Wireless Personal Area Networks (WPANs)
Outline

- IEEE Project 802 and 802.15 Working Group
- Bluetooth (IEEE 802.15.1)
- Coexistence (IEEE 802.15.2)
- LR-WPAN (ZigBee and IEEE 802.15.4)
IEEE Project 802 and 802.15 Working Group
IEEE Project 802

- IEEE 802 LAN/MAN Standards Committee (LMSC or IEEE Project 802)
- The first meeting of the IEEE Computer Society “Local Network Standards Committee” was held in February of 1980
- Lowest 2 layers of the Reference Model for Open Systems Interconnection (OSI)
- Well-known Working Group
  - 3: Ethernet
  - 11: WLAN
  - 15: WPAN
Wireless Personal Area Networks (WPAN)
- TG1: based on the Bluetooth v1.1 Foundation Specifications
- TG2: to facilitate coexistence of WPANs (802.15) and WLANs (802.11)
- TG3: for high-rate (20Mbit/s or greater) WPANs
- TG4: to investigate a low data rate solution with multi-month to multi-year battery life and very low complexity
- TG5: to determine the necessary mechanisms that must be present in the PHY and MAC layers of WPANs to enable mesh networking
IEEE 802.15 Working Group
IEEE 802 LAN/MAN Standards Committee

- 802.1
  Higher Layer LAN Protocols Working Group

- 802.11
  Wireless Local Area Network Working Group

- 802.15
  Wireless Personal Area Network Working Group

- 802.22
  Wireless Regional Area Networks

- TG1
  WPAN/Bluetooth Task Group

- TG2
  Coexistence Task Group

- TG3
  WPAN High Rate Task Group

- TG5
  WPAN Low Rate Task Group

- TG5
  Mesh Networking Task Group

- UWB
- Zigbee
## Comparison Between WPAN

<table>
<thead>
<tr>
<th>Project</th>
<th>Data Rate</th>
<th>Range</th>
<th>Configuration</th>
<th>Other Features</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>802.15.1 (Bluetooth)</strong></td>
<td>721 kbps</td>
<td>1 M (class3) 100 M (class1)</td>
<td>8 active device Piconet/Scatternet</td>
<td>Authentication, Encryption, Voice</td>
</tr>
<tr>
<td><strong>802.15.3 High Rate</strong></td>
<td>22, 33, 44, 55 Mbps</td>
<td>10 M</td>
<td>peer-to-peer</td>
<td>FCC part 15.249 QoS, Fast Join, Multi-media</td>
</tr>
<tr>
<td><strong>802.15.4 Low Rate</strong></td>
<td>Up to 250 kbps</td>
<td>10 M nominal 1~100 M (based on settings)</td>
<td>Star peer-to-peer</td>
<td>Battery life: multi-month to multi-year</td>
</tr>
</tbody>
</table>
Bluetooth
(IEEE 802.15.1)
Overview

- Initially developed by Swedish company Ericsson in 1994
  - Several thousand companies have signed on to make Bluetooth the low-power, short-range wireless standard
- Standards are published by an industry consortium known as “Bluetooth SIG (special interest group)”
  - IEEE 802.15.1
  - Newer version v1.2
- A universal short-range wireless capability on 2.4 GHz band
- In 10 meters, two Bluetooth devices can share up to 720Kbps rate
- Support data, audio, graphics, and even videos
Data/Voice Access Points

Ad Hoc Networking

Goals

Cable Replacement

Bluetooth Drivers

- low cost implementation
- small implementation size
- low power consumption
- robust, high quality data & voice transfer
- open global standard

Wireless Link Between All Mobile Devices
Networking Capability Brief

- Up to 8 devices can communicate in a small network called a “piconet”
- 10 piconets can coexist in the same coverage range
  - With insignificant degradation
- Security mechanism to protect each wireless link
Standards Documents

- > 1500 pages
- Divided into two groups:
  - core
    - protocol layers, architecture, radio, timer
  - profile
    - each profile specification discusses the use of the core spec. to implement a usage model
    - to define a standard of interoperability
    - two categories: cable replacement and wireless audio
Protocol Architecture

• Radio:
  - interface, frequency hopping, modulation, transmit power
  - GFSK modulation yields 432 kbps bidirectional / 721 kbps asymmetrical

• Baseband:
  - connection establishment in a piconet, addressing, packet format, timing, power control

• Link Management Protocol (LMP):
  - link setup, authentication, packet size
Protocol Architecture (cont’d)

- **Logical Link Control and Adaptation Protocol (L2CAP):**
  - adapts upper-layer protocols to baseband, connectionless service, connection-oriented service
- **Service Discovery Protocol (SDP):**
  - device info (service, characteristic), service query
Protocols

Applications

Higher Layers

Logical Link Control and Adapation Protocol (L2CAP)

Host Controller Interface (HCI)

Bluetooth Module

Radio

Baseband

Link Manager Protocol (LMP)
Bluetooth Chip Architecture

Source: Intel Developer Forum, Fall 2000
**Piconet**

- **Star Topology**
  - 1 Master, up to 7 active (sniff, hold) slaves
  - 256 parked slaves

