Home networking with Zigbee

By Mikhail Galeev
Embedded Systems Design
(04/20/04, 06:00:00 PM EDT)

Will Bluetooth, ZigBee, and 802.11 all have a place in your home? Here's what ZigBee offers for home wireless networking.

For the last few years, we've witnessed a great expansion of remote control devices in our day-to-day life. Five years ago, infrared (IR) remotes for the television were the only such devices in our homes. Now I quickly run out of fingers as I count the devices and appliances I can control remotely in my house. This number will only increase as more devices are controlled or monitored from a distance.

To interact with all these remotely controlled devices, we'll need to put them under a single standardized control interface that can interconnect into a network, specifically a HAN or home-area network. One of the most promising HAN protocols is ZigBee, a software layer based on the IEEE 802.15.4 standard. This article will introduce you to ZigBee—how it works and how it may be more appropriate than simply accumulating more remotes.

Why so many remotes? Right now, the more remotely controlled devices we install in our homes, the more remotes we accumulate. Devices such as TVs, garage door openers, and light and fan controls predominantly support one-way, point-to-point control. They're not interchangeable and they don't support more than one device. Because most remotely controlled devices are proprietary and not standardized among manufacturers, even those remotes used for the same function (like turning on and off lights) are not interchangeable with similar remotes from different manufacturers. In other words, you'll have as many separate remote control units as you have devices to control.

Some modern IR remotes enable you to control multiple devices by "learning" transmitting codes. But because the range for IR control is limited by line of sight, they're used predominantly for home entertainment control.

A HAN can solve both problems because it doesn't need line-of-sight communication and because a single remote (or other type of control unit) can command many devices.

First there was X-10

Of the few attempts to establish a standard for home networking that would control various home appliances, the X-10 protocol is one of the oldest. It was introduced in 1978 for the Sears Home Control System and the Radio Shack Plug'n Power System. It uses power line wiring to send and receive commands. The X-10 PRO code format is the de facto standard for power line carrier transmission.

X-10 transmissions are synchronized to the zero-crossing point of the AC power line. A binary 1 is represented by a 1ms burst of 120KHz at the zero-cross point and binary 0 by the absence of 120KHz. The network consists of transmitter units, receiver units, and bidirectional units that can receive and transmit X-10 commands. Receiving units work as remote control power switches to control home appliances or as remote control dimmers for lamps. The transmitter unit is typically a normally-open switch that sends a predefined X-10 command if the switch is closed. The X-10 commands enable you to change the status of the appliance unit (turn it on or off) or to control the status of a lamp unit (on, off, dim, bright). Bidirectional units may send their current status (on or off) upon request. A special code is used to accommodate the data transfer from analog sensors. Currently, a broad range of devices that control home appliances using the X-10 protocol is available from Radio Shack or web retailers such as www.smarthome.com and www.x10.com.

Availability and simplicity have made X-10 the best-known home automation standard. It enables plug-and-play operation with any home appliance and doesn't require special knowledge to configure and operate a home network.

The downside of its simplicity is slow speed, low reliability, and lack of security. The effective data transfer rate is 60bps, too slow for any meaningful data communication between nodes. High redundancy in transition is dictated by heavy signal degradation in the power line. For any power appliances, the X-10 transmission looks like noise and is subject to removal by the power line filters. Reliability and security issues rule out the use of the X-10 network for critical household applications like remote control of an entry door.

Table 1: 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 3#&956;A	4"32KB	Long battery life, low cost	Remote control, battery-operated products, sensors

In the last few years, new wireless local area networks (WLANs) such as Wi-Fi and Bluetooth became available. Table 1 shows the strengths and applications of these different systems. Wireless cameras for remote monitoring are an example of how to employ those technologies in home automation and control areas. But the problem is that those technologies don't satisfy the requirements for a HAN.

If we take a look at the type of data that circulates within a network of sensors and actuators, we may find that most of it is small packets that control devices or obtain their status. For many applications, such as wireless smoke and CO2 detectors or wireless home security, the device mostly stays in deep-sleep mode and only sends a short burst of information if a trigger event occurs. The main requirements for devices in such types of networks are:

- extremely low power consumption
- the ability to sleep for a long time
- simplicity
- low cost

A home network should also support different configurations, such as a star or mesh network, to effectively cover a household area of 30 to 70 meters.

What is ZigBee?

ZigBee is a home-area network designed specifically to replace the proliferation of individual remote controls. ZigBee was created to satisfy the market's need for a cost-effective, standards-based wireless network that supports low data rates, low power consumption, security, and reliability. To address this need, the ZigBee Alliance, an industry working group (www.zigbee.org), is developing standardized application software on top of the IEEE 802.15.4 wireless standard. The alliance is working closely with the IEEE to ensure an integrated, complete, and interoperable network for the market. For example, the working group will provide interoperability certification testing of 802.15.4

systems that include the ZigBee software layer.

