z is transmitting
to W

Z

X ← – – – Y
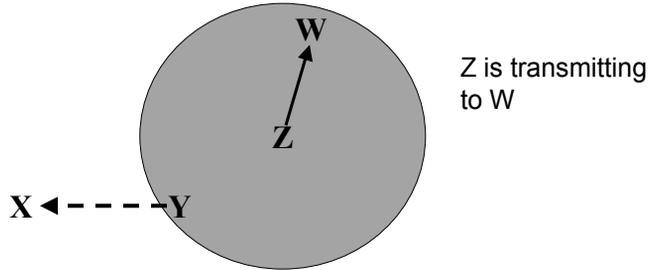
Y will not transmit to X
even though it cannot interfere

Presence of carrier ==≠=> hold off transmission

Problems with carrier sensing

Hidden terminal problem

Z

Y

W

W finds that medium is free
and it transmits a packet to Z
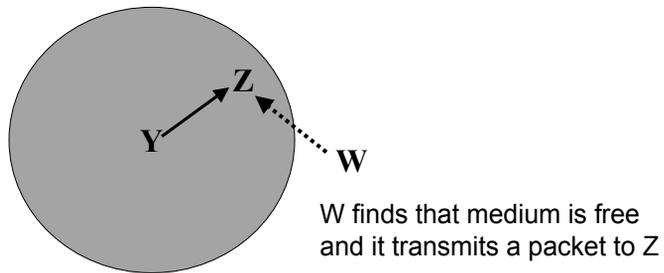
no carrier ==≠=> OK to transmit

Solving Hidden Node problem with RTS/CTS

- listen RTS
- wait <u>long enough</u> for the requested station to respond with CTS
- if (timeout) then ready to transmit

RTS   CTS

X   Z

Y   W
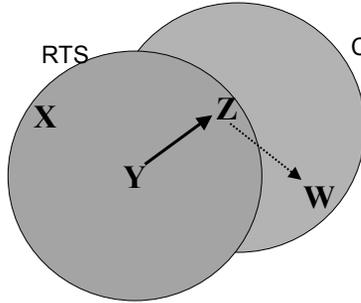
- listen CTS
- wait <u>long enough</u> for the transmitter to send its data

listen RTS ==> transmitter is close to me
listen CTS ==> receiver is close to me

Note: RTS/CTS does not solve exposed terminal problem. In the example above, X can send RTS, but CTS from the responder will collide with Y's data.

P. Bhagwat   97

802.11 MAC sublayer Management

Applications

Control

LLC

WEP

MAC   MAC Mgmt

PHY   MIB

DSSS FH IR OFDM

P. Bhagwat   98
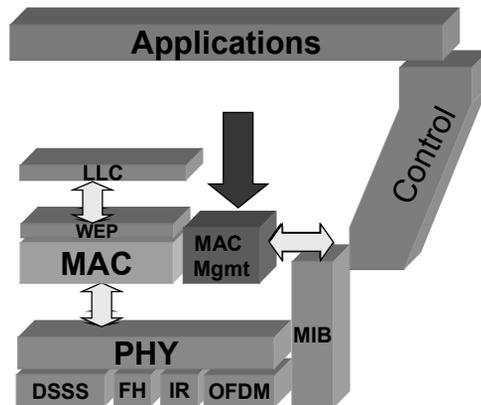
MAC Management: Beacon & Probes

Access Point

Access Point

Access Point

Probe Response

Probe Request
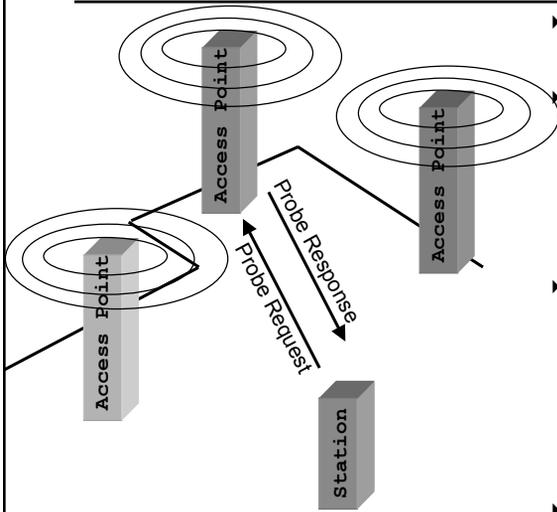
Station

- ▸ A station can first scan the network and discover the presence of BSS in a given area
- ▸ Scanning
  - ▸ Passive
    - ▸ listen for beacons on each channel
  - ▸ Active
    - ▸ send probe and wait for response on each channel
- ▸ Beacon and probe response packets contain:
  - ▸ AP timing information,
  - ▸ Beacon period,
  - ▸ AP capability information,
  - ▸ SSID,
  - ▸ PHY parameter set,
  - ▸ Traffic Indication Map (TIM)
- ▸ SSID (Service set identifier)
  - ▸ identifies an ESS or IBSS

