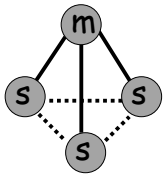


Personal Area Networking over Bluetooth

Pravin Bhagwat
Networking Research Group
AT&T Labs - Research
pravin@acm.org

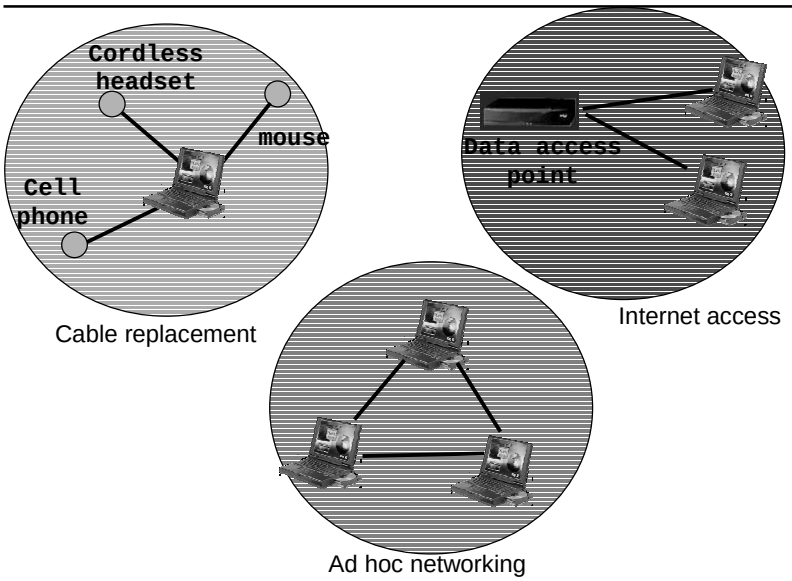
ACM Mobicom 2000
Half day tutorial
Aug 06, 2000
Boston, MA

Bluetooth

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

Why not use Wireless LANs?
- power
- cost

Value proposition of Bluetooth



Pravin Bhagwat (AT&T Labs) 3

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
- February 2000: There are 1,800+ adopters

Pravin Bhagwat (AT&T Labs) 4

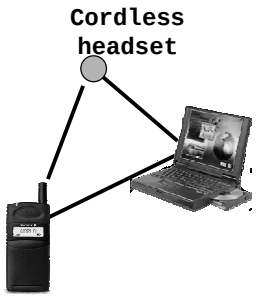
New Applications

Synchronization

User benefits

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

Cordless Headset



User benefits

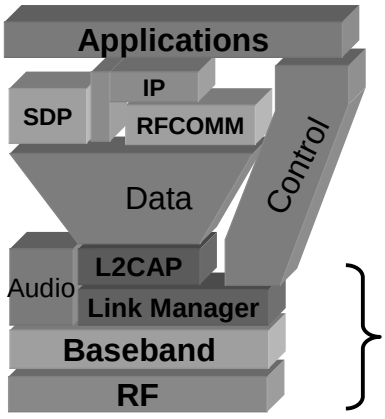
- **Multiple device access**
- **Cordless phone benefits**
- **Hands free operation**

Usage scenarios examples

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

Bluetooth Specifications

Bluetooth Specifications

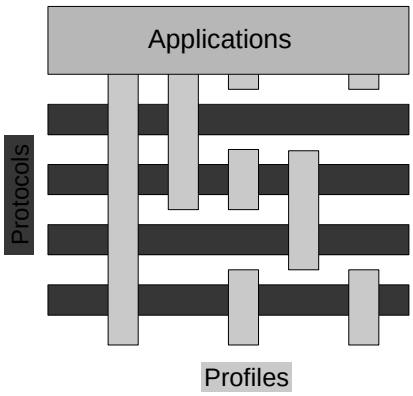


Single chip with RS-232, USB, or PC card interface

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

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

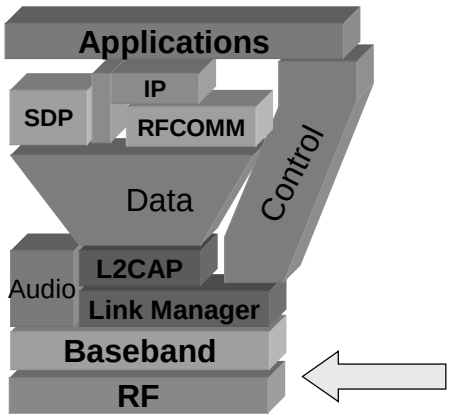


Pravin Bhagwat (AT&T Labs) 11

Technical Overview

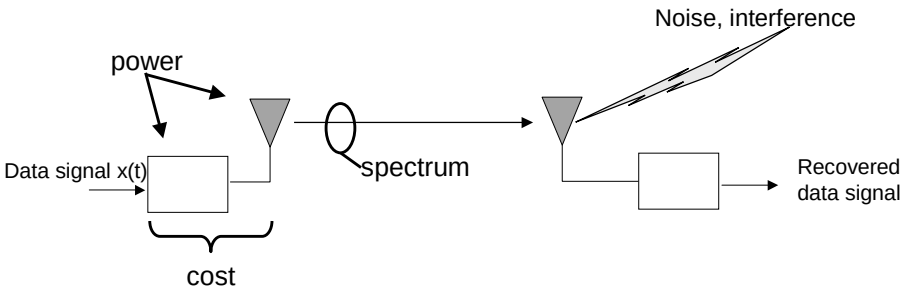
Pravin Bhagwat (AT&T Labs) 12

Bluetooth Radio Specification



Pravin Bhagwat (AT&T Labs) 13

Design considerations

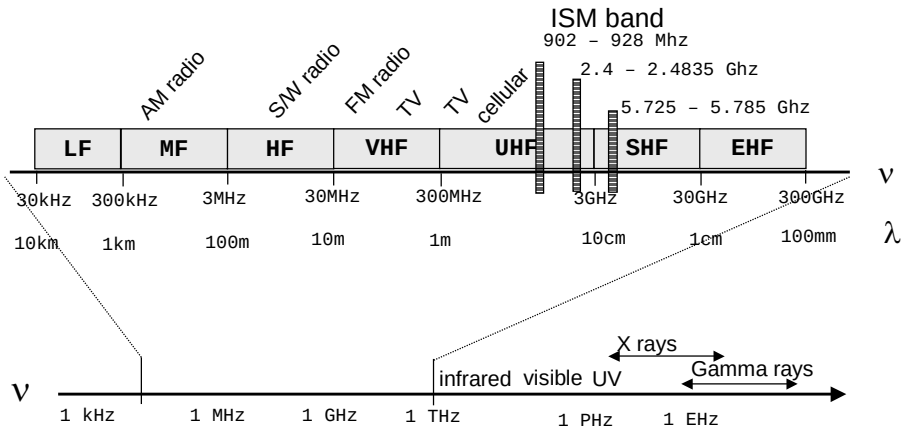


Goal

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

Pravin Bhagwat (AT&T Labs) 14

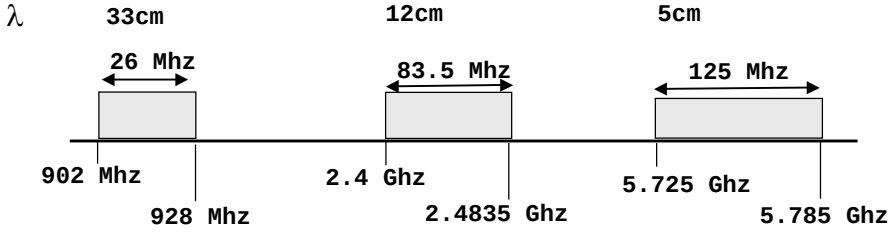
EM Spectrum



Propagation characteristics are different in each frequency band

Pravin Bhagwat (AT&T Labs) 15

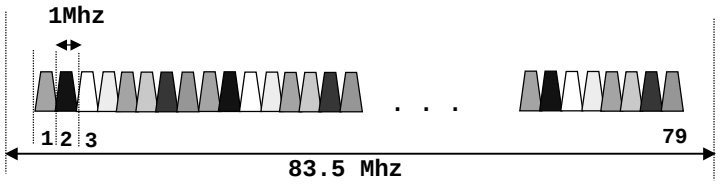
Unlicensed Radio Spectrum



cordless phones	802.11	unused
baby monitors	Bluetooth	
Wireless LANs	Microwave oven	

