Wireless Protocols for Internet of Things: Part I – Wireless Personal Area Networks

Raj Jain
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@cse.wustl.edu

These slides and audio/video recordings of this class lecture are at: http://www.cse.wustl.edu/~jain/cse574-14/
Overview

1. Internet of Things and Wireless Protocols for IoT
2. IEEE 802.15.4: Topologies, MAC, PHY
4. IEEE 802.15.4e Enhancements

Note: This is the 2\textsuperscript{nd} lecture in series of class lectures on IoT. Bluetooth and Bluetooth Smart are also used in IoT and were covered in the previous lectures. Future lectures will cover ZigBee and other protocols.
Machine-to-Machine (M2M)

- 1.1 Billion smart phones
- 244 Million smart meters
- 487 Million e-readers and tablets
- 2.37 Billion networked office devices
- 86 Million medical devices
- 45 Million connected automobiles
- 547 Million connected appliances
- 105 Million connected military devices
- 431 Million information technology devices
- 45 Million supervisory control and data acquisition (SCADA)
- 5+ Billion other (non-phone/tablet/e-reader) electronic devices


(Safari Book)

Washington University in St. Louis

http://www.cse.wustl.edu/~jain/cse574-14/

©2014 Raj Jain
Internet of Things

- Only 1% of things around us is connected. Refrigerator, car, washing machine, heater, a/c, garage door, should all be connected but are not.

- From 10 Billion today to 50 Billion in 2020 Should include processes, data, things, and people.

- $14 Trillion over 10 years
  ⇒ Third in the list of top 10 strategic technologies by Gartner (After Mobile devices, Mobile Apps, but before Clouds, …)

- a.k.a. Internet of Everything by Cisco
  Smarter Planet by IBM
  Industrial Internet by GE
  Cyber-Physical Systems (CPS)
  Internet of European Things (more popular in Europe)

Ref: “Gartner Identifies Top 10 Strategic Technologies,”
Ref: J. Bradley, “The Internet of Everything: Creating Better Experiences in Unimaginable Ways,” Nov 21, 2013,
Washington University in St. Louis http://www.cse.wustl.edu/~jain/cse574-14/
Wireless Protocols for IoT

- IEEE 802.11*
- Bluetooth/Bluetooth Smart*
- ZigBee/ZigBee Smart Energy 2.0
- IEEE 802.15.6-2012: Body Area Networking
- Wireless HART (Highway Addressable Remote Transducer Protocol)
- International Society of Automation (ISA) 100.11a
- Z-Wave
- MiWi (Microchip Technology Wireless)
- ANT+
- Wireless MBUS

*Note: Already covered in previous lectures of this course.
Other Protocols for IoT

- Powerline Communications (PLC)*
- 6LowPAN (IPv6 over Low Power Personal Area Networks)§
- Routing Protocol for Low Power and Lossy Networks (RPL)§
- ETSI M2M Architecture
- MQ Telemetry Transport (MQTT)
- BACnet
- LonWorks
- ModBus
- KNX
- ANSI CI-12

## IEEE 802.15.4

- Used by several “Internet of Things” protocols: ZigBee, 6LoWPAN, Wireless HART, MiWi, and ISA 100.11a

<table>
<thead>
<tr>
<th>Application</th>
<th>ZigBee</th>
<th>6LoWPAN</th>
<th>Wireless HART</th>
<th>MiWi</th>
<th>ISA 100.11a</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAC</td>
<td>802.15.4</td>
<td>802.15.4</td>
<td>802.15.4</td>
<td>802.15.4</td>
<td>802.15.4</td>
</tr>
<tr>
<td>PHY</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
IEEE 802.15.4 Overview

- Low Rate Wireless Personal Area Network (LR-WPAN)
- 2.4 GHz (most common). 16 5-MHz channels
- 250 kbps PHY \(\Rightarrow\) 50 kbps application data rate
- Peak current depends upon symbol rate \(\Rightarrow\) multilevel 4b/symbol)
- Similar to 802.11: Direct Sequence Spread Spectrum, CSMA/CA, Backoff, Beacon, Coordinator (similar to Access point)
- Lower rate, short distance \(\Rightarrow\) Lower power \(\Rightarrow\) Low energy
- Each node has a 64-bit Extended Unique ID (EUI-64):
  
  | U/M | G/L | OUI | 40 bits assigned by the manufacturer |
  | 1b  | 1b  | 22b | 40b |

