Zigbee: “Wireless Control That Simply Works”

William C. Craig
Program Manager Wireless Communications
ZMD America, Inc.

I. INTRODUCTION

There are many wireless monitoring and control applications for industrial and home markets which require longer battery life, lower data rates and less complexity than available from existing wireless standards. These standards provide higher data rates at the expense of power consumption, application complexity and cost. What these markets need, in many cases, is a standards-based wireless technology having the performance characteristics that closely meet the requirements for reliability, security, low power and low cost. This standards-based, interoperable wireless technology will address the unique needs of low data rate wireless control and sensor-based networks.

For such wireless applications, a standard has been developed by the IEEE [1]: "The IEEE 802.15 Task Group 4 is chartered to investigate a low data rate solution with multi-month to multi-year battery life and very low complexity. It is intended to operate in an unlicensed, international frequency band". Potential applications are home automation, wireless sensors, interactive toys, smart badges and remote controls. The scope of the task group is to define the physical layer (PHY) and the media access controller (MAC). An overview of the specification can be found in [2]. A graphical representation of the areas of responsibility between the IEEE standard, ZigBee Alliance, and User is presented in Figure 1. The definition of the application profiles is organized by the ZigBee™ Alliance [3].

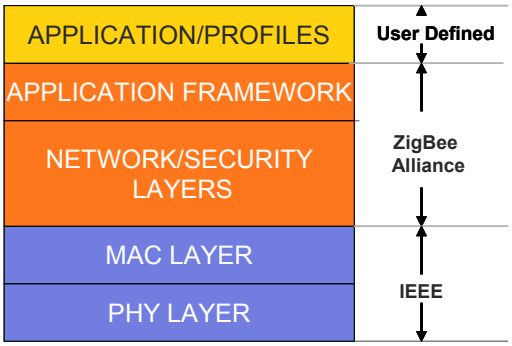

Figure 1 – IEEE 802.15.4 Stack

ZMD America, Inc.
craig@zmda.com

Since total system cost is a key factor for industrial and home wireless applications, a highly integrated single-chip approach is the preferred solution of semiconductor manufacturers developing IEEE 802.15.4 compliant transceivers. The IEEE standard at the PHY is the significant factor in determining the RF architecture and topology of ZigBee enabled transceivers currently sampling. Generally, CMOS is the desired technology to integrate both analog circuitry and high gate count digital circuitry for lower cost with the challenge being RF performance.

For these optimized short-range wireless solutions, the other key element above the Physical and MAC Layer is the Network/Security Layers for sensor and control integration. The ZigBee Alliance is in the process of defining the characteristics of these layers for star, mesh, and cluster tree topologies. The performance of these networks will complement the IEEE standard while meeting the requirements for low complexity and low power.

This paper will describe the characteristics of the IEEE 802.15.4 standard, RF design considerations of the PHY, ZigBee network topologies, and present a representative ZigBee application.

II. IEEE 802.15.4 OVERVIEW

The IEEE 802.15.4 standard defines two PHYs representing three license-free frequency bands that include sixteen channels at 2.4 GHz, ten channels at 902 to 928 MHz, and one channel at 868 to 870 MHz. The maximum data rates for each band are 250 kbps, 40 kbps and 20 kbps, respectively. The 2.4 GHz band operates worldwide while the sub-1 GHz band operates in North America, Europe, and Australia/New Zealand, Table 1. The IEEE standard is intended to conform to established regulations in Europe, Japan, Canada and the United States.

PHY	Frequency Band	Channel Numbering	Spreading Parameters		Data Parameters		
			Chip Rate	Modulation	Bit Rate	Symbol Rate	Modulation
868/915 MHz	868-870 MHz	0	300 kchip/s	BPSK	20 kb/s	20 kbaud	BPSK
	902-928 MHz	1 to 10	600 kchip/s	BPSK	40 kb/s	40 kbaud	BPSK
2.4 GHz	2.4-2.4835 GHz	11 to 26	2.0 Mchip/s	O-QPSK	250 kb/s	62.5 kbaud	16-ary Orthogonal

Table 1 - Frequency Bands and Data Rate

Both PHYs use Direct Sequence Spread Spectrum (DSSS). The modulation type in the 2.4 GHz band is O-QPSK with a 32 PN-code length and an RF bandwidth of 2 MHz. In the sub-1 GHz bands, BPSK modulation is used with a 15 PN-code length and operates in an RF bandwidth of 600 kHz in Europe and 1200 kHz in North America.

