Bluetooth Architecture
Overview

James Kardach
Principal Engineer
Bluetooth SIG Program Manager
Intel Corporation

Copyright © 1998 Intel Corporation

"The Bluetooth Specification is still preliminary. All information regarding Bluetooth is subject to change without notice."

* Third party marks and brands are the property of their respective owners.
Agenda

- What does Bluetooth do for you?
  - Usage model
- What is Bluetooth?
  - Compliance, compatibility
- What does Bluetooth do?
  - Technical points
- Who is Bluetooth?
  - History
- Architectural Overview of Bluetooth
What does Bluetooth do for you?

- Data/Voice Access Points
- Cable Replacement
- Personal Ad-hoc Networks

Bluetooth
What is Bluetooth?

- A hardware description
- An application framework

Latest Version on Bluetooth Website: www.Bluetooth.com
What is Bluetooth?

- A hardware description
- An application framework
Bluetooth devices will be tested against the specification.
# What does Bluetooth Do?

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Topology</strong></td>
<td>Supports up to 7 simultaneous links</td>
</tr>
<tr>
<td></td>
<td>Each link requires another cable</td>
</tr>
<tr>
<td><strong>Flexibility</strong></td>
<td>Goes through walls, bodies, cloths...</td>
</tr>
<tr>
<td></td>
<td>Line of sight or modified environment</td>
</tr>
<tr>
<td><strong>Data rate</strong></td>
<td>1 MSPS, 720 Kbps</td>
</tr>
<tr>
<td></td>
<td>Varies with use and cost</td>
</tr>
<tr>
<td><strong>Power</strong></td>
<td>0.1 watts active power</td>
</tr>
<tr>
<td></td>
<td>0.05 watts active power or higher</td>
</tr>
<tr>
<td><strong>Size/Weight</strong></td>
<td>25 mm x 13 mm x 2 mm, several grams</td>
</tr>
<tr>
<td></td>
<td>Size is equal to range. Typically 1-2 meters. Weight varies with length (ounces to pounds)</td>
</tr>
<tr>
<td><strong>Cost</strong></td>
<td>Long-term $5 per endpoint</td>
</tr>
<tr>
<td></td>
<td>~ $3-$100/meter (end user cost)</td>
</tr>
<tr>
<td><strong>Range</strong></td>
<td>10 meters or less</td>
</tr>
<tr>
<td></td>
<td>Up to 100 meters with PA</td>
</tr>
<tr>
<td></td>
<td>Range equal to size. Typically 1-2 meters</td>
</tr>
<tr>
<td><strong>Universal</strong></td>
<td>Intended to work anywhere in the world</td>
</tr>
<tr>
<td></td>
<td>Cables vary with local customs</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td>Very, link layer security, SS radio</td>
</tr>
<tr>
<td></td>
<td>Secure (its a cable)</td>
</tr>
</tbody>
</table>

- **Cable Replacement**

**Bluetooth**
Who is Bluetooth?

- Harald Blaatand “Bluetooth” II
  - King of Denmark 940-981
    - Son of Gorm the Old (King of Denmark) and Thyra Danebod (daughter of King Ethelred of England)

- This is one of two Runic stones erected in his capitol city of Jelling (central Jutland)
  - This is the front of the stone depicting the chivalry of Harald.
  - The stone’s inscription (“runes”) say:
    - Harald christianized the Danes
    - Harald controlled Denmark and Norway
    - Harald thinks notebooks and cellular phones should seamlessly communicate
Bluetooth RF Specifications

Specified for low cost, single chip implementation

- Noise floor margin for substrate noise and low current LNA
- Linearity set by near-far problem
- In-band image allows low-cost low IF
- VCO phase noise enables integrated VCO
- TX-RX turn around time enables single synthesizer
- 2.4 ISM band chosen for global use and process capabilities
Basic Baseband Protocol

- Spread spectrum frequency hopping radio
  - 79/23 one MHz channels
  - Hops every packet
    - Packets are 1, 3 or 5 slots long
  - Frame consists of two packets
    - Transmit followed by receive
  - Nominally hops at 1600 times a second (1 slot packets)
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!
The Piconet

- All devices in a piconet hop together
  - In forming 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)
Functional Overview

- **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
A radio must be enabled to accept pages or inquires

- Consumes 18 slots every 1.25 s (or so) for each scan
- slot is 0.625 ms
Inquiring for Radios

- Radio Wants to find other radios in the area
Inquiring for Radios

- Radio Wants to find other radios in the area
  - Radio A issues an Inquire (pages with the Inquire ID)
    - Radios B, C and D are doing an Inquire Scan
Radio Wants to find other radios in the area

