UG103.1

EMBER® APPLICATION DEVELOPMENT FUNDAMENTALS: WIRELESS NETWORKING

This document introduces some fundamental concepts of wireless networking. These concepts are referred to in other *Ember Application Development Fundamentals d*ocuments. If you are new to wireless networking, you should read this document first.

New in This Revision

Initial release (contents previously published).

Contents

1 Overview 2
2 Embedded Networking 2
3 Radio Fundamentals 3
3.1 Frequency Bands 4
3.2 Signal Modulation 4
3.3 Antennas 5
3.4 How Far Signals Travel 5
3.4.1 Radio Transmit Power 5
3.4.2 Signal Degradation 6
3.4.3 How Far Can the Radio Signal Go 6
4 Networking: Basic Concepts 7
5 Wireless Networking 7
6 Ember ZigBee Devices 7
6.1 Network Formation and Operation 9

1 Overview

As embedded system design has evolved, the need for networking support has become a basic design requirement. Like more general-purpose computers, embedded systems have moved toward wireless networking. Most wireless networks have pushed toward ever-higher data rates and greater point-to-point ranges. But not all design applications require high-end wireless networking capabilities. Low-data-rate applications have the potential to outnumber the classic high-data-rate wireless networks world wide. Simple applications such as lighting control, smart utility meters, HVAC control, fire/smoke/CO alarms, remote doorbells, humidity monitors, energy usage monitors, and countless others devices function very well with low-data-rate monitoring and control systems. The ability to install such devices without extensive wiring decreases installation and maintenance costs. Increased efficiencies and cost savings are the primary motives behind this applied technology.

A wireless sensor network (WSN) is a wireless network consisting of distributed devices using sensors at different locations to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion, or pollutants.

In addition to one or more sensors, each node in a sensor network is typically equipped with a radio transceiver or other wireless communications device, a small microcontroller, and an energy source, usually a battery. The size of a single sensor node can vary from shoebox-sized nodes down to devices the size of coins. The cost of sensor nodes is similarly variable, ranging from hundreds of dollars to a few dollars, depending on the size of the sensor network and the complexity required of individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed, and bandwidth.

Wireless personal area networks have emerged as a result of the IEEE 802.15.4 standard for low data rate digital radio connections between embedded devices. The ZigBee Alliance was formed to standardize industry efforts to supply technology for networking solutions that are based on 802.15.4, have low data rates, consume very little power, and are therefore characterized by long battery life. The ZigBee Standard makes possible complete and cost-effective networked homes and similar buildings where all devices are able to communicate for monitoring and control.

2 Embedded Networking

While the term wireless network may technically be used to refer to any type of network that functions without the need for interconnecting wires, the term most commonly refers to a telecommunications network, such as a computer network. Wireless telecommunications networks are generally implemented with radios for the carrier or physical layer of the network.

One type of wireless network is a wireless local area network, or LAN. It uses radio instead of wires to transmit data back and forth between computers on the same network. The wireless LAN has become commonplace at hotels, coffee shops, and other public places. The wireless personal area network (WPAN) takes this technology into a new area where the distances required between network devices is relatively small and data throughput is low.

In the control world, embedded systems have become commonplace for operating equipment using local special-purpose computer hardware. Wired networks of such devices are now common in manufacturing environments and other application areas. Like all computer networks, the interconnecting cable systems and supporting hardware are messy, costly, and sometimes difficult to install. To overcome these problems, wireless networking of embedded systems (that is, embedded networking) has become commonplace. However, the costly embedded networking solutions have only been justifiable in high-end applications where the costs are a secondary consideration. Low cost applications with low data rate communications requirements did not have a good standardized solution until the IEEE 802.15.4 standard for wireless personal area physical layer and medium access control layer (MAC) was released in 2003.[1]

[1] The current version as of this writing is the IEEE 802.15.4-2006 standard.

The ZigBee Alliance was formed to establish networking and application-level standards on top of the IEEE 802.15.4 standards, to allow flexibility, reliability, and interoperability. More recently, working groups (WG) have been formed within the Internet Engineering Task Force (IETF) to establish open standard approaches for routing (roll WG) and interfacing low-powered wireless devices to an IPV6 networks (6lowPan WG). Once these IETF working groups establish the standards, the role of the ZigBee Alliance shifts from setting standards to standards selection, compliance testing, and marketing.

