Providing reliable sensing and control using ZigBee wireless networks

This article demystifies ZigBee and demonstrates a light switch, a subset of a typical home networking environment, as an application example to describe the devices needed in the development of a wireless sensor network based on the ZigBee standard.

By Peter Wotton

The ZigBee protocol is a worldwide open standard providing low-power, wireless connectivity for a wide range of applications that perform monitoring or control functions. The standard overcomes the traditional limitations of low-power, wireless network solutions—such as short range, restricted coverage and vulnerability to node and radio link failures. It achieves this by building on the established IEEE802.15.4 standard for packet-based, wireless transport.

ZigBee enhances the functionality of IEEE802.15.4 by providing flexible, extendable network topologies with integrated setup and routing intelligence to facilitate easy installation and high resilience to failure. ZigBee networks also incorporate listen-before-talk and rigorous security measures that enable them to co-exist with other wireless technologies, such as Bluetooth and Wi-Fi, in the same operating environment.

The features of this wireless connectivity standard allow ZigBee-based products to be installed easily and cost effectively, and its built-in intelligence and flexibility allow networks to be easily adapted to changing needs by adding, removing or moving network devices. The protocol is designed to allow devices to appear and disappear from the network, so devices can be put into a power-saving mode when not active. This means that many devices in a ZigBee network can be battery powered, making them self-contained and reducing installation costs.

ZigBee includes measures to avoid interference between radio communications—such as its ability to automatically select the best frequency channel at initialization. Where possible, it will also adapt to a changing RF environment by automatically selecting another channel if the current channel proves problematic.

The range of a radio transmission is dependent on the operating environment; for example, indoors or outdoors. With a standard wireless microcontroller module such as the JN5121 (Figure 1) at around 0 dBm output power, a range of more than 450 meters can typically be achieved outdoors, but indoors this can be reduced due to absorption, reflection, diffraction and standing-wave effects caused by walls and other solid objects. High-power modules (>15 dBm output power) can achieve up to 10 times better range. In addition, range between devices can be extended in a ZigBee network, since the tree and mesh topologies, shown in Figure 2, can use intermediate nodes (routers) as stepping stones when passing data to the destination.

Typical applications and limitations

ZigBee is suitable for a range of applications covering commercial and domestic use. Some applications like long-term health monitoring and asset tracking in warehouses,