- Radio A issues an Inquire (pages with the Inquire ID)
  - Radios B, C and D are doing a Inquire Scan
- Radio B recognizes Inquire and responds with an FHS packet
  - Has slave’s *Device ID* and *Clock*
Radio Wants to find other radios in the area

- Radio A issues an Inquire (pages with the Inquire ID)
  - Radios B, C and D are doing a Inquire Scan
- Radio B recognizes Inquire and responds with an FHS packet
  - Has slave’s Device ID and Clock
Inquiring for Radios

- **Radio Wants to find other radios in the area**
  - Radio A Issues an Inquire (again)
  - Radios C and D respond with FHS packets
    - As radios C & D respond simultaneously packets are corrupted and Radio A won’t respond
    - Each radio waits a random number of slots and listens
Inquiring for Radios

- Radio Wants to find other radios in the area
  - Radio A Issues an Inquire (again)
Inquiring for Radios

- Radio Wants to find other radios in the area
  - Radio A Issues an Inquire (again)
  - Radios C respond with FHS packets
Radio Wants to find other radios in the area

- Radio A Issues an Inquire (again)
Radio Wants to find other radios in the area

- Radio A Issues an Inquire (again)
- Radios D respond with FHS packets
Inquiring for Radios

- **Radio Wants to find other radios in the area**
  - Radio A Issues an Inquire (again)
  - Radios D respond with FHS packets
  - Radio A now has information of all radios within range
Inquiry Procedure

- Inquiry has unique device address (all BT radio use)
  - Unique set of “Inquiry” hop frequencies
- Any device can inquire by paging the Inquiry address
- Correlater hit causes slave to respond with FHS packet
  - Device ID
  - Clock
Multiple slaves are expected to respond

- Correlater hit causes slave to
  - respond with FHS packet
  - Wait a random number of slots
  - Wait for another Inquiry page and repeat

- Master should end up with a list of slave FHS packets in area
Inquire Summary

- Paging radio Issues page packet with Inquire ID
- Any radio doing an Inquire scan will respond with an FHS packet
  - FHS packet gives Inquiring radio information to page
    - Device ID
    - Clock
  - If there is a collision then radios wait a random number of slots before responding to the page inquire
- After process is done, Inquiring radio has Device IDs and Clocks of all radios in range
Master Paging a Slave

- Paging assumes master has slaves *Device ID* and an idea of its *Clock*
Paging assumes master has slaves *Device ID* and an idea of its *Clock*

- A pages C with C’s *Device ID*
Master Paging a Slave

- Paging assumes master has slaves *Device ID* and an idea of its *Clock*
  - A pages C with C’s *Device ID*
  - C Replies to A with C’s *Device ID*
Master Paging a Slave

- Paging assumes master has slaves *Device ID* and an idea of its *Clock*
  - A pages C with C’s *Device ID*
  - C Replies to A with C’s *Device ID*
  - A sends C its *Device ID* and *Clock* (FHS packet)
Paging assumes master has slaves *Device ID* and an idea of its *Clock*

- A pages C with C’s *Device ID*
- C Replies to A with C’s *Device ID*
- A sends C its *Device ID* and *Clock* (FHS packet)
- A connects as a master to C
Master Paging a slave

- **Master pages slave (packet has slave ID) at slave page frequency (1 of 32)**
  - Master sends page train of 16 most likely frequencies in slave hop set
  - Slave ID sent twice a transmit slot on slave page frequency
  - Master listens twice at receive slot for a response
  - If misses, master sends second train on remaining 16 frequencies

- **Slave listens for 11 ms (page scan)**
  - If correlater triggers, slave wakes-up and relays packet at response frequency
  - Master responds with FHS packet (provides master’s *Device ID* and *Clock*)
  - Slave joins piconet

---

**Diagram Description**

- **Master**:
  - IDa
  - Sends page train
  - Listens for response

- **Slave**:
  - IDc
  - Listens for page train
  - Relays packet at response frequency

**Time**:

- 625 μs
Each slave page scans on unique sequence of 32 channels $f_k$

- Master pages 16 most likely channels for entire sleep period (nominally 1.25 seconds)

- If clocks are off, then second train sent on last 16 frequencies for entire sleep period
SYNCHRONOUS CONNECTION-ORIENTED (SCO) LINK

- circuit switching
- symmetric, synchronous services
- slot reservation at fixed intervals

ASYNCHRONOUS CONNECTION-LESS (ACL) LINK

- packet switching
- (a)symmetric, asynchronous services
- polling access scheme
## Packet Types/Data Rates