The ZigBee Alliance will also serve as the official test and certification group for ZigBee devices. ZigBee is the only standards-based technology that addresses the needs of most remote monitoring and control and sensory network applications.

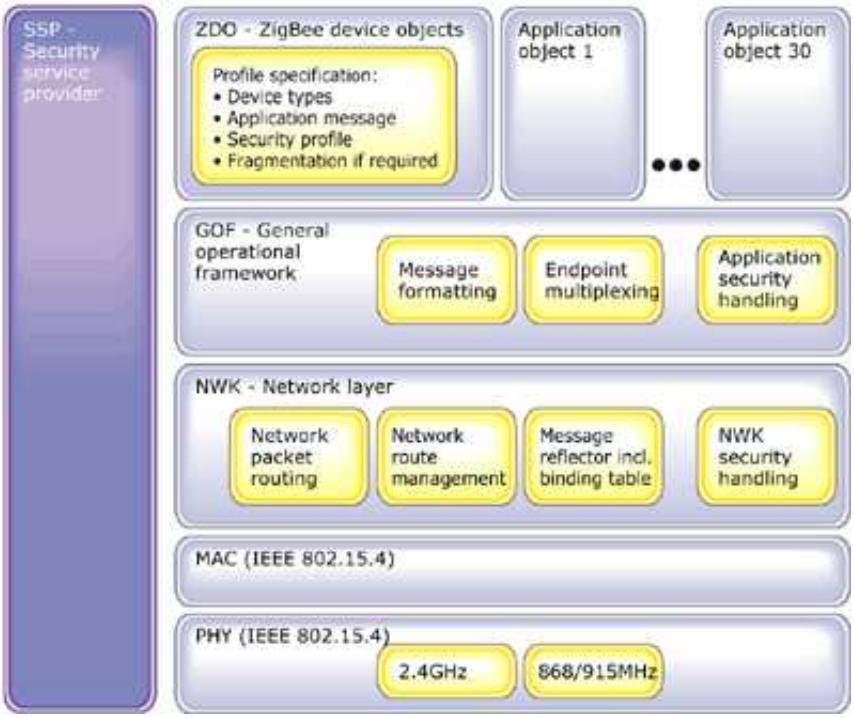

Figure 1: ZigBee stack architecture

It may be helpful to think of IEEE 802.15.4 as the physical radio and ZigBee as the logical network and application software, as Figure 1 illustrates. Following the standard Open Systems Interconnection (OSI) reference model, ZigBee's protocol stack is structured in layers. The first two layers, physical (PHY) and media access (MAC), are defined by the IEEE 802.15.4 standard. The layers above them are defined by the ZigBee Alliance. The IEEE working group passed the first draft of PHY and MAC in 2003. A final version of the network (NWK) layer is expected sometime this year.

ZigBee-compliant products operate in unlicensed bands worldwide, including 2.4GHz (global), 902 to 928MHz (Americas), and 868MHz (Europe). Raw data throughput rates of 250Kbps can be achieved at 2.4GHz (16 channels), 40Kbps at 915MHz (10 channels), and 20Kbps at 868MHz (1 channel). The transmission distance is expected to range from 10 to 75m, depending on power output and environmental characteristics. Like Wi-Fi, Zigbee uses direct-sequence spread spectrum in the 2.4GHz band, with offset-quadrature phase-shift keying modulation. Channel width is 2MHz with 5MHz channel spacing. The 868 and 900MHz bands also use direct-sequence spread spectrum but with binary-phase-shift keying modulation.

Frame structure

Figure 2 illustrates the four basic frame types defined in 802.15.4: data, ACK, MAC command, and beacon.