Pravin Bhagwat (AT&T Labs) 16

Bluetooth radio link

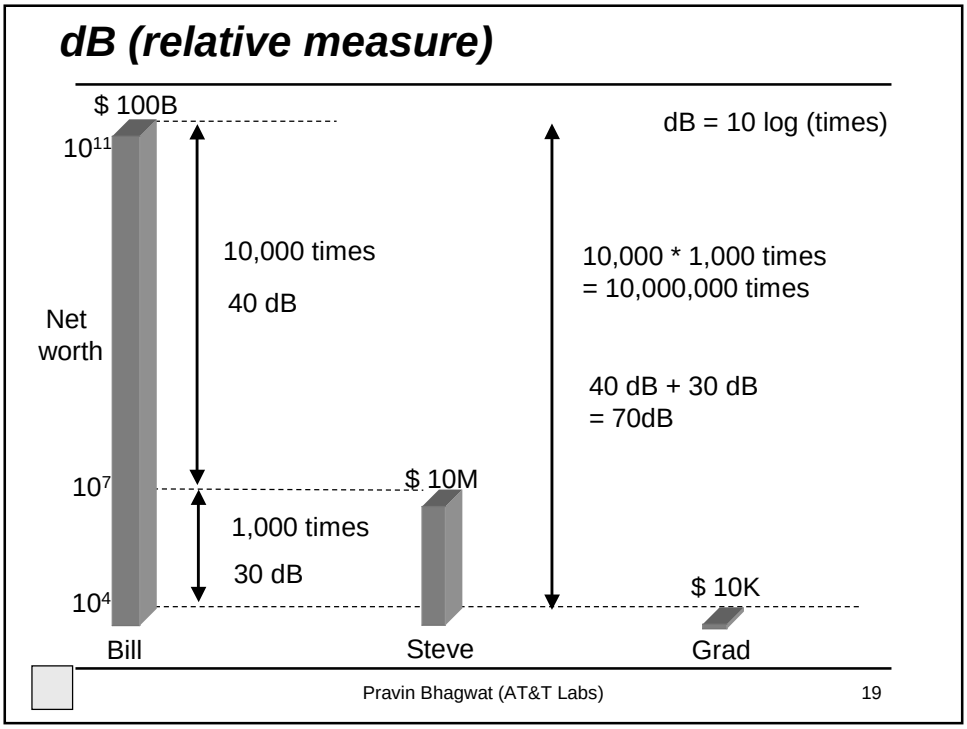


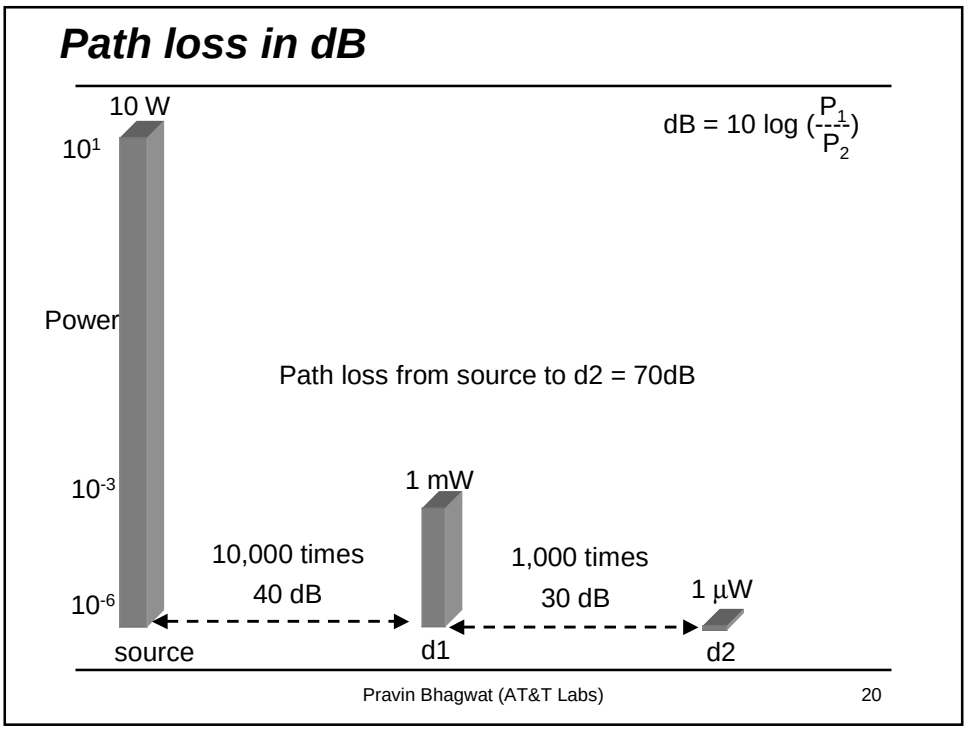
- frequency hopping spread spectrum
  - 2.402 GHz + k MHz, k=0, …, 78
  - 1,600 hops per second
- GFSK modulation
  - 1 Mb/s symbol rate
- transmit power
  - 0 dbm (up to 20dbm with power control)

Pravin Bhagwat (AT&T Labs) 17

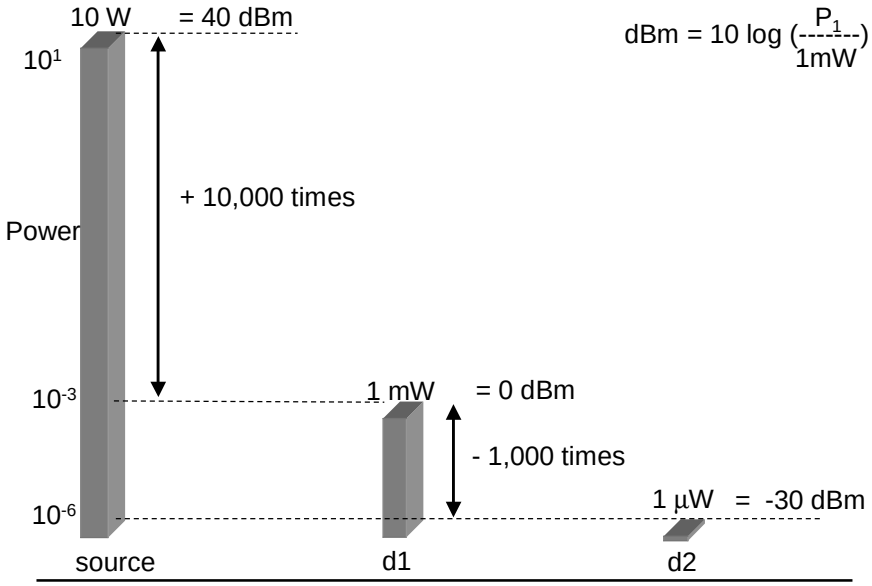
Review of basic concepts

Pravin Bhagwat (AT&T Labs) 18


dB (relative measure)
$ 100B
10^{11}
dB = 10 log (times)
10,000 times
40 dB
10,000 * 1,000 times
= 10,000,000 times
Net
worth
40 dB + 30 dB
= 70dB
10^{7}
$ 10M
1,000 times
30 dB
10^{4}
$ 10K
Bill
Steve
Grad
Pravin Bhagwat (AT&T Labs)
19

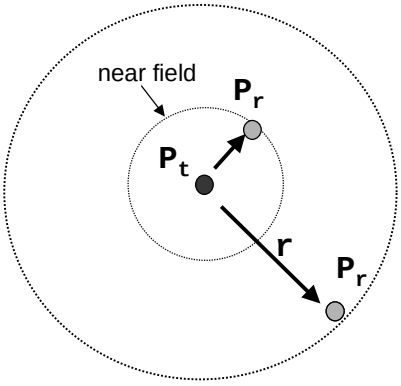

Path loss in dB
10 W
10^{1}
dB = 10 log ($\frac{P_1}{P_2}$)
Power
Path loss from source to d2 = 70dB
1 mW
10^{-3}
10,000 times
40 dB
1,000 times
30 dB
1 µW
10^{-6}
source
d1
d2
Pravin Bhagwat (AT&T Labs)
20

dBm (absolute measure of power)



Pravin Bhagwat (AT&T Labs) 21

Radio propagation: path loss



path loss in 2.4 Ghz band

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

near field $\propto r^2$ | far field $\propto r^{3.3}$

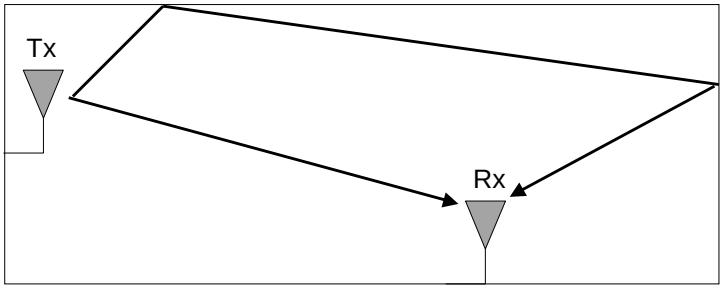
path loss $= 10 \log (4\pi r^2/\lambda)$ $r \leq 8m$

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

Pravin Bhagwat (AT&T Labs) 22

Fading and multipath

Fading: rapid fluctuation of the amplitude of a radio signal over a short period of time or travel distance

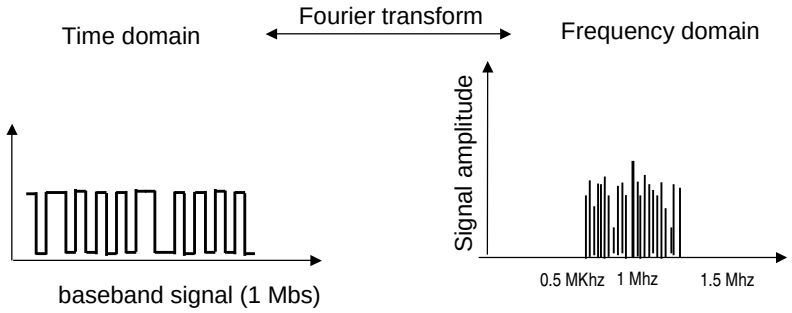


Effects of multipath

- Fading
- Varying doppler shifts on different multipath signals
- Time dispersion (causing inter symbol interference)

Pravin Bhagwat (AT&T Labs) 23

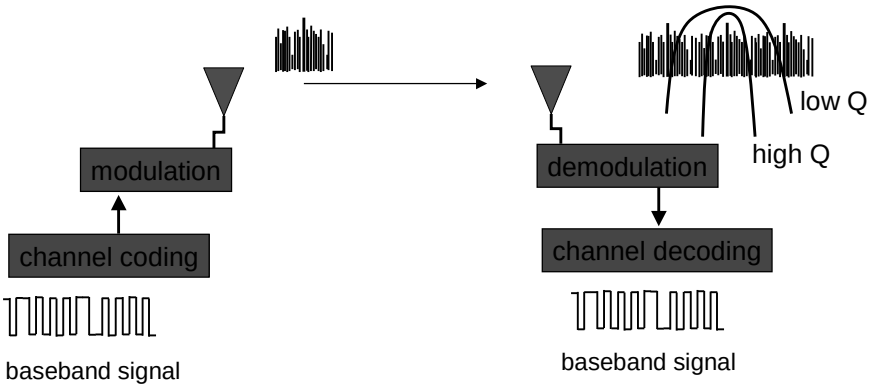
Bandwidth of digital data



- Baseband signal cannot directly be transmitted on the wireless medium
- Need to translate the baseband signal to a new frequency so that it can be transmitted easily and accurately over a communication channel

Pravin Bhagwat (AT&T Labs) 24

Channel coding and modulation

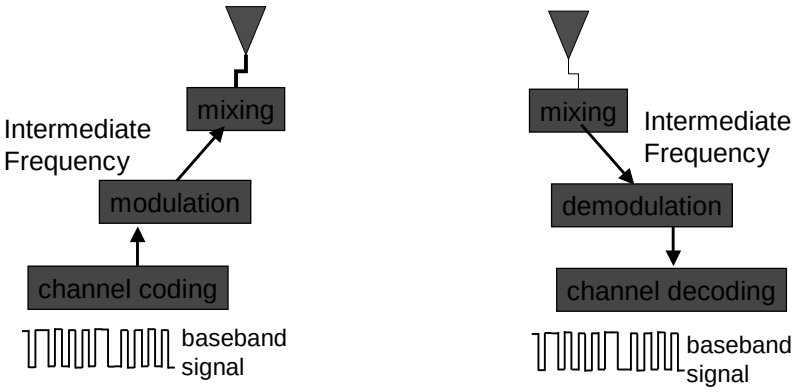


Challenges

- Modulation of 1Mhz baseband signal into 2.4Ghz band is difficult to achieve in one step
  - CMOS transistors do not operate at those frequencies
- Difficult to build filters with high Q factor