MAC Mgmt : Authentication & Association

AP2

AP3

1) Auth exchg

Unauthenticated
Unassociated

2) Association exchg

Authenticated
Unassociated

3) Data exchg

Authenticated
Associated

To DS

Access Point 1
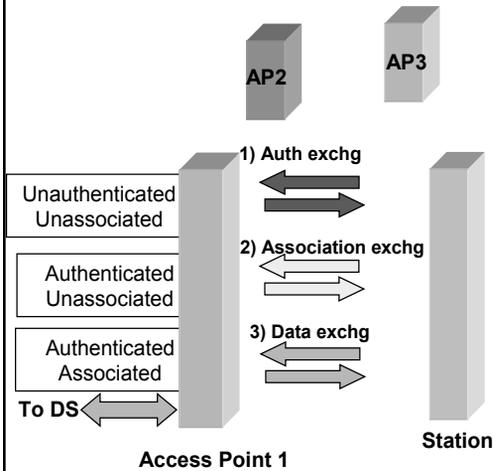
Station

- ■ With respect to an access point, a station can be in one of the following three states
  - ■ Unauthenticated/Unassociated
  - ■ Authenticated/Unassociated
  - ■ Authenticated/Associated
- ■ A station can pre-authenticate with several access points in advance to speedup roaming
- ■ A station can be associated with only one AP at a given time
- ■ Association state is used by the distribution system to figure out the current location of the station within the ESS.

MAC Mgmt : Power Management
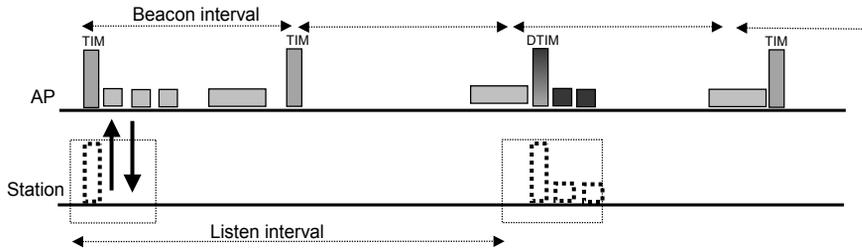
- A station which is synchronized with an AP clock can wake up periodically to listen for beacons
- Beacon packets contain Traffic Indication Map (TIM), a bit vector, which indicates whether a station has a packet buffered at AP
- The station sends a PS-Poll message to the AP asking the AP to release buffered packets for the station
- All broadcast and multicast frames are transmitted following beacons with DTIM flag set

P. Bhagwat   101

802.11 Frame Format

bytes

2	2	6	6	6	2	6	0 – 2312	4
Frame control	Duration ID	Addr 1	Addr 2	Addr 3	Seq ctrl	Addr 4	Frame body	CRC

802.11 MAC header (30 bytes)
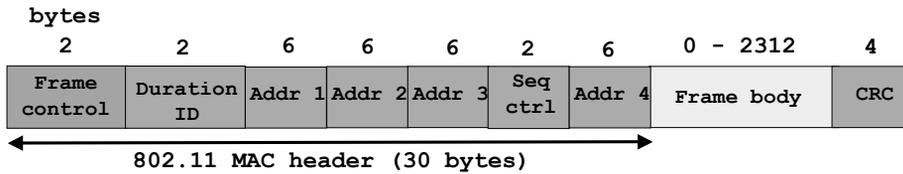
- 802.11 frame has more fields than other media type frames
- 30 bytes frame header appears too long!
- All fields are not present in all frames

P. Bhagwat   102

Frame Control Field

bytes 2
Frame control

bits

2	2	4	1	1	1	1	1	1	1	1
Prot Ver	Type	Subtype	To DS	From DS	More Frag	Retry	Pwr Mgmt	More Data	WEP	Order