- **Master:**
  - determines hopping scheme and timing
  - Administers piconet (polling)

- ** Logical Channels**
  - Asynchronous, packet oriented
  - Synchronous, connection-oriented (voice, slot reservation)
Connecting Steps

- Inquiry
  - used by master to find the identities of devices within range
- Inquiry scan
  - listening for an inquiry message
- Page
  - used by master to send PAGE message to connect to a slave by transmitting slave’s device address code (DAC)
- Page scan
  - slave listening for a paging packet with its DAC
Inquiry and Page Flowchart

Figure 5-2 State transition from standby into connection.
Frequency Hopping

- Typically, FH scheme uses carriers spacing of 1 MHz with up to 80 different frequencies
- So, with FH, there are 80 logical channels (theoretically)
  - When two piconets choose the same 1MHz-band, collision occurs
- The same hopping sequence is shared by all devices in the same piconet
  - hopping rate = 1600 hops/sec
  - one slot = 0.625 ms
Frequency Hopping (cont’d)

**Table 15.3** International Bluetooth Frequency Allocations

<table>
<thead>
<tr>
<th>Area</th>
<th>Regulatory Range</th>
<th>RF Channels</th>
</tr>
</thead>
<tbody>
<tr>
<td>U.S., most of Europe, and most other countries</td>
<td>2.4 to 2.4835 GHz</td>
<td>$f = 2.402 + n \text{ MHz, } n = 0,\ldots, 78$</td>
</tr>
<tr>
<td>Japan</td>
<td>2.471 to 2.497 GHz</td>
<td>$f = 2.473 + n \text{ MHz, } n = 0,\ldots, 22$</td>
</tr>
<tr>
<td>Spain</td>
<td>2.445 to 2.475 GHz</td>
<td>$f = 2.449 + n \text{ MHz, } n = 0,\ldots, 22$</td>
</tr>
<tr>
<td>France</td>
<td>2.4465 to 2.4835 GHz</td>
<td>$f = 2.454 + n \text{ MHz, } n = 0,\ldots, 22$</td>
</tr>
</tbody>
</table>
**Radio and Baseband Parameters**

<table>
<thead>
<tr>
<th><strong>Table 15.2 Bluetooth Radio and Baseband Parameters</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Topology</strong></td>
</tr>
<tr>
<td><strong>Modulation</strong></td>
</tr>
<tr>
<td><strong>Peak data rate</strong></td>
</tr>
<tr>
<td><strong>RF bandwidth</strong></td>
</tr>
<tr>
<td><strong>RF band</strong></td>
</tr>
<tr>
<td><strong>RF carriers</strong></td>
</tr>
<tr>
<td><strong>Carrier spacing</strong></td>
</tr>
<tr>
<td><strong>Transmit power</strong></td>
</tr>
<tr>
<td><strong>Piconet access</strong></td>
</tr>
<tr>
<td><strong>Frequency hop rate</strong></td>
</tr>
<tr>
<td><strong>Scatternet access</strong></td>
</tr>
</tbody>
</table>
Transmitter Output Powers

- **Class 1**: greatest distance (100m)
  - 1mW (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
FH-TDD-TDMA

- **TDD**
  - transmission alternates between TWO directions
- **TDMA**
  - multiple devices share the same piconet (logical) FH channel

*Figure 15.6 Frequency-Hop Time Division Duplex*
Links

- SCO (synchronous connection oriented)
  - fixed-bandwidth channel between a master and a slave
  - slots spaced by regular intervals
  - up to 3 SCO links per master
  - SCO packets are never retransmitted!
    - bandwidth-guaranteed, but not error-free-guaranteed
Links (cont’d)

• ACL (asynchronous connectionless)
  - a point-to-multipoint link between a master and ALL its slaves
  - only on slots NOT reserved for SCO links
    • but the communication can include a slave already involves in a SCO link
  - packet retransmission is applicable
    • packet-switched style
  - a slave can send only when it is addressed in the previous master-initiated slot
Scatternet

- A device in one piconet may also exist as part of another piconet as either a master or slave in each piconet
- Such overlapping is called a scatternet
Bluetooth Products

Headset Logitech Mobile Bluetooth Headset

Gaming, Handheld Accessory Sony Ericsson Remote Control Car

Mobile Phone X70
New Features in the Bluetooth Core Specification v1.2

- Faster connection
- Adaptive frequency hopping
- Extended SCO links
- Enhance QoS
Faster Connection

- In v1.1, the inquiry/page scan hopping sequence is determined by a function called \([\text{Xir4-0}]\).
- v1.2 adds a new **interlaced scan** for slaves:
  - Every odd hop uses the original definition in v1.1.
  - Every even hop uses frequency \([\text{Xir4-0 + 16}] \mod 32\).
  - Master’s inquiry is unchanged.
- If \((\text{scan interval}) < 2*(\text{scan window})\), then interlaced scan should not be used.
- The result is a speedup in inquiry and page procedures.
Interlaced Scan Sequence

