ZigBee: THE LOW DATA RATE WIRELESS TECHNOLGY FOR AD-HOC AND SENSOR NETWORKS

Manoj Kumar
STMicroelectronics Private Limited, Greater Noida, INDIA
manoj.kumar@st.com

Abstract: The Wireless technologies continue to find increasing applications in the home and industrial environments. Many home and industrial applications need low data rates for control purposes. Data acquisition and its transfer, building automation and security are the newer applications. It is desirable that the wireless sensors deployed for such applications have long battery lives. The suitability and advantages of ZigBee as a technology for such applications is explained. The paper consists of the theoretical background about ZigBee, its advantages over other wireless technologies for sensor environments and implementation examples.

1. INTRODUCTION TO 802.15.4 and ZigBee

There are several protocols which use 802.15.4 as its MAC layer. ZigBee is the most popular among these as of now.

There is sometimes confusion between 802.15.4 and ZigBee [1]. The ZigBee alliance (http://www.zigbee.org) is a consortium driven by industry and research institutions. It finalized the ZigBee specification in December 2004 and describes the higher layer protocols (networking, application) that operate on top of 802.15.4.

The recent IEEE 802.15.4 standard for low data rate wireless personal area networks (PANs) is widely considered as one of the technology candidates for wireless sensor networks.

Two network topologies are allowed by the standard, both of which rely on the presence of a central controller device known as the PAN coordinator. In a peer-to-peer topology, the devices can communicate with each other directly, as long as they are within the physical range. In a star shaped topology, the devices must communicate through a PAN coordinator. The network uses two types of channel access mechanisms, one based on the slotted CSMA-CA in which the slots are aligned with the beacon frames sent periodically by the PAN co-ordinator, and another based on unslotted CSMA-CA [2].

In the beacon enabled networks, channel time is divided into super-frames that are bounded by the beacon transmissions from the coordinator. The basic time units of the MAC protocol are the backoff periods to which all transmissions must be synchronized; at the 250 km/s data rate, the duration of one backoff period is tboff=0.32 ms. In the uplink direction individual nodes access the channel using CSMA-CA algorithm, and the channel must be idle

for two successive backoff periods before transmission can start [2]. If the channel is found busy, the random backoff countdown is repeated, possibly with a larger starting value.

The WPAN Low Rate Task Group (TG4) was chartered to investigate a low data rate solution with multi-month to multi-year battery life and very low complexity [3]. This standard specifies two physical layers: an 868 MHz/915 MHz direct sequence spread spectrum PHY and a 2.4 GHz direct sequence spread spectrum PHY. The 2.4 GHz PHY supports an over air data rate of 250 kb/s and the 868 MHz/915 MHz PHY supports over the air data rates of 20 kb/s and 40 kb/s. The physical layer chosen depends on local regulations and user preference. Potential applications are sensors, interactive toys, smart badges, remote controls, and home automation.

The ZigBee standard is a superset of the 802.15.4 standard and specifies the network security layer, application framework and application profiles so that ZigBee-certified equipment from different vendors will interoperate seamlessly. A ZigBee-certified application must conform to both the ZigBee standard and the 802.15.4 standard.

2. THE 802.15.4 AND ZigBee

In this section, the underlying standard for ZigBee i.e. 802.15.4 is discussed and its relationship to ZigBee is described.

2.1 The 802.15.4 PHY

The standard offers two PHY options based on the frequency band. Both are based on direct sequence spread spectrum (DSSS). The data rate is 250kbps at 2.4GHz, 40kbps at 915MHz and 20kbps at 868MHz. The higher data rate at 2.4GHz is attributed to a higher-order modulation scheme. Lower frequency provides longer range due to lower propagation losses. Low rate can be translated into better sensitivity and larger coverage area. Higher rate means higher throughput, lower latency or lower duty cycle. This information is summarized in **Error! Reference source not found.**. The channel spacing and frequency bands are shown in Figure 1.

The PHY provides two services: the PHY data service and PHY management service interfacing to the physical layer management entity (PLME). The PHY data service enables the transmission and reception of PHY protocol data units (PPDU) across the physical radio channel.

The features of the PHY are activation and deactivation of the radio transceiver, energy detection (ED), link quality indication (LQI), channel selection, clear channel assessment (CCA) and transmitting as well as receiving packets across the physical medium.

