Lecture: WPANs, Bluetooth

Instructor: Dr. Shantanu Kangude
skangude@lyle.smu.edu
Agenda

• WPANs – what and why
• Comparison to WLANs
• WPAN technologies
• Bluetooth – introduction
• Bluetooth Protocol Stack
• Summary
What are WPANs?

Wireless Personal Area Networks (WPANs)

- Short-range
- Low Power
- Low Cost
- Small networks
- Communication of devices within a Personal Operating Space

WPANs address wireless networking of portable and mobile computing devices such as PCs, PDAs, peripherals, cell phones and consumer electronics.
Data Rate vs Range

Wide range of data rates and applications
WPANs vs WLANs

• WPANs are not ‘small WLANs’
• Typical use scenarios are very different
  – Ethernet replacement vs peripheral cable replacement
• Network clients are more power sensitive
  – e.g. Laptops vs headsets
• WPANs need new protocols to meet application, user, power requirements
• Several WPAN standards and technologies
  – mostly differentiated by application
Bluetooth

• Bluetooth is an industry specification for short-range RF-based connectivity for portable personal devices

• Bluetooth is a global, RF-based (ISM band: 2.4GHz), short-range, connectivity solution for portable, personal devices
  – it is not just a radio, it is an end-to-end solution

• The Bluetooth spec comprises
  – a HW & SW protocol specification
  – usage case scenario profiles and interoperability requirements

• Standardized as IEEE 802.15.1
IEEE 802.15.3 – High Rate WPANs

• High-rate (20Mbit/s or greater) WPANs.
  – low power, low cost solutions addressing the needs of portable consumer digital imaging and multimedia applications

• MAC & PHY Features
  – Data Rates: 11, 22, 33, 44, & 55 Mbps.
  – Quality of Service isochronous protocol
  – Ad hoc peer-to-peer networking
  – Security
  – Low power consumption
  – Low cost
  – Designed to meet the demanding requirements of portable consumer imaging and multimedia applications
IEEE 802.15.4 – Low Rate WPANs

- A low data rate solution with multi-month to multi-year battery life and very low complexity
  - Unlicensed, international frequency band
- Potential applications are sensors, interactive toys, smart badges, remote controls, and home automation
- IEEE 802.15.4 features:
  - Data rates of 250 kbps, 40 kbps, and 20 kbps
  - Support for critical latency devices, such as joysticks
  - Automatic network establishment by the coordinator
  - Fully handshaked protocol for transfer reliability
  - Power management to ensure low power consumption
- 802.15.4a – New PHY with high precision ranging / location capability (1 meter accuracy and better)
- 802.15.4b – enhancements and clarifications to the IEEE 802.15.4-2003 standard
- 802.15.4c – 779-787 MHz band for the Chinese WPAN standard
- 802.15.4d – to support a new frequency allocation (950MHz -956MHz) in Japan
- 802.15.4e – a) better support the industrial markets and b) permit compatibility with modifications being proposed within the Chinese WPAN

- Zigbee is an industry group defining interoperability requirements
IEEE 802.15.5 – Mesh WPANs

• PHY and MAC mechanisms to enable mesh networking

• One of two connection arrangements
  – full mesh topology - each node is connected directly to each of the others
  – partial mesh topology - some nodes are connected to all the others, but some of the nodes are connected only to those other nodes with which they exchange the most data

• Mesh networks have the capability to provide:
  – Extension of network coverage without increasing transmit power or receive sensitivity
  – Enhanced reliability via route redundancy
  – Easier network configuration
  – Better device battery life due to fewer retransmissions
IEEE 802.15.6 – Body Area Networks (BANs)

• A communication standard optimized for low power devices and operation on, in or around the human body (but not limited to humans) to serve a variety of applications including medical, consumer electronics / personal entertainment and other
  – Range of 1-3 m
  – Extremely low power operation
Wireless USB

- Connection model is replacing USB wire
  - WUSB Host with up to 127 clients
- High speed at short range
  - 480 Mb/s at ~3 m
- Uses Ultra-Wideband (UWB) technology for PHY layer
- Being developed by USB Implementers Forum - a non-profit corporation founded by the group of companies that developed the Universal Serial Bus specification
Other WPAN Technologies

- RFID – ultra-low power WPANs with RFID technology
- Visible Light Communication – WPANs using visible light
- Ozmo Devices – Proprietary technology using WLAN hardware for WPAN
What does Bluetooth do for you?