- original
  - (AA…A)(BB…B) …

- New
  - switch even A’s with even B’s
    - (ABAB…AB)(BABA…BA) …
Adaptive Frequency Hopping (AFH)

- AFH is used to improve the performance of physical links in the presence of interference from other devices in the ISM band
- Basic idea: mask the bad channels
AFH (cont’d)

• Only the master can enable/disable AFH
• A master may request channel classification information from the slaves
  - Then the master classifies channels into *used* and *unused*
    • How to make the decision is not specified in the spec
  - The used/unused channels are used by all devices in the same piconet
• When an unused frequency is selected, a *Channel re-mapping function* will re-map the *unused* channel to an *used* channel pseudo-randomly
Coexistence
Overview

• WLAN and WPAN operate in the same ISM band
  – mutual interference between the systems
  – severe performance degradations are possible
• Many factors effect the level of interference
  – the distance between the WLAN and WPAN devices
  – the amount of data traffic flowing over each of the two networks
  – the power levels of the various devices
  – the data rate of the WLAN
  – types of information being sent over the wireless networks
• Performance degradations might discourage consumers to use more wireless devices
Overview (cont’d)

• If nothing is done
  – devices that transmit with relatively higher power or more interference resistant protocols get their data through
  – whereas the other devices suffers

• Coexistence is defined as ability of one system to operate in shared environment

• Good coexistence policy is such that it do not increase an interference to other systems using the same wireless channel
IEEE 802.15.2

- “IEEE 802.15.2 – Coexistence of Wireless Personal Area Networks with Other Wireless Devices Operating in Unlicensed Frequency Band” in 2003
- Defines coexistence methods for a WPAN to operate in the presence of frequency static or slow-hopping WLAN devices
- Basically the scope is limited to coexistence of Bluetooth (IEEE 802.15.1) devices and IEEE 802.11b devices
  - expected devices using these standards will have the largest market share
  - some of the proposed coexistence methods can be used also with other WPAN and WLAN standards
Categories of Coexistence Methods

• Collaborative methods
  – Exchange information between WPAN and WLAN network
  – A wired communication link between system is needed
  – Applicable only if WPAN master and WLAN station are located in the same physical equipment (like laptop)
  – Three different methods are defined

• Non-collaborative methods
  – Do not exchange information between two wireless networks
  – WPAN and WLAN devices do not have to be in the same equipment
  – Five different methods defined
## Collaborative Methods

<table>
<thead>
<tr>
<th>Name</th>
<th>Protocol layer</th>
<th>Needs operations from WPAN device</th>
<th>Needs operations from WLAN device</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alternating Wireless Medium Access (AWMA)</td>
<td>MAC</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Packet Traffic Arbitration (PTA)</td>
<td>MAC</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Deterministic Interference Suppression (DIS)</td>
<td>PHY</td>
<td>-</td>
<td>X</td>
</tr>
</tbody>
</table>
Alternating Wireless Medium Access (AWMA)

- AWMA is collaborative time division method
- IEEE 802.11b station sends a beacon periodically
  - Part of each beacon period is allocated for WLAN traffic and rest for WPAN traffic
- Lengths of these periods are included in the beacon
- Synchronization between WPAN and WLAN devices is needed
  - One WLAN station and WPAN master need wired connection
  - WLAN station sends a synchronization signal to WPAN master via this connection
AWMA (cont’d)

• Only for ACL connections
• Can prevent interference between WPAN devices in one piconet and all WLAN devices connected to same AP
  – Interference between WLAN devices that are connected to some other AP is prevented only if the APs are synchronized
• Quite ineffective
  – transmissions of one system are not allowed during the “empty” time windows reserved for the other system
Packet Traffic Arbitration (PTA)

- Can be used in case that coexisting WLAN device and WPAN device are in the same equipment
- Both devices are connected to packet traffic arbitrator (PTA-block)
- Before a device can send a packet it must request a approval for transmission from PTA-block
  - If the transmission do not results in a collision, PTA-block grants the approval
  - If both devices send their requests (almost) simultaneously, the one with higher priority is approved to transmit and the other have to wait
PTA (cont’d)

• Priorities can be selected deterministically
  – IEEE 802.11b ACK packet (highest)
  – IEEE 802.15.1 SCO packet
  – IEEE 802.11b data packet
  – IEEE 802.15.1 ACL packet (lowest)
  – or in random manner or using some other fairness criteria

• Can be used also with SCO links
• More efficient than previous method (No need to wait unless collisions are occurring)
Deterministic Interference Suppression (DIS)

- Frequency hopping bandwidth of BT is 1 MHz
  - can be considered as a narrowband interference to other frequency static or slow-hopping WLAN devices
- WLAN receiver can mitigate this narrowband interferer by programmable notch filter
  - stop band of ~1 MHz is hopping according to hopping process of WPAN device
- WLAN device must have an integrated WPAN unit which provides frequency hopping information of interfering WPAN transmission
- This method works purely on physical layer and mitigates only interference caused by WPAN devices to WLAN devices
## Non-Collaborative Methods

