

Wireless Personal Area Networks

David Tipper
Associate Professor
Graduate Telecommunications and Networking
Program
University of Pittsburgh
Slides 16

Wireless Networks



– Wireless Wide Area Networks (WWANs)

- Cellular Networks :
 - GSM, cdmaone (IS-95), UMTS, cdma2000 EVDO
- Satellite Networks:
 - Iridium, Globalstar, GPS, etc.



– Wireless Metro Area Networks (WMANs)

- IEEE 802.16 WiMAX



– Wireless Local Area Networks (WLANs)


- IEEE 802.11, a, b, g, etc. (infrastructure, ad hoc, sensor)

– Wireless Personal Area Networks (WPANs)

- IEEE 802.15 (Bluetooth), IrDa, Zigbee, sensor, etc.

Wireless Personal Area Network



- Origins in the BodyLAN project initiated by BBN in the early 1990s
- Networking “personal” devices – sensors, cameras, handheld computers, audio devices, etc. with a range of around 5 feet around a soldier
- Today: Networking digital cameras to cell phones to PDAs to laptops to printers to etc.,
- Most popular application – hands free headset to cellphone
- IEEE 802.15 standard (Bluetooth)  **Bluetooth**
The Official Bluetooth Website
 - Use band available globally for unlicensed users
 - Low powered – medium data rate ~100s kbps



What is a personal area network?



- Origins in the BodyLAN project initiated by BBN in the early 1990s for military
- Networking “personal” devices around a soldier
 - Now networking devices around an individual
 - sensors, cameras, handheld computers, audio devices, cell phone, printers, etc.
- Goal was smart technology that self configures, recognizes other units within range and provides on the fly communications
- Universal short-range wireless capability
 - Use band available globally for unlicensed users
 - Low powered – medium data rate



Applications of WPANs

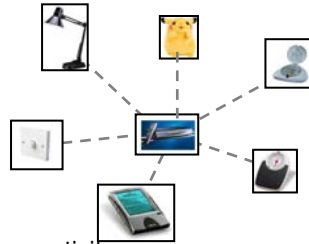


Cable Replacement

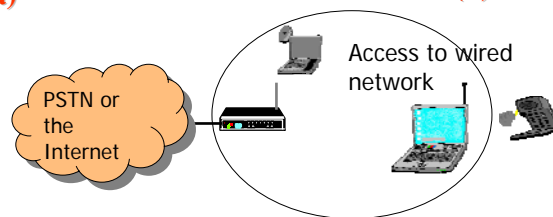


(a)

Ad hoc connectivity



(b)



(c)

Telcom 2720

6



The Official Bluetooth Website

Bluetooth



- Much of the WPAN focus today is around Bluetooth
- Originated by Ericsson, Nokia, IBM, Toshiba, Intel formed a WPAN special interest group (SIG) 1998
- Named after King of Denmark and Norway
 - Harald Blaatand (Bluetooth), 940 – 981.
- Specifies the complete system from the radio level up to the application level
- Protocol stack is partly in hardware and partly in software running on a microprocessor
- Embedded devices
 - Low power
 - Low cost
- Uses ISM band of spectrum



Telcom 2720

7

IEEE 802.15



- Started in 1997 as a sub-group of IEEE 802.11
- Focused on WPANS
- Initial functional requirements
 - Low power devices
 - Range of 0-10m
 - Low data rates (19.2-100 kbps)
 - Small sizes (0.5 cubic inches)
 - Low cost
 - Multiple networks in the same area
 - Up to 16 separate devices in a PAN
- IEEE Took over Bluetooth standardization in 2000
 - Today over 2500 companies as Bluetooth SIG members
<http://www.bluetooth.com>
 - Built-in Bluetooth chip shipped in more than 100 million cellular phones and laptops last year
 - Several millions of other communication devices
 - Cameras, headsets, microphones, keyboards etc.

