londonknowledgelab

Mobile and Ubiquitous Computing

Bluetooth Networking

George Roussos

g.roussos@dcs.bbk.ac.uk

Birkbeck

Bluetooth Overview

- A cable replacement technology
- Operates in the unlicensed ISM band at 2.4 GHz
- Frequency Hopping scheme (1600 hops/sec)
- Range 10+ or 100+ meters
- Single chip radio + baseband
- Design features:
  - robustness
  - low complexity
  - low power
  - low cost

Bluetooth Characteristics

- Bluetooth supports
  - Synchronous & asynchronous data channels.
    - Three simultaneous synchronous voice channels, or
    - One channel, with asynchronous data and synchronous voice
  - Data channel can support maximal 723.2 kb/s asymmetric (and still up to 57.6 kb/s in the return direction), or 433.9 kb/s symmetric.
- Bluetooth provides
  - point-to-point (only 2 nodes), or
  - point-to-multipoint connection.

Application Scenarios

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

Usage scenarios: Synchronization

User benefits

- **Proximity synchronization**
- **Easily maintained database**
- **Common**

Usage scenarios: Headset

User benefits

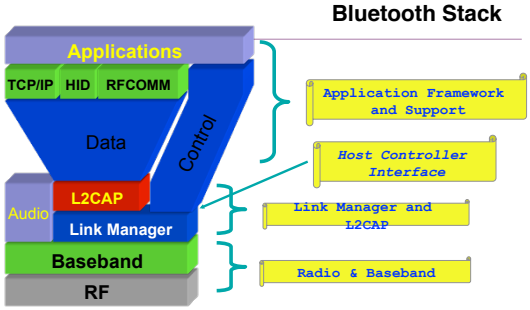
- **Multiple device access**
- **Cordless phone benefits**
- **Hand's free operation**

Usage scenarios: Data access points

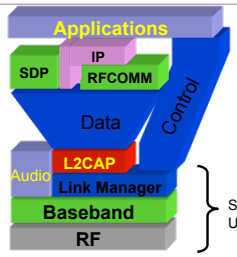
User benefits

- **No more connectors**
- **Easy internet access**
- **Common connection experience**

Bluetooth Stack



Bluetooth Stack



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

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

Power consciousness

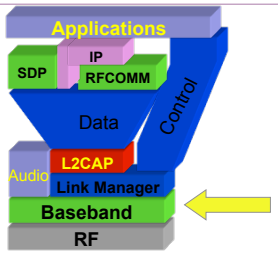
- Standby current < 0.3 mA
  - 3 months(*)
- Voice mode 8-30 mA
  - 75 hours
- Data mode average 5 mA
  (0.3-30mA, 20 kbps, 25%)
  - 120 hours
- Low-power architecture
  - Programmable data length (else radio sleeps)
  - Hold and Park modes: 60 μA
    - Devices connected but not participating
    - Hold retains AMA address, Park releases AMA, gets PMA address
    - Device can participate within 2 ms

(*)**Estimates calculated with 600 mAh battery and internal amplifier, power will vary with implementation**

Radio

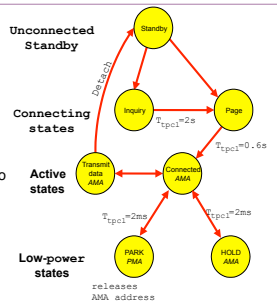
- Low Cost
  - Single chip radio (minimize external components)
  - Today's technology
  - Time division duplex
- Low Power
  - Standby modes
  - Sniff, Hold, Park
  - Low voltage RF
- Robust Operation
  - Fast frequency hopping 1600 hops/sec
  - Strong interference protection

Baseband



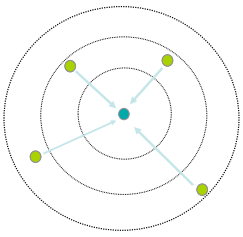
Baseband protocol

- Standby
  - Waiting to join a piconet
- Inquire
  - Ask about radios to connect to
- Page
  - Connect to a specific radio
- Connected
  - Actively on a piconet (master or slave)
- Park/Hold
  - Low-power connected states



Connection Setup

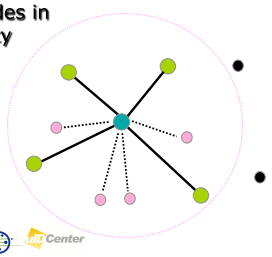
- Inquiry - scan protocol
  - to lean about the clock offset and device address of other nodes in proximity



Piconet formation

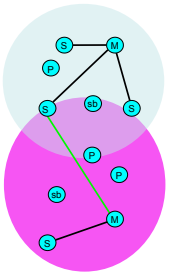
- Page - scan protocol
  - to establish links with nodes in proximity

Master
Active Slave
Parked Slave
Standby



The Bluetooth network topology

- Radio designation
  - Connected radios can be master or slave
  - Radios are symmetric (same radio can be master or slave)
- Piconet
  - Master can connect to 7 simultaneous or 200+ active slaves per piconet
  - Each piconet has maximum capacity (1 MSps)
  - Unique hopping pattern/ID
- Scatternet
  - High capacity system
  - Minimal impact with up to 10 piconets within range
  - Radios can share piconets!