00	01	10	11
Mgmt	Control	Data	Reserved

Mgmt	Control	Data
Association req	Power save (PS)-poll	Data
Association resp	Request to Send (RTS)	Data + CF+ACK
Re-association req	Clear to send (CTS)	Data + CF-Poll
Re-association resp	Acknowledgement (ACK)	Data + CF-ACK + CF-Poll
Probe req	Contention free (CF)-END	Null
Probe resp	CF-END + CF-ACK	CF-ACK
Beacon		CF-Poll
Announcement Traffic Indication Request (ATIM)		CF-ACK + CF-Poll
Disassociation		
Authentication		
De-authentication		

Data Forwarding Scenarios

station A to station B
- There is no guarantee that B will be able to hear A's transmission
- A must first send the packet to AP$_1$
- AP$_1$ will then forward that packet to B
- Need space for holding three addresses in the packet header

station A to station C
- A does not know whether C is associated with AP$_1$ or with another AP
- A must first send the packet to AP$_1$
- AP$_1$ will use the DS to forward that packet to AP$_2$

station A to station C via wireless DS
- Same as above except that the transmitted frame from AP$_1$ to AP$_2$ will contain four addresses

802.11 Privacy and Authentication

Applications

Control

LLC

WEP

MAC

MAC Mgmt

MIB

PHY

DSSS   **FH**   **IR**   **OFDM**
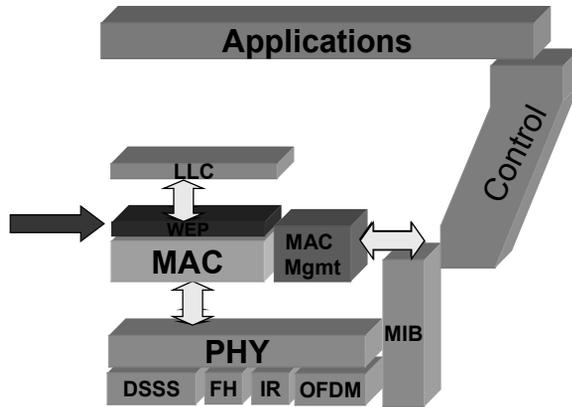

Wired Equivalent Privacy (WEP)

- Design Objectives
  - ▶ Confidentiality
    - Prevent others from eavesdropping traffic
  - ▶ Data Integrity
    - Prevent others from modifying traffic
  - ▶ Access Control
    - Prevent unauthorized network access

Provide same level of security as a physical wire

WEP design: adding privacy

<u>Sender</u>   <u>Receiver</u>

K IV⇨   Random   Random   ⇦ K IV
               key stream   key stream

Plain text ────→⊕───→ Cipher text, IV ────→⊕───→ Plain text
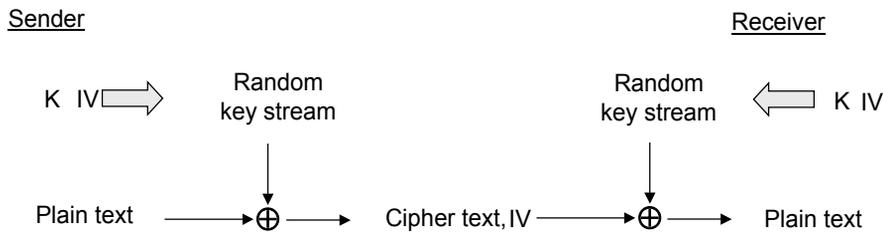
- A secret key is shared between a sender and a receiver
- Using the secret key the sender generates a random key stream
- XOR plain text with the random key stream
- XOR the cipher text with the same random key stream to recovers the plain text
- An eavesdropper cannot compute the plain text by inspecting the cipher text
- New key streams are refreshed periodically
    - Use initialization vector (IV) in conjunction with shared key
   - transmit IV in clear text along with the cipher text