<table>
<thead>
<tr>
<th>Name</th>
<th>Protocol layer</th>
<th>Needs operations from WPAN device</th>
<th>Needs operations from WLAN device</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adaptive Interference Suppression</td>
<td>PHY</td>
<td>-</td>
<td>X</td>
</tr>
<tr>
<td>Adaptive Packet Selection</td>
<td>MAC</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td>Packet Scheduling for ACL Links</td>
<td>MAC</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td>Packet Scheduling for SCO Links</td>
<td>MAC</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td>Adaptive Frequency-Hopping (AFH)</td>
<td>MAC</td>
<td>X</td>
<td>-</td>
</tr>
</tbody>
</table>
Adaptive Interference Suppression

- Similar to Deterministic Interference Suppression
- WLAN device do not need explicit knowledge of FH pattern nor timing of frequency hopping WPAN interferer
- WLAN transmitter uses adaptive signal processing methods to estimate the location of narrowband interference caused by WPAN and then filter out those frequencies
Adaptive Interference Suppression (cont’d)

**Figure 12—An adaptive notch filter or whitening filter**
Adaptive Packet Selection

- BT defines various packet types for both ACL and SCO connections
  - packet types differ especially in the **FEC code** used and the amount of channel occupied
- Basic idea is to dynamically select packet types such that maximal total network capacity is achieved
- Range limited
  - packet types with stronger FEC coding provide better throughput
  - SCO packet types are preferred in order HV1, HV2 and HV3
  - ACL packet types DM1, DM2, DM5 are preferred over DH1, DH2 and DH5
Adaptive Packet Selection (cont’d)

- Interference limited
  - FEC coding does not help that much WPAN throughput, but cause more interference to WLAN
  - SCO packet types are preferred in order HV3, HV2 and HV1.
  - ACL packet types DH1, DH2, DH5 are preferred over DM1, DM2 and DM5

- WPAN device can determine the limiting factor by monitoring RSSI (received signal strength indication) and BER (bit error rate)
  - Low RSSI value (and BER) indicates range (noise) limited channel
  - High RSSI value together with high BER indicates interference limited channel
Packet scheduling for ACL links

- This method consists of two parts: channel classification and master delay policy.
- Each BT device (adaptively) classify each of its FH channels to be ‘good’ or ‘bad’.
- Master device collects a table of channel conditions of all devices in piconet.
- In ACL links all slave transmissions are always followed right after master transmission.
- Consequently, the master can check both the slave's receiving channel and its own receiving channel before choosing to transmit a packet in a given frequency hop.
- If one (or both) of the channels are marked as ‘bad’, master delays its own transmission until both channels are ‘good’.
Packet scheduling for SCO links

• A new SCO packet type, EV3, is proposed
• This packet is based on HV3 packet
  – no FEC coding
  – 240 bits payload
  – one packet for every 6 slots.
• New features of EV3:
  – Slave transmissions are allowed only right after master transmission.
  – Master can select which two consecutive time slots of six (three options) are used
Packet scheduling for SCO links (cont’d)

- Selection of time slots are again made according to channel classification tables such that both receiving channels (slaves and masters) are ‘good’ if possible.

Figure A.1—Comparisons of HV3 and EV3 packet
Adaptive frequency hopping (AFH)

- This method is defined in IEEE 802.15.1
- This method dynamically changes the FH sequence of the Bluetooth/802.15.1 system in order to avoid the interference.
- Global channel classification is needed.
- Original FH pattern is mapped to subset of channels classified to be ‘good’.
- The mapping is such that also a new FH pattern becomes pseudorandom.
AFH (cont’d)

• To work properly, the method requires that there is enough ‘good’ channels.
  – In some countries (like USA), regulatory bodies have set a minimum number of FH channels.
  – Small number of FH channels also affect on system’s robustness.
• If number of ‘good’ channels is too small, some ‘bad’ channels can be included in hopping pattern.
• In this case QoS can be guaranteed, if SCO packets are preferred over ACL packets in allocation of ‘good’ channels.
Channel Classification

- Most of non-collaborative coexistence methods need a channel classification information.
- In channel classification each Bluetooth/IEEE 802.15.1 device classifies each FH channels to be either ‘good’ or ‘bad’.
- The major concern of the quality should be interference caused by some other system.
- IEEE 802.15.2 do not define exactly how this classification should be implemented, but it suggests that classification can be based e.g. on RSSI, PER or carrier sensing.
Channel Classification (cont’d)

• Since master device needs channel condition tables of its slaves, the tables can be exchanged using LMP messages.
• It is also possible to use implicit classification methods such as negative ACKs, in which cases the slave does not have to send any additional information to the master.
• Overall classification time can be reduced by grouping channels to blocks, which naturally reduce the accuracy.
Channel Classification (cont’d)

- In ‘Adaptive Frequency Hopping’ method, global state of each FH channel is needed
- The master obtains it by taking a weighted average of its own channel state and all the active slaves’ channel states
- Finally, a global channel state for one sub-channel is obtained by threshold comparison of the average, which have value in [0,1]
Current Status of Coexistence Method Development

• Citation from IEEE 802.15.2 task group’s web page:
  – “The task group is now in hibernation until further notice.”