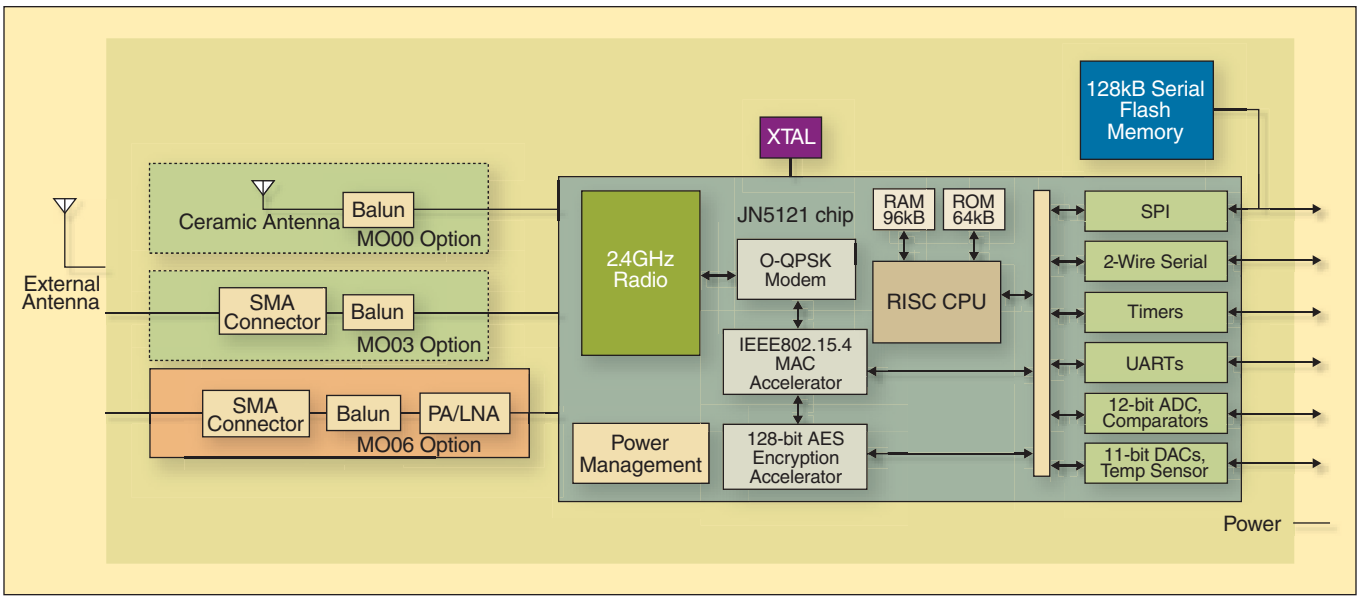

Figure 1. With output power at around 0 dBm, a range of more than 450 meters can typically be achieved outdoors with the wireless microcontroller module such as the JN5121. However, indoor range is lower due to absorption, reflection, diffraction and standing-wave effects caused by walls and other solid objects.

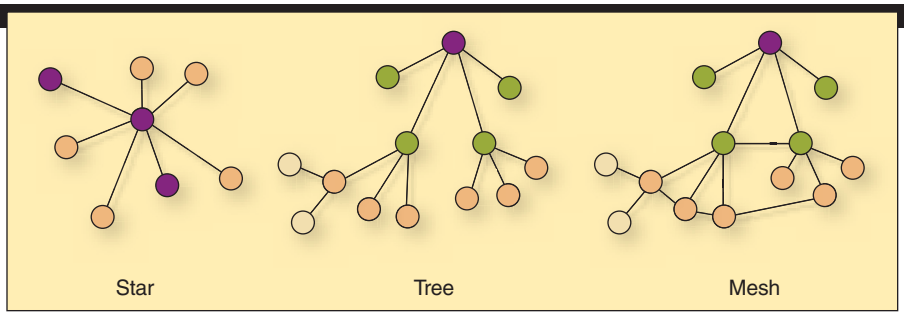

Figure 2. A ZigBee network can adopt one of the three topologies: star, tree or mesh.

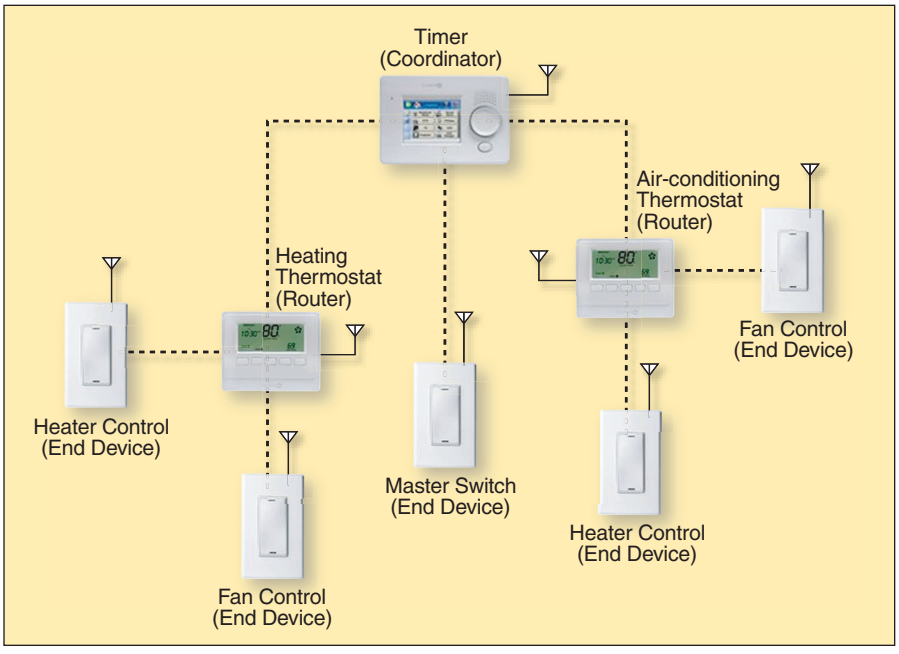

Figure 3. In a typical home heating network, a coordinator (in this case the timer) provides control for the heating thermostats or lights (the routers) through the switches (end devices).