Table 1 : 802.15.4 Frequency Bands and Modulation Parameters [4]

PHY (MHz)	Frequency Band (MHz)	Spreading Parameters		Data Parameters		No. of Channels
		Chip rate (k chip s/s)	Modulation	Bit rate (kbps)	Symbol Rate (ksymbols/s)	
868/915	868-868.6	300	BPSK	20	20	1
	902-928	600	BPSK	40	40	10
2450	2400-2483.5	2000	O-QPSK	250	62.5	16

2.2 The 802.15.4 and ZigBee

The relationship of ZigBee with 802.15.4 is depicted in Figure 2. The PHY and MAC functions are indicated next to the layers depicted in the figure. The ZigBee is a layer that is on top of the 802.15.4 and is responsible for network routing, address translation, packet segmentation and profiles. The user applications are written on top of ZigBee profiles.

The IEEE 802.15.4-2003 standard defines the two lower layers: the physical (PHY) layer and the medium access control (MAC) sub-layer. The ZigBee Alliance builds on this foundation by providing the network (NWK) layer and the framework for the application layer. The application layer framework consists of the application support sub-layer (APS) and the ZigBee device objects (ZDO). Manufacturer-defined application objects use the framework and share APS and security services with the ZDO [5].

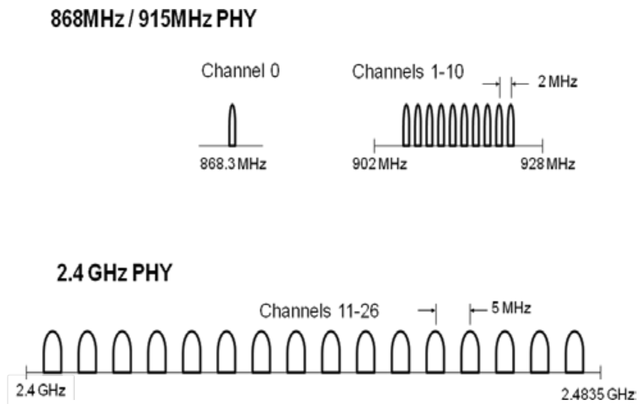

Figure 1 : The 802.15.4 Frequency Bands

IEEE 802.15.4-2003 has two PHY layers that operate in two separate frequency ranges: 868/915 MHz and 2.4 GHz. The lower frequency PHY layer covers both the 868 MHz European band and the 915 MHz band, used in countries such as the United States and Australia. The higher frequency PHY layer is used virtually worldwide.

2.3 The 802.15.4 Frame Structure

The 802.15.4 has four frame structures, each designated as PHY Protocol Data Unit (PPDU) in the standard for data transmissions – a beacon frame, a data frame, an acknowledgement frame and a MAC command frame.

All frames are structured in the similar fashion. The main difference is in the primary purpose or the

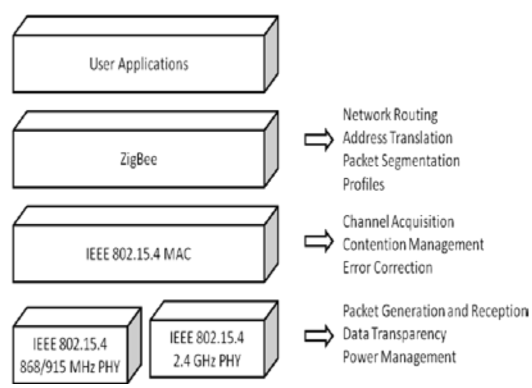

Figure 2 : 802.15.4 and ZigBee

payload. Each PPDU is constructed with a Synchronization header (SHR), a PHY header (PHR), and a PHY service data unit, composed of a MAC payload data unit (MPDU) as a data structure that services the MAC protocol layer. The frame structure format is shown in Figure 3**Error! Reference source not found.**.