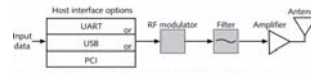
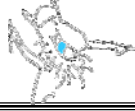


Figure 5-6 Functional block diagram of a Bluetooth transceiver

IEEE 802.15 today



- Task Group 1 (802.15.1)
 - PHY and MAC layer design for wirelessly connecting devices entering a *personal operating space* (POS)
 - POS is a 10m space around a person who is stationary or in motion
- Task Group 2 (802.15.2)
 - Coexistence of WLANs and WPANS
 - Interoperability between a WLAN and WPAN device
- Task Group 3 (802.15.3)
 - Higher data rates (up to 20 Mbps) (Kodak, Cisco, Motorola)
 - Multimedia applications like digital imaging and video
 - UWB radios – WiMedia protocol stack at higher layers
- Task Group 4 (802.15.4)
 - Low data rates and ultra low power/complexity devices for sensor networking
 - Home automation, smart tags, interactive toys, location tracking, etc.
 - Zigbee is now part of this group

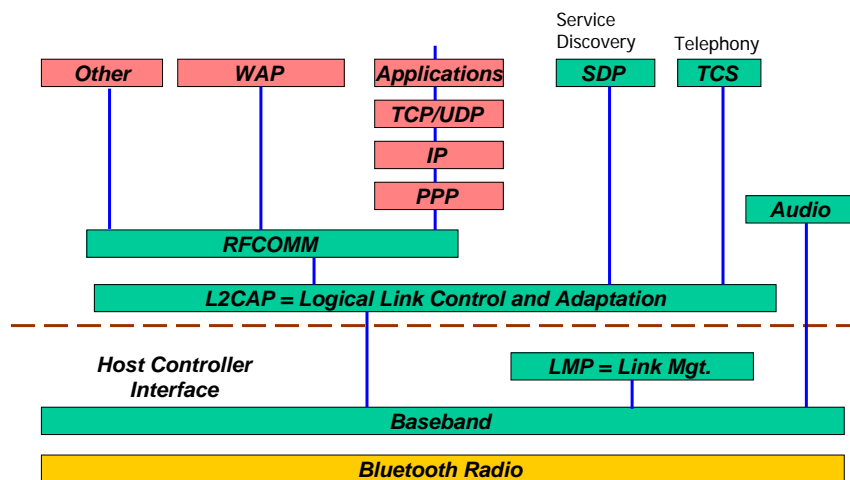


Bluetooth Protocol Architecture



- Bluetooth architecture has three types of protocols
 1. Core protocols
 - Radio
 - Baseband
 - Link manager protocol (LMP)
 - Logical link control and adaptation protocol (L2CAP)
 - Service discovery protocol (SDP)
 2. Cable replacement and Telephony protocols
 - RFCOMM
 - Telephony control specification – binary (TCS BIN)
 3. Adopted protocols
 - PPP
 - TCP/UDP/IP
 - WAP
 - Etc.

Example Protocol Stack



Bluetooth RF and Baseband Layers



- Operates in the same 2.4 GHz bands as IEEE 802.11b
- Channels are 1MHz wide (79 or 23 channels depending on country)
- Modulation :
 - GFSK at 1Mbps on air
 - Version 2.0 Enhanced Data Rate 2-level - GFSK : 2Mbps rate
- Error control depends on connection and rate either 1/3 convolutional coded FEC, 2/3 ccFEC, or ARQ
- Single chip implementation ~ \$8-10 a chip