which currently cannot be implemented with cabled systems, can be easily developed using ZigBee. Similarly, existing applications like lighting control and industrial plant monitoring that currently rely on cable-based solutions can be realized more cost effectively with wireless networks. It can also be beneficial in environments where cable-based solutions can be difficult and expensive to install. For example, in home security systems, sensors need to be easy to install (no cables or power supply wiring), and must be small and self-contained (battery powered).

There are many potential battery-powered wireless applications, from light switches, active tags and security detectors, to solar-powered monitoring. The ZigBee and IEEE802.15.4 protocols are specifically designed for battery-powered applications.

In practice, not all devices in a network can be battery powered, particularly those that need to be switched on all the time (and cannot sleep), such as routers and coordinators. Such devices can often be installed in a mains-powered appliance that is permanently connected to the mains supply (even if not switched on), for instance, a ceiling lamp or an electric radiator. This avoids the need to install a dedicated mains power connection for the network device.

Communications reliability and security

ZigBee employs a range of techniques to ensure reliable communications, since corruption could result from radio interference or poor transmission/reception conditions.

At a first level, ZigBee networks apply a coding mechanism to radio transmissions. The coding method employed in the 2400 MHz band uses quadrature phase-shift keying (QPSK) modulation with conversion of four-bit data symbols to 32-bit chip sequences. Due to this coding, there is a high probability that a message will get through to its destination intact, even if there are conflicting transmissions (more than one device transmitting in the same frequency channel at the same time).

The transmission scheme avoids transmitting data when there is activity on its chosen channel, known as carrier sense, multiple access with collision avoidance (CSMA-CA). Simply put, a node will listen on the channel to check if it is clear before beginning the transmission. If activity is detected on the channel then the node delays the transmission for a random amount of time and listens again. If the channel is clear, the transmission can begin otherwise the delay and listen cycle is repeated.

A further mechanism is built into this network to ensure that messages reach their destinations; when a message arrives at its destination, the receiving device sends an acknowledgment to say the message has been received. If the sending device does not receive an acknowledgment within a certain time interval, it can resend the original message several times until the message has been acknowledged.

In a mesh topology, the network has built-in intelligence to ensure that messages reach their destinations. If the default route to the destination node is down, due to a failed intermediate node or link, the network can 'discover' and implement alternative routes for message delivery.

These reliability measures allow such a network to operate in an insular, protected environment, even when there are other ZigBee networks nearby operating in the same frequency band. Therefore, adjacent ZigBee networks will not interfere with each other. In addition, ZigBee networks can operate in the neighborhood of networks based on other standards, such as Wi-Fi and Bluetooth, without any interference.

To offer high security; they incorporate measures to prevent intrusion from potentially hostile parties and from neighboring networks. To this end, a 'security toolbox' is included in a ZigBee network, offering:

- access control lists: only pre-defined 'friendly' nodes can join the network;
- 128-bit AES-based encryption: a high-security key-based encryption system—some wireless microcontrollers have this built in as a hardware function, preventing external agents from interpreting ZigBee network data; and
- message-freshness timers: timed-out messages are rejected, preventing message replay attacks on the network (for example, a malicious individual recording the open command to a garage door opener, and then replaying it to gain entry into the property).

As shown in Figure 2, a ZigBee network can adopt one of the three topologies: star, tree or mesh. The way that a message is routed from one node to another depends on the topology. A star network has a central node through which all messages travel. Tree networks have a top node with a branch/leaf structure below, and messages travel up the tree, as far as necessary, and then down the tree. Mesh networks have a tree-like structure in which some leaves are directly linked; messages can travel across the tree, when a suitable route is available.