Source: Bluetooth Architecture Overview
Dr. Chatschik Bisdikian, IBM Research
IEEE 802.15 document #99069r1
Bluetooth History

• The Bluetooth SIG (Special Interest Group) was formed in February 1998
  – Ericsson, IBM, Intel, Nokia, Toshiba
• There are 1100+ adopter companies
• The Bluetooth SIG went “public” in May 1998
• The Bluetooth SIG work (the spec: >1,500 pages) became public on July 26, 1999
What is Bluetooth?

- A hardware description
- An application framework

Source: Bluetooth Architecture Overview
Dr. Chatschik Bisdikian, IBM Research
IEEE 802.15 document #99069r1

Bluetooth Website: www.Bluetooth.com
IEEE 802 to Bluetooth Correspondence

Source: Mapping the Bluetooth Specification to IEEE P802
Tom Siep, Texas Instruments
IEEE 802.15 document #99071r3
What is Bluetooth?

- A hardware description
- An application framework

Source: Bluetooth Architecture Overview
James Kardach, Intel
IEEE 802.15 document #99053
## What does Bluetooth Do?

<table>
<thead>
<tr>
<th><strong>Topology</strong></th>
<th>Supports up to 7 simultaneous links</th>
<th>Each link requires another cable</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Flexibility</strong></td>
<td>Goes through walls, bodies, cloths...</td>
<td>Line of sight or modified environment</td>
</tr>
<tr>
<td><strong>Data rate</strong></td>
<td>1 MSPS, 720 Kbps</td>
<td>Varies with use and cost</td>
</tr>
<tr>
<td><strong>Power</strong></td>
<td>0.1 watts active power</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>
<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>
<td>~ $3-$100/meter (end user cost)</td>
</tr>
<tr>
<td><strong>Range</strong></td>
<td>10 meters or less</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>
<td>Cables vary with local customs</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td>Very, link layer security, SS radio</td>
<td>Secure (it's a cable)</td>
</tr>
</tbody>
</table>

### Cable Replacement

Source: Bluetooth Architecture Overview
James Kardach, Intel
IEEE 802.15 document #99053

---

*SMU ENGINEERING*
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

Source: Bluetooth Architecture Overview
Dr. Chatschik Bisdikian, IBM Research
IEEE 802.15 document #99069r1
Usage scenarios: Synchronization

User benefits

• Proximity synchronization
• Easily maintained database
• Common information database

Source: Bluetooth Architecture Overview
Dr. Chatschik Bisdikian, IBM Research
IEEE 802.15 document #99069r1
Usage scenarios: Headset

User benefits

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

Source: Bluetooth Architecture Overview
Dr. Chatschik Bisdikian, IBM Research
IEEE 802.15 document #99069r1
Usage scenarios: Data access points

User benefits

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

Source: Bluetooth Architecture Overview
Dr. Chatschik Bislikian, IBM Research
IEEE 802.15 document #99069r1

Remote Connections...
Characteristics

- Operates in the **2.4 GHz** band
  - Supports data rates up to 3 Mbps (enhanced) nominal
  - Original supports up to 1 Mbps nominal

- Uses **Frequency Hopping (FH) spread spectrum**, which divides the frequency band into a number of channels (2.402 - 2.480 GHz yielding 79 channels)

- Radio transceivers **hop** from one channel to another in a **pseudo-random fashion**, determined by the master

- Supports up to **8 devices in a piconet** (1 master and 7 slaves).