• Several vendors are developing hardware and software coexistence solutions, which are based on IEEE 802.15.2 standard.

• New WPAN standards (like 802.15.3 and .4) deal also with coexistence issues particular to those systems.
LR-WPAN
(ZigBee and IEEE 802.15.4)
New Trend of Wireless Technology

- Most Wireless industry focus on increasing high data throughput
  - 802.11b → 802.11a/g
- A set of applications requiring simple wireless connectivity, relaxed throughput, very low power, short distance and inexpensiveness
  - Industrial
  - Agricultural
  - Vehicular
  - Residential
  - Medical
## Comparison Between WPAN

<table>
<thead>
<tr>
<th>Project</th>
<th>Data Rate</th>
<th>Range</th>
<th>Configuration</th>
<th>Other Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.15.1 (Bluetooth)</td>
<td>721 kbps</td>
<td>1 M (class3)</td>
<td>8 active device</td>
<td>Authentication, Encryption, Voice</td>
</tr>
<tr>
<td></td>
<td></td>
<td>100 M (class1)</td>
<td>Piconet/Scatternet</td>
<td></td>
</tr>
<tr>
<td>802.15.3 High Rate</td>
<td>22, 33, 44, 55 Mbps</td>
<td>10 M</td>
<td>peer-to-peer</td>
<td>FCC part 15.249 QoS, Fast Join, Multi-media</td>
</tr>
<tr>
<td>802.15.4 Low Rate</td>
<td>Up to 250 kbps</td>
<td>10 M nominal</td>
<td>Star peer-to-peer</td>
<td>Battery life: multi-month to multi-year</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1~100 M (based on settings)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
What is ZigBee Alliance?

- An organization with a mission to define reliable, cost effective, low-power, wirelessly networked, monitoring and control products based on an open global standard
- The alliance provides interoperability, certification testing, and branding
- 45+ companies: semiconductor mfrs, IP providers, OEMs, etc.
- Defining upper layers of protocol stack: from network to application, including application profiles
- First profiles published mid 2003
Zigbee/IEEE 802.15.4 Protocol Stack

- Divided Responsibility
  - Lower (MAC/PHY) stacks IEEE 802.15.4
  - Upper stacks Zigbee Alliance
  - IEEE 802 compatible LLC protocol can be used
Wireless Markets

<table>
<thead>
<tr>
<th>TEXT</th>
<th>GRAPHICS</th>
<th>INTERNET</th>
<th>HI-FI AUDIO</th>
<th>STREAMING VIDEO</th>
<th>DIGITAL VIDEO</th>
<th>MULTI-CHANNEL VIDEO</th>
</tr>
</thead>
</table>

- **LONG RANGE**
  - **TEXT**
  - **GRAPHICS**
  - **INTERNET**
  - **HI-FI AUDIO**
  - **STREAMING VIDEO**
  - **DIGITAL VIDEO**
  - **MULTI-CHANNEL VIDEO**

- **SHORT RANGE**
  - **TEXT**
  - **GRAPHICS**
  - **INTERNET**
  - **HI-FI AUDIO**
  - **STREAMING VIDEO**
  - **DIGITAL VIDEO**
  - **MULTI-CHANNEL VIDEO**

- **LAN**
  - 802.11b
  - 802.11a/HL2 & 802.11g

- **PAN**
  - ZigBee
  - Bluetooth 2
  - Bluetooth 1

- **LOW < DATA RATE > HIGH**
ZigBee/IEEE 802.15.4 Market Feature

- Low power consumption
- Low cost
- Low offered message throughput
- Supports large network orders (≤ 65k nodes)
- Low to no QoS guarantees
- Flexible protocol design suitable for many applications
ZigBee Network Applications

ZigBee
LOW DATA-RATE RADIO DEVICES

INDUSTRIAL & COMMERCIAL
- monitors
- sensors
- automation
- control

PERSONAL HEALTH CARE
- monitors
- diagnostics
- sensors
- consoles
- portables
- educational

TOYS & GAMES
- TV VCR
- DVD/CD Remote control
- PC & PERIPHERALS
- mouse
- keyboard
- joystick

HOME AUTOMATION
- security
- HVAC
- lighting
- closures
How is ZigBee related to IEEE 802.15.4?