Although wireless networks eliminate messy cables and enhance installation mobility, the downside is the potential for interference that might block the radio signals from passing between devices. This interference may be from other wireless networks or from physical obstructions that interfere with the radio communications. Interference from other wireless networks can often be avoided by using different channels. ZigBee, for example, has a channel-scanning mechanism on start-up of a network to avoid crowded channels. Standards-based systems, such as ZigBee and WiFi, use mechanisms at the medium access control layer to allow channel sharing. In addition, ZigBee provides an interoperable standard for multi-hop wireless networking, allowing signals to reach their destination by traveling through multiple relay points. ZigBee networks can be comprised of many such relay points or “routers”, each one within range of one or more other routers, creating an interconnected “mesh” of devices that can provide redundant paths for data within the network that are automatically rediscovered and used to avoid interference in a local area. This concept is collectively referred to as “mesh networking”.

Another potential problem is that wireless networks may be slower than those that are directly connected through a cable. Yet not all applications require high data rates or large data bandwidth. Most embedded networks function very well at reduced throughputs. Application designers need to ensure their system data rates are within the range achievable with the system being used.

Wireless network security is also a problem, since the data can easily be overheard by eavesdropping devices. ZigBee has a set of security services designed around AES 128 encryption, so that application designers have a choice of security levels based on the needs of their applications. Careful design around these standards helps maintain high levels of network security.

Other networking standards exist such as Bluetooth. Each standard has its own unique strengths and essential areas of application. In the case of Bluetooth and ZigBee, the bandwidth of Bluetooth is 1 Mbps, while ZigBee's is one-fourth of this value. The strength of Bluetooth lies in its ability to allow interoperability and replacement of cables. ZigBee’s strength is low cost, long battery life, and mesh networks for large network operation. Bluetooth is meant for point-to-point applications such as handsets and headsets, whereas ZigBee is focused on the sensors and remote controls market, large distributed networks, and highly reliable mesh networking.

The *Fundamentals: ZigBee* document provides an in-depth discussion of the ZigBee Alliance, its efforts to standardize IEEE 802.15.4-based applications, and the characteristics of a ZigBee solution.

3 Radio Fundamentals

Radio is the wireless transmission of signals by modulation of electromagnetic waves with frequencies below those of visible light. Electromagnetic waves are, in the case of radio, a form of non-ionizing radiation, which travels by means of oscillating electromagnetic fields that pass through electrical conductors, the air, and the vacuum of space. Electromagnetic radiation does not require a medium of transport like a sound wave. Information can be imposed on electromagnetic waves by systematically changing (modulating) some property of the radiated waves, such as their amplitude or their frequency. When radio waves pass an electrical conductor, the oscillating fields induce an alternating current in the conductor. This can be detected and transformed into sound or other signals that reproduce the imposed information.

The word 'radio' is used to describe this phenomenon and radio transmission signals are classed as *radio frequency emissions*. The range or spectrum of radio waves used for communication has been divided into arbitrary units for identification. The FCC and NTIA arbitrarily define the radio spectrum in the United States as that part of

the natural spectrum of electromagnetic radiation lying between the frequency limits of 9 kilohertz and 300 gigahertz, divided into various sub-spectrums for convenience.

The following names are commonly used to identify the various sub-spectrums:

3 kHz to 30 kHz	Very Low Frequencies (VLF)
30 kHz to 300 kHz	Low Frequencies (LF)
300 kHz to 3,000 kHz	Medium Frequencies (MF)
3,000 kHz to 30,000 kHz	High Frequencies (HF)
30,000 kHz to 300,000 kHz	Very High Frequencies (VHF)
300,000 kHz to 3,000,000 kHz	Ultra High Frequencies (UHF)
3,000,000 kHz to 30,000,000 kHz	Super High Frequencies (SHF)
30,000,000 kHz to 300,000,000 kHz	Extremely High Frequencies (EHF)

Each of the sub-spectrums listed above are further subdivided into many other sub-portions or 'bands.' For example, the American AM Broadcast Band extends from 535 kHz to 1705 kHz, which is within the portion of the spectrum classified as *Medium Frequencies*.