- **Piconets** can combine to form **scatternets**
Architectural Overview

Applications

TCP/IP  HID  RFCOMM

Data

L2CAP

Control

Link Manager

Baseband

RF

Audio

And a little bit of this

Cover this

Cover this
What is a Piconet?

A collection of devices that share a channel

One unit will act as a **master** and the others as **slaves** for the duration of the piconet connection.

**Master** sets the **clock** and **hopping** pattern.

Each piconet has a **unique hopping pattern/ID**

Each **master** can connect to **7 simultaneous** or **200+ inactive (parked) slaves** per piconet

Source: Bluetooth Architecture Overview
Dr. Chatschik Bisdikian, IBM Research
IEEE 802.15 document #99069r1
A Scatternet is the linking of multiple co-located piconets through the sharing of common master or slave devices.

A device can be both a master and a slave.

Radios are symmetric (same radio can be master or slave)

High capacity system, each piconet has maximum capacity (720 Kbps)

Radios can share piconets!

Source: Bluetooth Architecture Overview
Dr. Chatschik Bisdikian, IBM Research
IEEE 802.15 document #99069r1
The Bluetooth “lower” layers

- Radio (RF)
  - The Bluetooth radio front-end
    - 2.4GHz ISM band; 1Mbps
    - 1,600 hops/sec; 0dBm (1mW) radio (up to 20dBm)
- Baseband (BB)
  - Piconet/Channel definition
  - “Low-level” packet definition
  - Channel sharing
- Link Management (LM)
  - Definition of link properties
    - encryption/authentication
    - polling intervals set-up
    - SCO link set-up
    - low power mode set-up
Transmitter Output Powers

• Class 1: greatest distance (100m)
  – 1 mW (0dBm) to 100mW (+20dBm)
  – power control mandatory

• Class 2: (10m)
  – 0.25 (-6dBm) ~ 2.4mW (+4dBm)
  – power control optional

• Class 3: (1m)
  – lowest power, 1mW
Basic Baseband Protocol

- Spread spectrum frequency hopping radio
- 79/23 one MHz channels
- Hops every packet
  - Packets are 1, 3 or 5 slots long – no hopping during multi-slot packets
- Frame consists of two packets
  - Transmit followed by receive
  - Nominally hops at 1600 times a second

Source: Bluetooth Architecture Overview
James Kardach, Intel
IEEE 802.15 document #99053
Physical Layer

• Synchronous Connection-Oriented (SCO) link
  – circuit switching
  – symmetric, synchronous services
  – slot reservation at fixed intervals
  – Usually used for voice

• Asynchronous Connection-less (ACL) link
  – packet switching
  – (a)symmetric, asynchronous services
  – polling access scheme
Baseband link types

- **Polling-based (TDD) packet transmissions**
  - 1 slot: 0.625msec (max 1600 slots/sec)
  - master/slave slots (even-/odd-numbered slots)

- **Synchronous connection-oriented (SCO) link**
  - “circuit-switched”, periodic single-slot packet assignment
  - symmetric 64Kbps full-duplex

- **Asynchronous connection-less (ACL) link**
  - packet switching
  - asymmetric bandwidth, variable packet size (1, 3, or 5 slots)
    - max. 721 kbps (57.6 kbps return channel)
    - 108.8 - 432.6 kbps (symmetric)

Source: IEEE 802.15.1 Tutorial
Tom Siep, Texas Instruments
IEEE 802.15 document #01046r1
Link Access

- A TDD scheme is used where master and slave alternatively transmit
- The packet aligned with the slot start
  - Packets may extend over up to five time slots.