Pravin Bhagwat (AT&T Labs) 25

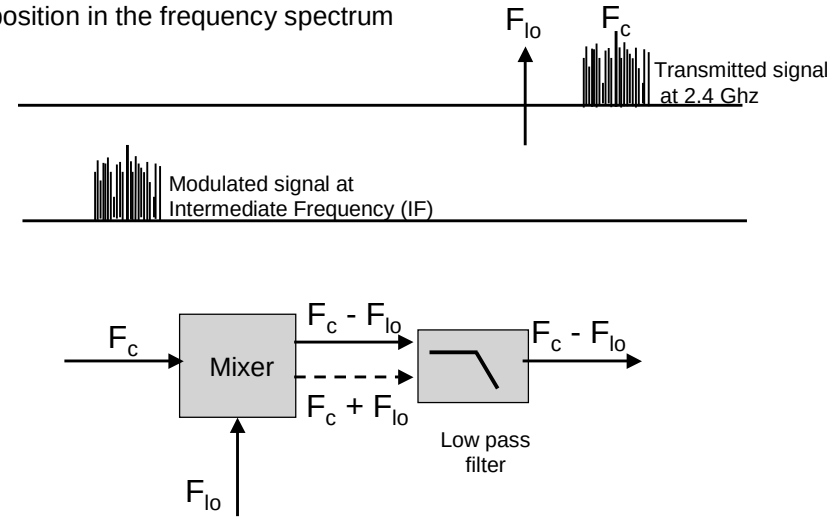
Radio architecture: typical design



Pravin Bhagwat (AT&T Labs) 26

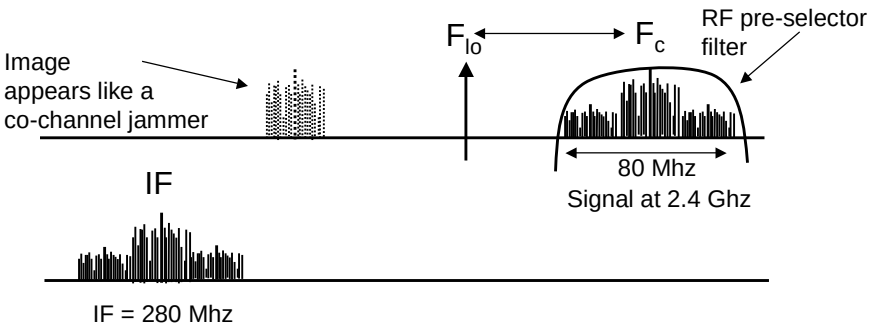
Mixing

The process of translating the information signal to a different position in the frequency spectrum



Pravin Bhagwat (AT&T Labs) 27

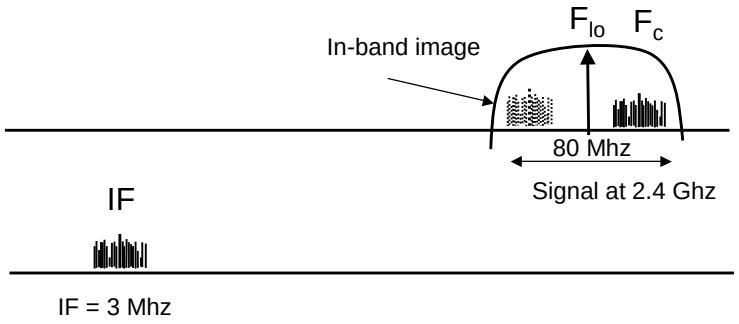
Image rejection



- Good image rejection performance when F_{lo} is sufficiently far away from F_c
- That is, when IF frequency is high
- To allow single chip integrated radio, IF should be moved down to lower frequency

Pravin Bhagwat (AT&T Labs) 28

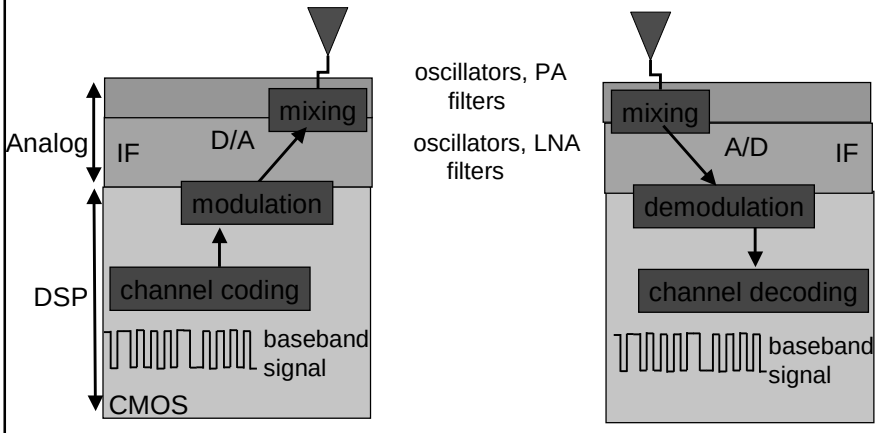
Image rejection with Low IF



- To allow single chip integrated radio, IF is moved down to 3 Mhz which allows construction of the filter on-chip with low power
- It is impossible to build a RF pre-selector filter to remove the in-band image
- So a special RF architecture is used called “image-reject” mixer to suppress in-band interference arising from the image.

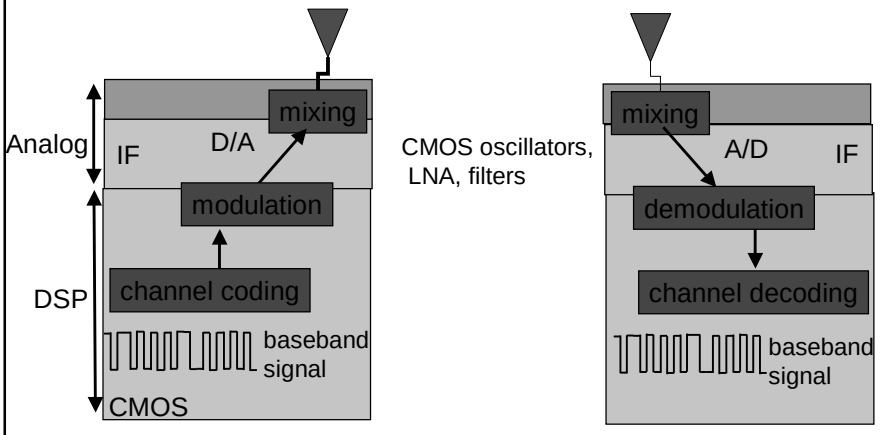
Pravin Bhagwat (AT&T Labs) 29

Radio architecture: typical design



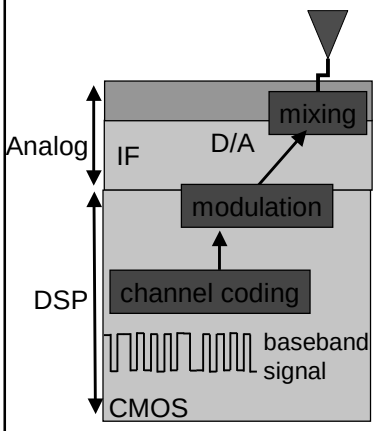
Pravin Bhagwat (AT&T Labs) 30

Radio architecture: Bluetooth



Pravin Bhagwat (AT&T Labs) 31

Single chip radio: challenges



- 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 (10μv) 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

Pravin Bhagwat (AT&T Labs) 32

Bluetooth Radio

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

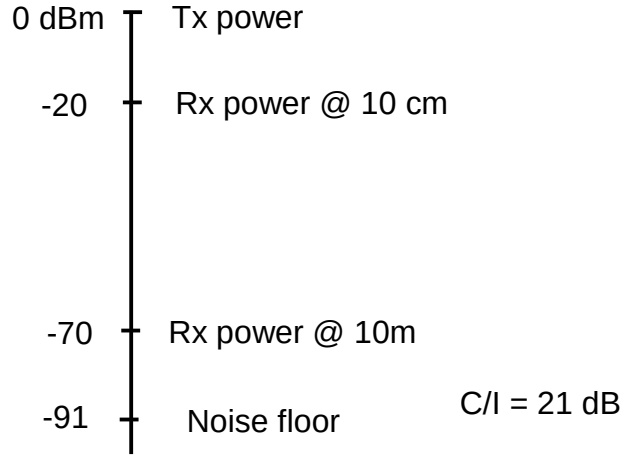
Bluetooth Radio

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

Bluetooth Radio

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

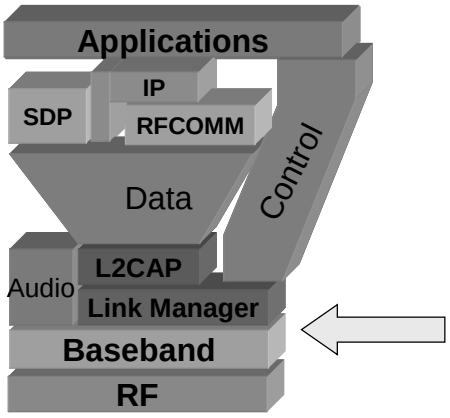
Transmit power & receiver sensitivity



Radio: design rationale

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

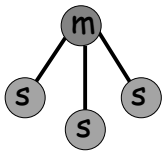
Baseband



Bluetooth Physical link

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

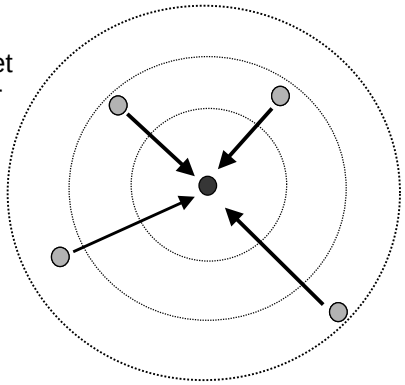
- Piconet
  - Master can connect to 7 slaves
  - Each piconet has max capacity (1 Mbps)
  - hopping pattern is determined by the master