ZMD America, Inc.
craig@zmda.com

III. RF DESIGN CONSIDERATIONS

A representative sub-1 GHz transceiver is shown in Figure 2. The IC contains a 900 MHz physical layer (PHY) and portion of the media access controller (hardware-MAC). The remaining MAC functions (software-MAC) and the application layer are executed on an external microcontroller. All PHY functions are integrated on the chip with minimal external components required for a complete radio. A low-cost crystal is used as a reference for the PLL and to clock the digital circuitry. To optimize energy consumption in sleep mode while still keeping an accurate time base, a Real Time Clock reference can be used.

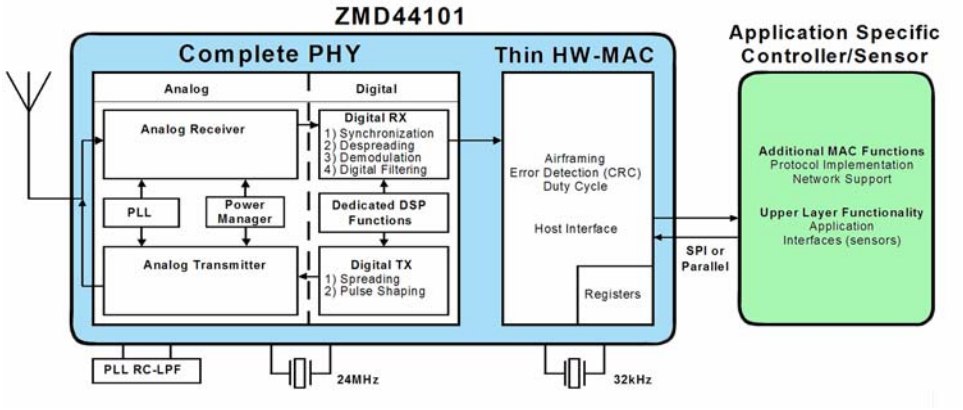

Figure 2 – Sub-1 GHz Transceiver Block Diagram

The analog portion of the receiver converts the desired signal from RF to the digital baseband. Synchronization, despreading and demodulation are done in the digital portion of the receiver. The digital part of the transmitter does the spreading and baseband filtering, whereas the analog part of the transmitter does the modulation and conversion to RF. The three main analog blocks - the direct-conversion receiver, direct-conversion transmitter, and fractional-N PLL, are discussed as follows.

The choice of the receiver architecture is mainly a compromise between performance, cost (considering both silicon area and external components), and power consumption [4]. A direct-conversion receiver (DCR) architecture (or Zero-IF architecture) was selected as there is no image frequency and IF filtering required. Further advantages are that the channel select filters are low-pass filters, instead of band-pass filters, and the baseband frequency is the lowest possible. The DCR architecture provides the additional benefits of lower cost, complexity, and power consumption [5].

The transmitter architecture is also direct-conversion. Since BPSK modulation is used, only one baseband path is required. A differential

ZMD America, Inc.
craig@zmda.com

architecture was used to minimize common mode noise. The output can be single-ended or differential. The single-ended output was selected for the advantages of lower cost, an on chip TR switch, and eliminates the requirement for an external balun.

Table 1 shows the channel allocation in the sub-1 GHz bands of the IEEE standard which sets the required bandwidth and frequency resolution. This had major impact on the PLL topology. The goal was one PLL circuit for the 868/915 MHz bands using a fixed crystal frequency. To meet these requirements, a fractional-N PLL architecture was chosen. An additional benefit is the software controlled fractional-N PLL provides the adaptability to meet future worldwide spectrum expansion in the range of 860 to 930 MHz. [6]

IV. ZIGBEE NETWORK CONSIDERATIONS

In the interest of brevity, many network specific features of the IEEE 802.15.4 standard are not covered in detail in this paper. However, these are necessary for the efficient operation of ZigBee networks. These features of the PHY include receiver energy detection, link quality indication and clear channel assessment. Both contention-based and contention-free channel access methods are supported with a maximum packet size of 128 bytes, which includes a variable payload up to 104 bytes. Also employed are 64-bit IEEE and 16-bit short addressing, supporting over 65,000 nodes per network. The MAC provides network association and disassociation, has an optional superframe structure with beacons for time synchronization, and a guaranteed time slot (GTS) mechanism for high priority communications. The channel access method is carrier sense multiple access with collision avoidance (CSMA-CA).

