M. Tech. Credit Seminar Report, Electronic Systems Group, EE Dept, IIT Bombay
submitted Nov 2004

Zigbee – Wireless sensor networking for automation

A.D.Darji (Roll No. 04307303)
Supervisor: Prof. H.K.Pillai

Abstract

There are a multitude of standards like Bluetooth and WiFi for mid to high data rates for voice, PC LAN, video etc. However, up till now there hasn't been wireless network standard that meet the unique needs of sensors and control devices for industrial and home automation. Sensors and controls do not need high bandwidth but they do need low latency, very low energy consumption for long battery life and for large device array support. The zigbee alliance is providing standardized base set of solutions for automation. Zigbee is one of the promising protocols, a software layer based on IEEE 802.15.4 standard for Low rate wireless personal area network (LR-WPAN). After a brief discussion on various fieldbuses for networked control this report gives detail study of IEEE 802.15.4 standard. Focus is made on Medium Access Control (MAC) for wireless application. Report also describes application areas of zigbee stack and comparison with existed wireless standard. This report also discusses the technical considerations and system requirements necessary for implementation on LR-WPAN.

1 Introduction

The Fieldbus (FB) concept is the equivalent of a local area network for process control and measurement devices. It allows devices in a system to be connected on a single "bus" cable and for data to flow quickly and efficiently to and from the processing nodes of the network. The ever decreasing cost and evolution of LAN technology have led to fieldbuses being adopted to communicate between the controller and its controlled devices. Fieldbus standardizes the way devices connect and therefore allows the easy integration of devices from multiple vendors. Fieldbuses such as AS-1, Devicenet, Industrial Ethernet, Field bus and Profibus are becoming more popular in control system implementation for use in automated manufacturing system. These fieldbuses allow sensor, controller and actuators to be connected to a network as node instead of hard wiring the devices with point to point connection. Fieldbus implementation reduces system wiring and provides easy system diagnosis and maintenance [1].

In the next few years it is expected that low rate wireless personal area networks (LR-WPAN) will be used in a wide variety of embedded applications, including home automation, industrial sensing and control, environment monitoring and sensing. In these applications numbers of embedded devices running on batteries are distributed in an area and they communicate on wireless radio. Compared to wireless local area network (WLAN) which aim to provide high through-put, low

latency for traditional file transfer and multimedia applications, the required data rate for LR-WPAN applications is expected to be only on the order of tens of kbps. The MAC protocol plays a significant role in determining the efficiency of wireless channel bandwidth and energy cost of communication. Recently, a new standard named IEEE 802.15.4 has been developed. The goal of this standard is to provide a physical-layer and MAC-layer standard with ultra low complexity, cost and power for low data-rate wireless connectivity among fixed embedded devices [2].

In this report, I discuss classification and performance of networked control system. Apart from these, wireless control MAC standard IEEE 802.15.4 and for Zigbee application is also presented.

2 Motivation

Point to point communication architecture for embedded communication has been successfully implemented in industries for decades. Traditional point to point control system is no longer suitable to meet the new requirements, such as wireless, modularity, decentralization of control, integrated diagnostic, quick and easy maintenance and low cost. The implementation of network architecture can improve the efficiency, flexibility and reliability. It also reduces the installation, reconfiguration and maintenance time and cost. At the same time new network based architecture may introduce time delay uncertainty between sensor, actuator and controller. This time delay is due to sharing of common medium and computational time required for signal processing. Time delay depends on the protocol adapted and hardware chosen. Time delay can degrade a system's performance and even cause system instability. The proper message transmission protocol is necessary to guarantee network quality of service (QoS). So performance analysis and comparison is very much useful for choosing proper network protocol which gives optimized performance in terms of data-rate, cost and power requirement.

3 Control Network Basic

Networks are broadly classified in two categories; Data network and control network. Data network is useful for transfer of large data packet and relatively infrequent bursty transmission over wide area with high data rate. In contrast control network useful to transfer small but frequent control signals among a relatively large sets of nodes to meet time critical requirement of real time control system. Many different network types have been promoted for use in control systems. We first compare three of them: the Ethernet bus, with Carrier Sense Multiple Access with Collision Detection (CSMA/CD), token passing bus (e.g., ControlNet), and Controller Area Network (CAN) bus (e.g., DeviceNet). A detailed discussion of the medium access control (MAC) mechanism for each network is provided. The MAC is responsible for providing both the satisfaction of the time-critical/real-time response requirement over the network and the quality and reliability of the communication between nodes on the network [3] [1].In this section, we discuss the MAC mechanism of three types of control networks. The MAC mechanism describes the

protocol for btaining access to the network. Therefore the discussion and comparison thus focuses on the MAC mechanisms.