P. Bhagwat   107

WEP design: adding data integrity

<u>Sender</u>   <u>Receiver</u>

K, IV ⇨   Random   Random   ⇦ K, IV
               key stream   key stream

Plain text ICV ────→⊕───→ Cipher text, IV ────→⊕───→ Plain text ICV
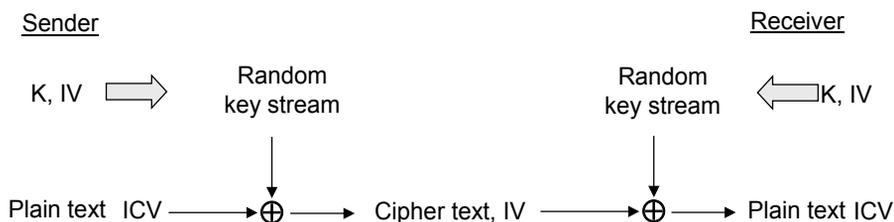
- The problem is that cipher text can be modified without any knowledge of the key
    - Just flip some bits in the cipher text
    - After decrypting the cipher text, receiver will not know that the plain text has been corrupted
- Solution:
    - Computer 32 bit CRC of plain text and append it with plain text before generating the cipher text
    - If cipher text is modified, CRC check will fail and the frame will be discarded

P. Bhagwat   108

WEP design: adding Authentication

Sender   AP

K ◀┄┄┄┄┄┄┄┄┄ shared key ┄┄┄┄┄┄┄┄┄▶ K

Distributed out of band

◀──────────── Challenge (Nonce) ────────────

Response (Nonce encrypted with secret key) ──────────▶

Decrypted response OK?
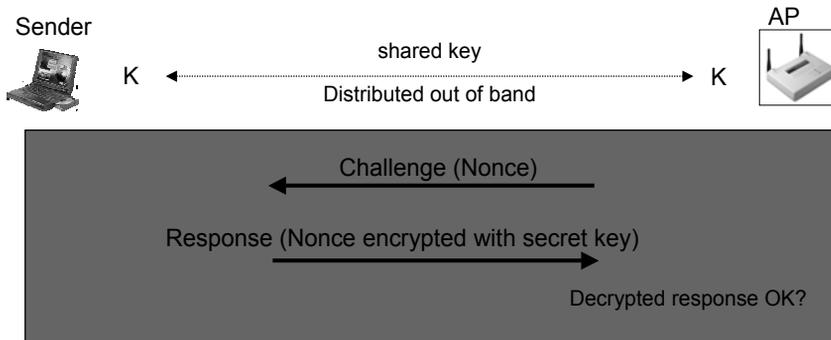
Summary
- ▸ Shared secret keys are distributed out of band
- ▸ AP sends a challenge to the station
- ▸ Station responds with a WEP encrypted packet
- ▸ AP verifies station's response

P. Bhagwat   109

Where is the problem ?

Problem #1: improper use of stream ciphers

K, IV ⟹ key stream   key stream ⟸ K, IV

b   b

C1
C2

P1
P2 ──────▶ ⊕ ──▶ Cipher text, IV ──────▶ ⊕ ──▶
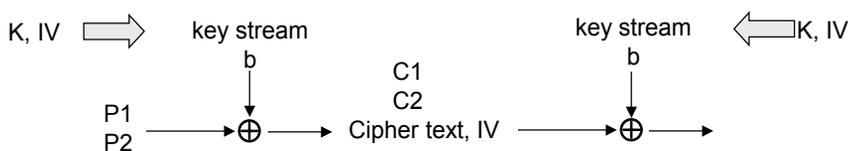
- ▸ Two messages should never be encrypted using the same key streams
- ▸ Suppose P1 and P2 are encrypted using the same key stream
  - ● C1 = P1 XOR b
  - ● C2 = P2 XOR b
- ▸ Adversary can compute C1 + C2 = P1 + b + P2 + b

    = P1 + P2

- ▸ Usually XOR of two plain texts is enough to recover both plain texts
- ▸ Moreover, if one plain text is known other can be computed trivially

P. Bhagwat   110

Key stream reuse in WEP

K, IV ⟹ 2^{24} possible
              key streams
                  b   b
                  | C1 |
                  ↓   C2   ↓
P1 ──────────→ ⊕ ──────→ Cipher text, IV ──────→ ⊕ ──────→
P2
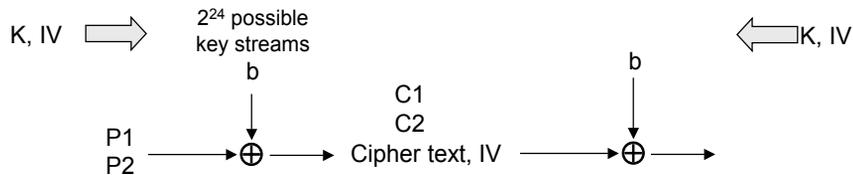
▸ Key stream is a function of secret key and initialization vector
▸ IV vector is only 24 bits long; since there are only 16 million
  combinations, eventually key streams will be recycled
▸ Since IV vector is transmitted in clear text, Key stream reuse is easy
  detect by passive eavesdropping
▸ An eavesdropper can record all instances of key stream reuse
  ● Require 1K * 16 million = 16 GB space
▸ Worse yet, most 802.11 cards when reset start counting IV from 0
  ● so, key streams are recycled more frequently