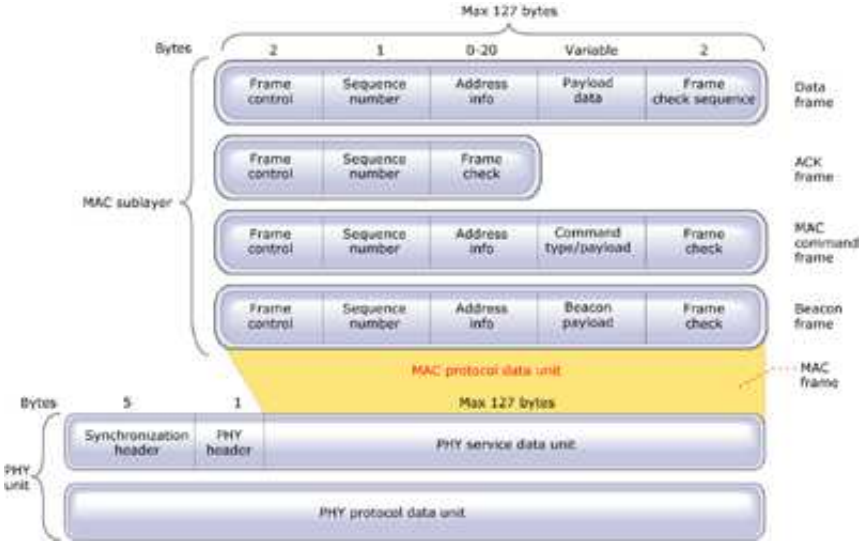

Figure 2: The four basic frame types defined in 802.15.4: Data, ACK, MAC command, and beacon

The *data frame* provides a payload of up to 104 bytes. The frame is numbered to ensure that all packets are tracked. A frame-check sequence ensures that packets are received without error. This frame structure improves reliability in difficult conditions.

Another important structure for 802.15.4 is the *acknowledgment (ACK) frame*. It provides feedback from the receiver to the sender confirming that the packet was received without error. The device takes advantage of specified "quiet time" between frames to send a short packet immediately after the data-packet transmission.

A *MAC command frame* provides the mechanism for remote control and configuration of client nodes. A centralized network manager uses MAC to configure individual clients' command frames no matter how large the network.

Finally, the *beacon frame* wakes up client devices, which listen for their address and go back to sleep if they don't receive it. Beacons are important for mesh and cluster-tree networks to keep all the nodes synchronized without requiring those nodes to consume precious battery energy by listening for long periods of time.

Channel access, addressing

Two channel-access mechanisms are implemented in 802.15.4. For a non"beacon network, a standard ALOHA CSMA-CA (carrier-sense medium-access with collision avoidance) communicates with positive acknowledgement for successfully received packets. In a beacon-enabled network, a superframe structure is used to control channel access. The superframe is set up by the network coordinator to transmit beacons at predetermined intervals (multiples of 15.38ms, up to 252s) and provides 16 equal-width time slots between beacons for contention-free channel access in each time slot. The structure guarantees dedicated bandwidth and low latency. Channel access in each time slot is contention-based. However, the network coordinator can dedicate up to seven guaranteed time slots per beacon interval for quality of service.

Device addresses employ 64-bit IEEE and optional 16-bit short addressing. The address field within the MAC can contain both source and destination address information (needed for peer-to-peer operation). This dual address information is used in mesh networks to prevent a single point of failure within the network.

Device types

ZigBee networks use three device types:

- The *network coordinator* maintains overall network knowledge. It's the most sophisticated of the three types and requires the most memory and computing power.
- The *full function device (FFD)* supports all 802.15.4 functions and features specified by the

standard. It can function as a network coordinator. Additional memory and computing power make it ideal for network router functions or it could be used in network-edge devices (where the network touches the real world).
- The *reduced function device (RFD)* carries limited (as specified by the standard) functionality to lower cost and complexity. It's generally found in network-edge devices.

Power and beacons

Ultra-low power consumption is how ZigBee technology promotes a long lifetime for devices with nonrechargeable batteries. ZigBee networks are designed to conserve the power of the slave nodes. For most of the time, a slave device is in deep-sleep mode and wakes up only for a fraction of a second to confirm its presence in the network. For example, the transition from sleep mode to data transition is around 15ms and new slave enumeration typically takes just 30ms.

ZigBee networks can use beacon or non-beacon environments. Beacons are used to synchronize the network devices, identify the HAN, and describe the structure of the superframe. The beacon intervals are set by the network coordinator and vary from 15ms to over 4 minutes. Sixteen equal time slots are allocated between beacons for message delivery. The channel access in each time slot is contention-based. However, the network coordinator can dedicate up to seven guaranteed time slots for noncontention based or low-latency delivery.

The *non-beacon mode* is a simple, traditional multiple-access system used in simple peer and near-peer networks. It operates like a two-way radio network, where each client is autonomous and can initiate a conversation at will, but could interfere with others unintentionally. The recipient may not hear the call or the channel might already be in use.

Beacon mode is a mechanism for controlling power consumption in extended networks such as cluster tree or mesh. It enables all the clients to know when to communicate with each other. Here, the two-way radio network has a central dispatcher that manages the channel and arranges the calls. The primary value of beacon mode is that it reduces the system's power consumption.