3.1 Ethernet (CSMA/CD)

Ethernet uses the CSMA/CD mechanism for resolving contention on the communication medium. The CSMA/CD protocol is specified in the IEEE 802.3 network standard. When a node wants to transmit, it listens to the network. If the network is busy, it waits until the network is idle; otherwise it transmits immediately. If two or more nodes listen to the idle network and decide to transmit simultaneously, the messages of these transmitting nodes collide and the messages are corrupted. While transmitting, a node must also listen to detect a message collision. On detecting a collision between two or more messages, a transmitting node stops transmitting and waits a random length of time to retry its transmission. This random time is determined by the standard Binary Exponential Backoff (BEB) algorithm: the retransmission time is randomly chosen between 0 and $(2^i - 1)$ slot times [15], where i denotes the i^{th} collision event detected by the node and one slot time is the minimum time needed for a round-trip transmission. However, after 10 collisions have been reached, the interval is fixed at a maximum of 1023 slots. After 16 collisions, the node stops attempting to transmit and reports failure back to the node microprocessor. Further recovery may be attempted in higher layers [3].

3.2 ControlNet (Token Passing Bus)

MAP, PROFIBUS, and ControlNet are typical examples of token-passing bus control networks. These are deterministic networks because the maximum waiting time before sending a message frame can be characterized by the token rotation time. The token bus protocol (IEEE 802.4) allows a linear, multidrop, tree-shaped, or segmented topology [16]. The nodes in the token bus network are arranged logically into a ring, and, in the case of ControlNet, each node knows the address of its predecessor and its successor. During operation of the network, the node with the token transmits data frames until either it runs out of data frames to transmit or the time it has held the token reaches the limit. The node then regenerates the token and transmits it to its logical successor on the network. If a node has no message to send, it just passes the token to the successor node. The physical location of the successor is not important because the token is sent to the logical neighbor. Collision of data frames does not occur, as only one node can transmit at a time. The protocol also guarantees a maximum time between network accesses for each node, and the protocol has provisions to regenerate the token if the token holder stops transmitting and does not pass the token to its successor. Nodes can also be added dynamically to the bus and can request to be dropped from the logical ring [3].

3.3 DeviceNet (CAN Bus)

CAN is a serial communication protocol developed mainly for applications in the automotive industry but also capable of offering good performance in other time-critical industrial applications. The CAN protocol is optimized for short messages and uses a CSMA/Arbitration on Message Priority (CSMA/AMP) medium access method. Thus the protocol is message-oriented, and each message has a specific priority that is

used to arbitrate access to the bus in case of simultaneous transmission. The bit-stream of a transmission is synchronized on the start bit, and the arbitration is performed on the following message identifier, in which logic '0' is dominant over a logic '1.' A node that wants to transmit a message waits until the bus is free and then starts to send the identifier of its message bit by bit. Conflicts for access to the bus are solved during transmission by an arbitration process at the bit level of the arbitration field, which is the initial part of each frame. Hence, if two devices want to send messages at the same time, they first continue to send the message frames and then listen to the network. If one of them receives a bit different from the bit it sends out, it loses the right to continue to send its message, and the other wins the arbitration. With this method, an ongoing transmission is never corrupted.

In a CAN-based network, data are transmitted and received using message frames that carry data from a transmitting node to one or more receiving nodes. Transmitted data do not necessarily contain addresses of either the source or the destination of the message. Instead, each message is labeled by an identifier that is unique throughout the network. All other nodes on the network receive the message and accept or discard it, depending on the configuration of mask filters applied to the identifier. This mode of operation is known as multicast [3].

4 Wireless Network Architecture for Automation

Field buses are highly reliable technology for embedded automation because they are optimized for transmitting a large number of short messages. In industrial automation and control, response time is much more important than throughput. For wireless automation, the bandwidth demand is moderate .The major requirements of wireless automation are real time response, long service life , high reliability and low cost. Thus most of the LAN technologies are not applicable to wireless automation without profound change [4].

