Inside Look at ZigBee™ Wireless Networks

ESC-252
Embedded Systems Conference
Silicon Valley, April 2007

Christopher Leidigh
President
Alektrona Corporation

Jim Higgins
Vice President
Alektrona Corporation

1 Introduction

1.1 The ZigBee™ Alliance

The ZigBee™ Alliance is a fee-based organization similar to PCI, USB, and SDIO groups. There are approximately one dozen promoter companies and hundreds of participant and technology adopter companies. The participation in the ZigBee Alliance is global and the resulting specifications become open standards. There are many certified platforms and the number of shipping products continually increases.

1.2 ZigBee's™ Focus

Think of ZigBee™ as a combination of Ethernet, TCP/IP, RIP, and SNMP. However, it is wireless, natively supports mesh routing, and enables very low power consumption. ZigBee™ is geared towards wireless sensor network applications like environmental monitoring and low data rate control applications. It is not geared towards high data rate communication applications like audio, video, or bulk data.

1.3 Technology Comparison

How does ZigBee™ compare to standards such as BlueTooth (802.15.1) and WLAN (802.11)? One of the principle differences is implementation complexity and cost. In comparison to BlueTooth and WLAN technologies, ZigBee™ has low complexity and low cost. The power profile of ZigBee™ devices allow for years of battery operation whereas BlueTooth and WLAN technologies are far more power hungry. They all operate in the 2.4GHz ISM band, but the MAC/PHY (802.15.4) specification, upon which ZigBee™ is specified, also allows for 868 and 900MHz ISM band radios. ZigBee has the lowest data rate of the all three technologies.

1.4 TCP/IP & OSI Comparison

The ZigBee™ Specification is built on top of the IEEE 802.15.4 MAC/PHY standard and specifies from the network layer through the application layer. Think of ZigBee as a combination of TCP/IP, RIP, and SNMP.

1.5 Topologies & Device Types

A ZigBee™ network can be a star, tree, or mesh topology. A node can be classified as one of two types: a full function device (FFD) or a reduced functionality device (RFD). ZigBee coordinators and router are FFDs and under the current specifications must be line-powered. The ZigBee™

coordinator is the focal point of network formation, but beyond that distinction it serves no different than any other router node. Router nodes are present in the tree and mesh topologies and serve to hop messages between nodes that are not within RF range of each other. They also serve as receive message queues for RFDs that typically battery operated devices that spend the majority of their time in a deep power saving sleep mode.

2 Hardware

2.1 Radios and SoCs

Many first, second, and third tier semiconductor vendors are shipping IEEE 802.15.4 compatible radios. Some vendors also sell SoCs that integrate a microcontroller and a IEEE 802.15.4 radio. SoCs typically offer the most compelling price points.

2.2 Modules

There are many vendors that produce ZigBee compliant modules. Some modules may use a SoC or a combination of a ZigBee complaint microcontroller and radio. These modules are typically already taken through regulatory compliance, which significantly reduces the testing requirements for the end product, and may offer higher transmit power and improved received sensitivity. For low volume applications, cases where time to market is critical, or in instances where the cost and specialized knowledge of RF design is prohibitive, modules are an attractive option.

2.3 Antennas

There are multiple antenna technologies to consider, with each having a price, performance, and packaging tradeoff. ¼ wave whips offer the best gain, and radiation pattern, but are costly. Ceramic patch antennas have hemispherical radiation patterns, good gain, and offer direct PCB mounts. Ceramic chip antennas are very low cost, but are low gain. PCB Trace antennas only cost the space on the PCB and have minimal gain.

2.4 Design Considerations

What will your system look like? How many routers will it require, how will they be powered? What will your power profile look like? How will the system be commissioned and maintained? What is the plan to manage interference? What level of interoperability and compliance are being sought? IEEE 802.15.4 radios/SoCs are tightly bound to the software stacks, there is limited a la carte. Both hardware and software must be simultaneously considered during the design phase.

3 Software

3.1 ZigBee's™ Value Add to 802.15.4

ZigBee™ adds standards based tree and mesh message routing to 802.1.5.4. It also adds standard application concepts that handle the logical binding of devices and standard application profiles for multi-vendor compatibility and allowance for manufacturer defined profiles.