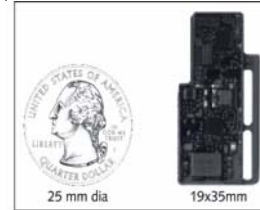


Figure 5-5 Bluetooth transceiver

Bluetooth FHSS



Employs *frequency hopping* spread spectrum

Reduce interference with other devices

Pseudorandom hopping
1600 hops/sec- time slot is defined as 625 microseconds

Packet 1-5 time slots long
TDD up/downlink
System is FH/FDMA/TDD

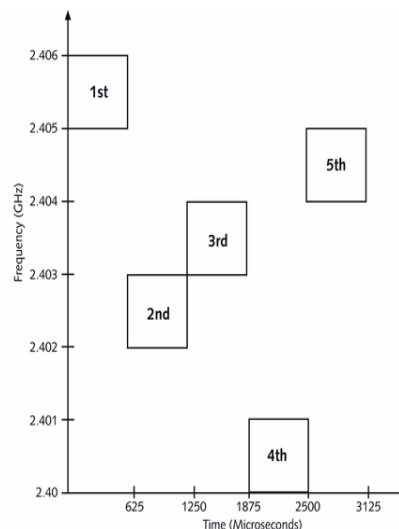


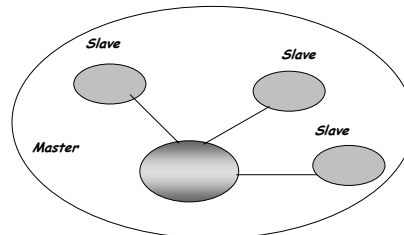
Figure 5-8 Bluetooth FHSS

Bluetooth Device Address



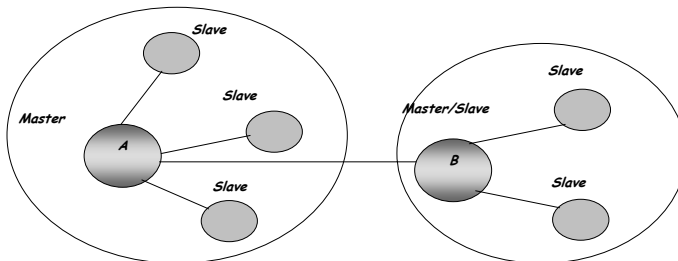
- Each Bluetooth device has a 48 bit IEEE 802 MAC address
 - Called the Bluetooth Device Address (BD_ADDR)
- This MAC address is split into three parts
 - The Non-significant Address Part (NAP)
 - Used for encryption seed
 - The Upper Address part (UAP)
 - Used for error correction seed initialization and FH sequence generation
 - The Lower Address Part (LAP)
 - Used for FH sequence generation
- Additional address fields are used once in a piconet
 - Active member address
 - Address valid as long as device is active slave in a piconet
 - Parked member address
 - Address valid as long as a device is a parked slave in a piconet

Bluetooth Architecture



- Scattered ad-hoc topology – called a “scatter-net”
- A “cell” or “piconet” is defined by a Master device
 - The master controls the frequency hopping sequence
 - The master also controls the transmission within its piconet using a TDMA structure
- There is NO contention within a piconet
- There is interference between piconets in the same geographic space

Bluetooth Architecture (2)

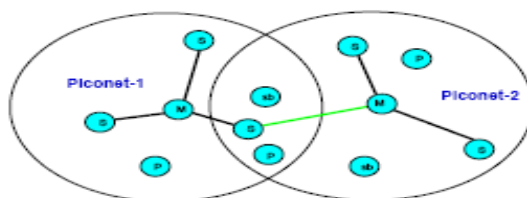


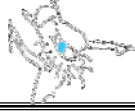
- A device can belong to several piconets
- A device can be the master of only one piconet
- A device can be the master of one piconet and slave of another piconet or a slave in different piconets

Bluetooth Architecture (3)



- The Master device is the device that initiates an exchange of data
- The Slave device is a device that responds to the Master
 - Slaves use the frequency hopping pattern specified by the Master
- A slave can transmit ONLY in response to a Master
- A Master device can simultaneously control seven slave devices and might have up to 200 slave devices in a piconet
- Multiple piconets in the same geographic space interfere with each other
 - FH-SS is used so multiple piconets can coexist in same space





Bluetooth connections



- Synchronous connection-oriented (SCO) link
 - “Circuit-switched”
 - periodic single-slot packet assignment
 - Symmetric 64 kbps full-duplex
 - Up to three simultaneous links from master
- Asynchronous connection-less (ACL) link
 - Packet data
 - Variable packet size (1-5 slots)
 - Asymmetric bandwidth – point to multipoint
 - Maximum Asymmetric rate: 723.2 kbps (57.6 kbps return channel)
 - Symmetric data rates: 108.8 - 432.6 kbps (see Table 13.1)
 - FEC/ARQ used for error control

Bluetooth Power Control



- Three classes of devices exist
 - Class 1: 100 mW (20 dBm) (~100m)
 - Class 2: 2.5 mW (4 dBm) (~10m)
 - Class 3: 1 mW (0 dBm) (~1m)
- Mixture of devices can exist in a piconet
- Range of devices is subject to their class
- Mandatory power control is implemented
 - Steps of 2 dB to 8 dB
 - Only the power required for adequate RSS is to be used
 - Based on feedback (closed loop) using link management protocol control commands



Clock Synchronization



- Each Bluetooth device has a free running clock called the native clock or CLKN
 - A Master device uses its CLKN for timing
 - A Slave device determines an offset from its own CLKN to synchronize to the Master
 - The Master also uses an offset to determine the slave's clock to establish an initial connection with a slave