Piconet

- One unit acts as the master of the Piconet, whereas the others acts as slaves.
- Up to seven slaves can be active.
- More slaves can be synchronized & locked to the master in parked state.
- The channel access for all the slaves in a piconet is controlled by the master.

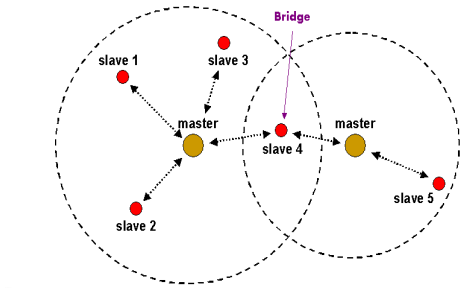
Piconet characteristics

- All devices in a piconet hop together
  - To form a piconet: master gives slaves its *clock* and *device ID*
    - Hopping pattern determined by *device ID* (48-bit)
    - Phase in hopping pattern determined by *Clock*
- Non-piconet devices are in standby
- Piconet Addressing
  - Active Member Address (AMA, 3-bits)
  - Parked Member Address (PMA, 8-bits)

Scatternet

- Scatternet is formed by multiple Piconets with overlapping coverage areas.
- Each Piconet can only have a single master
- Slaves can participate in different Piconets on a time-division multiplex basis.
- A master in one Piconet can be a slave in another Piconet.
- Each Piconet has its own hopping channel in a Scatternet.

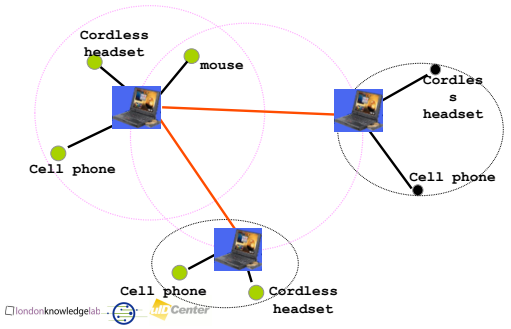
Scatternet



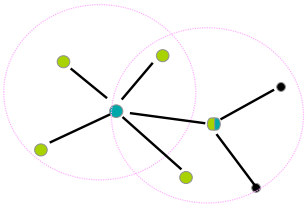
Addressing

- 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

Inter piconet communication



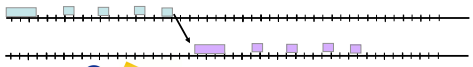
Scatternet, scenario



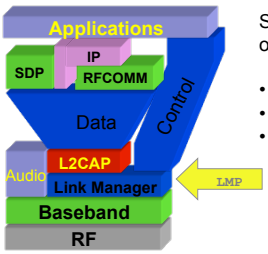
How to schedule presence in two piconets?

Forwarding delay ?

Missed traffic?



Link Manager Protocol



Setup and Management of Baseband connections

- Piconet Management
- Link Configuration
- Security

Link Manager Protocol

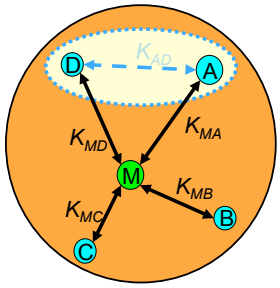
- Piconet Management
  - Attach and detach slaves
  - Master-slave switch
  - Establishing SCO and ACL links
  - Handling of low power modes (Sniff, Hold, Park)
- Link Configuration
  - packet type negotiation
  - power control
- Security functions
  - Authentication
  - Encryption

Bluetooth security features

- Fast frequency hopping (79 channels)
- Low transmit power (range <= 10m)
- Authentication of remote device
  - based on link key (128 Bit)
  - May be performed in both directions
- Encryption of payload data
  - Stream cipher algorithm (≤ 128 Bit)
  - Affects all traffic on a link
- Initialization
  - PIN entry by user

Link keys in a piconet

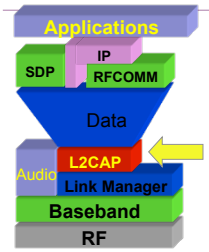
- Link keys are generated via a PIN entry
- A different link key for each pair of devices is allowed
- Authentication:
  - Challenge-Response Scheme
- Permanent storage of link keys