Non-beacon mode is typically used for security systems where client units, such as intrusion sensors, motion detectors, and glass-break detectors, sleep 99.999% of the time. Remote units wake up on a regular, yet random, basis to announce their continued presence in the network. When an event occurs, the sensor wakes up instantly and transmits the alert ("Somebody's on the front porch"). The network coordinator, powered from the main source, has its receiver on all the time and can therefore wait to hear from each of these stations. Since the network coordinator has an "infinite" source of power it can allow clients to sleep for unlimited periods of time, enabling them to save power.

Beacon mode is more suitable when the network coordinator is battery-operated. Client units listen for the network coordinator's beacon (broadcast at intervals between 0.015 and 252s). A client registers with the coordinator and looks for any messages directed to it. If no messages are pending, the client returns to sleep, awaking on a schedule specified by the coordinator. Once the client communications are completed, the coordinator itself returns to sleep.

This timing requirement may have an impact on the cost of the timing circuit in each end device. Longer intervals of sleep mean that the timer must be more accurate or turn on earlier to make sure that the beacon is heard, both of which will increase receiver power consumption. Longer sleep intervals also mean the timer must improve the quality of the timing oscillator circuit (which increases cost) or control the maximum period of time between beacons to not exceed 252s, keeping oscillator circuit costs low.

Security

Security and data integrity are key benefits of the ZigBee technology. ZigBee leverages the security model of the IEEE 802.15.4 MAC sublayer which specifies four security services:

- access control—the device maintains a list of trusted devices within the network
- data encryption, which uses symmetric key 128-bit advanced encryption standard

- frame integrity to protect data from being modified by parties without cryptographic keys
- sequential freshness to reject data frames that have been replayed—the network controller compares the freshness value with the last known value from the device and rejects it if the freshness value has not been updated to a new value

The actual security implementation is specified by the implementer using a standardized toolbox of ZigBee security software.

Network layer

The NWK layer associates or dissociates devices using the network coordinator, implements security, and routes frames to their intended destination. In addition, the NWK layer of the network coordinator is responsible for starting a new network and assigning an address to newly associated devices.

The NWK layer supports multiple network topologies including star, cluster tree, and mesh, all of which are shown in Figure 3.

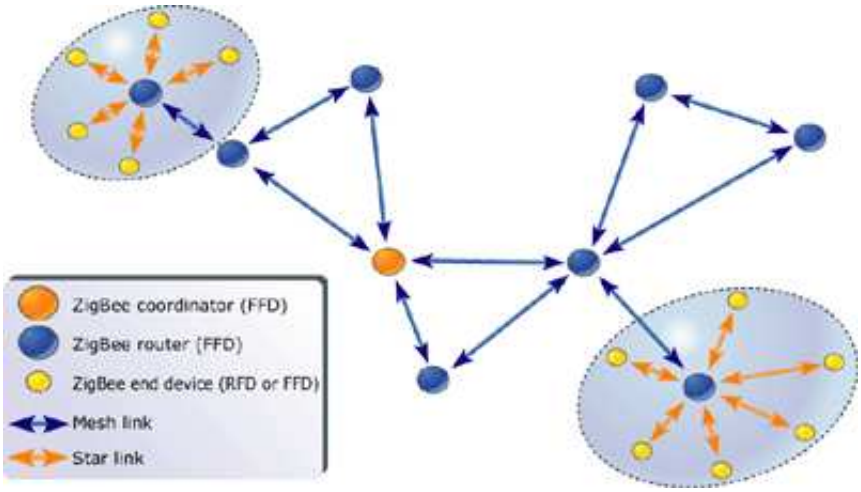

Figure 3: ZigBee network model

In a star topology, one of the FFD-type devices assumes the role of network coordinator and is responsible for initiating and maintaining the devices on the network. All other devices, known as end devices, directly communicate with the coordinator.

In a mesh topology, the ZigBee coordinator is responsible for starting the network and for choosing key network parameters, but the network may be extended through the use of ZigBee routers. The routing algorithm uses a request-response protocol to eliminate sub-optimal routing. Ultimate network size can reach 264 nodes (more than we'll probably need). Using local addressing, you can configure simple networks of more than 65,000 (2^{16}) nodes, thereby reducing address overhead.

The *General Operation Framework (GOF)* is a glue layer between applications and rest of the protocol stack. The GOF currently covers various elements that are common for all devices. It includes subaddressing and addressing modes and device descriptions, such as type of device, power source, sleep modes, and coordinators. Using an object model, the GOF specifies methods, events, and data formats that are used by application profiles to construct set/get commands and their responses.