Discovering Bluetooth Devices



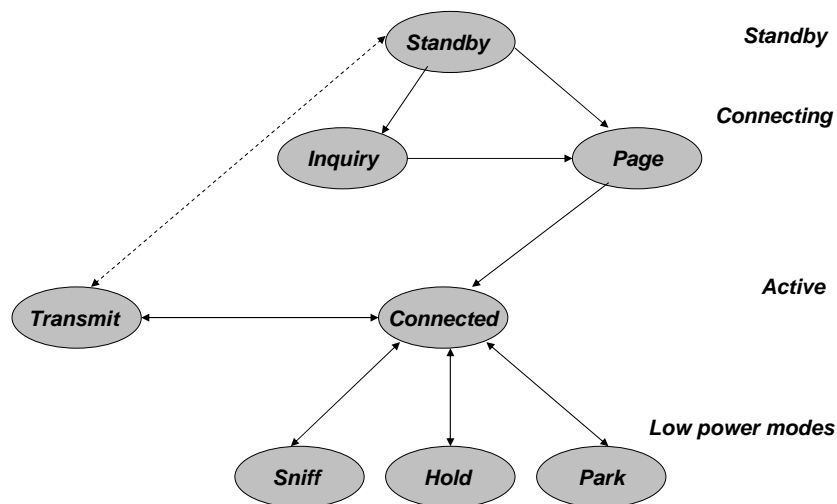
- A device wishes to discover what Bluetooth devices exist in its vicinity and what services they offer
- Performs an "inquiry" procedure
 - It transmits a series of inquiry packets on different frequencies and awaits a response
 - Devices scanning for inquiries use a sliding window to detect such inquiries
 - If an inquiry is detected by a scanning device it responds with a "frequency hop synchronization" (FHS) packet that enables completion of a successful connection
 - FHS contains ID and clock info
 - If collision occurs on inquiry – device implement random backoff and retries
 - Connection is established
 - Device that initiates connection is *master* in resulting piconet

Paging a device



- Paging is similar to “inquiry” except that the slave address is known
 - Slave clock/frequency hopping pattern is known
 - The page packet is transmitted at the expected frequency of the slave
- The Master sends a page train with a duration of 10 ms covering 16 frequency hops, repeat if necessary
- The Slave listens for its own device access code (DAC) for the duration of a scan window
- The Slave sends a “slave response” when its own DAC is heard
- The Master sends a “master response”
- The Slave responds to the master with its own DAC using the Master’s clock included in FHS packet

Bluetooth connection states



Connection States (2)



- Standby (default)
 - Waiting to join a piconet
- Inquire
 - Discover device within range or find out unknown destination address
- Page
 - Establish actual connection using device access code (DAC)
- Connected
 - Actively on a piconet (master or slave)
- Park/Hold/Sniff (Low-power connected states)
 - Hold mode stops traffic for a specified period of time
 - Sniff mode reduces traffic to periodic sniff slots
 - Park mode gives up its active member address and ceases to be a member of the piconet
- Active
 - Unit participates on channel – master schedule transmissions

Service Discovery



- After “inquiry” or “paging” an ACL or SCO is set up
- SCO is used for telephony or audio connection
- If ACL connection, the Master sets up an L2CAP connection with the slave
 - L2CAP is logical link control layer
 - Responsible for segmenting and reassembling data packets
 - L2CAP allows several protocols to be multiplexed over it using a Protocol and Service Multiplexer (PSM) number – emulates serial port
- The master’s service discovery client can use SDP to obtain the services that slave devices within the piconet can offer
- The Master can then decide what slave devices to communicate with and what services to employ



Service Discovery

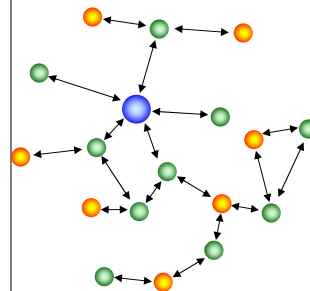


- After “inquiry” or “paging” an ACL or SCO is set up
- SCO is used for telephony or audio
- If ACL connection, the Master sets up an L2CAP connection with the slave
 - L2CAP is logical link control layer
 - Responsible for segmenting and reassembling data packets
 - L2CAP allows several protocols to be multiplexed over it using a Protocol and Service Multiplexor (PSM) number – emulates serial port
- The master’s service discovery client can use SDP to obtain the services that slave devices within the piconet can offer
- The Master can then decide what slave devices to communicate with and what services to employ

