Bluetooth Technology

Farinaz Edalat, Ganesh Gopal, Saswat Misra, Deepti Rao

April 26, 2001
Bluetooth

- A new global standard for data and voice
- Goodbye Cables!
Ultimate Headset
Automatic Synchronization

In the Office

At Home

Bluetooth
# Bluetooth Specifications

<table>
<thead>
<tr>
<th><strong>Connection Type</strong></th>
<th>Spread Spectrum (Frequency Hopping)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MAC Scheme</strong></td>
<td>FH-CDMA</td>
</tr>
<tr>
<td><strong>Spectrum</strong></td>
<td>2.4 GHz ISM</td>
</tr>
<tr>
<td><strong>Modulation</strong></td>
<td>Gaussian Frequency Shift Keying</td>
</tr>
<tr>
<td><strong>Transmission Power</strong></td>
<td>1 mw – 100 mw</td>
</tr>
<tr>
<td><strong>Aggregate Data Rate</strong></td>
<td>1 Mbps</td>
</tr>
<tr>
<td><strong>Range</strong></td>
<td>30 ft</td>
</tr>
<tr>
<td><strong>Supported Stations</strong></td>
<td>8 devices</td>
</tr>
<tr>
<td><strong>Voice Channels</strong></td>
<td>3</td>
</tr>
<tr>
<td><strong>Data Security- Authentication Key</strong></td>
<td>128 bit key</td>
</tr>
<tr>
<td><strong>Data Security-Encryption Key</strong></td>
<td>8-128 bits (configurable)</td>
</tr>
</tbody>
</table>
Bluetooth Protocol Stack

Composed of protocols to allow Bluetooth devices to locate each other and to create, configure and manage both physical and logical links that allow higher layer protocols and applications to pass data through these transport protocols.
Transport Protocol Group (contd.)

- **Radio Frequency (RF)**
  - Sending and receiving modulated bit streams

- **Baseband**
  - Defines the timing, framing
  - Flow control on the link.

- **Link Manager**
  - Managing the connection states.
  - Enforcing Fairness among slaves.
  - Power Management

- **Logical Link Control & Adaptation Protocol**
  - Handles multiplexing of higher level protocols
  - Segmentation & reassembly of large packets
  - Device discovery & QoS
Additional transport protocols to allow existing and new applications to operate over Bluetooth. Packet based telephony control signaling protocol also present. Also includes Service Discovery Protocol.
Middleware Protocol Group *(contd.)*

- **Service Discovery Protocol (SDP)**
  - Means for applications to discover device info, services and its characteristics.

- **TCP/IP**
  - Network Protocols for packet data communication, routing

- **RFCOMM**
  - Cable replacement protocol, emulation of serial ports over wireless network
Application Group

Consists of Bluetooth aware as well as un-aware applications.
**Master - Slave**

**Master**
- Device in Piconet whose clock and hopping sequence are used to synchronize all other devices (slaves) in the Piconet.
- It also carries out Paging procedure and also Connection Establishment.

**Slaves**
- Units within the piconet that are synchronized to the master via its clock and hopping sequence.
- After connection establishment, Slaves are assigned a temporary 3 bit member address to reduce the no. of addressing bits required.
**Piconets**

- **Point to Point Link**
  - Master - slave relationship
  - Bluetooth devices can function as masters or slaves

- **Piconet**
  - It is the network formed by a Master and one or more slaves (max 7).
  - Each piconet is defined by a different hopping channel to which users synchronize to.
  - Each piconet has max capacity (1 Mbps).
  - Hopping pattern is determined by the master.
Piconet Structure

- Master
- Active Slave
- Parked Slave
- Standby

Bluetooth 14
Physical Link Types

- **Synchronous Connection Oriented (SCO)**
  - Point to Point Full Duplex between Master & Slave
  - Established once by master & kept alive till released by Master
  - Typically used for Voice connection (to guarantee continuity)
  - Master reserves slots used for SCO link on the channel to preserve time sensitive information

- **Asynchronous Connection Link (ACL)**
  - It is a momentary link between master and slave.
  - No slots are reserved.
  - It is a Point to Multipoint connection.
  - Symmetric & Asymmetric links possible
Packet Types

Control packets
- ID*
- Null
- Poll
- FHS
- DM1

Data/voice packets
- Voice
  - HV1
  - HV2
  - HV3
  - DV
- data
  - DM1
  - DM3
  - DM5
- DH1
- DH3
- DH5

Access Code
- Header
- Payload

Bluetooth
Packet Structure

72 bits  |  54 bits  |  0 - 2744 bits

Access Code  |  Header  |  Payload

Voice

No CRC
No retries
FEC (optional)