Application level security

- Builds on-top of link-level security
  - creates trusted device groups
- Security levels for services
  - authorization required
  - authentication required
  - encryption required
- Different or higher security requirements could be added:
  - Personal authentication
  - Higher security level
  - Public key

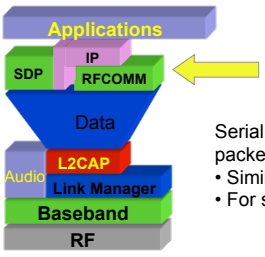
L2CAP



Logical Link Control and Adaptation Protocol

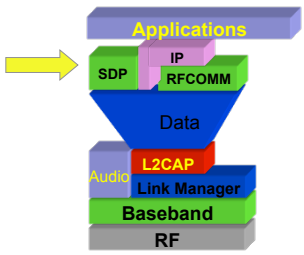
- L2CAP provides
  - Protocol multiplexing
  - Segmentation and Re-assembly
  - Quality of service negotiation
  - Group abstraction

Serial Port Emulation using RFCOMM



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

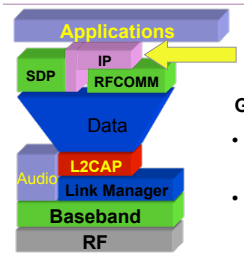
Bluetooth Service Discovery Protocol



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

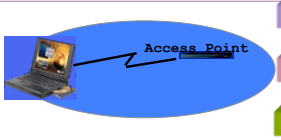
IP over Bluetooth V 1.0



GOALS

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

LAN access point profile



IP
PPP
RFCOMM
L2CAP
LMP
Baseband

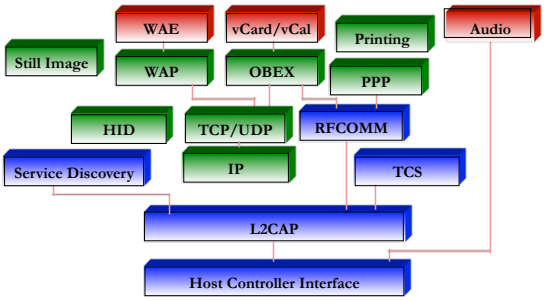
Security
- Authentication
- Access control

Efficiency
- header and data compression

Auto-configuration

Lower barrier for deployment

Protocol pathways



Bluetooth protocols

- Host Controller Interface (HCI)
  - provides a common interface between the Bluetooth host and a Bluetooth module
    - Interfaces in spec 1.0: USB; UART; RS-232
- Link Layer Control & Adaptation (L2CAP)
  - A simple data link protocol on top of the baseband
    - connection-oriented & connectionless
    - protocol multiplexing
    - segmentation & reassembly
    - QoS flow specification per connection (channel)
    - group abstraction

Bluetooth protocols

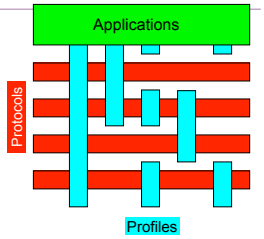
- Service Discovery Protocol (SDP)
  - Defines a service record format
    - Information about services provided by *attributes*
    - Attributes composed of an ID (name) and a value
    - IDs may be universally unique identifiers (UUIDs)
  - Defines an inquiry/response protocol for discovering services
    - Searching for and browsing services

Bluetooth protocols

- RFCOMM (based on GSM TS07.10)
  - emulates a serial-port to support a large base of legacy (serial-port-based) applications
  - allows multiple "ports" over a single physical channel between two devices
- Telephony Control Protocol Spec (TCS)
  - call control (setup & release)
  - group management for gateway serving multiple devices
- Legacy protocol reuse
  - resuse existing protocols, e.g., IrDA's OBEX, or WAP for interacting with applications on phones

Interoperability & Profiles

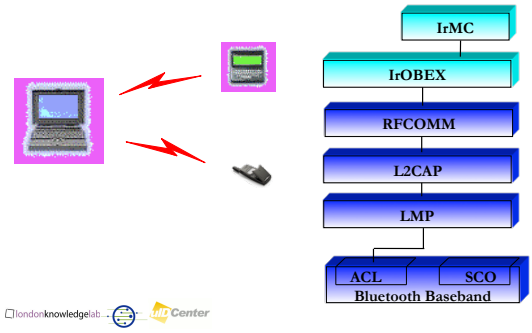
- Represents default solution for a usage model
- Vertical slice through the protocol stack
- Basis for interoperability and logo requirements
- Each Bluetooth device supports one or more profiles