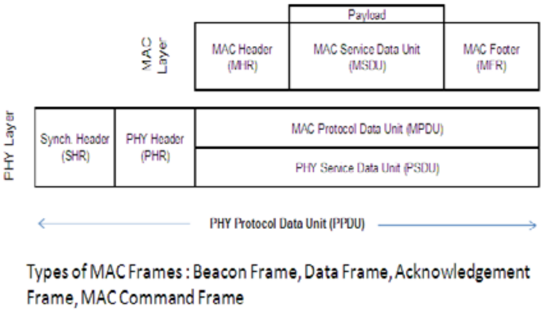

Figure 3 : The frame format

2.4 Key 802.15.4 Terms

PAN coordinator. The PAN coordinator is the node (strictly speaking, the coordinator node) that initiates the network and is the primary controller of the network. The PAN coordinator may transmit beacons and can communicate directly with any device in range. Depending on the network design, it may have memory sufficient to store information on all devices in the network, and must have memory sufficient to store routing information as required by the algorithm employed by the network.

Coordinator. The coordinator may transmit beacons and can communicate directly with any device in range. A coordinator may become a PAN coordinator, should it start a new network.

Device. A network device does not beacon and can directly communicate only with a coordinator or PAN coordinator.

Full function device (FFD). An FFD can operate in any of the three network roles (PAN coordinator, coordinator, or device). It must have memory sufficient to store routing information as required by the algorithm employed by the network. The complete protocol set is implemented in an FFD.

Reduced function device (RFD). An RFD is a very low cost device, with minimal memory requirements. It can only function as a network device. Its role is limited to star topology or an end device in peer-to-peer network. It cannot become a PAN coordinator.

2.5 Topologies

The IEEE 802.15.4 standard supports multiple network topologies. In the standard, two general types are discussed — star networks and peer-to-peer networks. In the star network, the master device is the PAN coordinator (an FFD), and the other network nodes may either be FFDs or RFDs. In the peer-to-peer network, FFDs are used, one of which is the PAN coordinator. RFDs may be used in a peer-to-peer network, but they can only communicate with a single FFD belonging to the network, and so do not save true "peer-to-peer" communication.

A ZigBee system consists of several components. The most basic one is the device. A device can be a full-function device (FFD) or reduced-function device (RFD). A network shall include at least one FFD, operating as the PAN coordinator. The FFD can operate in three modes: a personal area network (PAN) coordinator, a router, or a device. A RFD is intended for simple applications that do not need to send large amounts of data. A FFD can talk to RFDs or FFDs while a RFD can only talk to a FFD.

In the star topology, Figure 4, the communication is established between devices and a single central controller, called the PAN coordinator. The PAN coordinator may be AC powered while other devices will most likely be battery powered. Applications for this topology include home automation, personal computer (PC) peripherals, toys and games. After a FFD is activated for the first time, it may establish its own network and become the PAN coordinator. Each star-topology network chooses a PAN identifier, which is not currently used by any other

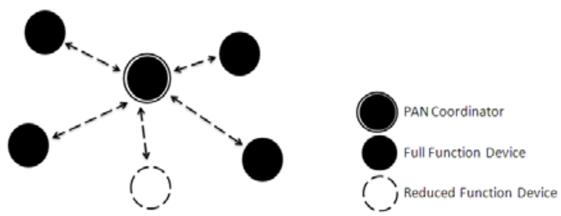

Figure 4 : The star topology

network within the communication range. This allows each star network to operate independently. Beacon is used to synchronize every node with PAN coordinator.

In peer-to-peer (mesh) topology, Figure 5, there is also one PAN coordinator. In contrast to star topology, any device can communicate with any other device as long as they are in range of one another. A peer-to-peer network can be ad hoc, self-organizing and self-healing. Applications such as industrial control and monitoring, wireless sensor networks, asset and inventory tracking would benefit from such topology. It also allows multiple hops to route messages from any device to any other device in the network. It can provide reliability by multipath routing. Beacon is not used for peer-to-peer topology. This reduces control and increases collisions as compared to the beacon enabled network.