Possible attack: Message decryption

▸ Inject known plain text in the network by e-mail spamming, or ping
▸ Passively record encrypted packets
▸ By computing XOR of known plain text with encrypted packet, it is
  possible to compute the RC4 key stream that was used to encrypt
  the known plain text
▸ Build a dictionary of key streams
  ● Map each value to IV to its associated key stream
▸ Once this dictionary is built, any packet can be decrypted
    ● Record the packet
    ● Inspect the IV
    ● Pull out the key stream associated with the observed IV from the
      dictionary
    ● XOR the key stream with the encrypted packet and obtain the plain text
▸ The same dictionary can also be used to inject any message in the
  network

Possible attack: Breaking Authentication

Station   shared key   AP

K ◄┄┄┄┄┄┄┄┄┄┄┄┄┄┄┄┄┄┄┄┄┄┄┄┄┄► K

                              Distributed out of band

                              Challenge (Nonce)
                    ◄─────────────────────────────

        Response (Nonce encrypted with secret key)
                    ─────────────────────────────►

                                                    Decrypted response OK?
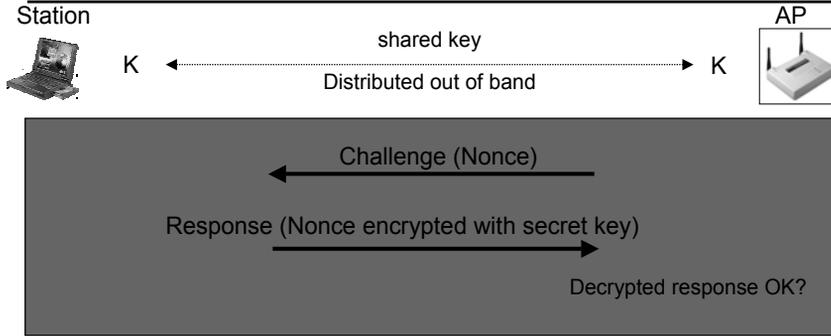
▸ The previous attack relies on finding a known plain text and its encrypted version to compute the key stream
▸ By snooping 802.11 Authentication protocol, this pair can be collected for free
▸ Using this key stream, an adversary station can respond to any new challenge from the AP !

More problems

Problem #2: improper use of CRC

| **Frame body** | **ICV** | | **Frame body** | **ICV** | **If CRC OK then accept.** |

encrypt ↓   **decrypt** ↑

Sender   Receiver
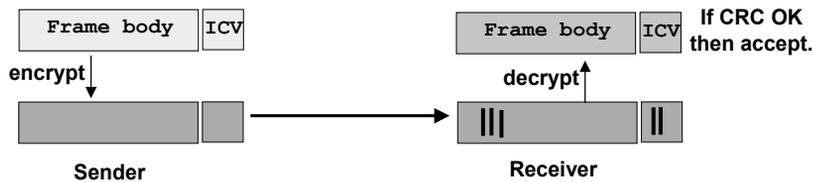
▸ Integrity check value (ICV) is good at detecting random bit errors, not intentional modifications to the packet
▸ An adversary can modify an encrypted packet such that those changes cannot be detected by CRC test at the receiver
▸ This is possible because encryption function (XOR) as well as CRC are both linear operations
   ● (M, c(M)) XOR (R, c(R)) = (M XOR R, c(M XOR R))
▸ The modified message after decryption will pass the CRC test !