Link Manager



- The Link manager manages the following operations
 - Attaching slaves to the piconet
 - Allocates an active member address to a slave
 - Breaks connections to slaves
 - Establishes SCO or ACL links
 - Changes the connection state of devices (like sniff, park or hold)
- Uses the Link Management Protocol (LMP) to connect between devices



Comments



- A device can be part of several piconets simultaneously (scatternet)
 - This implies that the device should maintain multiple sets of clocks and timers and switch between them
 - The throughput of the device is substantially reduced compared to what it might have if connected to a single piconet
- Audio part of Bluetooth specifies different codecs
 - Supports A-law and μ -law for PCM
 - Also supports DPCM
- RFCOMM (Radio Frequency Virtual Communications Port Emulation)
 - Similar to RS-232 serial connections
- *No handoffs* between piconets for mobile users

Bluetooth Packet Fields



- Access code – used for timing synchronization, offset compensation, paging, and inquiry
- Header – used to identify packet type, packet numbering, slave address, error checking info and control info
- Payload – contains user voice, data or both and payload header, if present

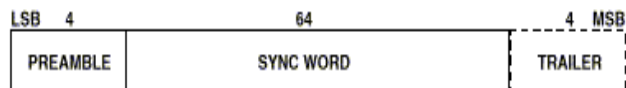
Baseband Frame Format



- General packet format



- Access code



- Payload

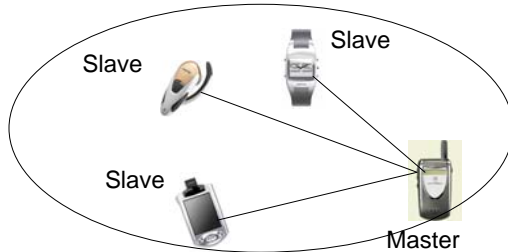
- Voice field: fixed length, 240 bits
- Data field: Payload header, body, CRC
<Header: single-slot vs. multi-slot packets>

Packet Header Fields



- AM_ADDR – contains “active mode” address of one of the slaves
- Type – identifies type of packet
- Flow – 1-bit flow control
- ARQN – 1-bit acknowledgment
- SEQN – 1-bit sequential numbering schemes
- Header error control (HEC) – 8-bit error detection code

Security



- Due to low radio range – security threat must be in very close range
- Link Management Protocol layer of Bluetooth provides security and encryption services
 - Security in piconet involves identifying device itself, not who is using device

- Three security mode in Bluetooth
 - Level 1: No security
 - Level 2: Service-level security is established after connection is made
 - Level 3: Link-level security is performed before a connection is made

Authentication



- Authentication involves verifying that a device should be allowed to join piconet
 - Bluetooth uses a challenge-response strategy to confirm that other device knows a shared identical secret key
 - Secret key entered as PIN by hand
 - Version 1.1 improves authentication process by first confirming roles of master and slave before generating response number

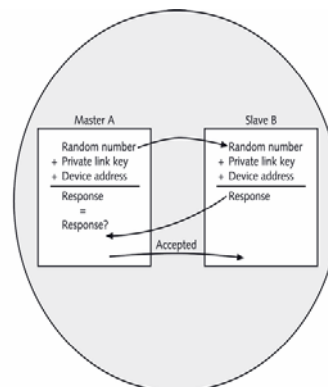


Figure 5-18 Authentication

Encryption



- Encoding communications ensures that transmissions cannot be intercepted and decoded
- Three encryption modes
 - Encryption Mode 1—Nothing is encrypted
 - Encryption Mode 2—Traffic from master to one slave is encrypted, but traffic from master to multiple slaves is not
 - Encryption Mode 3—All traffic is encrypted
 - Uses variable bit key (64 is default value)

State of Bluetooth



- Bluetooth shipped in over a 1 Billion devices
- Bluetooth challenges
 - Reduce Cost ~\$8-10 for port – versus \$5 for cable
 - Conflicts with other devices in radio spectrum
 - Limited security
- Most of the focus in the standards group is on other 802.15 tasks
- IEEE 802.15.4 for low power low data rate WPANs (Zigbee)
- IEEE 802.15.5 Mesh Networking WPANs
- IEEE 802.15.3 for high data rate WPANs (WiMedia) 802.15.3a focus is Ultra WideBand (UWB) WPANs