Actual application profiles are defined in the individual profiles of the IEEE's working groups. Each ZigBee device can support up to 30 different profiles. Currently, only one profile, Commercial and Residential Lighting, is defined. It includes switching and dimming load controllers, corresponding remote-control devices, and occupancy and light sensors.

The ZigBee stack is small in comparison to other wireless standards. For network-edge devices with limited capabilities, the stack requires about 4Kb of the memory. Full implementation of the protocol stack takes less than 32Kb of memory. The network coordinator may require extra RAM for a node

devices database and for transaction and pairing tables. The 802.15.4 standard defines 26 primitives for the PHY and MAC layers; probably another dozen will be added after finalizing the NWK layer specification. Those numbers are still modest compared to 131 primitives defined for Bluetooth. Such a compact footprint enables you to run Zigbee on a simple 8-bit microcontroller such as an HC08- or 8051-based processor core.

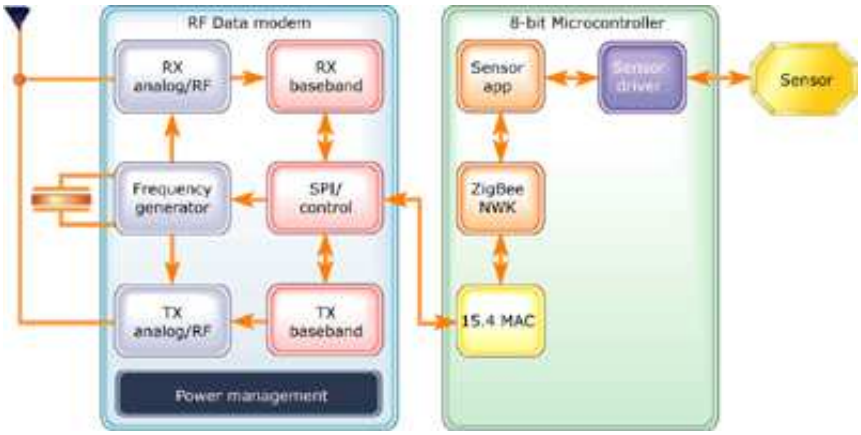

Figure 4: A typical ZigBee-enabled device will consist of RF IC and 8-bit microprocessor with peripherals connected to an application sensor or actuators

As Figure 4 shows, a typical ZigBee-enabled device includes a radio frequency integrated circuit (RF IC) with a partially implemented PHY layer connected to a low-power, low-voltage 8-bit microcontroller with peripherals, connected to an application sensor or actuators. The protocol stack and application firmware reside in on-chip flash memory. The entire ZigBee device can be compact and cost efficient.

Motorola and Atmel already offer a set of RF ICs and microcontrollers for ZigBee. Chipcon is sampling 802.15.4-compliant RF ICs for the 2.4GHz band. Currently, a ZigBee chip set costs about $7, but that price should fall to $2 after market acceptance. Studies suggest that it will happen in the new few years. It may take a year or more to determine how much ZigBee will be accepted in the market.

Consulting the crystal ball

IEEE 802.15.4 is a new standard that still needs to pass through the circles of rigorous technology critics and establish its own place in the industry. Predictions for the future of ZigBee-enabled devices are a popular topic for numerous market-research firms. But as with any crystal ball reading, the results of those analyses are subject to interpretation.

While I intend to stay objective, I believe, based on protocol features implemented in 802.15.4, that ZigBee has a bright future. Backed by IEEE, ZigBee has the potential to unify methods of data communication for sensors, actuators, appliances, and asset-tracking devices. It offers a means to build a reliable but affordable network backbone that takes advantage of battery-operated devices with a low data rate and a low duty cycle. ZigBee can be used in many applications, from industrial automation, utility metering, and building control to even toys. Home automation, however, is the biggest market for ZigBee-enabled devices. This follows from the number of remote controlled devices (or devices that may be connected wirelessly) in the average household. This cost-effective and easy-to-use home network potentially creates a whole new ecosystem of interconnected home appliances, light and climate control systems, and security and sensor subnetworks.

Mikhail Galeev is a senior engineer at Motorola with seven years experience in firmware design for embedded systems. He holds a BS in applied physics from Rostov State University, Russia, and an MSEE from the University of South Alabama, Mobile. You may reach him at Mikhail.Galeev@motorola.com.

Further Reading

Callaway, Edgar and Edgar Callaway, Jr. *Wireless Sensor Networks: Architectures and Protocols*. CRC Press, 2003.

Barrett, Raymond, Edgar Callaway, and Jose Gutierrez. *IEEE 802.15.4 Low-Rate Wireless Personal Area Networks: Enabling Wireless Sensor Networks*. Inst of Elect & Electronic, 2003.