<table>
<thead>
<tr>
<th>SEGMENT</th>
<th>TYPE</th>
<th>SCO link</th>
<th>ACL link</th>
<th>Data Rates (Kbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>0000</td>
<td>0000</td>
<td></td>
</tr>
<tr>
<td>0000</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td></td>
</tr>
<tr>
<td>0001</td>
<td>POLL</td>
<td>POLL</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0010</td>
<td>FHS</td>
<td>FHS</td>
<td></td>
</tr>
<tr>
<td>0011</td>
<td>DM1</td>
<td>DM1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0100</td>
<td>NULL</td>
<td>NULL</td>
<td></td>
</tr>
<tr>
<td>0101</td>
<td>HV1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0110</td>
<td>HV2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0111</td>
<td>HV3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1000</td>
<td>DV</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1001</td>
<td>AUX1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1010</td>
<td>NULL</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1011</td>
<td>NULL</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1100</td>
<td>NULL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1101</td>
<td>NULL</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1110</td>
<td>NULL</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1111</td>
<td>NULL</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **TYPE:** DM1, DH1, DM3, DH3, DM5, DH5
- **SCo link:** NULL, POLL, FHS, DM1
- **ACL link:** NULL, POLL, FHS, DM1
- **Data Rates (Kbps):** symmetric (108.8, 172.8, 256.0, 384.0, 576.0, 721.0), asymmetric (108.8, 172.8, 384.0, 576.0, 721.0)
Mobile = Battery life

- Low power consumption*
  - Standby current < 0.3 mA
    ⇒ 3 months
  - Voice mode 8-30 mA
    ⇒ 75 hours
  - Data mode average 5 mA
    (0.3-30mA, 20 kbit/s, 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
Bluetooth Security

- Provides link layer security between any two Bluetooth radios
  - Authentication (E1 algorithm)
    - Challenge/Response system
  - Encryption (privacy)
    - Encrypts data between two devices
    - Stream cipher with E0 algorithm
  - Key management and usage
    - Configurable Encryption key length (0-16 bytes)
      - Government export regulations
      - Radio negotiate key size
    - Key generation with E2-E3 algorithms
      - Authentication and Encryption keys
Bluetooth Radio Modules

• Complete radio on a module
  ♦ Designed to meet “Limited Module Compliance” requirements
    • Pre-certified to meet global regulatory requirements
    • Allows devices assembled with modules to be “self-certified”
  ♦ USB or Serial Interface
  ♦ Solder-ball connections
  ♦ External Antennae

Production Module

- 25 mm dia
- 17x33mm
- 19x35mm
- 25x25mm
- 36x43mm

Compact FLASH Card
The international 2.4 GHz ISM band

- **Requirements**
  - Channel bandwidth limited to 1 MHz
  - Spectrum spreading must be employed
  - Multiple uncoordinated networks may exist and cause interference
  - Microwave ovens also use this band
  - 2.4 GHz IC electronics must run at high current levels

- **Bluetooth solution**
  - 1 Mb/s symbol rate exploits maximum channel bandwidth
  - Fast frequency hopping and short data packets avoids interference
  - CVSD voice coding enables operation at high bit error rates
  - Air interface tailored to minimize current consumption
  - Relaxed link budget supports low cost single chip integration
Bluetooth is global

- One version for the world
  - Architecture compliant with global emission rules (2.4 GHz ISM band)
    - Working through FCC, EC, MPT for spectrum and power harmonization
  - Architecture compliant and safe for use on airlines
    - Working with FAA, JAA, FCC, airplane manufacturers and airlines
  - Reviewing security architecture with affected countries
Software Goals

♦ Good out of box experience
  ♦ Should provide value with existing applications
    ♦ Utilize existing APIs and protocols where possible
  ♦ Should be introduced with hardware that provides value
    ♦ Notebooks
    ♦ Cellphones
    ♦ Handhelds
  ♦ Should support the usage model
    ♦ Data access points (POTs Modem, cellphone, …)
    ♦ Cable replacement (Speaking laptop, instant postcard, …)
    ♦ Ad-hoc networking (File exchange, …)
- **PC Windows* example supporting the Bluetooth usage model**
  - WDM Driver
    - Windows* 2000
    - Windows 98*
Summary

- **Bluetooth is a radio system (not a radio)**
  - Hardware
  - Software framework
  - Interoperability requirements
- **Bluetooth Radio System is optimized for mobility**
  - Primarily cable replacement
    - NOT a WLAN technology
  - Targeted for Global use by mobile users