802.15.4 Standard

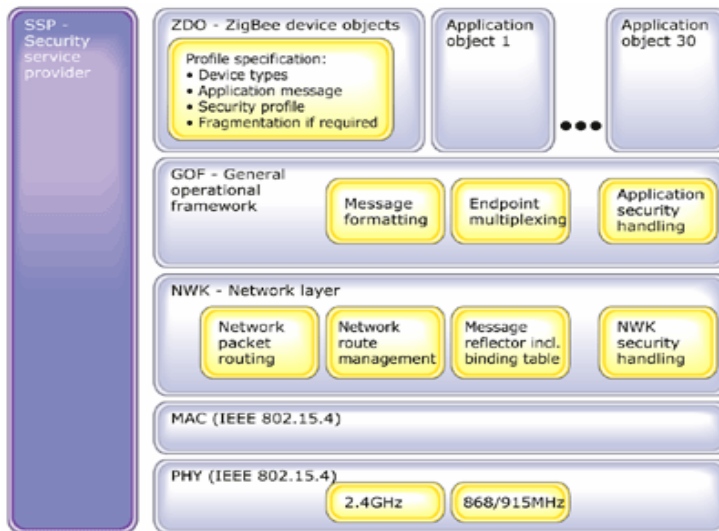


•Focus on low data rates/low power/moderate range/low complexity devices for WPAN sensor networks

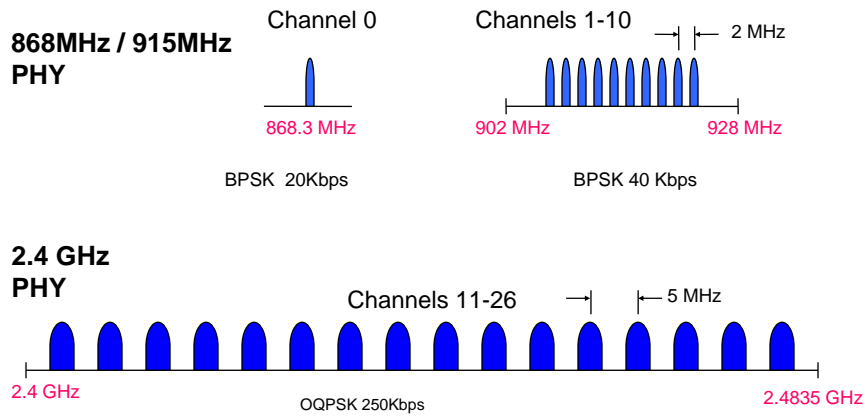
- Took over Zigbee interest group work
- Data rates of 250 kb/s, 40 kb/s and 20 kb/s.
- Distances 10-50 meters
- Star or Peer-to-Peer operation.
- Support for low latency devices.
- Full handshake protocol for transfer reliability.
- Very Low power consumption.
- Frequency Bands of Operation
 - 16 channels in the 2.4GHz ISM* band
 - 10 channels in the 915MHz ISM band
 - 1 channel in the European 868MHz band.
- Early applications: home/factory monitoring, medical monitoring



ZigBee Stack Architecture



IEEE 802.15.4 Frequency Bands

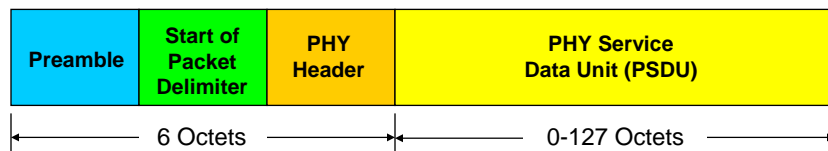


IEEE 802.15.4 PHY Packet Structure



PHY Packet Fields

- Preamble (32 bits) – synchronization
- Start of Packet Delimiter (8 bits)
- PHY Header (8 bits) – PSDU length
- PSDU (0 to 1016 bits) – Data field