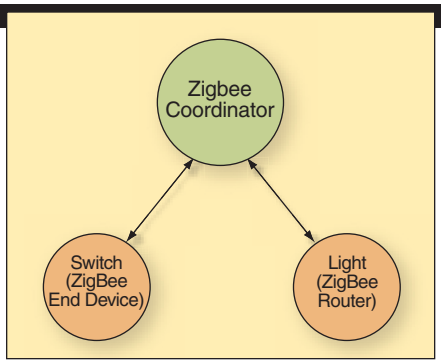

Figure 4. Illustrates a ZigBee light switch application, which is a subset of the home network.

There is always one node that takes a coordinating role in a network; the central node in a star topology, the top node in a tree/mesh topology. There must also be nodes with the role of relaying messages from one neighboring node to another.

Nodes in a network

The ZigBee standard has the capacity to address up to 65535 nodes in a single network, using just three general types of node at the network level: coordinator, router and end device.

All ZigBee networks must have only one coordinator, irrespective of the network topology. At the network level, the coordinator is mainly needed at system initialization. The tasks of the coordinator at the network layer are to:

- select the frequency channel to be used by the network (usually the one with the least detected activity);
- start the network; and
- allow child nodes to connect to it (i.e., to join the network).

The coordinator can also provide message routing, security management and other services. In a tree or mesh network, the presence of at least one router is required to:

- relay messages from one node to another; and
- allow child nodes to connect to it.

The main tasks of an end device at the network level are sending and receiving messages. An end device can often be battery powered and, when not transmitting or receiving, can sleep in order to conserve power. Note that end devices cannot relay messages and cannot allow other nodes to connect to the network through them.

An application example

In a typical home network environment such as that shown in Figure 3, a coordinator (in this case the timer) provides control for the heating thermostats or lights (the routers) through the switches (end devices). We can illustrate how such a network works by taking a subset of this example—a ZigBee light switch application shown in Figure 4—using an evaluation kit from Jennic. The kit

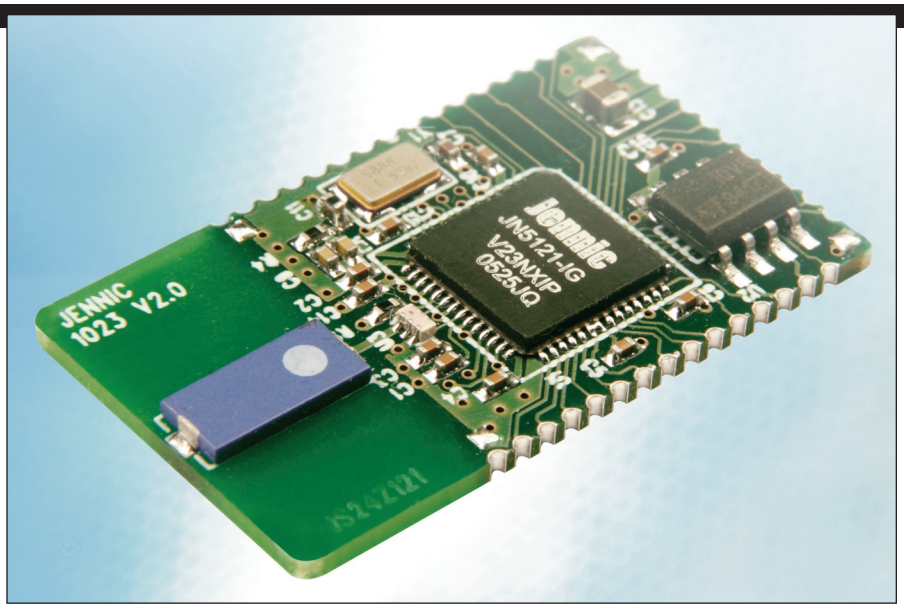

Figure 5. An evaluation module comprises the wireless microcontroller, a crystal oscillator, decoupling components, printed antenna, and a suite of library functions to provide all the elements required to develop a complete network application.

enables the development of sensor network applications for ZigBee, comprising wireless microcontroller plus a suite of library functions that provide all the elements required to build network products, including device drivers, typical sensor and control drivers; the development environment is based on GNU-C tools.