- No segmentation/reassembly. Max MAC frame size is 127 bytes with a payload of 77+ bytes.
IEEE 802.15.4 Topologies

- Star and peer-to-peer
- Two types of devices: Full Function device (FFD), Reduced Function device (RFD)

Ref: IEEE 802.15.4-2011
Washington University in St. Louis
http://www.cse.wustl.edu/~jain/cse574-14/
©2014 Raj Jain
Coordinator

- FFDs can become coordinator and can also route messages to other nodes
- RFDs cannot become coordinator and can only be a leaf
- FFD that starts a PAN becomes the coordinator
- In star topology, all communication is to/from the coordinator
- In P2P topology, FFDs can communicate directly also.
- Each piconet has a PAN ID and is called a cluster.
- Nodes join a cluster by sending association request to the coordinator. Coordinator assigns a 16-bit short address to the device. Devices can use either the short address or EUI-64 address.
Cluster Tree Network

- A coordinator can ask another FFD to become a coordinator for a subset of nodes. Tree ⇒ No loops

Diagram:
- First PAN Coordinator
- Pan Coordinators
- Full Function Device
- Reduced Function Device

Ref: IEEE 802.15.4-2011
Washington University in St. Louis
http://www.cse.wustl.edu/~jain/cse574-14/
IEEE 802.15.4 MAC

Beacon-Enabled CSMA/CA

- Coordinator sends out beacons periodically
- Part of the beacon interval is inactive ⇒ Everyone sleeps
- Active interval consists of 16 slots
- Guaranteed Transmission Services (GTS): For real-time services. Periodic reserved slots.
- Other slots are available for contention. Slotted CSMA.

Ref: IEEE 802.15.4-2011
Washington University in St. Louis  http://www.cse.wustl.edu/~jain/cse574-14/
**IEEE 802.15.4 MAC (Cont)**

- **Beaconless Operation**: Unslotted CSMA
  - If coordinator does not send beacons, there are no slots
- Acknowledgements if requested by the sender.
- Short inter-frame spacing (SIFS) if previous transmission is shorter than a specified duration. Otherwise, Long inter-frame spacing (LIFS)

**Acknowledged Transmissions**

- Long Frame
  - ACK
  - Short Frame
  - ACK
  - t\(_{\text{ack}}\)
  - LIFS
  - SIFS

**Unacknowledged Transmissions**

- Long Frame
  - Short Frame
  - LIFS
  - SIFS

Washington University in St. Louis  
http://www.cse.wustl.edu/~jain/cse574-14/  
©2014 Raj Jain
802.15.4 CSMA/CA

- Wait until the channel is free.
- Wait a random back-off period
  If the channel is still free, transmit.
- If the channel is busy, backoff again.
  Backoff exponent limited to 0-2 in battery life-extension mode.
- Acknowledgement and Beacons are sent without CSMA-CA.
# MAC Frame Format

<table>
<thead>
<tr>
<th>Frame Control</th>
<th>Seq. #</th>
<th>Dest. PAN Id</th>
<th>Dest. Addr.</th>
<th>Src PAN Id</th>
<th>Src Addr.</th>
<th>Aux. Security Header</th>
<th>Payload</th>
<th>FCS</th>
</tr>
</thead>
<tbody>
<tr>
<td>16b</td>
<td>8b</td>
<td>0/16b</td>
<td>0/16/64b</td>
<td>0/16b</td>
<td>0/16/64b</td>
<td>0/40/48/80/70b</td>
<td></td>
<td>16b</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Frame Type</th>
<th>Security enabled</th>
<th>Frame Pending</th>
<th>Ack Reqd</th>
<th>PAN Id Compression</th>
<th>Rsvd</th>
<th>Dest. Addr. Mode</th>
<th>Frame version</th>
<th>Src. Addr. mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>Beacon</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>001</td>
<td>Data</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>010</td>
<td>Ack</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>01</td>
<td>01</td>
</tr>
<tr>
<td>011</td>
<td>MAC Command</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>Other</td>
<td>Reserved</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>11</td>
<td>11</td>
</tr>
</tbody>
</table>