- ZigBee takes full advantage of a powerful physical radio specified by IEEE 802.15.4
- ZigBee adds logical network, security and application software
- ZigBee continues to work closely with the IEEE to ensure an integrated and complete solution for the market
802.15.4 Technology: General Characteristics

- Data rates of 250 kbps, 40 kbps, and 20 kbps
- Star or peer-to-peer operation
- Allocated 16 bit short or 64 bit extended addresses
- Allocation of guaranteed time slots (GTSs)
- CSMA-CA channel access
- Fully acknowledged protocol for transfer reliability
- Low power consumption
- Energy detection (ED)
- Link quality indication (LQI)
- 16 channels in the 2450 MHz band, 10 channels in the 915 MHz band, and 1 channel in the 868 MHz band (European)
- Extremely low duty-cycle (<0.1%)
IEEE 802.15.4 Basics

- 802.15.4 is a simple packet data protocol for lightweight wireless networks
  - Channel Access is via Carrier Sense Multiple Access with collision avoidance and optional time slotting
  - Message acknowledgement and an optional beacon structure
  - Multi-level security
  - Works well for
    - Long battery life, selectable latency for controllers, sensors, remote monitoring and portable electronics
  - Configured for maximum battery life, has the potential to last as long as the shelf life of most batteries
IEEE 802.15.4 Device Types

- There are two different device types:
  - A full function device (FFD)
  - A reduced function device (RFD)

- The FFD can operate in three modes serving:
  - Device
  - Coordinator (PAN coordinator)

- The RFD can only operate in a mode serving:
  - Device
**FFD vs RFD**

- **Full function device (FFD)**
  - Network coordinator capable
  - Talks to any other device

- **Reduced function device (RFD)**
  - Cannot become a network coordinator
  - Talks only to a FFD
  - Very simple implementation
WPAN and PAN Coordinator

WPAN

- The most basic component in IEEE 802.15.4 system is device (FFD or RFD)
- Two or more devices within a POS communicating on the same physical channel constitute a WPAN
- Network (POS) includes at least one FFD that operates as the PAN coordinator

PAN coordinator

- Can initiate, terminate or route communication
- Can allocate short addresses (16 bit) to devices
- In star topology, devices communicate solely with the PAN coordinator
Star Topology

PAN coordinator

- Full Function Device (FFD)
- Reduced Function Device (RFD)
- Communications Flow
Example
Peer-Peer Topology

Communications Flow

PAN coordinator

- Full Function Device (FFD)
- Reduced Function Device (RFD)
- Communications Flow
Example
Addressing

- Each independent PAN will select a unique **PAN identifier**
- All devices operating on a network shall have unique **64-bit extended address**. This address can be used for direct communication within the PAN
  - Or can use a 16-bit short address, which is allocated by the PAN coordinator when the device is associated
IEEE 802.15.4 Physical Layer
IEEE 802.15.4 PHY Overview

- **PHY functionalities:**
  - Activation and deactivation of the radio transceiver
  - Energy detection within the current channel
  - Link quality indication for received packets
  - Clear channel assessment for CSMA-CA
  - Channel frequency selection
  - Data transmission and reception

- **PHY provides 2 services**
  - PHY data service
  - PHY management service
IEEE 802.15.4 PHY Overview

- Operating Frequency Bands

**868MHz/915MHz PHY**

- Channel 0: 868.3 MHz
- Channels 1-10: 902 MHz to 928 MHz, 2 MHz bandwidth

**2.4 GHz PHY**

- Channels 11-26: 2.412 GHz to 2.427 GHz, 5 MHz bandwidth
Frequency Bands and Data Rates

The standard specifies two PHYs:

- 868 MHz/915 MHz direct sequence spread spectrum (DSSS) PHY (11 channels)
  - 1 channel (20kbps) in European 868MHz band
  - 10 channels (40kbps) in 915 (902-928)MHz ISM band
- 2450 MHz direct sequence spread spectrum (DSSS) PHY (16 channels)
  - 16 channels (250kbps) in 2.4GHz band
### Frequency Bands and Data Rates (cont’d)

**Table 1. Frequency bands and data rates**

<table>
<thead>
<tr>
<th>Band</th>
<th>Bit rate</th>
<th>Symbol mapping</th>
<th>Symbol rate</th>
<th>Chip modulation</th>
<th>Chip rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>868-868.6 MHz (Europe, 1 ch)</td>
<td>20 kb/s</td>
<td>Binary</td>
<td>20 ksym/s</td>
<td>BPSK</td>
<td>300 kchip/s</td>
</tr>
<tr>
<td>902-928 MHz (U.S., 10 ch)</td>
<td>40 kb/s</td>
<td>Binary</td>
<td>40 ksym/s</td>
<td>BPSK</td>
<td>600 kchip/s</td>
</tr>
<tr>
<td>2400-2483.5 GHz (worldwide, 16 ch)</td>
<td>250 kb/s</td>
<td>16-ary quasi – orthogonal</td>
<td>62.5 ksym/s</td>
<td>O-QPSK</td>
<td>2 Mchip/s</td>
</tr>
</tbody>
</table>
## PHY Frame Structure

**PHY packet fields**
- Preamble (32 bits) – synchronization
- Start of packet delimiter (8 bits) – shall be formatted as “11100101”
- PHY header (8 bits) – PSDU length
- PSDU (0 to 127 bytes) – data field