ZigBee defines the network, security, and application framework profile layers for an IEEE 802.15.4-based system. ZigBee's network layer supports three networking topologies; star, mesh, and cluster tree as shown in Figure 3. Star networks are common and provide for very long battery life operation. Mesh, or peer-to-peer, networks enable high levels of reliability and scalability by providing more than one path through the network. Cluster-tree networks utilize a hybrid star/mesh topology that combines the benefits of both for high levels of reliability and support for battery-powered nodes.

ZMD America, Inc.
craig@zmda.com

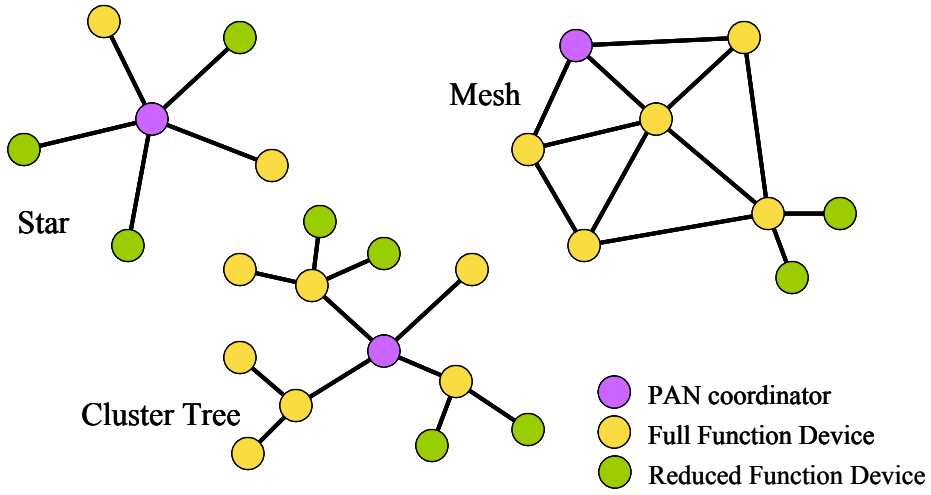

Figure 3 – ZigBee Network Topologies

To provide for low cost implementation options, the ZigBee *Physical* Device type distinguishes the type of hardware based on the IEEE 802.15.4 definition of reduced function device (RFD) and full function device (FFD). An IEEE 802.15.4 network requires at least one FFD to act as a network coordinator. The description of each Physical Device type is found in Table 2. [7]

Reduced Function Device	Full Function Device
Limited to star topology	Can function in any topology
Cannot become network coordinator	Capable of being Network coordinator
Talks only to network coordinator (FFD)	Capable of being a coordinator
Simple implementation – min RAM and ROM.	Can talk to any other device (FFD/RFD)
Generally battered powered	Generally line powered

Table 2 – ZigBee Physical Device Types

An RFD is implemented with minimum RAM and ROM resources and designed to be a simple send and/or receive node in a larger network. With a reduced stack size, less memory is required, thus a less expensive IC. ZigBee RFDs are generally battery powered. RFDs can search for available networks, transfer data from its application as necessary, determine whether data is pending, request data from the network coordinator, and sleep for extended periods of time to reduce battery consumption. RFDs can only talk to an FFD, a device with sufficient system resources for network routing. The FFD can serve as a network coordinator, a link coordinator or as just another communications device. Any FFD can talk to other FFD and RFDs. FFDs discover other FFDs and RFDs to establish communications, and are typically line powered.

The ZigBee *Logical* Device type distinguishes the *Physical* Device types (RFD or FFD) deployed in a specific ZigBee network. The *Logical* Device types are ZigBee Coordinators, ZigBee Routers, and ZigBee End Devices. The ZigBee

ZMD America, Inc.
craig@zmda.com

Coordinator initializes a network, manages network nodes, and stores network node information. The ZigBee Router participates in the network by routing messages between paired nodes. The ZigBee End Device acts as a leaf node in the network and can be an RFD or FFD. ZigBee application device types distinguish the type of device from an end-user perspective as specified by the Application Profiles.