- **Frame Type**
  - 000: Beacon
  - 001: Data
  - 010: Ack
  - 011: MAC Command
  - Other: Reserved

- **PAN Id and Addr**
  - 00: PAN Id and Addr no present
  - 01: Reserved
  - 10: 16-bit short address
  - 11: 64-bit extended address

Ref: IEEE 802.15.4-2011
Washington University in St. Louis
[http://www.cse.wustl.edu/~jain/cse574-14/](http://www.cse.wustl.edu/~jain/cse574-14/)
©2014 Raj Jain
**IEEE 802.15.4-2011 PHY Bands**

<table>
<thead>
<tr>
<th>PHY (MHz)</th>
<th>Band (MHz)</th>
<th>kchip/s</th>
<th>Modulation</th>
<th>kb/s</th>
<th>ksymbols/s</th>
</tr>
</thead>
<tbody>
<tr>
<td>2450 DSSS</td>
<td>2400-2483.5</td>
<td>2000</td>
<td>O-QPSK</td>
<td>250</td>
<td>62.5</td>
</tr>
<tr>
<td>2450 CSS</td>
<td>2400-2483.5</td>
<td></td>
<td></td>
<td>250</td>
<td>167</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1000</td>
<td>167</td>
</tr>
<tr>
<td>915 (USA)</td>
<td>902-928</td>
<td>600</td>
<td>BPSK</td>
<td>40</td>
<td>40</td>
</tr>
<tr>
<td></td>
<td>902-928</td>
<td>1600 (PSS)</td>
<td>ASK</td>
<td>250</td>
<td>50</td>
</tr>
<tr>
<td></td>
<td>902-928</td>
<td>1000</td>
<td>O-QPSK</td>
<td>250</td>
<td>62.5</td>
</tr>
<tr>
<td>868 (Europe)</td>
<td>868-868.06</td>
<td>300</td>
<td>BPSK</td>
<td>20</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>868-868.06</td>
<td>400 (PSS)</td>
<td>ASK</td>
<td>250</td>
<td>12.5</td>
</tr>
<tr>
<td></td>
<td>868-868.06</td>
<td>400</td>
<td>O-QPSK</td>
<td>100</td>
<td>25</td>
</tr>
<tr>
<td>780 (China)*</td>
<td>779-787</td>
<td>1000</td>
<td>O-QPSK</td>
<td>250</td>
<td>62.5</td>
</tr>
<tr>
<td>950 (Japan)</td>
<td>950-956</td>
<td>-</td>
<td>GFSK</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>950-956</td>
<td>300</td>
<td>BPSK</td>
<td>20</td>
<td>20</td>
</tr>
<tr>
<td>UWB Sub-GHz</td>
<td>250-750</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UWB Low Band</td>
<td>3244-4742</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UWB High Band</td>
<td>5944-10234</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Note: 314-316 MHz and 430-434 MHz bands are also used in China.*
IEEE 802.15.4-2011 PHYs

1. **Offset Quadrature Phase Shift Keying** (O-QPSK) modulation with Direct Sequence spread spectrum (DSSS). DSSS reduces the settling time and lock time.

2. **Binary Phase Shift Keying** (BPSK) modulation with DSSS Phy.

3. **Amplitude Shift Keying** (ASK) with Parallel Sequence Spread Spectrum (PSSS).

4. **Chirp Spread Spectrum** (CSS) with Differential Quadrature Phase-shift keying (DQPSK) modulation.

5. **Ultra-Wide Band** (UWB) with combined Burst Position modulation (BPM) and BPSK modulation.

6. **m-ary Phase-Shift Keying** (MPSK) modulation (m=4 ⇒ QPSK).