3.2 Stack Architecture & Services

The ZigBee™ stack is divided into two main areas: the network layer and the application layer. The network layer is responsible and provides services for network formation, security, routing including discovery and maintenance, and address assignment. The application layer maintains binding tables, defines the ZigBee Device Object (ZDO), and supports manufacturer-defined application objects.

3.3 Choosing a ZigBee™ Stack

When choosing a ZigBee stack one should consider the following. What is the specification conformance level? What radios, microcontrollers, and modules are supported? How much code/RAM, performance is available for the application? What compiler and application development tools are available? What are the license terms of the stack?

3.4 Commissioning

Commissioning is the physical deployment, addressing, and logical binding of nodes to form a functional network. The challenges of commissioning a ZigBee network include: The physical distribution of nodes, the quantity of nodes, and RF interference, minimal device UIs. There are efforts within the alliance to draft commissioning standards, but for now it is roll your own. Some commissioning techniques include pre-configuration, application level addressing, intuitive installer feedback, and lockdown of stable network configurations.

3.5 Mesh Routing

Routes are discovered dynamically and message delivery is largely independent of parent child relationships, but in the 1.0 specification there are cases where the routing logic degenerates to utilizing short addresses for routing. The ZigBee 2006 specification addresses some of these shortcomings by throwing out the tree-like address assignment scheme for a stochastic addresses assignment mechanism that is more appropriate for mobile nodes and to maximize usage of the 16-bit address space.

3.6 Debugging Hints

Use a quality ZigBee™ network analyzer. One with visualization is a huge help when the number of nodes is more than what can fit comfortably on your desk. Build plenty of prototypes and deploy them to wring out problems early in the development cycle. Add extra UIs (buttons and LEDs) to the prototypes to aid in debugging. Finally think about testing locations, enclosures, and using high capacity batteries to simulate mains power.

4 Coexistence

801.15.4 and ZigBee™ were designed for coexistence with other ISM band radios. There are several ZigBee™ channels in the 2.4GHz band that do not overlap with 802.11 and the high processing gain in the DSS modulation reduces interference problems. Currently 802.15.4 and ZigBee™ do not define a frequency hopping mechanism, which is a feature required in industrial applications and settings. In general ZigBee's™ coexistence with other radio technologies is extremely good.

5 Power

ZigBee™ and 802.1.5.4 support sleeping end nodes. Devices may go into deep power down modes where they are drawing less than 1uA. In many cases 4-5 years of operation are achievable on standard alkaline AA batteries. A typical receive current operation is about 32mA, and transmit operation can, for high power nodes, range from 90-120mA. ZigBee routers are problematic since they must always be mains-powered due to their constant current consumption of ~32mA.

6 Compliance & Interoperability

ZigBee™ defines several levels of compliance. One compliance level is a ZigBee™ Compliant Platform (ZCP) and is applied to modules or platforms that are meant for end products. Another is compliance level is called ZigBee Network Capable (ZNC). ZNC addresses end-products that are built on a ZCP, and use a non-public profile. The final compliance level is ZigBee Certified Product (ZCP). This program applies to end-products that use a public profile. Compliance testing is performed at approved test houses, as of December 2006 were NTS Corp. and TUV Rheinland Group.

7 Gateways and Bridges

The Gateway Working Group is responsible for two specifications. The first is a Bridge Device specification which has been approved and the second is a Gateway specification still under development. A ZigBee Bridge Device (ZBD) allows bridging different channels and/or frequency bands across an IP network. A ZigBee Gateway Device (ZGD) defines standard mechanisms for accessing ZigBee networks from an IP network.

8 ZigBee™'s Future

ZigBee™ is an evolving and improving standard. Some potential changes that are in the pipeline include: Frequency agility, new 900/868 band channels and speed increase to 250kbps, message fragmentation, beaconed networks and sleepy routers. Additionally, we will start to see stacks or partitioned stacks running on more capable processors. ZigBee™ is a standard-based wireless technology that addresses a number of key problems that other technologies do not address or only address in proprietary single vendor solutions.