Cluster-tree network, Figure 6, is a special case of a peer-to-peer network in which most devices are FFDs and a RFD may connect to a cluster-tree network as a leaf node at the end of a branch. Any of the FFD can act as a router and provide synchronization services to other devices and routers. Only one of these routers is the PAN coordinator. The PAN coordinator forms the first cluster by establishing itself as the cluster head (CLH) with a cluster identifier (CID) of zero, choosing an unused PAN identifier, and broadcasting beacon frames to neighboring devices. A candidate device receiving a

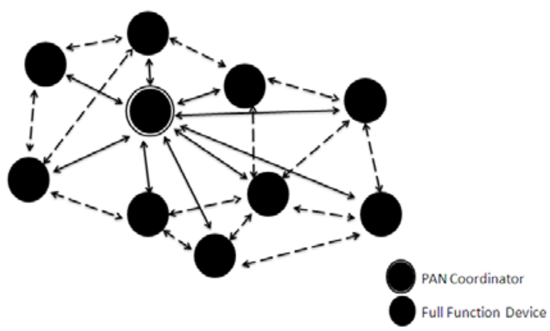

Figure 5 : Peer-to-peer topology

beacon frame may request the CLH to join the network. If the PAN coordinator permits the device to join, it will add this new device as a child device in its neighbor list. The newly joined device will add the CLH as its parent in its neighbor list and begins transmitting periodic beacons such that other candidate devices may then join the network at that device. Once application or network requirements are met, the PAN coordinator may instruct a device to become the CLH of a new cluster adjacent to the first one. The advantage of this multicluster, hierachial structure is the increased coverage area at the cost of increased message latency.

The ZigBee networks starts its formation as soon as the devices become active. The first FFD device that starts communication can establish itself as a ZigBee co-ordinator. All other devices that join later can request the ZigBee co-ordinator to join the network. Since no outside intervention is needed in this case, the ZigBee networks are considered to be self-forming networks.

Another feature of the mesh networking is that the network re-organizes itself in such a manner that the communication between the nodes continues even if some of the node stop to respond due to their movement of battery getting depleted.

Similarly ZigBee offers the ad-hoc networking, meaning thereby that the devices act as data pipes for the data that is not necessarily meant for them i.e. these devices may neither be the source or the destination of the data being forwarded or received.

3. ZigBee AND ZigBee PRO

The main differences between the ZigBee-2006v and the 2007 new release called ZigBee-PRO are.

Stochastic addressing: In the first ZigBee implementation the address was chosen by the Coordinator regarding the node position in the network tree. Now the 16b network address is chosen randomly. If the nodes choose the same address ir is solved using the 64b IEEE 802.15.4 MAC address.

Mesh data management: in the previous implementation each node had to keep a table of any of the routes from and to the gateway to any device (if it was in the routing path), now the nodes just save the way to get to the gateway (reducing the memory space needed). The gateway (a node supposed to have higher

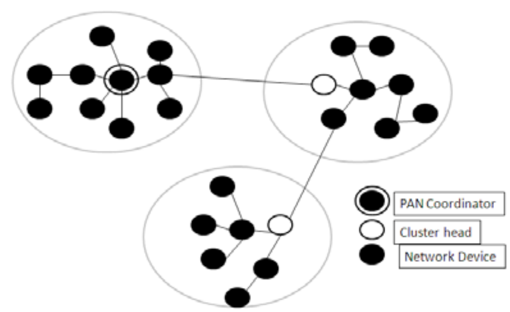

Figure 6 : Cluster tree topology

RAM resources) stores the path (with all the hops) to any of the nodes. When the gateway has to send a packet to a specific node it appends the information about the hops which has to be taken in the same packet. This method is called "many to one".

Fragmentation: large data packages can be easily fragmented.

Dynamic best channel choice: the nodes will move to another channel if the current one has interferences or noise (energy over a specific threshold).

Asymmetric connections: the links among the nodes are not always symmetric and the quality of the connection is different from node A to B than from node B to A, this is due to several reasons like the load of the node the interferences, the noise... for this reason the PRO version tries to take this issue into account and to make the best possible paths.

Security: The 2006 ZigBee implementation used up to AES 128b and a global network key to create secure communications. The new version has a more complex system which let each couple of nodes to have their own key so that p2p encryption can be performed. A peer to peer link encryption layer is added.

4. BATTERY LIFE

The ZigBee compliant radios switch automatically to switch mode and remain in this mode until there is a need for these to communicate. The ZigBee alliance does not specify the RF power. The IEEE 802.15.4 does specify a minimum power of 1mW. There are techniques that allow the RF power to be increased with sacrifice of the battery life. In some industrial applications, it is desirable to have high power ZigBee radios for better industrial controls. The sleep mode time and the lowest supply voltage that guarantees the correct operation are the two major parameters which affect the life of the node or the battery.