3.1 Frequency Bands

The radio spectrum is regulated by government agencies and by international treaties. Most transmitting stations, including commercial broadcasters, military, scientific, industrial, and amateur radio stations, require a license to operate. Each license typically defines the limits of the type of operation, power levels, modulation types, and whether the assigned frequency bands are reserved for exclusive or shared use. Three frequency bands can be used for transmitting radio signals without requiring licensing from the United States Government:

900 MHz: The 900 MHz band was used extensively in different countries for different products including pages and cellular devices.

This band was considered to have good range characteristics. However it can be less popular for products because it is not a worldwide unlicensed band, and products therefore need to be modified depending on where they are being used.

2400 MHz: The 2400 MHz band is a very commonly-used frequency band. This band was one of the first worldwide unlicensed bands and therefore became popular for wireless consumer products.

Typical wireless technologies that use this band are 802.11b (1-11 Mbps), 802.11g (1-50 Mbps) and 802.15.4, as well as numerous proprietary radio types.

5200-5800 MHz: The 5200 MHz band has three sub-bands, the lowest being for indoor home use only, while the 5800 MHz frequencies can be used for long distance wireless links at very fast speeds (30 – 100 Mbps).

A common strategy is to use 2400 MHz in residential and home environments. The ZigBee Standard endorses the use of this band.

3.2 Signal Modulation

Modulation is the process of changing the behavior of a signal so that it transfers information. Modulation can also be thought of as a way to encode information to be transmitted to a receiver that decodes, or demodulates, the information into a useful form.

The basic radio frequency (RF) signal has a fundamental frequency that can be visualized as an alternating current whose frequency is referred to as the *carrier wave frequency*. The earliest method used for encoding information onto the carrier wave involved switching the carrier wave on and off in a specific time duration pattern. This was known as continuous wave (CW) mode. The carrier frequency can also be varied in its amplitude (that is, signal strength) or its frequency. These two modulation methods are called amplitude modulation (AM) and frequency

modulation (FM), respectively. It is possible to impose a signal onto the carrier wave using these three basic modulation techniques and creative variations of these techniques.

The EM2xx and EM35x use a form of *offset quadrature phase-shift keying* (OQPSK) to modulate the carrier wave. Phase-shift keying (PSK) is a digital modulation scheme that conveys data by changing, or modulating, the phase of a reference signal such as the carrier wave. PSK is a derivative of FM techniques.

All digital modulation schemes use a finite number of distinct signals to represent digital data. In the case of PSK, a finite number of phases are used. Each of these phases is assigned a unique pattern of binary bits. Usually, each phase encodes an equal number of bits. Each pattern of bits forms the symbol that is represented by the particular phase. The demodulator, which is designed specifically for the symbol set used by the modulator, determines the phase of the received signal and maps it back to the symbol it represents, thus recovering the original data. To do so the receiver must compare the phase of the received signal to a reference signal. Such a system is termed coherent.

3.3 Antennas

An antenna (or aerial) is an arrangement of electrical conductors designed to emit or capture electromagnetic waves. The ability of an antenna to emit a signal that can be detected by another antenna is referred to as radio propagation. Antennas are made to a certain size based on the operating frequencies. An antenna from a 2400 MHz radio cannot be used effectively on a 5800 MHz radio, or vice versa. However, an antenna from one type of 2400 MHz technology, such as WiFi or Bluetooth, can be used in another 2400 MHz technology, such as ZigBee.

Two fundamental types of antennas are described with reference to a specific three dimensional space:

- Omni-directional (radiates equally in all directions)
- Uni-directional (also known as directional) (radiates more in one direction than in the other). All antennas radiate some energy in all directions in free space, but careful construction results in substantial transmission of energy in certain directions and negligible energy radiated in other directions.

Because of the nature of mesh networking, in general an omni-directional antenna is desired to provide as many communication paths as possible.

3.4 How Far Signals Travel

The distance a radio signal will travel and the amount of information that can be transmitted is based on:

- The amount of power the antenna is transmitting into the air.
- The distance between the transmitting and receiving stations.
- How much radio signal strength the receiving radio needs.
- What types of physical/electrical obstructions are in the way.