Source: IEEE 802.15.1 Standard
Bluetooth Packet Format

- Access Code used for synchronization, dc offset compensation, and identification.
  - identifies all packets exchanged on a physical channel
  - helps differentiate co-located Bluetooth networks

<table>
<thead>
<tr>
<th>Access Code</th>
<th>Hdr</th>
<th>Payload</th>
</tr>
</thead>
<tbody>
<tr>
<td>68/72</td>
<td>54</td>
<td>0 – 2745 bits</td>
</tr>
<tr>
<td>bits</td>
<td>bits</td>
<td></td>
</tr>
</tbody>
</table>

SMU ENGINEERING
Types of Access Codes

- Channel access code (CAC) – identifies a piconet
- Device access code (DAC) – used for paging and subsequent responses
- Inquiry access code (IAC) – used for inquiry purposes

• NOTE: Inquiry and Paging comprise the network discovery and setup procedures as discussed later
Access Code

• Preamble – used for DC compensation
  – 0101 if LSB of sync word is 0
  – 1010 if LSB of synch word is 1

• Sync word – 64-bits, derived from:
  – 7-bit Barker sequence
  – Lower address part (LAP)
  – Pseudonoise (PN) sequence

• Trailer
  – 0101 if MSB of sync word is 1
  – 1010 if MSB of sync word is 0
Bluetooth Packet Header

- LT_ADDR: 3-bit logical transport address (also Active Mode address)
- TYPE: 4-bit type code - determines how many slots the current packet will occupy
- FLOW: 1-bit flow control – used for ACL packets
- ARQN: 1-bit acknowledge indication - used to inform the source of a successful transfer of payload data with CRC and can be positive (ACK) or negative (NAK).
- SEQN: 1-bit sequence number
- HEC: 8-bit header error check

- The total header consists of 18 bits
  - encoded with a rate 1/3 FEC resulting in a 54-bit header.
Payload Format

• Payload header
  – L_CH field – identifies logical channel
  – Flow field – used to control flow at L2CAP level
  – Length field – number of bytes of data
• Payload body – contains user data
• CRC – 16-bit CRC code
Logical Channels

- Link control (LC)
- Link manager (LM)
- User asynchronous (UA)
- User isochronous (UI)
- Use synchronous (US)
Error Correction Schemes

• 1/3 rate FEC (forward error correction)
  – Used on 18-bit packet header, voice field in HV1 packet

• 2/3 rate FEC
  – Used in DM packets, data fields of DV packet, FHS packet and HV2 packet

• ARQ
  – Used with DM and DH packets
ARQ Scheme Elements

- Error detection – destination detects errors, discards packets
- Positive acknowledgment – destination returns positive acknowledgement
- Retransmission after timeout – source retransmits if packet unacknowledged
- Negative acknowledgment and retransmission – destination returns negative acknowledgement for packets with errors, source retransmits
# Packet Types/Data Rates

## Packet Types

<table>
<thead>
<tr>
<th>SEGMENT</th>
<th>TYPE</th>
<th>SCO link</th>
<th>ACL link</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0000</td>
<td>NULL</td>
<td>NULL</td>
</tr>
<tr>
<td></td>
<td>0001</td>
<td>POLL</td>
<td>POLL</td>
</tr>
<tr>
<td></td>
<td>0010</td>
<td>FHS</td>
<td>FHS</td>
</tr>
<tr>
<td></td>
<td>0011</td>
<td>DM1</td>
<td>DM1</td>
</tr>
<tr>
<td>2</td>
<td>0100</td>
<td>DV</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0101</td>
<td>HV1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0110</td>
<td>HV2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0111</td>
<td>HV3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1000</td>
<td>DM3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1001</td>
<td>AUX1</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1010</td>
<td></td>
<td>DM3</td>
</tr>
<tr>
<td></td>
<td>1011</td>
<td></td>
<td>DH3</td>
</tr>
<tr>
<td></td>
<td>1100</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1101</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>1110</td>
<td></td>
<td>DM5</td>
</tr>
<tr>
<td></td>
<td>1111</td>
<td></td>
<td>DH5</td>
</tr>
</tbody>
</table>