WEP current status

- Note that attacks don't try to deduce the key. Knowledge of key stream is enough to launch all sorts of attacks
- Possible Solutions
  - ▸ Long IV's which never repeat for the lifetime of the shared secret
  - ▸ Replace CRC by a strong message authentication code which depends on the key and IV
- WEP2 addresses the first problem, but not the other
- A recent paper by Fluhrer, Mantin, and Shamir has discovered many inherent weaknesses in RC4 stream cipher. They have shown that RC4 is completely insecure when used used in a way prescribed by WEP, in which a fixed secret key is concatenated with known IV modifiers.
- 802.11i working group is now looking into using AES instead of WEP. AES will fix both problems of WEP
  - ▸ AES is a block cipher
  - ▸ AES includes a strong keyed message authentication code
- Bill Arbaugh's web-page (http://www.cs.umd.edu/~waa/wireless.html) is good source of info on this topic.

Bluetooth Vs. 802.11
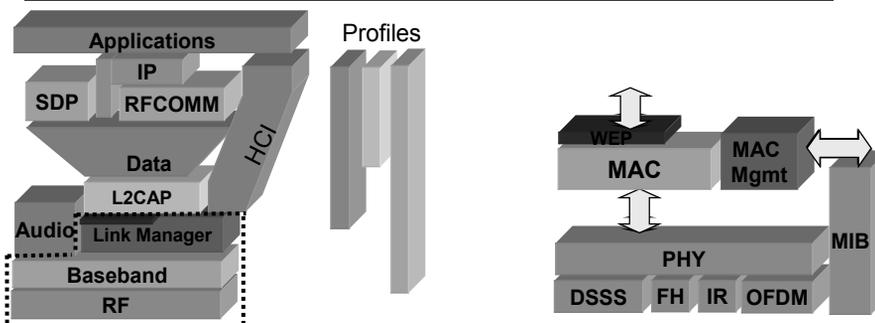
- Bluetooth is a (top down) market driven consortium
  - ▸ Business interests take precedence over technical considerations
  - ▸ Designed primarily for voice; data an afterthought
- 802.11 is a (bottom up) open standard effort
  - ▸ Good piece of engineering except for WEP
  - ▸ Designed primarily for data; voice an afterthought

Bluetooth Vs. 802.11: Radio issues

Radio is typically the most costly component in a wireless network interface

- Bluetooth radio is (will be) inexpensive because
  - ‣ It is a frequency hopper (which is relatively easy to build)
  - ‣ Its sensitivity is poor
  - ‣ It uses very simple modulation technique (GFSK) (requires less silicon)
  - ‣ It is possible to package both baseband and radio in a single chip
  - ‣ Potentially market for Bluetooth radios is (will be?) large if every mobile phone vendors decide to embed Bluetooth in their products
- 802.11 DSSS radios are costly today, but
  - ‣ if market for 802.11 continues to grow, their price may become competitive to Bluetooth
  - ‣ DSSS radios are superior to Bluetooth in terms of range, speed, BER performance
  - ‣ Due to better range, it may be cheaper to cover an area with 802.11
  - ‣ 802.11 can be operated at 0 dBm to reduce power consumption

P. Bhagwat   117

Radio architecture: 802.11 DSSS (typical)

Why is 802.11 radio supposed to be expensive and Bluetooth radio supposed to be cheap?