3.4.1 Radio Transmit Power

Radio transmit power is measured in watts, and typically discussed in terms of dBm, decibels referenced to 1 milliwatt. Converting wattage to dBm allows radio link calculations using simple addition and subtraction.[2]

For example, a typical power amplified wireless radio card transmits at 100 milliwatts (or mW), which translates to a power output of 20 dBm.

If 1 mW, or 0 dBm, is the baseline for power in decibels, then +3 dBm is some power level above 1 mW (2 mW to be specific). This is the standard output power of the EM250/EM260/EM351/EM357 devices. In Boost Mode, that can be increased to +5 dBm, or 3.16 mW, on the EM2xx platforms and +8 dBm, or 6.3 mW, on the EM35x platforms. Using a power amplifier module can increase the transmit power to 20 dBm, but this requires more power to operate.

[2] dBm= 10*log10(P/ 0.001)

3.4.2 Signal Degradation

The radio also needs to be able to hear a radio signal at a certain level. The minimum signal strength required for a receiver to understand the data is called the *receive sensitivity*.

As the radio signal travels through the air, it weakens. When a radio signal leaves the transmitting antenna the dBm is a high number (for example: 20 dBm). As it travels through the air, it loses strength and drops to a negative number. At some point, a minimum value for dBm is reached, below which the radio will no longer successfully receive the transmission. This value represents the "receive sensitivity" or "RX sensitivity". This value will vary with the type of radio used but is typically between -90 dBm and -100 dBm. Refer to the data sheet for your radio chip for specific receive sensitivity figures.

If you can achieve a signal level of -75 dBm and your radio has an Rx sensitivity of -95 dBm, you have 20 dBm of extra signal to accommodate interference and other issues. This is called margin.

3.4.3 How Far Can the Radio Signal Go

If you know the power out, and the receiver sensitivity, you can determine whether you can broadcast over a given distance. In the following example, you want to know if you can receive a signal over five miles. To do so, you need to know the free space loss between the radio transmitter and the receiver.

For example, free space loss of a 2.4 GHz signal at 5 miles is 118.36 dB. So, you can estimate signal strength over the range of the network as:

What	Add or subtract it	The value
Transmitter power	+	15 dBm
Transmitter antenna gain	+	14 dBi
Receiver antenna gain	+	14 dBi
Transmitter's coaxial cable loss	-	2 dB
Receiver's coaxial cable loss	-	2 dB
Free Space Loss @ 5 miles	-	118.36 dB
	Total:	-79.36 dBm

n other words, a 15 dBm radio hooked into a 14 dBi antenna, transmitting 5 miles through free space to another radio hooked up to a 14 dBi antenna, yields approximately -79 dBm of signal. Note that antennae with gain are necessarily directional, and would need to be aimed at each other. However, physical obstructions such as buildings or trees would have a substantial impact on these calculations. Typical ZigBee networks use smaller, lower-cost antennas without the gain increase and only use power amplifiers if extended range is required. Occasionally, external low noise amplifiers (LNAs) may also be employed to boost RX sensitivity of incoming signals just before they reach the radio.

This calculation is provided as an example. The Ember® development kits for the EM250/EM260/EM351/EM357 come with a functional test application (“nodetest”) that can be used to perform empirical range testing for an embedded wireless network in virtually any environment (see documents AN702, AN704, and AN710, *Bringing up Custom Devices for the EM250, EM260*, and *EM35x*, respectively, for information on using nodetest). Silicon Labs recommends that basic range testing be conducted in the expected environment to evaluate whether extended range is required.

4 Networking: Basic Concepts

A network is a system of computers and other devices (such as printers and modems) that are connected in such a way that they can exchange data. This data may be informational or command-oriented, or a combination of the two.

A networking system consists of hardware and software. Hardware on a network includes physical devices such as a computer workstations, peripherals, and computers acting as file servers, print servers, and routers. These devices are all referred to as nodes on the network.

If the nodes are not all connected to a single physical cable, special hardware and software devices must connect the different cables in order to forward messages to their destination addresses. A *bridge or repeater* is a device that connects networking cables without examining the addresses of messages or making decisions as to the best route for a message to take. In contrast, a *router* contains addressing and routing information that lets it determine, from a message's address, the most efficient route for the message. A message can be passed from router to router several times before being delivered to its target destination.