Pravin Bhagwat (AT&T Labs) 39

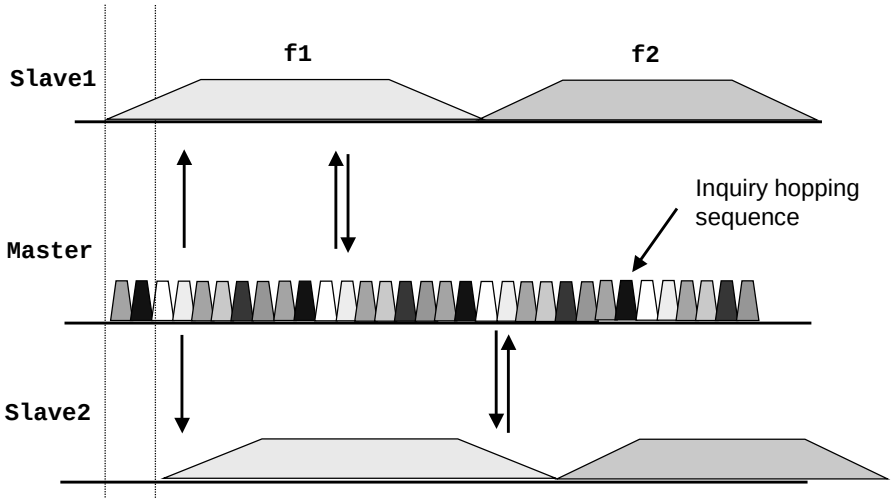
Connection Setup

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



Pravin Bhagwat (AT&T Labs) 40

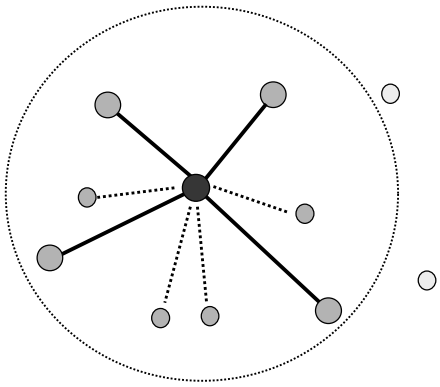
Inquiry on time axis



Pravin Bhagwat (AT&T Labs) 41

Piconet formation

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



Master
Active Slave
Parked Slave
Standby

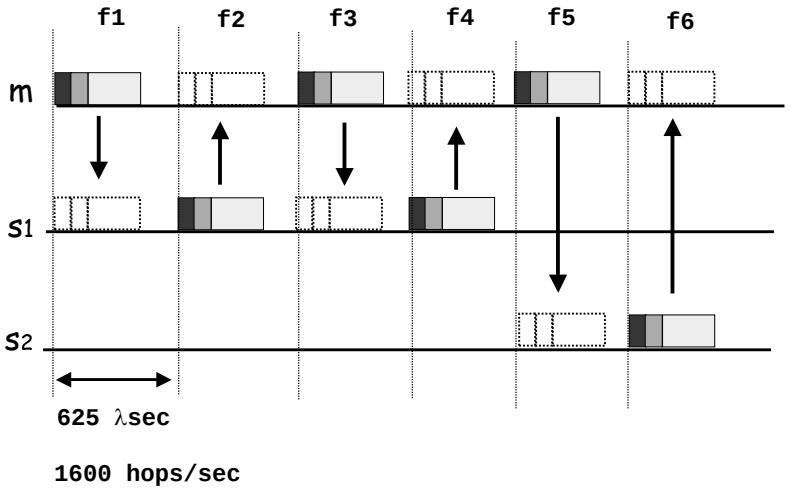
Pravin Bhagwat (AT&T Labs) 42

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

Piconet channel

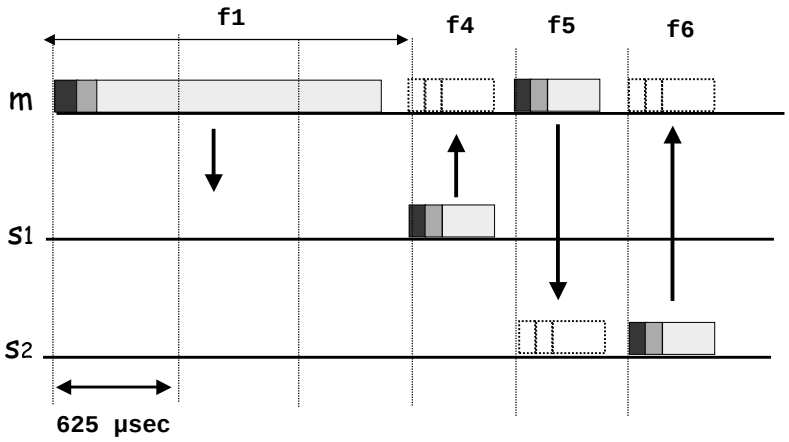
FH/TDD



1600 hops/sec

Multi slot packets

FH/TDD

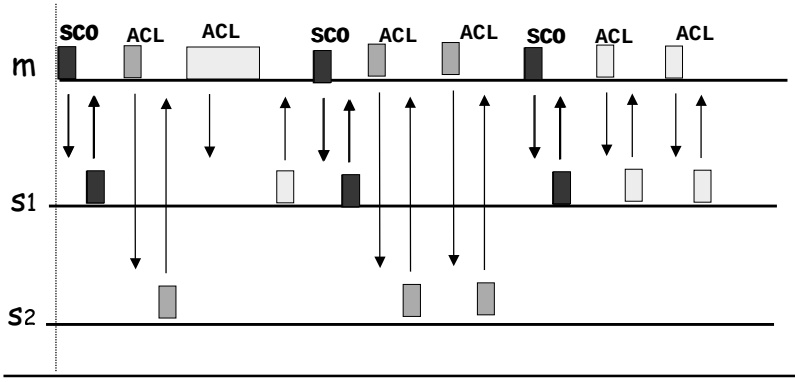


Data rate depends on type of packet

Pravin Bhagwat (AT&T Labs) 45

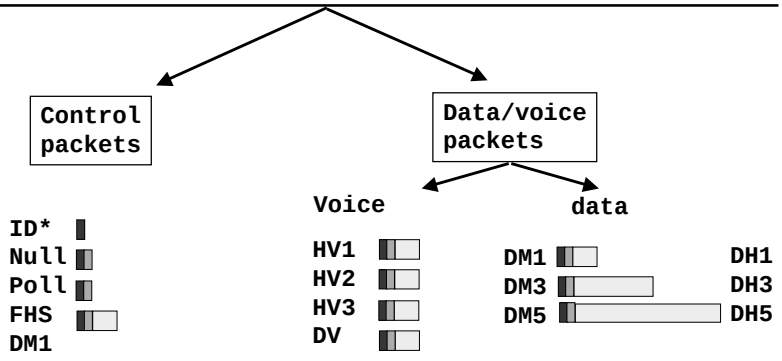
Physical Link Types

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



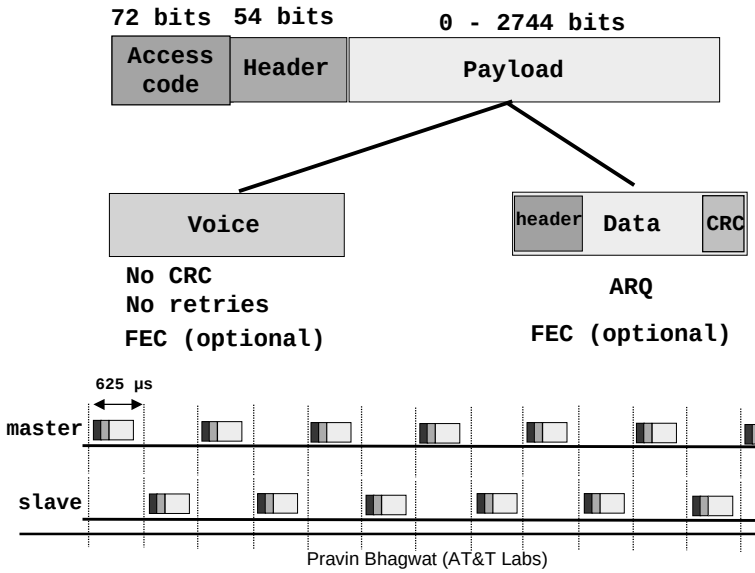
Pravin Bhagwat (AT&T Labs) 46

Packet Types



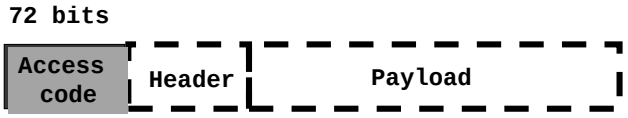
Pravin Bhagwat (AT&T Labs) 47

Packet Format



Pravin Bhagwat (AT&T Labs) 48

Access Code

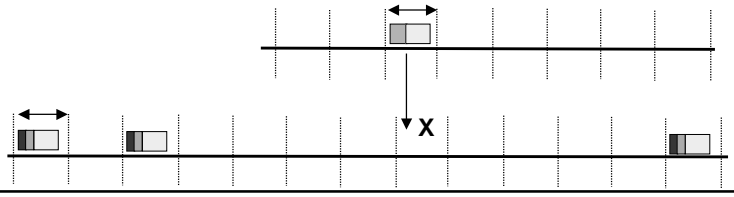


Purpose

- Synchronization
- DC offset compensation
- Identification
- Signaling

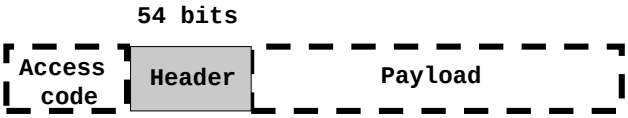
Types

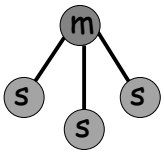
- Channel Access Code (CAC)
- Device Access Code (DAC)
- Inquiry Access Code (IAC)



Pravin Bhagwat (AT&T Labs) 49

Packet Header





Purpose

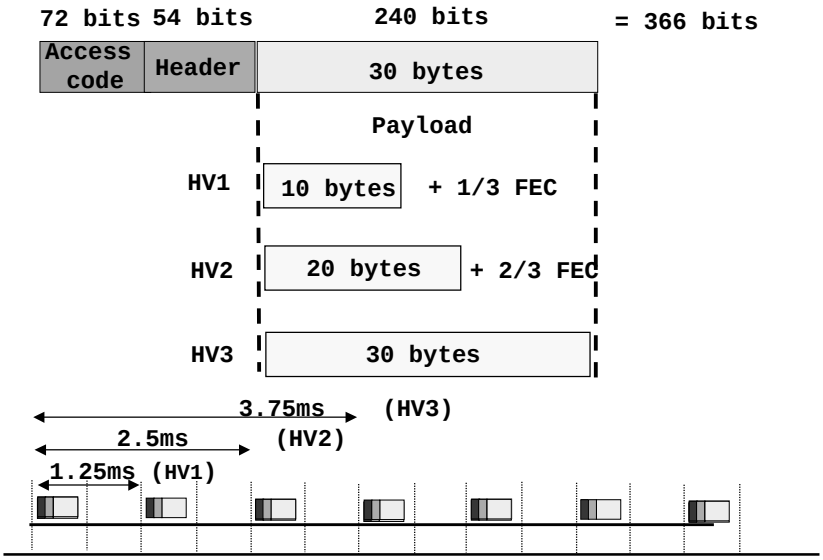
- Addressing (3) → Max 7 active slaves
- Packet type (4) → 16 packet types (some unused)
- Flow control (1)
- 1-bit ARQ (1) → Broadcast packets are not ACKed
- Sequencing (1) → For filtering retransmitted packets
- HEC (8) → Verify header integrity

total	18 bits

Encode with 1/3 FEC to get 54 bits

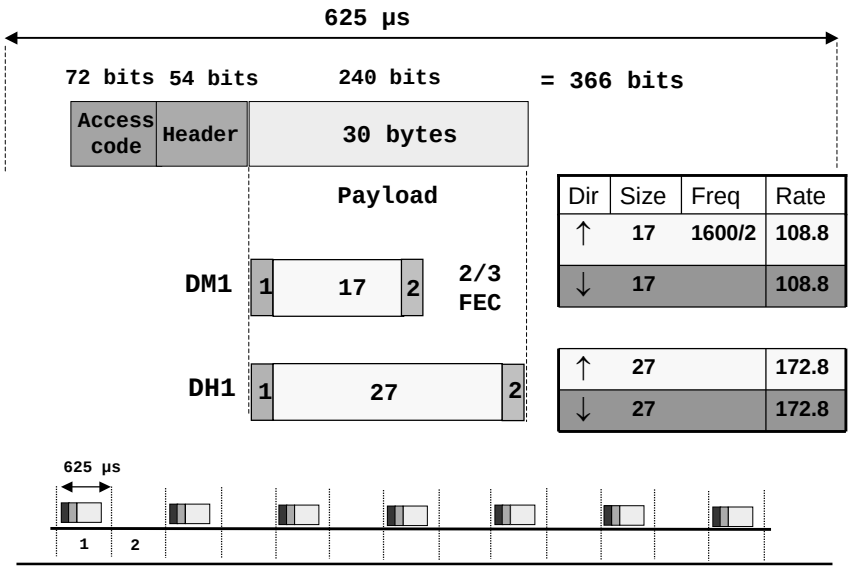
Pravin Bhagwat (AT&T Labs) 50

Voice Packets (HV1, HV2, HV3)