<table>
<thead>
<tr>
<th>Sync Header</th>
<th>PHY Header</th>
<th>PHY Payload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preamble</td>
<td>Start of Packet Delimiter</td>
<td>Frame Length (7 bit)</td>
</tr>
<tr>
<td>4 Octets</td>
<td>1 Octets</td>
<td>1 Octets</td>
</tr>
</tbody>
</table>

**PHY Service Data Unit (PSDU)**

0-127 Bytes
General Radio Specifications

- Transmit Power
  - Capable of at least –3dBm

- Receiver Sensitivity
  - -85 dBm (2.4GHz) / -91dBm (868/915MHz)

- Link quality indication
  - A characterization of the strength and/or quality of a received packet
  - The measurement may be implemented using
    - Receiver energy detection
    - Signal to noise ratio estimation
General Radio Specifications (cont’d)

- Clear Channel Assessment (CCA)
  - CCA Mode 1: energy above threshold (ED threshold)
  - CCA Mode 2: carrier sense only (modulation and spreading characteristics of IEEE 802.15.4)
  - CCA Mode 3: carrier sense with energy above threshold

- The ED threshold shall be at most 10 dB above the specified receiver sensitivity

- The CCA detection time shall equal to 8 symbol periods
IEEE 802.15.4 MAC
MAC Functionalities

- Beacon management
- Channel access mechanism
- Dynamic channel selection (GTS management)
- Frame reception and acknowledgments
- (Dis)association
- Security (AES-128)
Beacon Management

- Beacon enabled mode vs. Beacon disabled mode
  - Slotted CSMA/CA (superframe structure) vs. Unslotted CSMA/CA
- Coordinators generate beacons
  - Either broadcasting or unicasting of beacons
- Synchronization performed using beacons
Channel Access Mechanism

- Two type channel access mechanism, based on the network configuration:
  - In non-beacon-enabled networks → unslotted CSMA/CA channel access mechanism
  - In beacon-enabled networks → slotted CSMA/CA channel access mechanism
    - The superframe structure will be used
Data Transfer Model - from Device to Coordinator

- In a beacon-enable network, device finds the beacon to synchronize to the superframe structure. Then using slotted CSMA/CA (with GTS) to transmit its data.
- In a non beacon-enable network, device simply transmits its data using unslotted CSMA/CA.

Communication to a coordinator:
- In a beacon-enabled network:
  - Coordinator
  - Network Device
  - Beacon
  - Data
  - Acknowledgment (optional)

- In a non beacon-enabled network:
  - Coordinator
  - Network Device
  - Data
  - Acknowledgment (optional)
  - Communication to a coordinator
Data Transfer Model - from Coordinator to Device

- In a beacon-enable network, the coordinator indicates in the beacon that “data is pending”
  - Device periodically listens to the beacon and transmits a MAC command request using slotted CSMA/CA if necessary

Communication from a coordinator
In a beacon-enabled network
Data Transfer Model - from Coordinator to Device (cont’d)

- In a non beacon-enable network, a device transmits a MAC command request using unslotted CSMA/CA
  - If the coordinator has its pending data, the coordinator transmits data frame using unslotted CSMA/CA
  - Otherwise, the coordinator transmits a data frame with zero length payload

Communication from a coordinator in a non beacon-enabled network
MAC Frame Formats

DATA FRAME

ACKNOWLEGDMEN

MAC COMMAND FRAME

BEACON FRAME

PHY layer

Sync. header  PHY header

PHY protocol data unit (PPDU)

PHY sub layer

MAC layer

Frame control  Sequence number  Address info  Payload  Frame check sequence

Frame control  Sequence number  Frame check sequence

Frame control  Sequence number  Address info  Command payload  Frame check sequence

Frame control  Sequence number  Address info  Beacon payload  Frame check sequence

MAX. 127 bytes

2 1 0-20 Variable 2

2 1
Superframe Structure

Total 16 slots

15ms * $2^n$ where $0 \leq n \leq 14$

Network beacon
- Transmitted by network coordinator. Contains network information, frame structure and notification of pending device messages

Contention period
- Access by any device using slotted CSMA-CA

Guaranteed Time Slot
- Reserved for devices requiring guaranteed bandwidth

up to 7 GTSs
Superframe with Inactive Part

\[ SD = a_{\text{BaseSuperframeDuration}} \times 2^{SO} \text{ symbols} \]

\[ BI = a_{\text{BaseSuperframeDuration}} \times 2^{BO} \text{ symbols} \]
Superframe with Inactive Part (cont’d)

- There are two parameters
  - SO (Superframe Order): to determine the length of the active period
  - BO (Beacon Order): to determine the length of the beacon interval

- In CFP, a GTS may consist of multiple slots, all of which are assigned to a single device, for either transmission (t-GTS) or reception (r-GTS)
  - GTS = guaranteed time slots