ARQ
FEC (optional)

header  |  Data  |  CRC
Access Code

- **Purpose**
  - Synchronization
  - DC offset compensation
  - Identification
  - Signaling

- **Types**
  - *Channel Access Code (CAC)*
    - Identifies a piconet.
  - *Device Access Code (DAC)*
    - Used for signalling procedures like paging and response paging.
  - *Inquiry Access Code (IAC)*
    - General IAC is common to all devices, Dedicated IAC is for a dedicated group of Bluetooth devices that share a common characteristic.
Packet Header

- Addressing (3 bits)
- Packet type (4 bits)
- Flow Control (1 bit)
- 1-bit ARQ
- Sequencing (1 bit)  
  For filtering retransmitted packets
- HEC (8 bit)  
  Verify header integrity
Connection State Machine

- **Standby**
  - Inquiry
  - Transmit data
  - Connected
- **Connected**
  - Park
  - Hold
  - Sniff

Bluetooth 20
Connection State Machine (contd.)

- **Inquiry Scan**
  - A device that wants to be discovered will periodically enter this mode and listen for inquiry packets.

- **Inquiry**
  - Device sends an Inquiry packet addressed to GIAC or DIAC
  - Transmission is repeated on the inquiry hop sequence of frequencies.

- **Inquiry Response**
  - When an inquiry message is received in the inquiry scan state, a response packet (FHS) containing the responding device address must be sent after a random number of slots.
Inquiry Response
Connection State Machine (*contd.*).

- **Page**
  - The master uses the clock information, about the slave to be paged, to determine where in the hop sequence, the slave might be listening in the page scan mode.
  - The master sends a page message.

- **Page Scan**
  - The page scan substate can be entered by the slave from the standby state or the connection state. It listens to packets addressed to its DAC.

- **Page Response**
  - On receiving the page message, the slave enters the slave page response substate. It sends back a page response consisting of its ID packet which contains its DAC, at the frequency for the next slot from the one in which page message was received.
Power Control Modes

**Sniff Mode**

- This is a low power mode in which the listening activity of the slave is reduced.
- In the sniff mode, the slave listens for transmissions only at fixed intervals $T_{\text{sniff}}$, at the offset slot $D_{\text{sniff}}$ for $N_{\text{sniff}}$ times. These parameters are given by the LMP in the master when it issues the SNIFF command to the slave.

**Hold Mode**

- Slave temporarily (for $T_{\text{hold}}$ sec) does not support ACL packets on the channel (possible SCO links will still be supported).
- By this capacity can be made free to do other things like scanning, paging, inquiring, or attending another piconet.
- The slave unit keeps its active member address (AM_ADDR).
Power Control Modes (contd.)

- **Park Mode**
  - This is a very low power mode with very little activity.
  - The slave however, stays synchronized to the channel.
  - The parked slaves regularly listen for beacon signals at intervals decided by the beacon structure communicated to the slave during the start of parking.
  - The parked slave has to be informed about a transmission in a beacon channel which is supported by the master to keep parked slaves in synchronization and send them any other information.
  - Any message to be sent to a parked member are sent over the broadcast channel.
  - It also helps the master to have more than seven slaves.
Security

Security Measures
- Limited/Restricted Access to authorized users.
- Both Link Level Encryption & Authentication.
- Personal Identification Numbers (PIN) for device access.
- Long encryption keys are used (128 bit keys).
- These keys are not transmitted over wireless. Other parameters are transmitted over wireless which in combination with certain information known to the device, can generate the keys.
- Further encryption can be done at the application layer.

Security values
- Device Address-Public
- Authentication Key(128 bits)-Private
- Encryption Key(8-128 bits)-Private
- Random Number
Frequency Hop Spread-Spectrum

- Bluetooth channel is represented by a pseudo random hopping sequence through the entire 79 RF frequencies
- Nominal hop rate of 1600 hops per second
- Channel Spacing is 1 MHz
Bluetooth devices use a Time-Division Duplex (TDD) scheme.
Channel is divided into consecutive slots (each 625 μs).
One packet can be transmitted per slot.
Subsequent slots are alternatively used for transmitting and receiving:
  - Strict alternation of slots between the master and the slaves.
  - Master can send packets to a slave only in EVEN slots.
  - Slave can send packets to the master only in the ODD slots.

![Diagram of Time-Division Duplex Scheme]

The diagram illustrates the allocation of slots for transmission and reception in Bluetooth.
Performance Analysis of Link
(Reference: Pedersen and Eggers, VTC 2000)

• Results collected from “real” Bluetooth link

• two notebook PC’s
  • PC cards from Digianswer
    - full power devices $P_t = 20$ dBm
  • Indoor Measurements
    - stationary master and slave
  • Outdoor Measurements
    - slave moves in circle $R = 3\, \mu$ at 1.5 RPM
Test Parameters

- Testing done from a master to a single slave
  - No major sources of interference

- Tests used DH5 packet only

![Diagram of Bluetooth packet structure]

- 72 bits Access Code
- 54 bits Header
- 0 - 2744 bits Payload
  - 8-bit HEC
  - 16-bit payload CRC
Results: Indoor
Results: Outdoor
How reliable are Bluetooth Devices?