7. **Gaussian Frequency-Shift Keying** (GFSK).
Offset-QPSK

- Offset-QPSK: QPSK ⇒ Max 180 phase difference ⇒ Large amplitude shifts after low pass filtering
- O-QPSK ⇒ Change 1-bit at a time
  1st-bit of the 2-bit symbol is used to change I-component
- 2nd-bit of the 2-bit symbol is used to change Q-Component and Q is offset by 1 bit ⇒ Max 90 phase difference ⇒ Smaller amplitude shifts after filtering

Washington University in St. Louis
http://www.cse.wustl.edu/~jain/cse574-14/
Parallel Sequence Spread Spectrum

- Direct Sequence Spread Spectrum uses a L-bit bi-polar spreading code $A = \{a_1, a_2, \ldots, a_L\}$, $a_k \in \{+1, -1\}$
- By cyclically shifting the spreading code, $k$ other uni-polar spreading codes are obtained:
  $B_i = \{b_{i,1}, b_{i,2}, \ldots, b_{i,L}\}$, $b_{i,k} = (a_{(k+i) \mod L} + 1)/2 \in \{1, 0\}$
- These spreading codes are applied to the data sequence in parallel and a $k$-ary sum is transmitted
- Increases the resistance to multipath fading

Ref: H. Schwetlick, “PSSS-Parallel Sequence Spread Spectrum – A Potential Physical Layer for OBAN?,”
http://oban.tubit.tu-berlin.de/5-PSSS-Schwetlick.pdf
Washington University in St. Louis http://www.cse.wustl.edu/~jain/cse574-14/ ©2014 Raj Jain
Chirp Spread Spectrum

- **Chirp**: A signal with continuously increasing (or decreasing) frequency (Whale sound)
- **Chirp Spread Spectrum**: signal is frequency modulated with frequency is increasing (or decreasing) from min to max (or max to min) ⇒ power is *spread* over the entire spectrum

An impulse in time domain results in a ultra wide spectrum in frequency domain and essentially looks like a white noise to other devices.
**Ultra-Wideband (UWB)**

- FCC rules restrict the maximum noise generated by a wireless equipment (0 dBm = 1mW, -40 dBm = 0.1 μW)
- It is possible to generate very short (sub-nano sec) pulses that have spectrum below the allowed noise level
  \(\Rightarrow\) Possible to get Gbps using 10 GHz spectrum
- FCC approved UWB operation in 2002
- UWB can be used for high-speed over short distances
- UWB can see through trees and underground (radar)
  \(\Rightarrow\) collision avoidance sensors, through-wall motion detection
- Position tracking: cm accuracies. Track high-value assets

<table>
<thead>
<tr>
<th>Power dBm/MHz</th>
<th>0</th>
<th>-40</th>
</tr>
</thead>
<tbody>
<tr>
<td>GHz</td>
<td>2</td>
<td>4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cell phones</th>
</tr>
</thead>
<tbody>
<tr>
<td>FCC Part 15 Limit = -41.3 dBm/MHz</td>
</tr>
</tbody>
</table>

Graph showing the comparison of power and cell phones with the FCC Part 15 Limit.
Sub-nanosecond impulses are sent many million times per second.

Became feasible with high-speed switching semiconductor devices.

Pulse width = 25 to 400 ps.

Impulses may be position, amplitude, or polarity modulated.

0.25 ns Impulse $\Rightarrow$ 4 B pulses/sec $\Rightarrow$ 100's Mbps.

802.15.4 uses pulse position and binary phase shift keying modulation.
Advantages of UWB

- Very low energy consumption: Good Watts/Mbps
- Line of sight not required. Passes through walls.
- Sub-centimeter resolution allows precise motion detection
- Pulse width much smaller than path delay
  - Easy to resolve multipath
  - Can use multipath to advantage
- Difficult to intercept (interfere)
- All digital logic ⇒ Low cost chips
- Small size: 4.5 mm² in 90 nm process for high data rate designs
Direct sequence (DS-UWB)

- Championed by Motorola/XtremeSpectrum
- Uses CDMA with multiple chips per bit
- Chips are encoded using pulse
- This is the scheme used in 802.15.4
- Low power density $\Rightarrow$ Good for body area network
IEEE 802.15.4e Enhancements

- Low latency deterministic operation: pre-assigned slots
- Channel adaptation: Different channels used by different nodes for contention free period
- Time slotted channel hopping: Higher layers coordinate the slot allocation along with its frequency. Good for harsh industrial environments.
- Each device can select its listening channel
- Transmitter and receiver coordinate their cycles (very low duty cycle)
- Transmit only when requested by receiver
Summary