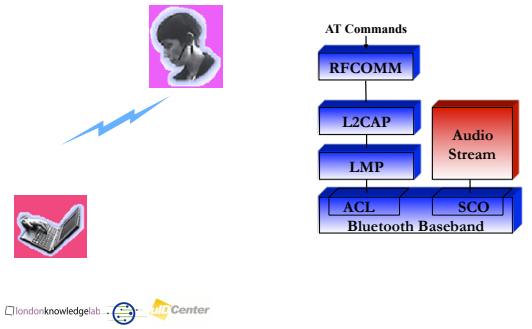
Profiles

- Generic Access Profile
  - Service Discovery Application Profile
  - Serial Port Profile
    - Dial-up Networking Profile
    - Fax Profile
    - Headset Profile
    - LAN Access Profile (using PPP)
    - Generic Object Exchange Profile
      - File Transfer Profile
      - Object Push Profile
      - Synchronization Profile
  - *TCS_BIN-based profiles*
    - Cordless Telephony Profile
    - Intercom Profile

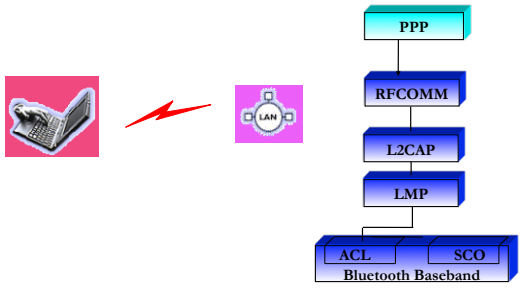
Synchronization profile



Headset profile

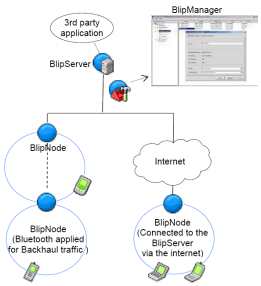


LAN access point profile



Trail Recording

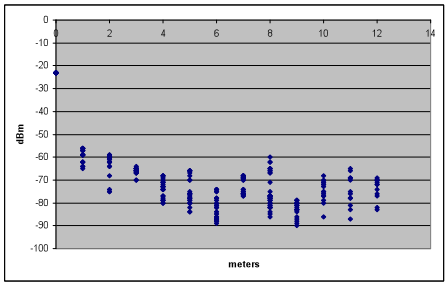
- BlipSystems
  - Platform for Bluetooth aware devices
  - Java API to write Bluetooth applications
  - Continues inquiry
- Identify location by closest blip node
  - Record discovered devices and signal strength in log files



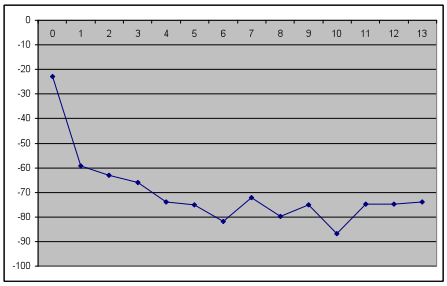
Sample Log Files

- Computer - Handheld PC/PDA (clam shell), 17/2/2005:3:31:13:453, 00:A0:96:09:1C:D0, 193.61.44.28, 00:02:C7:0D:97:8D, {-28 dBm}
- Imaging - Printer, 17/2/2005:3:31:21:556, 00:A0:96:09:1C:D0, 193.61.44.28, 00:30:6E:EA:29:2F, {-75 dBm}
- Imaging - Printer, 17/2/2005:3:31:22:8, 00:A0:96:09:1C:D0, 193.61.44.28, 00:30:6E:EA:29:2F, {-75 dBm}
- Computer - Handheld PC/PDA (clam shell), 17/2/2005:3:31:23:846, 00:A0:96:09:1C:D0, 193.61.44.28, 00:02:C7:0D:97:8D, {-28 dBm}
- Imaging - Printer, 17/2/2005:3:31:26:654, 00:A0:96:09:1C:D0, 193.61.44.28, 00:30:6E:EA:29:2F, {-73 dBm}
- Imaging - Printer, 17/2/2005:3:31:31:777, 00:A0:96:09:1C:D0, 193.61.44.28, 00:30:6E:EA:29:2F, {-85 dBm}
- Imaging - Printer, 17/2/2005:3:31:32:376, 00:A0:96:09:1C:D0, 193.61.44.28, 00:30:6E:EA:29:2F, {-79 dBm}

Distance Bluetooth signal strength - 1



Distance Bluetooth signal strength – 2



Summary

- Bluetooth is a global, RF-based (ISM band: 2.4GHz), short-range, connectivity technology & solution for portable, personal devices
  - it is not just a radio
  - create piconets on-the-fly (appr. 1Mbps)
    - piconets may overlap in time and space for high aggregate bandwidth
- The Bluetooth spec comprises
  - a HW & SW protocol specification
  - usage case scenario profiles and interoperability requirements
- 1999 Discover Magazine Awards finalist
- To learn more: *http://www.bluetooth.com*