Pravin Bhagwat (AT&T Labs) 51

Data rate calculation: DM1 and DH1

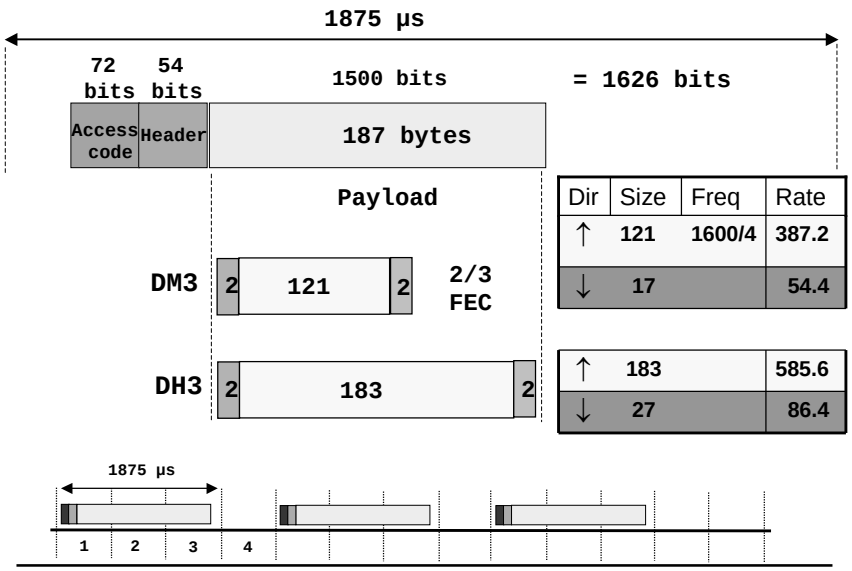


Dir	Size	Freq	Rate
↑	17	1600/2	108.8
↓	17		108.8

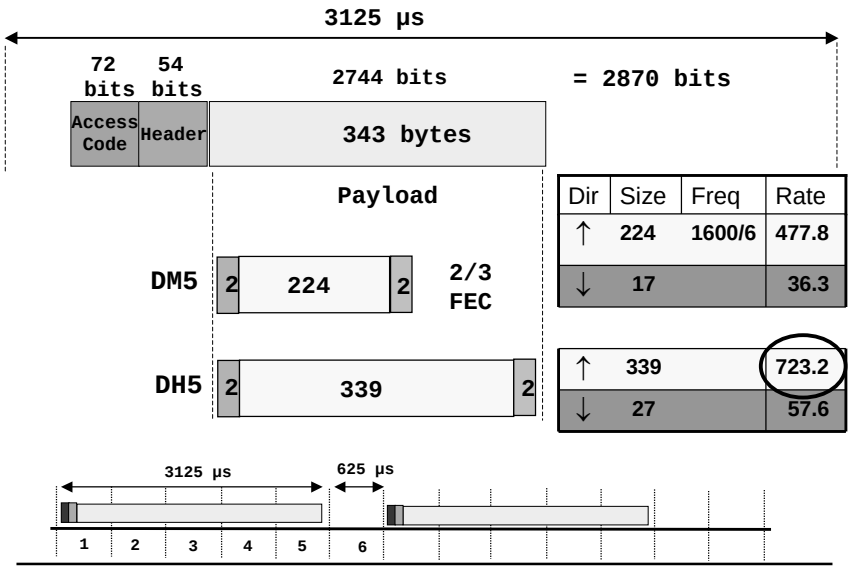
↑	27	172.8
↓	27	172.8

Pravin Bhagwat (AT&T Labs) 52

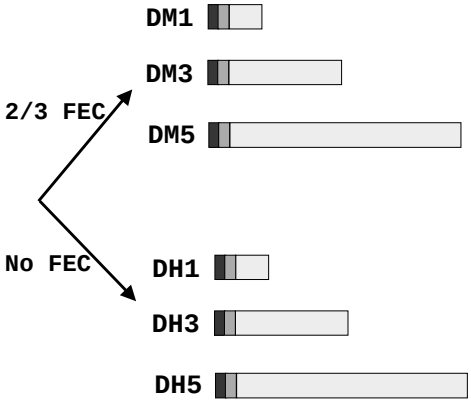
Data rate calculation: DM3 and DH3



Data rate calculation: DM5 and DH5



Data Packet Types

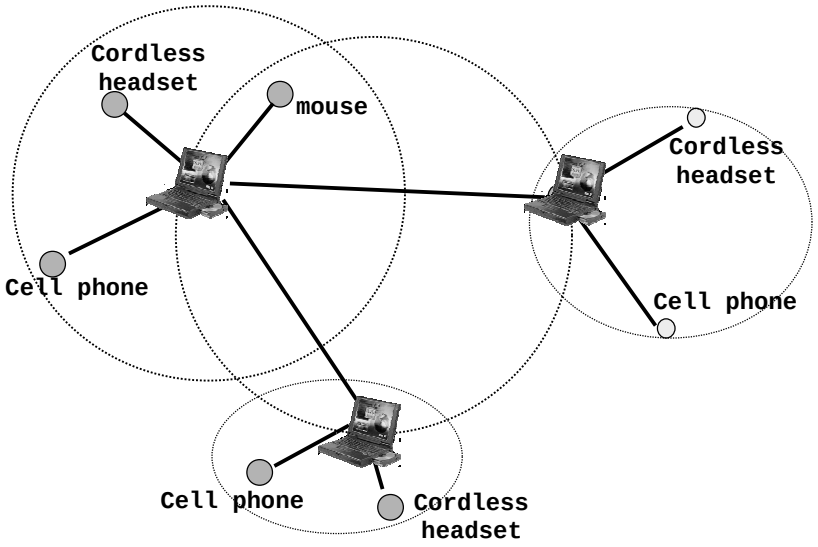


Symmetric	Asymmetric	
108.8	108.8	108.8
258.1	387.2	54.4
286.7	477.8	36.3

Symmetric	Asymmetric	
172.8	172.8	172.8
390.4	585.6	86.4
433.9	723.2	57.6

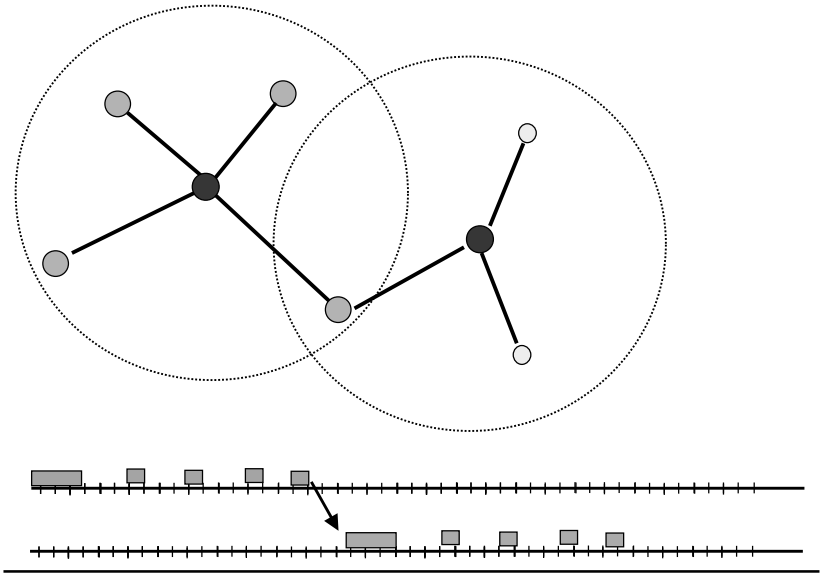
Pravin Bhagwat (AT&T Labs) 55

Inter piconet communication



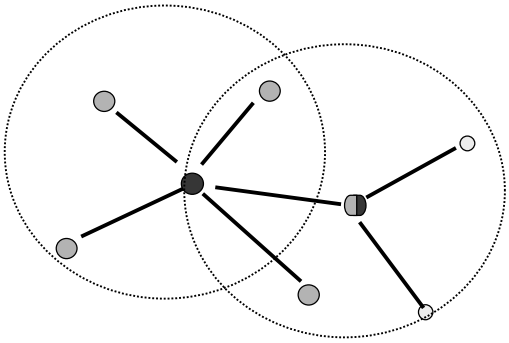
Pravin Bhagwat (AT&T Labs) 56

Scatternet



Pravin Bhagwat (AT&T Labs) 57

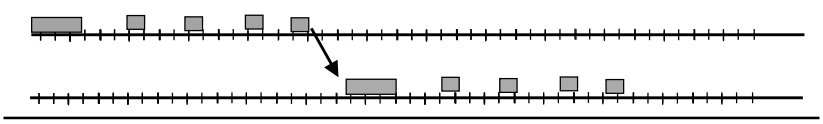
Scatternet, scenario 2



How to schedule presence in two piconets?

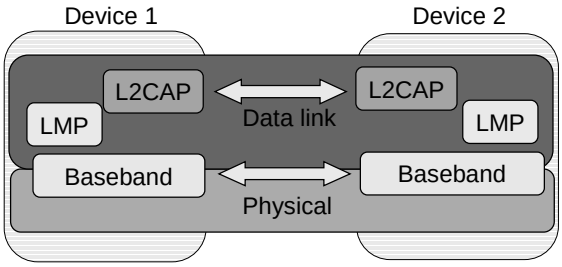
Forwarding delay ?

Missed traffic?