1. IoT fueled initially by smart grid is resulting in several competing protocols: BlueTooth Smart, ZigBee Smart, ...
2. IEEE 802.15.4 is a low-data rate wireless personal area network and is the PHY and MAC layer used by many IoT protocols, such as ZigBee, and WirelessHART.
3. 802.15.4 uses full function and reduced function devices. FFDs can act as coordinator. Allows a star, mesh, or a cluster tree topology. Uses slotted/unslotted CSMA/CA. Supports Guaranteed transmission services for low-latency application.
5. UWB allows transmission with very low average power spread over a large band.
Reading List

Wikipedia Pages

- http://en.wikipedia.org/wiki/IEEE_802.15.4
- http://en.wikipedia.org/wiki/IEEE_802.15.4a
- http://en.wikipedia.org/wiki/Carrier_sense_multiple_access_with_collision_avoidance
- http://en.wikipedia.org/wiki/Personal_area_network
References

Acronyms

- 6LowPAN: IPv6 over Low Power Personal Area Network
- AMCA: Asynchronous Multi-Channel Adaptation
- ANSI: American National Standards Institute
- ANT: Name of a company
- ASK: Amplitude Shift Keying
- BPM: Burst Position Modulation
- BPSK: Binary Phase Shift Keying
- CDMA: Code Division Multiple Access
- COSEM: Company Specification for Energy Metering
- CPS: Cyber-Physical Systems
- CRC: Cyclic Redundancy Check
- CSL: Coordinated Sampled Listening
- CSMA: Carrier Sense Multiple Access
- CSMA/CA: Carrier Sense Multiple Access with Collision Avoidance
- CSS: Chirp Spread Spectrum
- dBm: deci-Bell milli-Watt
### Acronyms (Cont)

- **DLMS**: Device Language Message Specification
- **DQPSK**: Differential Quadrature Phase-shift keying
- **DSME**: Deterministic and Synchronous Multi-Channel Extension
- **DSSS**: Direct Sequence Spread Spectrum
- **ETSI**: European Telecommunications Standards Institute
- **EUI-64**: Extended Unique Identifier
- **FCC**: Federal Communications Commission
- **FFD**: Full Function device
- **FSK**: Frequency Shift Keying
- **GFSK**: Gaussian Frequency-Shift Keying
- **GHz**: Giga Hertz
- **GTS**: Guaranteed Transmission Services
- **HART**: Highway Addressable Remote Transducer Protocol
- **ID**: Identifier
- **IEEE**: Institution of Electrical and Electronics Engineer
- **IoT**: Internet of Things
Acronyms (Cont)

- ISA: International Society of Automation
- LECIM: Low energy critical infrastructure monitoring
- LIFS: Long Inter-frame Spacing
- LLDN: Low-Latency Deterministic Network
- LR-WPAN: Low-Rate Wireless Personal Area Networks
- MAC: Media Access Control
- MHz: Mega Hertz
- MPSK: m-ary Phase-Shift Keying
- OFDM: Orthogonal Frequency Division Multiplexing
- OUI: Organizationaly Unique Identifier
- PAN: Personal Area Network
- PCA: Priority Channel Access
- PHY: Physical Layer
- PLC: Powerline Communications
- PPDU: Physical Layer Protocol Data Unit
- PSSS: Parallel Sequence Spread Spectrum
Acronyms (Cont)

- **QPSK**: Quadrature Phase Shift Keying
- **RFD**: Reduced Function device
- **RFID**: Radio Frequency Identifier
- **RIT**: Receiver Initiated Transmission
- **RPL**: Routing Protocol for Low Power and Lossy Networks
- **RX**: Receiver
- **SCADA**: Supervisory control and data acquisition
- **SIFS**: Short inter-frame spacing
- **SUN**: Smart metering utility network
- **TSCH**: Time Slotted Channel Hopping
- **UWB**: Ultra Wide Band
- **WirelessHART**: Wireless Highway Addressable Remote Transducer Protocol
- **WPAN**: Wireless Personal Area Network