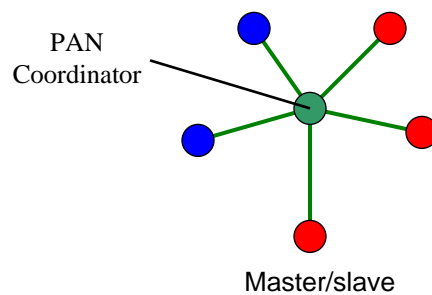


IEEE 802.15.4 Device Classes



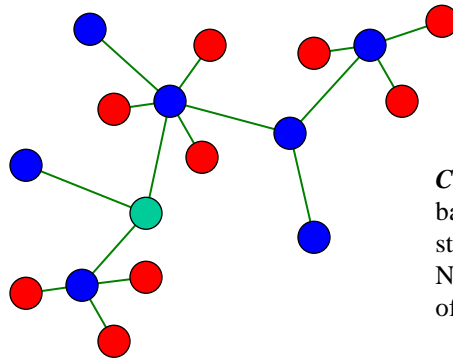
- Three Device Classes
 - Full function device (FFD)
 - Any topology
 - Can maintain connection to multiple devices
 - Talks to any other device
 - PAN Coordinator (PANC)
 - FFD responsible for starting and maintaining networks
 - First FFD powered on in a area becomes PANC
- Reduced function device (RFD)
 - Limited to star topology
 - Talks only to a network coordinator
 - Can not be a relay for other RFD or FFD
 - Very simple implementation – expect to transmit 0.1%-2% of the time → long battery life

IEEE 802.15.4 Topologies



- Full function device
- Reduced function device

IEEE 802.15.4 Topologies

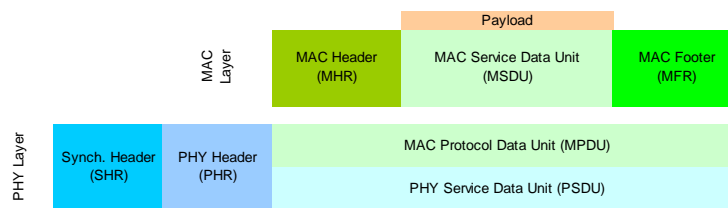


Clustered stars:
 basically a tree composed of multiple stars
 Note backbone/trunk of tree made up of FFDs

- Full function device
- Reduced function device

— Communications flow

IEEE 802.15.4 MAC Overview



Uses 802.15 64bit static MAC addresses

4 Types of MAC Frames:

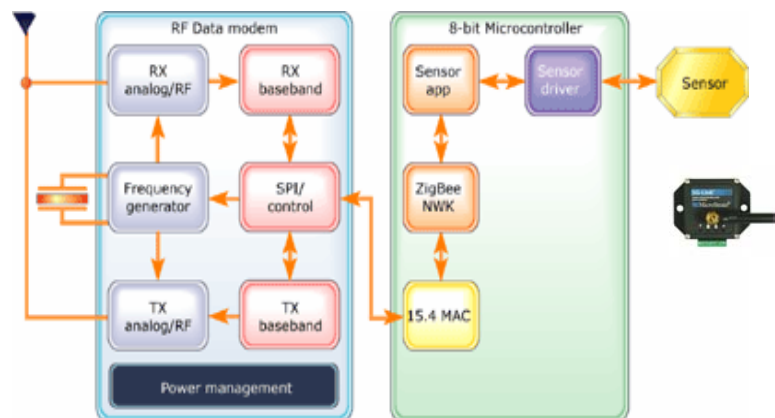
- Data Frame
- Beacon Frame – from PANC defines timeslots
- Acknowledgment Frame
- MAC Command Frame
- CSMA/CA is used except for synchronous traffic which get guaranteed time slots

IEEE 802.15.4 MAC



- Periodic data
 - Application defined rate (e.g. **sensors**)
- Intermittent data
 - Application/external stimulus defined rate (e.g. **light switch**)
- Repetitive low latency data
 - Allocation of time slots (e.g. **mouse**)
- Security
 - Three modes:
 1. Unsecured
 2. Access control list mode – devices only communicated with stored list of addresses
 3. Secured mode
 - Symmetric key for authentication and encryption with 4,6,8,12, 14 octets length key options
 - Frame/message integrity – (checksum like security feature)
 - Sequential freshness – frames numbered

Typical ZigBee-Enabled Device Design



Typical design consist of RF IC and 8-bit microprocessor with peripherals connected to an application sensor or actuators