4.1 Zigbee Stack

A new standard for communications technology in control is IEEE 802.15.4 and a non-profit consortium called the Zigbee Alliance is developing protocols using the physical layer of IEEE 802.15.4 **(Figure 1)**.The focus of the Zigbee standard is specifically monitoring and control, and it permits monitoring over 10 to 100meters, with over 250 nodes per network, with very small system resource usage and very low battery power usage. Zigbee is slower than Bluetooth, but goes farther, has more nodes, and is very cost effective. Zigbee networks interface easily with 802.11b networks for longer and faster data transmission. It is likely that Zigbee networks will be useful for flow control applications on the plant floor and in remote stations like pumping plants and sewage lift stations where all the devices can be interconnected by a Zigbee network instead of hardwiring [6].

The intent of IEEE 802.15.4 is to address applications where existing WPAN solutions are too expensive and the performance of a technology such as Bluetooth™ is not required. IEEE 802.15.4 LR-WPANs complement other WPAN technologies

by providing very low power consumption capabilities at very low cost, thus enabling applications that were previously impractical [9].

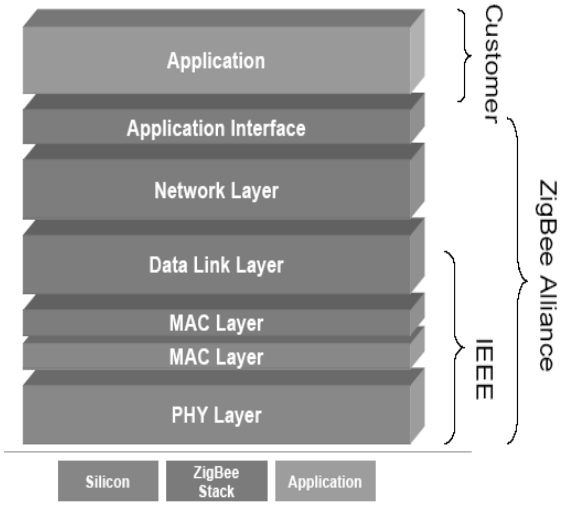

Figure 1: Zigbee alliance-IEEE- customer relation [5]

Table 1: IEEE 802.15.4 features [7]

Property	**Range**
Raw data rate	868 MHz: 20 kb/s; 915 MHz: 40 kb/s; 2.4 GHz: 250 kb/s
Range	10–20 m
Latency	Down to 15 ms
Channels	868/915 MHz: 11 channels 2.4 GHz: 16 channels
Frequency band	Two PHYs: 868 MHz/915 MHz and 2.4 GHz
Addressing	Short 8-bit or 64-bit IEEE
Channel access	CSMA-CA and slotted CSMA-CA
Temperature	Industrial temperature range –40 to +85 C

4.2 The Network Layer

Like all IEEE 802 standards, the IEEE 802.15.4 draft standard encompasses only those layers up to and including portions of the data link layer (DLL). Higher-layer protocols are at the discretion of the individual applications. In traditional wired networks, the network layer is responsible for topology construction and maintenance, as well as naming and binding services, which incorporate the necessary tasks of addressing, routing, and security. In fact, it is important for any network layer implementation built on the already energy conscious IEEE 802.15.4 draft standard to be equally conservative. Network layers built on the standard are expected to be self-

organizing and self-maintaining, to minimize total cost to the consumer. The IEEE 802.15.4 draft standard supports multiple network topologies, including both star and peer-to-peer networks **(Figure 2)**. The topology is an application design choice; some applications, such as PC peripherals, may require the low-latency connection of the star network, while others, such as perimeter security, may require the large-area coverage of peer-to-peer networking. Multiple address types, including both physical (i.e., 64-bit IEEE) and short (i.e., 8-bit network-assigned) are provided