In order for nodes to exchange data, they must use a common set of rules defining the format of the data and the manner in which it is to be transmitted. A *protocol* is a formalized set of procedural rules for the exchange of data. The protocol also provides rules for the interactions among the network's interconnected nodes. A network software developer implements these rules in software applications that carry out the functions required by the protocol.

Whereas a router can connect networks only if they use the same protocol and address format, a gateway converts addresses and protocols to connect dissimilar networks. Such a set of interconnected networks can be referred to as an internet, intranet, wide area network (WAN), or other specialized network topology. The term Internet is often used to refer to the largest worldwide system of networks, also called the World Wide Web. The basic protocol used to implement the World Wide Web is called the Internet protocol, or IP.

A networking protocol commonly uses the services of another, more fundamental protocol to achieve its ends. For example, the Transmission Control Protocol (TCP) uses the Internet Protocol (IP) to encapsulate the data and deliver it over an IP network. The protocol that uses the services of an underlying protocol is said to be a client of the lower protocol; for example, TCP is a client of IP. A set of protocols related in this fashion is called a protocol stack.

5 Wireless Networking

Wireless networking mimics the wired network, but replaces the wire with a radio signal as the data interconnection medium. Protocols are essentially the same as used in wired networks, although some additional functionality has been added, so that the two types of networks remain interoperable. However, wireless networks have emerged that do not have a wired counterpart requiring interoperability. These specialized networks have their own hardware and software[3] foundations to enable reliable networking within the scope of their unique environments.

6 Ember ZigBee Devices

Silicon Labs has developed networking hardware (the Ember EM2xx and EM35x integrated circuit families) and software (the EmberZNet PRO stack and development tools) to facilitate implementation of a wireless personal area network of devices for sensing and control applications. The diagram in Figure 1 represents a typical wireless device using ZigBee technologies. The RF data modem is the hardware responsible for sending and receiving data on the network. The microcontroller represents the computer control element that originates messages and responds to any information received. The sensor block can be any kind of sensor or control device. Such a system

[3] Most networking protocols are based, to some degree, on the Open Systems Interconnection (OSI) Model.

can exist as a node on a ZigBee network without any additional equipment. Any two such nodes, with compatible software, can form a network. Large networks can contain thousands of such nodes.

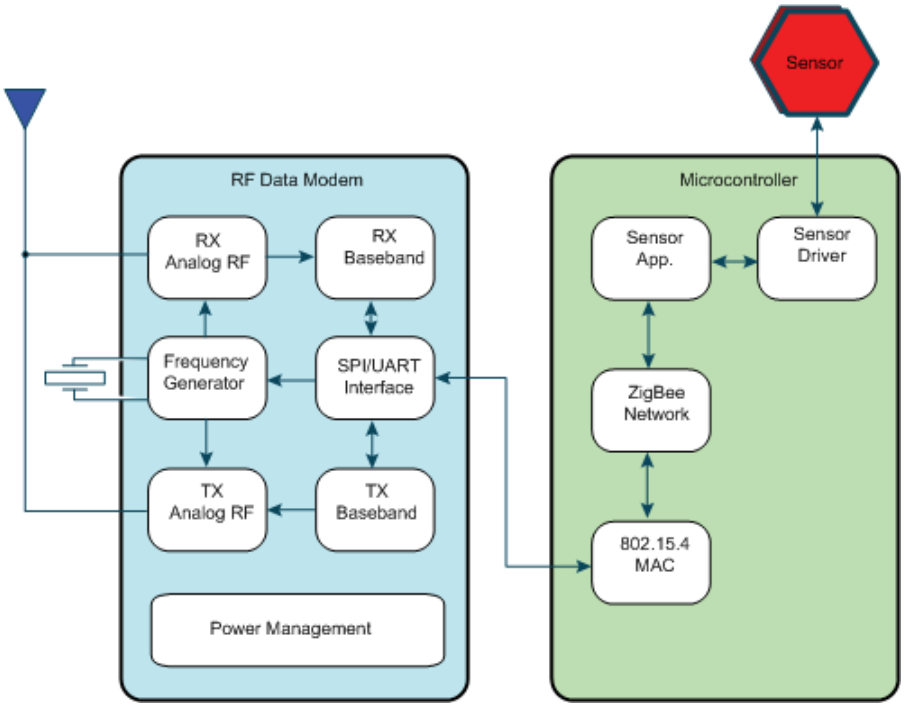

Figure 1. Typical ZigBee Device Block Diagram

The EM250/EM351/EM357 provide both the RF and microcontroller portions of Figure 1. The EM260 (and the EM35x chips when used as “network coprocessors”) provide only the RF and networking part of the system, acting as a coprocessor to any microcontroller, DSP or similar device required for the application.