5. ZigBee COMPARISON WITH OTHER WIRELESS TECHNOLOGIES

The comparison of ZigBee with various other wireless technologies is given in Table 2. It is clear that ZigBee offers very good battery life, particularly for those cases when data transmission is not too heavy. This makes ZigBee an ideal candidate for industrial control applications.

6. EXAMPLE APPLICATIONS

One interesting application of the zigbee associated with the MEMS is the tracking of the expensive equipments inside warehouses, store or hospitals where the movement information can be sent by the ZigBee device to all other nearby devices which, in turn would communicate it up to the central node. In the following paragraphs, a few applications developed using ZigBee are described.

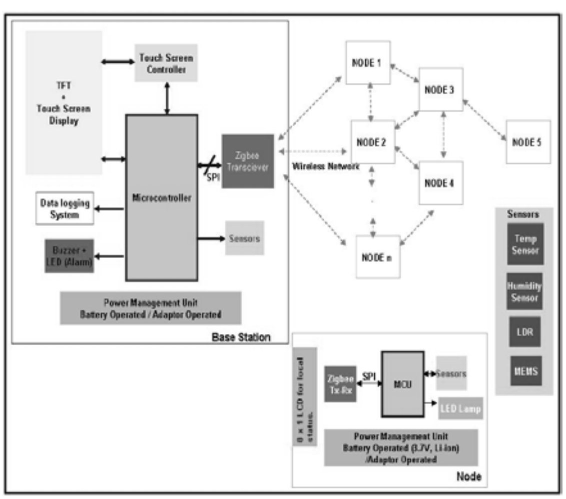

Figure 7 : Building Automation System

6.1 Application: Wireless Sensor Network inside a building

The wireless building automation system, Figure 7 consists of several sensors spread in the various building areas. These sensors communicate to each other in ad-hoc manner sending their own information and forwarding the information received from other nodes. In a smaller and different version of this, it is possible to have many sensors on one node and information regarding many sensors from each of these 'smart node' to the 'smart base station'. In the example application, this scenario is shown.

Table 2 : ZigBee Compared with other wireless technologies

Parameter	Bluetooth	Wireless LAN	ZigBee
Frequency band	2.4 GHz	2.4 GHz	2.4 GHz
Physical/MAC layers	IEEE 802.15.1	IEEE 802.11b	IEEE 802.15.4
Range	10 m	75 to 90 m	Indoors: up to 30 m Outdoors (line of sight): up to 100 m
Current consumption	60 mA (Tx mode)	400 mA (Tx mode) 20 mA (Standby mode)	25-35 mA (Tx mode) 3 µA (Standby mode)
Raw data rate	1 Mbps	11 Mbps	250 Kbps
Protocol stack size	250 KB	1 MB	32 KB 4 KB (for limited function end devices)
Typical network join time	>3 sec	variable, 1 sec typically	30 ms typically
Typical Battery Life (Days)	1-7	0.5-5	100-1000
Interference avoidance method	FHSS (frequency-hopping spread spectrum)	DSSS (direct-sequence spread spectrum)	DSSS (direct-sequence spread spectrum)

Minimum quiet bandwidth required	15 MHz (dynamic)	22 MHz (static)	3 MHz (static)
Maximum number of nodes per network	7	32 per access point	64 K
Number of channels	19	13	16

Each of the 'smart node' has sensors like temperature, ambient light (LDR), motion (MEMS). The information from all these sensors is collected and sent to the 'smart base station' periodically. The

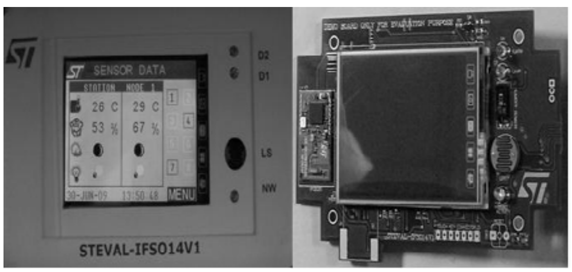

Figure 8 : The 'Smart Monitoring Station'

base station, Figure 8 , has the possibility to display the sensed parameter at each of the nodes and can control the action at the nodes.