- In CAP, the concept of slots is not used
  - Instead, the whole CAP is divided into smaller “contention slots”
  - Each “contention slot” is of 20 symbols long
    - This is used as the smallest unit for contention backoff
  - Then devices contend in a slotted CSMA/CA manner
GTS Concepts

- A guaranteed time slot (GTS) allows a device to operate on the channel within a portion of the superframe
- A GTS shall only be allocated by the PAN coordinator
  - ... and is announced in the beacon
- The PAN coordinator can allocate up to 7 GTSs at the same time
- The PAN coordinator decides whether to allocate GTS based on
  - Requirements of the GTS request
  - The current available capacity in the superframe
A GTS can be de-allocated in two ways
- At any time at the discretion of the PAN coordinator
- By the device that originally requested the GTS

A device that has been allocated a GTS may also operate in the CAP

A data frame transmitted in an allocated GTS shall use only short addressing

The PAN coordinator should store the info of devices with GTS
- including starting slot, length, direction, and associated device address
Before GTS starts, the GTS direction shall be specified as either transmit or receive.

Each device may request one transmit GTS and/or one receive GTS.

- Each GTS may consist of multiple “MACRO” slots.

A device shall only attempt to allocate and use a GTS if it is currently tracking the beacon.

- If a device loses synchronization with the PAN coordinator, all its GTS allocations shall be lost.

The use of GTSs of an RFD is optional.
Slotted CSMA/CA Algorithm

- The backoff period boundaries of every device in the PAN shall be aligned with the superframe slot boundaries of the PAN coordinator
  - i.e. the start of first backoff period of each device is aligned with the start of the beacon transmission

- The MAC sublayer shall ensure that the PHY layer commences all of its transmissions on the boundary of a backoff period
Slotted CSMA/CA Algorithm (cont’d)

- Each device shall maintain three variables for each transmission attempt
  - NB: number of slots the CSMA/CA algorithm is required to backoff while attempting the current transmission
  - BE: the backoff exponent which is related to how many backoff periods a device shall wait before attempting to assess a channel
  - CW: (a special design)
    - Contention window length, the number of backoff slots that needs to be clear of channel activity before transmission can commence
    - It is initialized to 2 and reset to 2 if the channel is sensed to be busy
    - So a station has to detect two CCA before contending
Slotted CSMA/CA

1. Slotted?
   - Y: $NB = 0, CW = 2$
   - N: $BE = \text{lesser of } (2, \text{macMinBE})$
      - Y: $BE = \text{macMinBE}$
      - N: Locate backoff period boundary

Optional

2. Delay for random($2^{BE} - 1$) unit backoff periods

3. Perform CCA on backoff period boundary

4. $CW = 2, NB = NB + 1, BE = \min(BE + 1, aMaxBE)$
   - N: $NB < \text{macMaxCSMABackoffs}$
     - Y: Failure
   - Y: $CW = CW - 1$
      - N: $CW = 0$?
        - Y: Success
        - N: $NB > \text{macMaxCSMABackoffs}$
          - Y: Failure
          - N: Locate backoff period boundary
Unslotted CSMA/CA

There is no concept of CW in this part.
Battery Life Extension

- **Power Consumption Considerations**
  - In the applications that use this standard, most of the devices will be battery powered
  - Battery powered devices will require *duty-cycling* to reduce power consumption
  - The application designer should decide on the balance between battery consumption and message latency

- **Battery Life Extension**
  - A station can only send in the first 5 slots after the beacon
    - Beacons are variable lengths
    - SIFS has to be taken, after which 2 CCA’s are needed before contending
    - If a station does not find a chance to transmit in the first 5 slots, it has to wait until the next beacon
Battery Life Extension (cont’d)

Beaconing Device

- Minimum Beacon
- Listen Interval (when no frame detected)

- First Five Full Backoff Periods after the Beacon IFS period
- 2560 us
- 160 symbols
- 80 octets

- 576 us
- 36 symbols
- 18 octets

- SIFS

- Backoff Period

- Always at least three backoff periods available to start transmission

- Transmit Frame
Security

- Devices can have the ability to
  - Maintain an access control list
  - Use symmetric cryptography

- Security modes
  - Unsecured mode
  - Access control list mode
  - Secured mode
Security Services

- Access control
- Data encryption
- Frame integrity
- Sequential freshness
Application - the Lock of My Door

The lock @ your front door

LOCKED since 2.5 hours. Last user: Pertti. See use history.


Not just a lock, but part of an e-business (huge value/bit)
Tell Me More about this Painting

- The museum installs radio tags to paintings. Users receive the tag IDs in the terminals, which then translate the ID into local/global web pages.
- The tag may be a beacon that announces the id periodically, or a passive device that wakes up on terminal’s demand. Very low power demands (parasitic?) would allow permanent embedding.
- The ID could be an URL, HP Cooltown-style.
My Universal Privilege Device

- Announces my access privileges to things & services. Maybe identity & authentication as well
- At home, I am the superuser. At office, a humble worker :-(
- Only works on me. Talks to the various login controls and hooks me up with minimum hassle
Thanks