EmberZNet PRO networks support the device types listed in Table 1.

Table 1. EmberZNet PRO Node Types

Node type	Description
`EMBER_COORDINATOR` (ZigBee coordinator)	The coordinator initiates network formation, and functions as a routing device that relays messages and can act as a parent to other nodes. This device is normally always powered on.
`EMBER_ROUTER` (ZigBee router)	A full-function routing device that relays messages and can act as a parent to other nodes. These devices must be always powered on.
`EMBER_END_DEVICE` (ZigBee end device with `RXOffWhenIdle` flag cleared)	An end device whose radio is always on, but communicates only through its parent and will not relay messages.
`EMBER_SLEEPY_END_DEVICE` (ZigBee end device with `RXOffWhenIdle` flag set)	An end device whose radio can be turned off to save power.
`EMBER_MOBILE_END_DEVICE` (ZigBee end device with `RXOffWhenIdle` flag set)	An end device that can move through the network. The EmberZNet PRO stack always assumes a Mobile End Device is a sleepy node. Not a ZigBee standard device type.

Coordinator and router devices form the basis of the network and route data for other devices in the network.

End devices send and receive messages only from their parent. A parent is a router/coordinator in direct communication range of the “child” end device. The parent acts as a proxy for inbound and outbound traffic pertaining to that end device “child”. This allows the end devices to sleep while their parent holds messages for them until they wake up. End devices do not relay messages for other devices.

6.1 Network Formation and Operation

The coordinator initiates network formation. In a mesh network, after the coordinator forms the network it can function as a router. The EmberZNet PRO libraries enable any device to act as a coordinator and form a network. After forming a network, the coordinator can accept requests from other devices that wish to join the network. Depending on the stack and application profile used, the coordinator might also perform additional duties after network formation. An application profile describes the messages and network setting for a particular application, such as smart energy. See the document UG103.2, *Ember Application Development Fundamentals: ZigBee* for more information.

A device finds a network by scanning channels. When a device finds a network with the correct profile that is open to joining, it can request to join that network. A device can send a join request to the network’s coordinator or one of its router nodes. If the application is using a trust center, the trust center can further specify security conditions under which join requests are accepted or denied. See the document UG103.5, *Ember Application Development Fundamentals: Security* for more information about security.

All nodes that communicate on a network transmit and receive on the same channel, or frequency. ZigBee uses a personal area network identifier (PAN ID) to identify a network. The PAN ID provides a way for two networks to exist on the same channel while still maintaining separate traffic flow. Note that when two networks exist in the same channel they have to share time on the air.

The network layer discovers and maintains available routes so that the user application does not need to know anything about the underlying routes used to deliver a message to a destination node. Route discovery varies among networks and routing mechanisms. The two general approaches are active and dynamic discovery:

- **Active route discovery** tries to keep certain routes up to date at all times. This consumes additional network overhead but means that routes are available whenever a node wishes to send data.
- **Dynamic, or on-demand, route discovery** incurs less overhead network traffic but can cause a delay when a route changes because of shifting radio conditions or network rearrangements.

In an EmberZNet PRO stack, after a route between a source node and target node is discovered, the source node sends the message to the first node in the route, as specified in the source node’s routing table. Each intermediate node uses its own routing table to forward the message to the next node along the route, until the message reaches the target node. The information about the route is next-hop, where each node knows what the next hop should be for delivery to a particular destination. If a route fails, the source node must find a new route.

CONTACT INFORMATION

Silicon Laboratories Inc.

400 West Cesar Chavez
Austin, TX 78701
Tel: 1+(512) 416-8500
Fax: 1+(512) 416-9669
Toll Free: 1+(877) 444-3032

Please visit the Silicon Labs Technical Support web page for ZigBee products:
www.silabs.com/zigbee-support and register to submit a technical support request