Pravin Bhagwat (AT&T Labs) 58

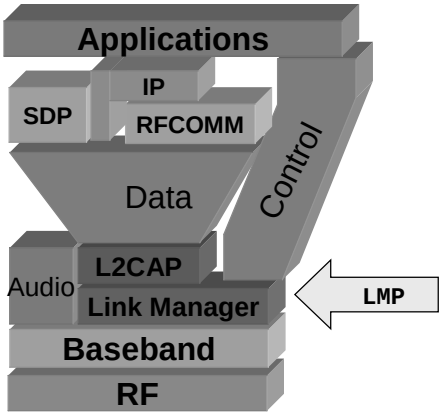
Baseband: Summary



- 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)

Pravin Bhagwat (AT&T Labs) 59

Link Manager Protocol



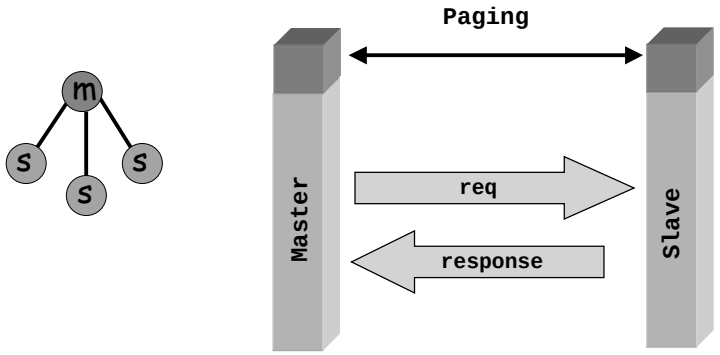
Setup and management of Baseband connections

- Piconet Management
- Link Configuration
- Security

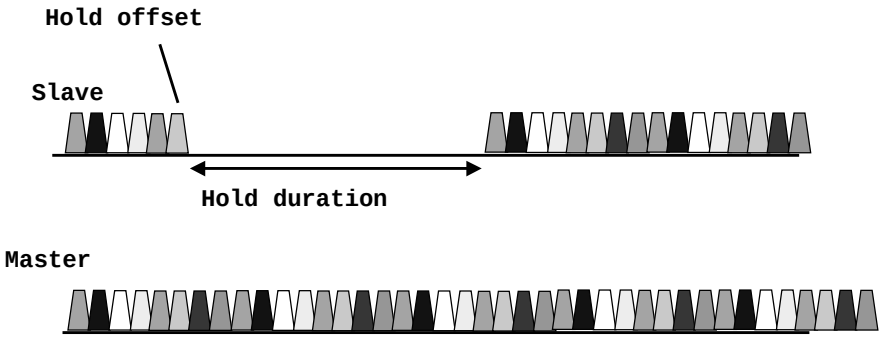
Pravin Bhagwat (AT&T Labs) 60

Piconet Management

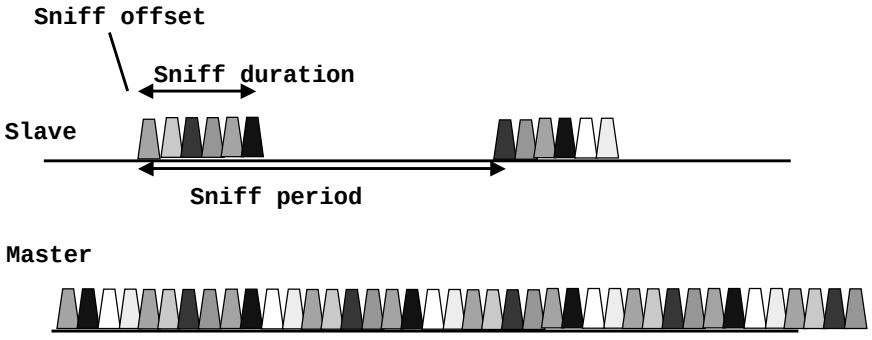
- Attach and detach slaves
- Master-slave switch
- Establishing SCO links
- Handling of low power modes (Sniff, Hold, Park)



Low power mode (hold)



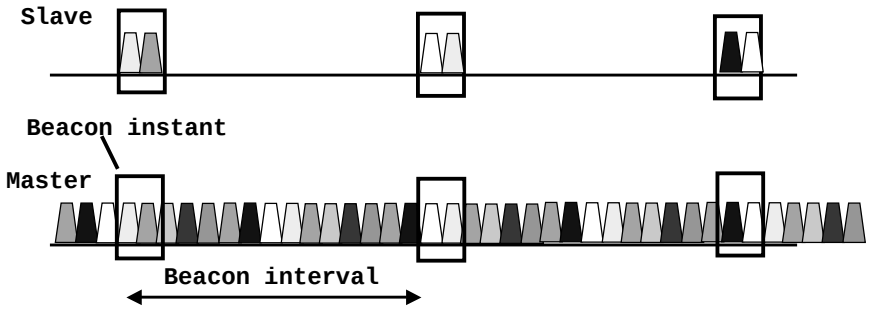
Low power mode (Sniff)



- Traffic reduced to periodic sniff slots

Pravin Bhagwat (AT&T Labs) 63

Low power mode (Park)

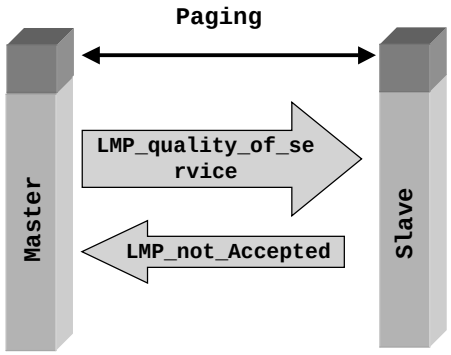


- Power saving + keep more than 7 slaves in a piconet
- Give up active member address, yet maintain synchronization
- Communication via broadcast LMP messages

Pravin Bhagwat (AT&T Labs) 64

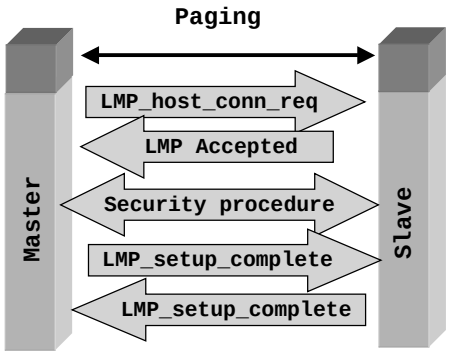
Link Configuration

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



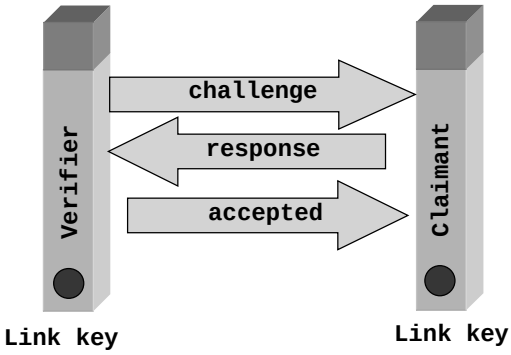
Connection establishment & Security

- 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



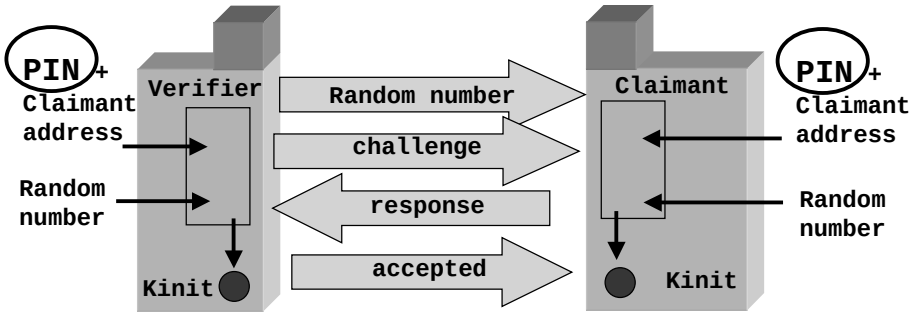
Authentication

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



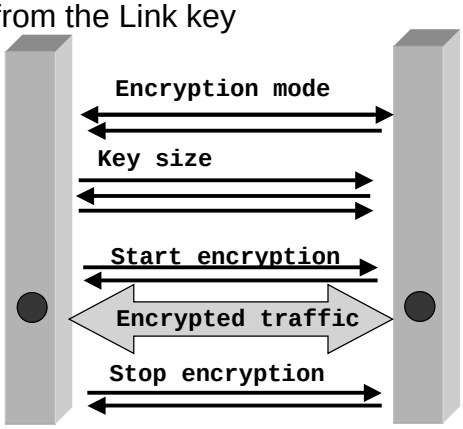
Pairing (key distribution)

- 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

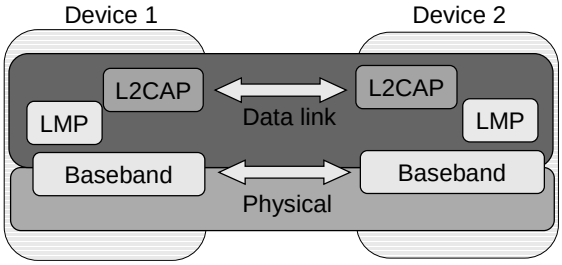


Encryption

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

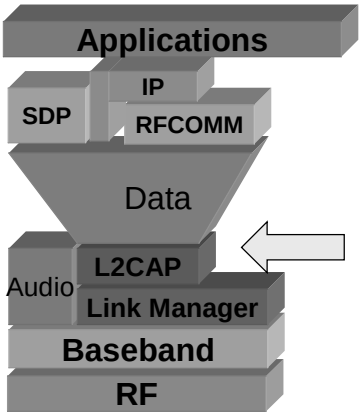


Link Manager Protocol Summary



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

L2CAP

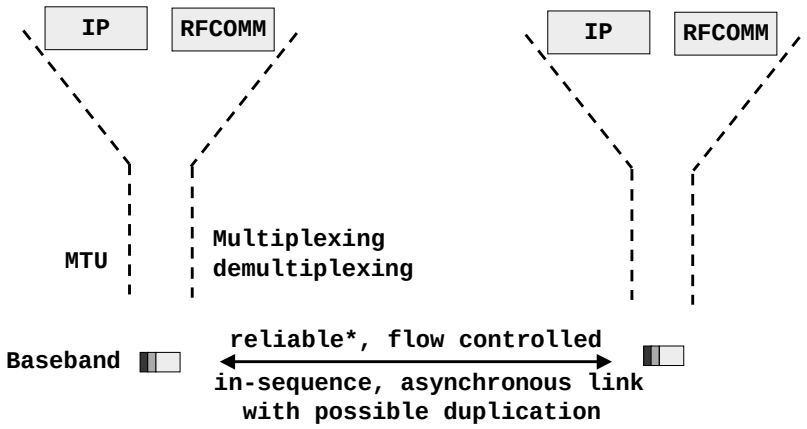


Logical Link Control and Adaptation Protocol

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

Pravin Bhagwat (AT&T Labs) 71

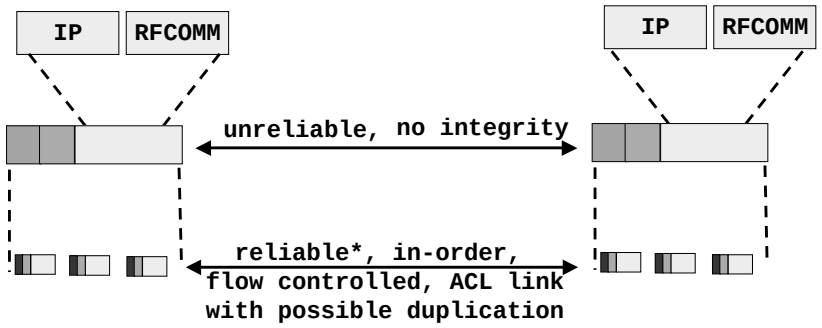
Why baseband isn't sufficient



- Baseband packet size is very small (17min, 339 max)
- No protocol-id field in the baseband header