The prototype implementation is done using ZigBee module (SPZB250) and a 32-bit Microcontroller (STM32x), as in Figure 7. The 'smart nodes' are similar to the 'smart base station' and have the capability of displaying their own parameters even when not connected to the 'smart base station'.

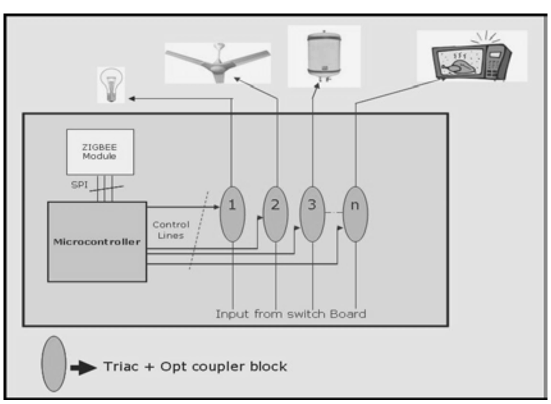

Figure 9 : ZigBee node Controlling AC loads

Another feature is that the nodes can be associated to the real AC loads for switching on and off those equipments. One such implementation has been done to switch on and off the electric bulb in a manner shown in Figure 9.

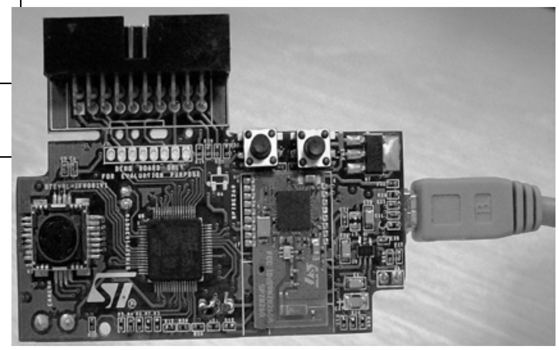

Figure 10 : ZigBee used to send images

6.2 APPLICATION : The Zigbee transmitter and receiver for Images

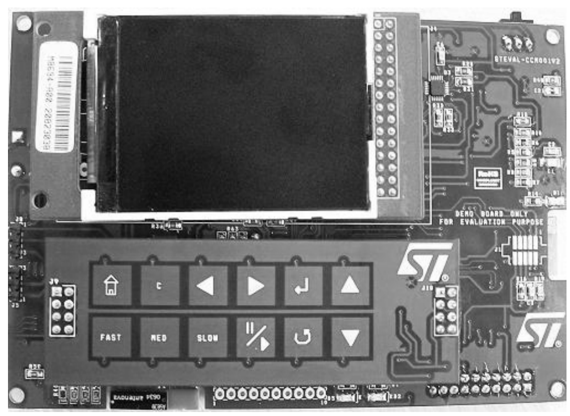

Figure 11 : The ZigBee receiver and display unit

A ZigBee based image transfer has been implemented in another application. A standard CMOS camera captures the images, processes the

jpeg image and sends it using ZigBee to another ZigBee module that is in turn connected to a local display. This application is tested for point to point connection only. In this scenario, the nodes are expected to be in the active condition. It is possible to configure the node in this case in a manner that the data transfer occurs only when there is a need based on a pre-defined condition.

7. REFERENCES

[1] A. Willig, K. Matheus and A. Wolisz," Wireless Technology in Industrial Networks", Proceedings of the IEEE, Vol 93, No.6, June 2005, pp 1130-1151.

[2] J. Misic, S. Shafi and V. Misic,"Cross-Layer Activity Management in an 802.15.4 Sensor Network", IEEE Communications Magazine, January 2006, pp131-136.
[3] G. Roberts, "IEEE 802.15 Overview of WG and Task Groups", IEEE 802.15 TG DRAFT TUTORIALS.
[4] J.A. Gutierrez, E.H. Callaway, R.L. Barrett, " Low-Rate Wireless Personal Area Networks, Enabling Wireless sensors with IEEE 802.15.4", IEEE Press, 2004.
[5] ZigBee Specifications, January 17 2008.