Wireless Technology Comparison Chart



Standard	Bandwidth	Power Consumption	Protocol Stack Size	Stronghold	Applications
Wi-Fi	Up to 54Mbps	400+mA TX, standby 20mA	100+KB	High data rate	Internet browsing, PC networking, file transfers
Bluetooth	1Mbps	40mA TX, standby 0.2mA	~100+KB	Interoperability, cable replacement	Wireless USB, handset, headset
ZigBee	250kbps	30mA TX, standby 356 μ A	34KB/14KB	Long battery life, low cost	Remote control, battery-operated products, sensors

802.15.3 WPANS



- High Data Rate WPANS - Applications
 - Multimedia
 - Streaming audio and video
 - Interactive audio and video
 - Data
 - PDAs, PCs, printers
 - Projectors
 - Digital imaging
 - Still image and video
 - Camera to kiosk

Requirements



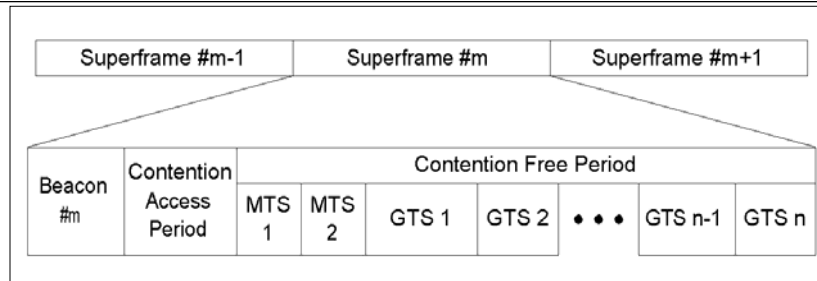
- Data rate and Range: 22 Mbps ~100m, 55Mbps ~50m
- QoS capable
- Security
- Quick join/unjoin
- Basic security/authentication
- Low power, cost, size, complexity
- Piconet, not network connectivity
- Connect up to 256 devices in a Piconet

Qualities of the 802.15.3 MAC



- PAN Coordinator (PNC) – Device (DEV) topology
 - PNC assigns time for connections
 - Commands go to and come from the PNC.
- Communication is peer-to-peer
- Quality of Service
 - TDMA architecture with guaranteed time slots (GTSs)
- Security and Authentication
 - No Security Mode
 - Security Mode – uses AES with 128 bit key
 - Security Key for encryption key distribution
 - Authentication Key for Challenge/Response auth.

Basic structure is the superframe



3 parts to the superframe

- Beacon
- Contention Access Period (CAP)
- Contention Free Period (CFP)
 - CFP has GTSs and MTSs

Access methods



- Beacon
 - TDMA, only sent by the PNC
- CAP (Contention Access Period)
 - CSMA/CA, types of data and commands can be restricted by PNC
 - PNC can replace the CAP with management time slots (MTSs) using slotted-aloha access.
- CFP (Contention Free Period)
 - TDMA, assigned by the PNC
 - GTSs are unidirectional

PNC selection/handover



- Alternate coordinators (ACs) broadcast capabilities
- Based on criteria, “best” AC is chosen and becomes the PNC
- PNC begins to issue beacon
- PNC hands over task if more “capable” AC joins the piconet
 - Exception only if security policy is verified

Commands



- Commands support:
- PNC selection and handover
 - Association and disassociation
 - Information request commands
 - Repeater service
 - Power management commands
 - Device information
 - Retransmission
 - Request and modify GTS allocations

MAC support



- Peer Discovery
- Multirate support
- Repeater service
- Dynamic channel selection
- Power management
- Transmit power control

Physical Layer Characteristics



- 2.4 GHz band
 - Unlicensed operation
 - 15 MHz RF bandwidth
 - 3 or 4 non-overlapping channels
 - Similar to 802.11 for coexistence
- 5 data rates
 - 11-55 Mb/s with multi-bit symbols and coding
 - Use Trellis Coded Modulation (TCM) for coding

Modulation and Rates



Modulation	Coding	Data rate	Sensitivity
QPSK	8 state TCM	11 Mb/s	-82 dBm
DQPSK	None	22 Mb/s	-75 dBm
16-QAM	8 state TCM	33 Mb/s	-74 dBm
32-QAM	8 state TCM	44 Mb/s	-71 dBm
64-QAM	8 state TCM	55 Mb/s	-68 dBm

TCM was originally used in phone modems, many publications > 20 years old – type of FEC allows correction of 1 bit error – detect multiple errors

Equipment when???

Evolving Hybrid Network