ZigBee's self-forming and self-healing mesh network architecture permits data and control messages to be passed from one node to other node via multiple paths. This feature extends the range of the network and improves data reliability. This peer-to-peer capability may be used to build large, geographically dispersed networks where smaller networks are linked together to form a 'cluster tree' network. ZigBee provides a security toolbox to ensure reliable and secure networks. Access control lists, packet freshness timers and 128-bit encryption protect data transmission and ZigBee wireless networks. [8]

V. ZIGBEE APPLICATIONS

ZigBee networks consist of multiple traffic types with their own unique characteristics, including periodic data, intermittent data, and repetitive low latency data. The characteristics of each are as follows:

- Periodic data – usually defined by the application such as a wireless sensor or meter. Data typically is handled using a beaconing system whereby the sensor wakes up at a set time and checks for the beacon, exchanges data, and goes to sleep.
- Intermittent data – either application or external stimulus defined such as a wireless light switch. Data can be handled in a beaconless system or disconnected. In disconnected operation, the device will only attach to the network when communications is required, saving significant energy.
- Repetitive low latency data – uses time slot allocations such as a security system. These applications may use the guaranteed time slot (GTS) capability. GTS is a method of QoS that allows each device a specific duration of time as defined by the PAN coordinator in the Superframe to do whatever it requires without contention or latency.

For example, an automatic meter reading application represents a periodic data traffic type with data from water or gas meters being transmitted to a line powered electric meter and passed over a powerline to a central location. Using the beaconing feature of the IEEE standard, the respective RFD meter wakes up and listens for the beacon from the PAN coordinator, if received, the RFD requests to join the network. The PAN coordinator accepts the request. Once connected, the device passes the meter information and goes to sleep. This capability provides for very low duty cycles and enables multi-year battery life. Intermittent traffic types, such as wireless light switches, connect to the network

ZMD America, Inc.
craig@zmda.com

when needed to communicate (i.e. turn on a light). For repetitive low latency applications a guaranteed time slot option provides for Quality of Service with a contention free, dedicated time slot in each superframe that reduces contention and latency. Applications requiring timeliness and critical data passage may include medical alerts and security systems. In all applications, the smaller packet sizes of ZigBee devices results in higher effective throughput values compared to other standards.

ZigBee networks are primarily intended for low duty cycle sensor networks (<1%). A new network node may be recognized and associated in about 30 ms. Waking up a sleeping node takes about 15 ms, as does accessing a channel and transmitting data. ZigBee applications benefit from the ability to quickly attach information, detach, and go to deep sleep, which results in low power consumption and extended battery life.

VI. SUMMARY

This paper has combined the characteristics of the IEEE 802.15.4 standard with the maturing ZigBee specification in defining the wireless profiles for low data rate monitoring and control applications. The capabilities of both will result in the availability of a technology tailored specifically for the low power, low cost, and low complexity applications in the industrial, residential, and home today and in the future.

VII. REFERENCES

[1] Homepage of IEEE 802.15 WPAN Task Group 4 (TG4), http://grouper.ieee.org/groups/802/15/pub/TG4.html

[2] Ed Callaway, P. Gorday, L. Hester, J.A. Gutierrez, M. Neave, B. Heile, V. Bahl, "Home networking with IEEE 802.15.4: A developing standard for low-rate wireless personal area networks," *IEEE Communication Magazine*, vol. 40, no. 8, pp. 70-77, August 2002.

[3] Homepage of ZigBee™ Alliance, http://www.zigbee.org/

[4] B. Razavi, *RF Microelectronics*, Prentice Hall 1998.

[5] D. Pozar, *Microwave and RF Design of Wireless Systems*, 2001.

[6] Göpfert, L. and the ZMD Engineering Team, *A Fully-Integrated 900MHz CMOS RF Transceiver Including Digital Baseband for IEEE 802.15.4/ZigBee Application*.

[7] P. Kinney, *ZigBee Technology: Wireless Control that Simply Works*, White Paper dated 2 October 2003.

[8] Frenzel, L., *A Supplement to Electronic Design*, *Wireless Control That Simply Works*, January 12, 2004.

ZMD America, Inc.
craig@zmda.com