Pravin Bhagwat (AT&T Labs) 72

Need a multiprotocol encapsulation layer

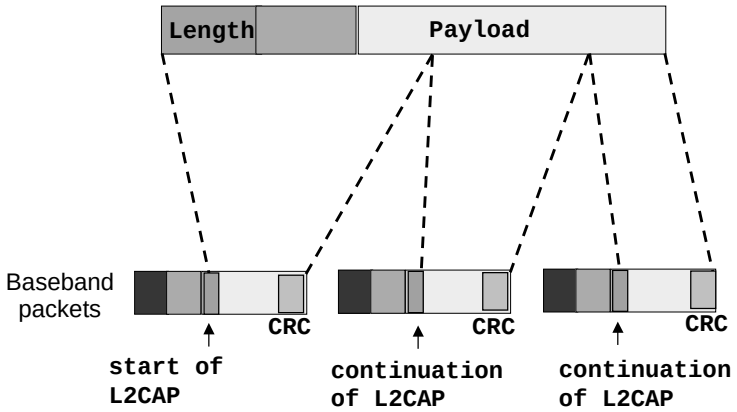


Desired features
- Protocol multiplexing
- Segmentation and re-assembly
- Quality of service

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

Pravin Bhagwat (AT&T Labs) 73

Segmentation and reassembly

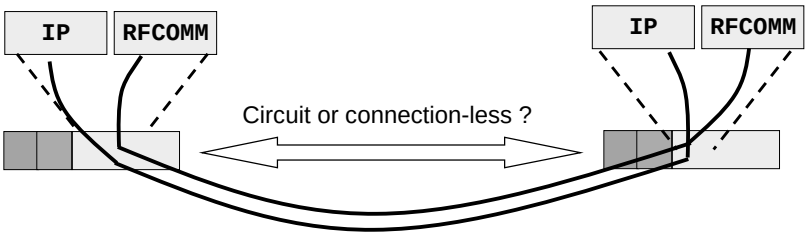


- cannot cope with re-ordering or loss
- mixing of multiple L2CAP fragments not allowed
- If the start of L2CAP packet is not acked, the rest should be discarded

min MTU = 48
672 default

Pravin Bhagwat (AT&T Labs) 74

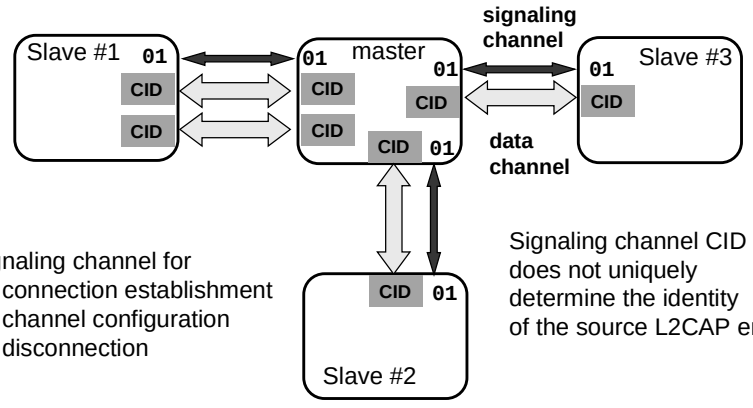
Multiplexing and Demultiplexing



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)

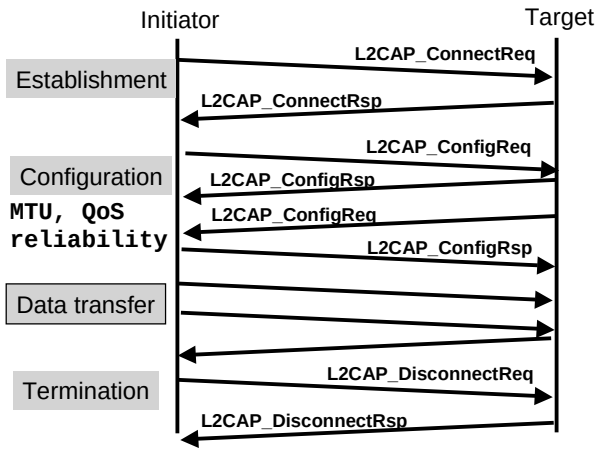
L2CAP Channels



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

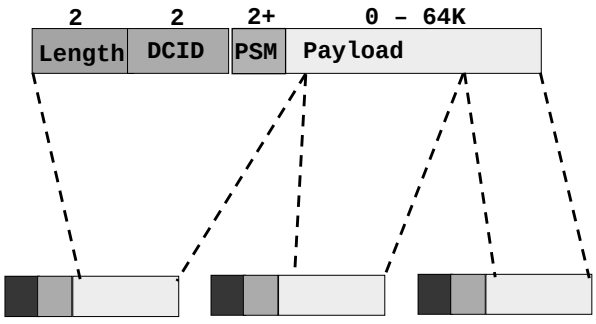
Signaling channel CID does not uniquely determine the identity of the source L2CAP entity

L2CAP connection: an example



Pravin Bhagwat (AT&T Labs) 77

L2CAP Packet Format (Connectionless)



Not fully developed yet.

Pravin Bhagwat (AT&T Labs) 78

L2CAP: Summary

Design constraints:

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

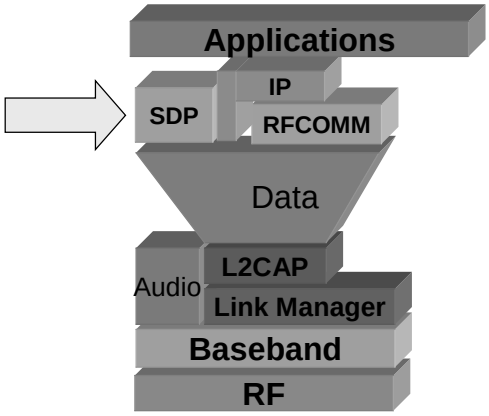
Assumptions about the lower layer

- 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

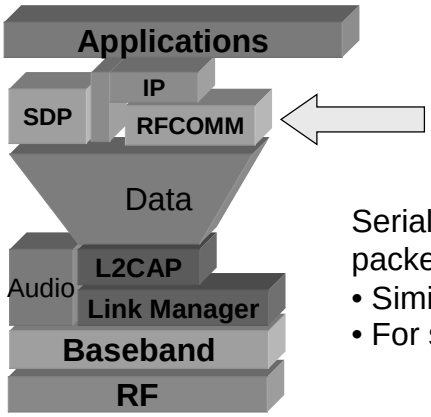
Bluetooth Service Discovery Protocol



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

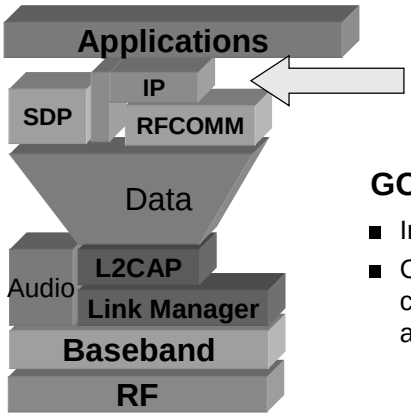


Serial Port emulation on top of a packet oriented link
• Similar to HDLC
• For supporting legacy apps

Serial line emulation over packet based MAC

- 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
- Options
  - collect MTU bytes and then send
  - wait until a timeout
  - send whatever is available

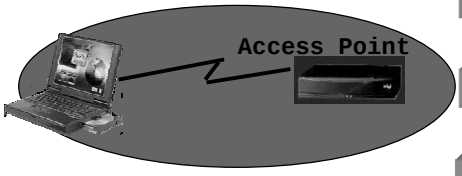
IP over Bluetooth V 1.0

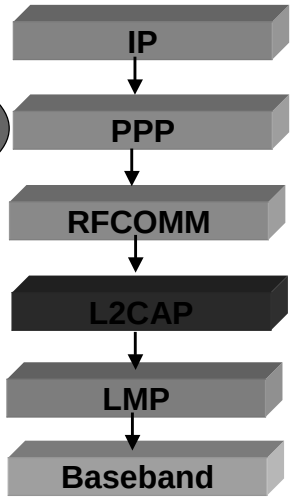


GOALS

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

LAN access point profile



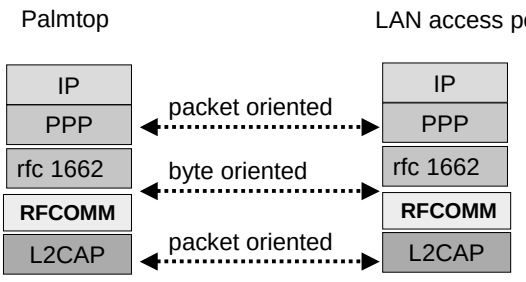


Why use PPP?

- Security
  - Authentication
  - Access control
- Efficiency
  - header and data compression
- Auto-configuration
- Lower barrier for deployment

Pravin Bhagwat (AT&T Labs) 85

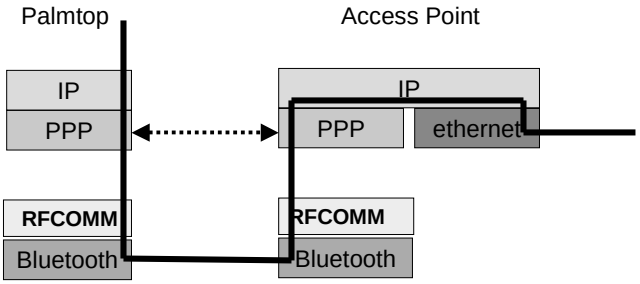
Inefficiency of layering



- Emulation of RS-232 over the Bluetooth radio link could be eliminated

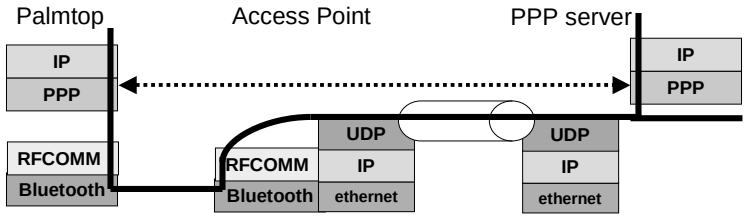
Pravin Bhagwat (AT&T Labs) 86

Terminate PPP at LAN access point



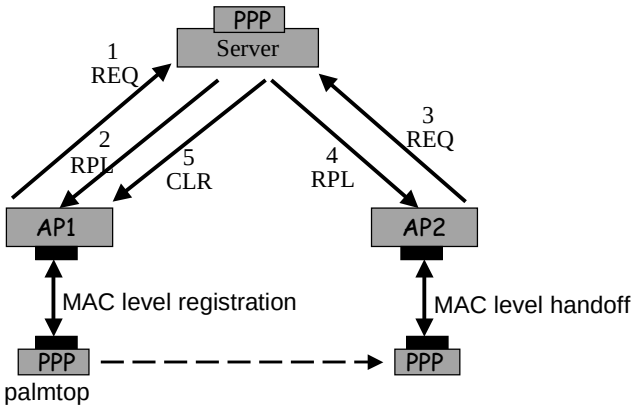
- PPP server function at each access point
  - management of user name/password is an issue
  - roaming is not seamless