## Data Rates (Kbps)

<table>
<thead>
<tr>
<th>TYPE</th>
<th>symmetric</th>
<th>asymmetric</th>
</tr>
</thead>
<tbody>
<tr>
<td>DM1</td>
<td>108.8</td>
<td>108.8</td>
</tr>
<tr>
<td>DH1</td>
<td>172.8</td>
<td>172.8</td>
</tr>
<tr>
<td>DM3</td>
<td>256.0</td>
<td>384.0</td>
</tr>
<tr>
<td>DH3</td>
<td>384.0</td>
<td>576.0</td>
</tr>
<tr>
<td>DM5</td>
<td>286.7</td>
<td>477.8</td>
</tr>
<tr>
<td>DH5</td>
<td>432.6</td>
<td>721.0</td>
</tr>
</tbody>
</table>

DMx = FEC encoded  
DHx = No FEC  
DV = data + voice  
HV = voice  

Source: Bluetooth Architecture Overview  
James Kardach, Intel  
IEEE 802.15 document #99053
Multi-slave Access

- The master always has full control over the piconet.
- Slaves can communicate only with the master and not with other slaves.
- A slave is allowed to transmit in the slave-to-master slot only when addressed by the LT_ADDR in the packet header in the preceding master-to-slave slot.
  - the slave shall not transmit if header is in error or if address doesn’t match

Source:
IEEE 802.15.1 Standard
Link Manager Protocol (LMP)

- LMP used for link setup and control
  - LMP messages shall be interpreted and acted upon by the LM
  - shall not be directly propagated to higher protocol layers

- LMP messages:
  - Connection Control
  - Security
  - Informational Requests
  - Switching between Modes of Operation
Channel Control

• States of operation of a piconet during link establishment and maintenance

• Major states
  – Standby – default state
  – Connection – device connected
Bluetooth States

• Standby: Initial state

• Inquiry: Master sends an inquiry packet. **Slaves scan for inquiries and respond with their address and clock after a random delay (CSMA/CA)**

• Page: Master in page state invites devices to join the piconet.
  – Page message is sent in 3 consecutive slots (3 frequencies)
  – Slave enters page response state and sends page response including its device access code
  – Master informs slave about its clock and address so that slave can participate in piconet. Slave computes the clock offset

• Connected: A short 3-bit logical address is assigned

• Transmit: Actively exchange data
Channel Control

- Interim substates for adding new slaves
  - Page (master) – device issued a page
  - Page scan (slave) – device is listening for a page
  - Master response – master receives a page response from slave
  - Slave response – slave responds to a page from master
  - Inquiry (master) – device has issued an inquiry for identity of devices within range
  - Inquiry scan (slave) – device is listening for an inquiry
  - Inquiry response (slave) – device receives an inquiry response
Figure 15.12  Bluetooth State Transition Diagram
Combined Inquiry and Inquiry Scan

Src:
http://www.shiratori.i.rie.tohoku.ac.jp/~deba/PAPER/Journal/WINET-onlineFinal.pdf
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

Source: Bluetooth Architecture Overview
Dr. Chatschik Bisdikian, IBM Research
IEEE 802.15 document #99069r1
Inquiry Procedure

• Potential master identifies devices in range that wish to participate
  – Transmits ID packet with inquiry access code (IAC)
  – Occurs in Inquiry state

• Device receives inquiry
  – Enter Inquiry Response state
  – Returns FHS packet with address and timing information
  – Moves to page scan state
Page Procedure

• Master uses devices address to calculate a page frequency-hopping sequence
• Master pages with ID packet and device access code (DAC) of specific slave
• Slave responds with DAC ID packet
• Master responds with its FHS packet
• Slave confirms receipt with DAC ID
• Slaves moves to Connection state
Slave Connection State Modes

- **Active** – participates in piconet
  - Listens, transmits and receives packets
- **Sniff** – only listens on specified slots
- **Hold** – does not support ACL packets
  - Reduced power status
  - May still participate in SCO exchanges
  - Node can do something else: scan, page, inquire
- **Park** – does not participate on piconet
  - Still retained as part of piconet
  - Gives up its 3-bit active member address and gets an 8-bit parked member address
  - Packets for parked stations are broadcast to 3-bit zero address
Logical Link Control and Adaptation Protocol (L2CAP)

- 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

- L2CAP permits higher level protocols and applications to transmit and receive upper layer data packets (L2CAP SDUs) up to 64 kB in length
  - also permits per-channel flow control and retransmission via the flow control and retransmission modes

- L2CAP is based around the concept of 'channels'. Each one of the endpoints of an L2CAP channel is referred to by a channel identifier (CID)
L2CAP Data Flows

- L2CAP is packet-based but follows a communication model based on channels.
- A channel represents a data flow between L2CAP entities in remote devices.
  - Channels may be connection-oriented or connectionless.