The single-chip IEEE 802.15.4 wireless microcontroller combines a 32-bit RISC core, fully compliant 2.4 GHz IEEE802.15.4 transceiver and integrated 64 Kbytes ROM and 96 Kbytes RAM memory blocks. The microcontroller features a high-level of integration allowing very small low-power modules to be constructed; for example, the RAM allows support of router and coordinator functions without the need for an additional external SRAM. It also includes an integrated hardware MAC for highly secure AES encrypted data flow, integrated sleep oscillator and power-saving facilities.

To complete a typical network node, the wireless microcontroller requires an additional crystal oscillator, flash memory, decoupling components and printed antenna. A reference module (Figure 5) providing this complete setup can be readily customized to suit a network application.

The wireless light switch application described here implements the ZigBee home controls-lighting (HCL) profile. Three sensor boards are required for this application—one to start the network, a second sensor board to act as the switch, and a third sensor board to act as the light. After the network has started, simple binding is used to link together the switch and the light.

This example illustrates all three types of ZigBee device:

- a coordinator that starts the network, binds together end points residing on other devices on the basis of the clusters they possess (this is known as 'indirect binding' and 'end device binding'), and then routes data between those end points;
- a router, which runs the light application; and
- an end device, which runs the switch application; the end device would typically be battery powered.

On the sensor board programmed as the coordinator, the software starts the device as a ZigBee coordinator and an LED is used to show when the network has successfully started. All of the functions associated with acting as a ZigBee coordinator (such as allowing other devices to join the network, allocating addresses to those devices, binding end points on other nodes and relaying data) are performed automatically by the ZigBee protocol stack and are completely transparent to the user. This allows the user's application code to be made as simple as possible.

On the sensor board that is programmed as the light, and which functions as a ZigBee router, the software searches for a network and requests to join it; a request is then sent to the coordinator for end device binding.

On the sensor board programmed as the switch, and which functions as a ZigBee end device, the software searches for a network and requests to join it and again sends a request to the coordinator for end device binding.

This application uses simple binding to link the light and the switch together via the coordinator. When the ZigBee protocol stack on the coordinator receives the two requests for end device binding, it attempts to match them together. If successful, it adds them to its binding table.

Matching is done between end points with identical input and output clusters. In this case, the light has an input cluster with the switch_remote_control ID number, as specified in the ZigBee home controls-lighting (HCL) profile. The switch has an output cluster with the same cluster ID. Therefore, when the coordinator receives the two binding requests, it will match them together.

If two more requests are then received by the coordinator for the same two end points, the entry is removed from the binding table.

Once a pair of end points is bound, data may be sent from either node without a destination address. The packets are automatically sent to the coordinator, which then consults the binding table to find the destination and relays the data to that address.

Sumary

ZigBee has been considered by some in the industry to be quite a complex standard to implement. In this article we have demonstrated that this is not necessarily the case, particularly where the ZigBee protocol is provided with a simple application-programming interface (API). The availability of devices such as single-chip wireless microcontrollers, together with complete hardware and software support—which vendors are even providing completely online—means it is indeed possible to easily set up a high-performance, reliable and secure wireless sensor network using the standard. RFD

ABOUT THE AUTHOR

Peter Wotton is product manager for Jennic's networking products in Sheffield, United Kingdom. With a BEng (Hons) in electronic and electrical engineering from Sheffield, UK, and an MIEE, he has considerable experience in the communications and electronics industry. He has spent more than nine years with Jennic and prior to joining Jennic, he worked for nine years on ASIC, telecom networks and communications system design at Nortel Networks' Harlow Laboratories.