L2TP style tunneling



- Tunneling PPP traffic from access points to the PPP server
  - 1) centralized management of user name/password
  - 2) reduction of processing and state maintenance at each access point
  - 3) seamless roaming

Seamless roaming with PPP



Pravin Bhagwat (AT&T Labs) 89

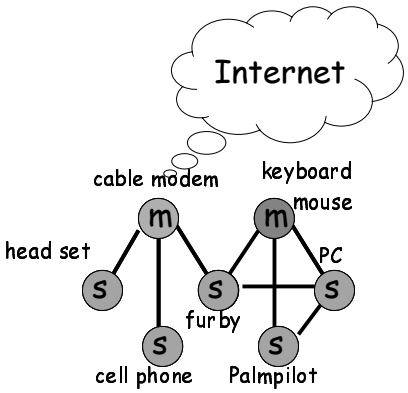
IP over Bluetooth

Next steps

IP based network connectivity	peer-to-peer connectivity	Internet connectivity for non-PC devices
IP over wireless media	Decentralized techniques for link formulation, naming, addressing, and routing	Investigation of the right design point for running IP over toasters, light switches, & fire alarms

Pravin Bhagwat (AT&T Labs) 90

Research challenges



Plug-n-play applications

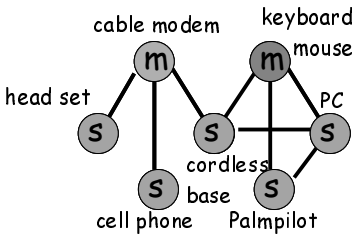
Resource Discovery

Routing over scatternets

Techniques for link formation

Will the current solutions for each layer work in this environment?

What is different in this scenario ?



Connection oriented, low-power link technology

Small, multi-hop networks

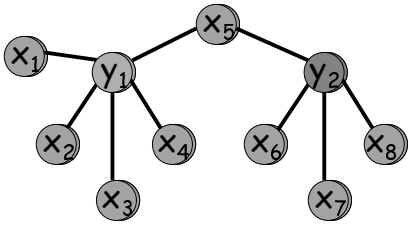
Simple devices

Isolated network

Dynamic network

Applications ---> services ----> routing ----> link creation

Link Formation



The problem does not exist in most wired/wireless networks

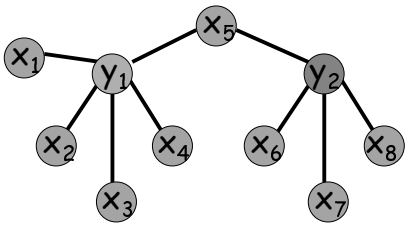
Proximity ≠ Link

Low power modes require careful use of broadcast

Maintaining connectivity in absence of application traffic seems wasteful

Hints from higher layer are needed

Routing over Scatternets



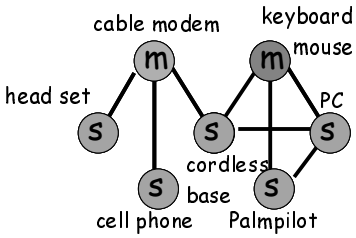
Nodes must co-operate to forward packets (MANET style protocols)

Forwarding at Layer 2 or Layer 3?

Bridging or routing ?

What interface should be exported to the layer above?
Better coupling with the service discovery layer is needed

Service discovery



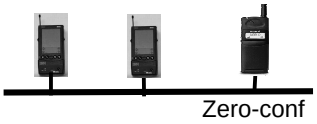
Need solutions for address allocation, name resolution, service discovery

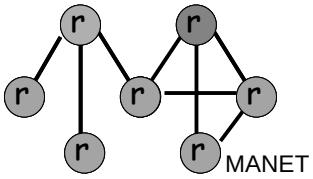
Existing solutions in the Internet depend on infrastructure

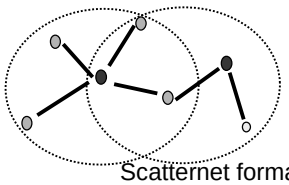
Judicious use of Multicast/broadcast is needed

These goals are similar to what Zero-conf WG is already working on

Point to ponder







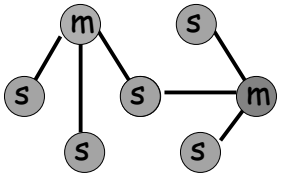
Will Zero-conf on top of MANET on top of scatternet construction algorithm solve our problem?

Layered and simple, but potential inefficiencies

Cross-layer optimizations are worth considering

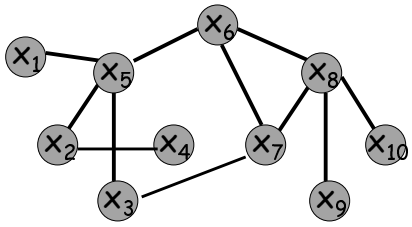
Scatternet enumeration

Problem: given N Bluetooth nodes how many different ways can scatternets be formed?



- node type constraint
  - master | slave | bridge
- degree constraint
  - degree (master) <= 7
  - degree (bridge) >= 2 , <= max
- connectivity constraint
  - no slave to slave link
  - no master to master link (makes it a bi-partite graph)

Graph enumeration

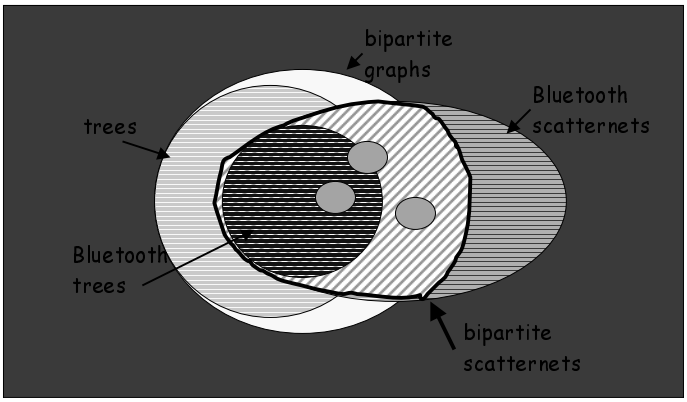


- Assign a label x_i to each node
- $x_1x_2^2x_3^2x_4x_5^4x_6^3x_7^3x_8^4x_9x_1$
- deg. seq. $\underline{d}$ = (1,2,2,1,4,3,3,3,4,1,1)
- $\sum d_i$ = 2 * edges

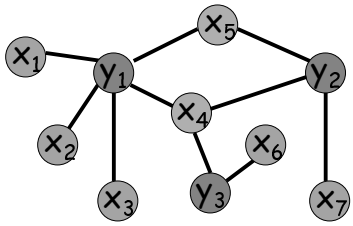
$$\Pi_{i=1}^{j} \Pi_{j=1}^{N} (1 + x_i x_j) = \sum n(\underline{d})\, x_1^{d_1} \ldots x_n^{dn}$$

- How to cope with the combinatorial explosion?
  E.g., for n = 10, the product has 2^{45} terms

Scatternet topology space



Modeling Bluetooth constraints: an example



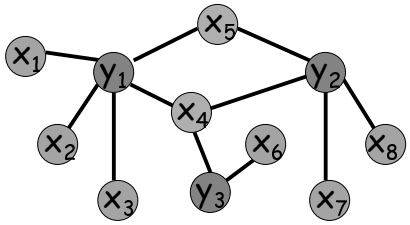
- 5 slaves (d = 1)
- 2 bridges (d = 2, 3)
- 3 masters

- slave = ($y_1 + y_2 + y_3$)
- bridge 1 = ($y_1y_2 + y_1y_3 + y_2y_3$)
- bridge 2 = ($y_1y_2y_3$)

$$P = (y_1 + y_2 + y_3)^5(y_1y_2 + y_1y_3 + y_2y_3)^1(y_1y_2y_3)^1$$

there are 56 possible choices of bridge nodes, so total number of ways = $56.3^5.3.1$

Modeling Bluetooth constraints



- In general
  - q1 slaves (d = 1)
  - q2 bridges (d = 2)
  - . . .
  - qk bridges (d = k)
- slave = ($y_1 + y_2 + y_3 . .$)
- bridge 1 = ($y_1y_2 + y_1y_3 + y_2y_3 . .$)
- bridge 2 = ($y_1y_2y_3 + y_1y_2y_3 . .$)
- . .
- bridge k = ($y_1y_2y_{3\ldots} + y_2y_3y_4 . .$)

$$P = \tau_1(y)^{q1}\,\tau_2(y)^{q2}\,\tau_3(y)^{q3} \ldots \tau_k(y)^{qk}$$

Managing combinatorial explosion

- Elementary symmetric functions can be expressed in terms of power sums,
  - e.g. $\tau_2(y) = y_1y_2 + y_1y_3 \ldots + y_{m-1}y_m$

    $= {}^1\!/_2((\sum y_i)^2 - (\sum y_i^2))$

$$P = \tau_1(y)^{q1}\,\tau_2(y)^{q2}\,\tau_3(y)^{q3} \ldots \tau_k(y)^{qk}$$

- Expand in terms of power sums
- compute modulo w.r.t. a high degree polynomial, e.g., y^7

Scatternet topology space

MASTERS	SLAVES	EDGES	SCATTERNETS
2	8	9	1024
2	8	11	1792
2	8	≤ 12	6848
3	7	9	45,927
3	7	11	76,545
3	7	≤ 12	244,944
4	6	9	276,480
4	6	11	186,624
4	6	≤ 12	820,800

N = 10 nodes

Pravin Bhagwat (AT&T Labs) 103

Open problems

- Estimation of the traffic carrying capacity of Scatternets
- Enumeration of large size ad hoc networks
- Decentralized algorithms for network construction
- Dynamics of information propagation in large size ad hoc networks
- A killer application

Pravin Bhagwat (AT&T Labs) 104

References

- Bluetooth—The universal radio interface for ad hoc, wireless connectivity, Jaap Haartsen. Ericsson review 03, 1998. (http://www.ericsson.com/review/issues.taf)
- Bluetooth version 1.0 specifications
  http://www.bluetooth.com/developer/specification/core.asp
  - Part A, Radio Specification
  - Part B, Baseband
  - Part C, Link Manager Protocol
  - Part D, Logical Link Control and Adaption Protocol Specification
  - Part E, Service Discovery Protocol (SDP)
- Bluetooth version 1.0 profiles
  http://www.bluetooth.com/developer/specification/profiles.asp
  - Part K:9, LAN access profile
- Future updates will be posted at:
  http://www.research.att.com/~pravinb/bluetooth/

Thank you