P. Bhagwat   118
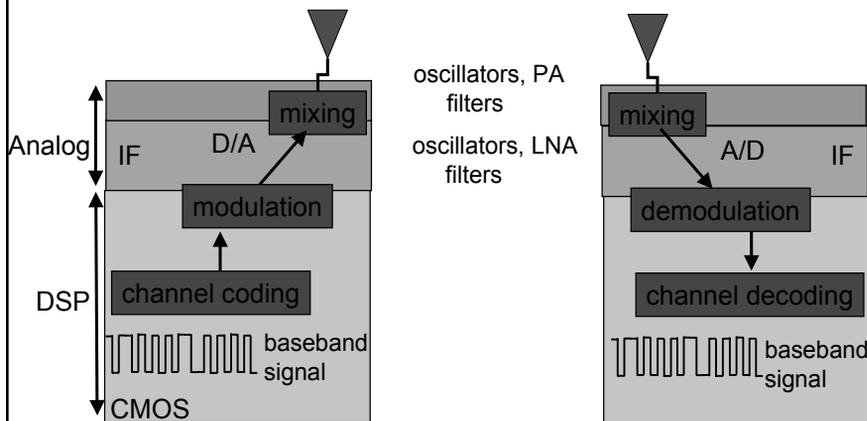
Radio architecture: Bluetooth

mixing

Analog | IF | D/A

modulation

DSP | channel coding

baseband signal

CMOS

CMOS oscillators, LNA, filters

mixing

A/D | IF

demodulation

channel decoding

baseband signal

P. Bhagwat   119
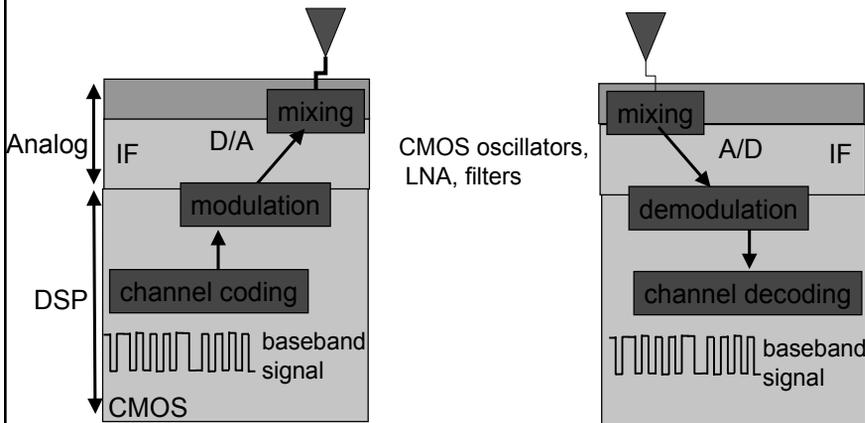
Single chip radio: challenges

mixing

Analog | IF | D/A

modulation

DSP | channel coding

baseband signal

CMOS
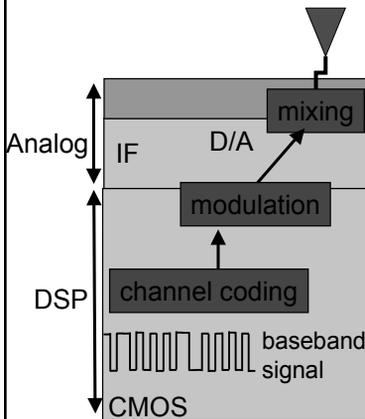
- Integrating a low-noise on chip synthesizer
- Handling the wide dynamic range of input interference signals
- Low power draw
- Cross talk between analog/analog and analog/digital circuits
- Achieving good linearity in an integrated filter
- Dealing with very low-level input signals ($10\mu v$) in the presence of IC substrate noise
- Dealing with high-level (-5dBm) input signals while keeping a low voltage power supply
- Achieving desired design performance in the presence of 15-20% component variations for R & C

P. Bhagwat   120

Bluetooth Vs. 802.11: MAC issues

	Bluetooth	802.11
Access Method	TDD Good for voice, but difficult for data	CSMA Good for data, but difficult for voice
Robustness to interference	ARQ	ARQ
Hidden nodes	Not an issue	RTS/CTS
Power Management	Yes	Yes
Power Control	Possible	Not possible
Paging	Possible	Not possible
Scalability	Limited	Stable at high loads
Future safe?	Not sure	Yes

Bluetooth Vs. 802.11: Market issues

	Bluetooth	802.11
Cost	Potential for low cost implementation exists but the market size will eventually determine the price point	Technology advances and market growth can reduce cost, even if tight single integration is not achieved in the near term
Market size	Potentially huge if every consumer electronic device is Bluetooth enabled	It is unlikely that 802.11 will penetrate the cosumer electronic device market in the near future
Form factor	Smaller due to single chip integration	Multi chip solution
Power consumption	Lower due to low power transmitter and tight integration	Will reduce in the future
Interoperability	The biggest problem of Bluetooth at present	802.11 is a more mature technology
Applications	Still looking for a killer app.	TCP/IP

Concluding remarks

- Will Bluetooth survive?
  - ▸ Bluetooth is ideal for cable replacement
  - ▸ Initial applications of Bluetooth will exploit its point-to-point or point-to-multipoint connectivity feature
  - ▸ Attempts to turn it into a LAN technology will face tough competition from 802.11b and 802.11a
  - ▸ Multi-hop over Bluetooth is still a technically challenging problem
  - ▸ Higher chances of success in Europe and Asia
- 802.11
  - ▸ Will continue to grow in
    - ● Public spaces, home, industry vertical, and enterprise market
  - ▸ 802.11 will provide a viable alternative to 3G in public places