Source: IEEE 802.15.1 Standard
Bluetooth protocols

- **Host Controller Interface (HCI)**
  - provides a common interface between the Bluetooth host and a Bluetooth module

- **Service Discovery Protocol (SDP)**
  - Defines an inquiry/response protocol for discovering services

- **RFCOMM (based on GSM TS07.10)**
  - emulates a serial-port to support a large base of legacy (serial-port-based) applications

- **Telephony Control Protocol Spec (TCS)**
  - call control (setup & release)
  - group management for gateway serving multiple devices

- **Legacy protocol reuse**
  - reuse existing protocols, e.g., IrDA’s OBEX, or WAP for interacting with applications on phones
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

Source: Bluetooth Architecture Overview
Dr. Chatschik Bisdikian, IBM Research
IEEE 802.15 document #99069r1
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

Source: Bluetooth Architecture Overview
Dr. Chatschik Bisdikian, IBM Research
IEEE 802.15 document #99069r1
Headset profile

Source: Bluetooth Architecture Overview
Dr. Chatschik Bisdikian, IBM Research
IEEE 802.15 document #99069r1
LAN access point profile

Source: Bluetooth Architecture Overview
Dr. Chatschik Bisdikian, IBM Research
IEEE 802.15 document #99069r1
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

Source: Bluetooth Architecture Overview
James Kardach, Intel
IEEE 802.15 document #99053
Bluetooth security features

- Fast frequency hopping (79 channels)
- Low transmit power (range $\leq 10\text{m}$)
- Authentication of remote device
  - based on link key (128 Bit)
  - May be performed in both directions
- Encryption of payload data
  - Stream cipher algorithm ($\leq 128$ Bit)
  - Affects all traffic on a link
- Initialization
  - PIN entry by user
Coexistence with WLANs

• Wi-Fi (802.11 b/g) and Bluetooth both use 2.4 GHz ISM band that is 83 MHz-wide

• Bluetooth uses Frequency Hopping Spread Spectrum (FHSS)
  – 79 different 1 MHz-wide channels in this band

• Wi-Fi uses 22 Mhz wide channels
  – Can use only 3 non-overlapping channels
  – 22 of Bluetooth channels in a single Wi-Fi channel
  – Bluetooth packets will interfere with Wi-Fi packets
  – Wi-Fi rate management algorithm will reduce data rate, make problem worse

• Result: Reduced performance, worse voice quality
Coexistence Solutions

• Collaborative
  – For devices that include both Wi-Fi and Bluetooth like laptops, smartphones
  – TDMA for radio channel – alternate access between BT & Wi-Fi

• Non-collaborative
  – Adaptive packet selection and scheduling (APSS)
    • Use shorter packets
    • Disable FEC
  – Adaptive frequency hopping (AFH)
    • selectively remove from the hopping sequence those channels on which interference is present
Adaptive Frequency Hopping

- Bluetooth removes active Wi-Fi channel from hopping list, avoids collisions

Source: WiFi and Bluetooth fight for bandwidth
Richard A Quinnell - Contributing Editor
EDN, August 4 2005
Summary

- Wireless personal area networks are used for 1-10m communications
- Several standards based on application scenarios
- Bluetooth most widely used WPAN standard
  - upto 3 Mbps, uses Frequency hopping, has application specific profiles
  - coexistence issues with 802.11 b/g reduced by adaptive packet selection and hop sequencing