• Indoor:
  - Within 10 meters
  - Within 25 meters, with LOS
  - Further…?
  - Concrete, Glass….?

• Outdoor:
  - Within 150-220 meters with LOS
  - More than 220 meters
• Goal: Find a bound on the BER as a function of network size
The Problem

- Occasionally, two piconets will use overlapping frequencies
Assumptions and Parameters

• “Open” (LOS) indoor room; circular with radius R

• Received power is a random variable
  - mean received power falls off as $d^2$
  - for fixed $d$, signal fading is Rician with $K = 6$dB

• Interference from other Bluetooth devices only
  - ignore 802.11, microwaves

• Time offset of each Piconet is uniform $[0,T]$
SIR calculation

- For a reference piconet

\[
\Gamma(t) = \frac{P_s(t)}{N(t) \sum_{j=1}^{N_o} P^j_I(t) + N_o W/2}
\]

\(f(t)\) because the interfering and receiving devices within a piconet change with time

- Ignore noise power

- 2.5 nW for device within Bluetooth specs operating at 1Mbps with BER < .001
SIR Calculation (cont.)

\[ \Gamma = \frac{P_s}{\sum_{j=1}^{N} P_i^j} \]

Probability of Outage:

\[ P_{out} = P[P_s < v \sum_{j=1}^{N_b} P_i^j] \]

\[ P_{out} = \sum_{n=0}^{M-1} P[P_s < vP_{I,n} \mid N_b = n] P[N_b = n] \]

- Total interference power from n interfering piconets
- Prob. that exactly n piconets are interfering
SIR Calculation (cont.)

- Evaluation of $P_{out}$ is complicated and requires numerical techniques (see reference).
- Some results (for $R = 5m$; uniform distribution):
  
<table>
<thead>
<tr>
<th>Interferers</th>
<th>Lower Bound on $P_{out}$</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$V = 14dB$</td>
<td>$V = 11dB$</td>
</tr>
<tr>
<td>1</td>
<td>1.14 %</td>
<td>1.03 %</td>
</tr>
<tr>
<td>2</td>
<td>2.27 %</td>
<td>2.04%</td>
</tr>
</tbody>
</table>

- In general $P_{out}$ increases linearly with $M$:
  
  $$P_{out} \sim \frac{(M-1)}{N_f}$$
Other Technologies

- **IrDA**
  - Infrared, LOS, serial data comm.
  - Point to point
  - Intended for Data Communication
  - Simple to configure and use
  - Both devices must be stationary, for synchronization
  - Can not penetrate solid objects
IrDA vs Bluetooth

- **Bluetooth Advantages**
  - Point to Multipoint
  - Data & Voice
  - Broadcast
  - Easier Synchronization due to omnidirectional and no LOS requirement
  - Devices can be mobile
  - Range 10 m

- **IrDA**
  - Currently 16 Mbps
  - Ample security and very less interference
  - Already ubiquitous & Low cost
Bluetooth: Today and Tomorrow...

- First market-ready product shipped November 2000
  - Digital headset produced by GN Netcom $300

**Bluetooth-Enabled Equipment**

- 2005: About 1.4 Billion Bluetooth-enabled products
  - Largest market: digital mobile phones
  - 2nd largest: computing & peripherals
  - 3rd largest: PC Cards, adapters, headsets

- 2001: Top 2 markets – mobile phones and PC Cards & adapters

![Bluetooth-Enabled Equipment Chart]

Dig. Mobile Phones 74%
Computing & Peripherals 14%
Accessories/Cards/Adapters 8%
Other 4%

Bluetooth 43
Bluetooth: Today and Tomorrow.. (cont.)

• Will Bluetooth become a household name?
Conclusions

- A new global standard for data and voice
- Eliminate Cables
- Low Power, Low range, Low Cost network devices
- Delivers Automatic synchronicity between devices
- Future Improvements
  - Master-Slave relationship can be adjusted dynamically for optimal resource allocation and utilization
  - Adaptive, closed loop transmit power control can be implemented to further reduce unnecessary power usage
References

[1] **Bluetooth Consortium**:  
- http://www.bluetooth.com  
- http://www.ericsson.com/bluetooth/

[2] **Bluetooth Tutorial**:  
- http://www.ee.iitb.ernet.in/uma/~aman/bluetooth  
- http://www.palowireless.com