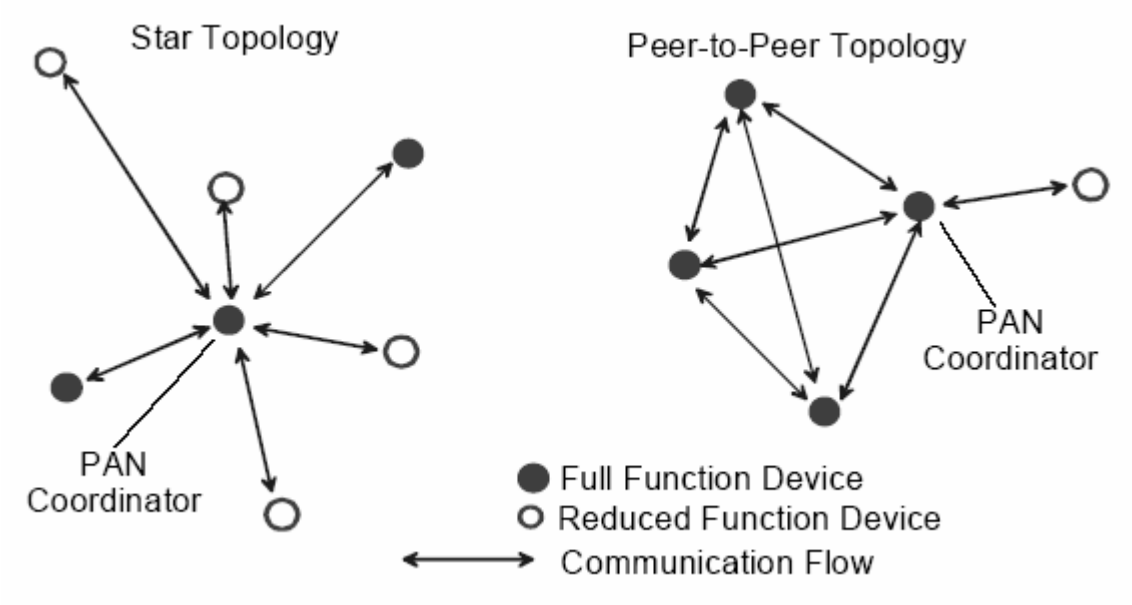

Figure 2: Star and peer-to-peer topology examples [8]

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 [8].

4.3 The Data Link Layer

The IEEE 802 project splits the DLL into two sublayers, the MAC and logical link control (LLC) sublayers. The LLC is standardized in 802.2 and is common among the 802 standards such as 802.3, 802.11, and 802.15.1, while the MAC sub - layer is closer to the hardware and may vary with the physical layer implementation. **Figure 3** shows how IEEE 802.15.4 fits into the International Organization for

Standardization (ISO) open systems interconnection (OSI) reference model [7]. The IEEE 802.15.4 MAC provides services to an IEEE 802.2 type I LLC through the service-specific convergence sublayer (SSCS), or a proprietary LLC can access the MAC services directly without going through the SSCS. The SSCS ensures compatibility between different LLC sublayers and allows the MAC to be accessed through a single set of access points. Using this model, the 802.15.4 MAC provides features not utilized by 802.2, and therefore allows the more complex network topologies mentioned above. The features of the IEEE 802.15.4 MAC are association and disassociation, acknowledged frame delivery, channel access mechanism, frame validation, guaranteed time slot management, and beacon management.

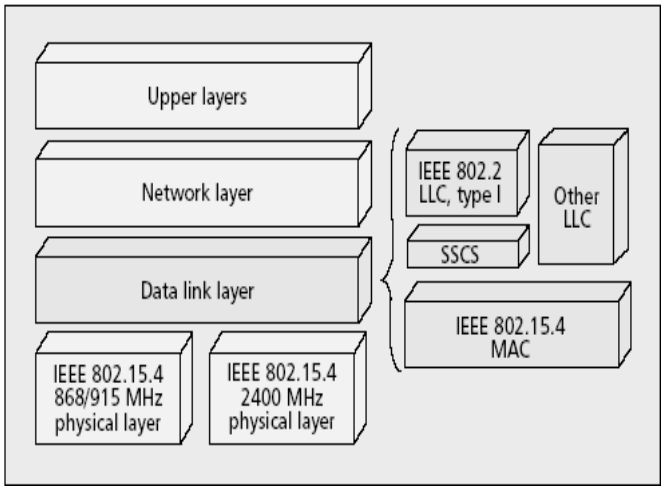

Figure 3: IEEE 802.15.4 in the ISO-OSI layered network model [7].

The MAC sublayer provides two services to higher layers that can be accessed through two service access points (SAPs). The MAC data service is accessed through the MAC common part sublayer (MCPS-SAP), and the MAC management services are accessed through the MAC layer management entity (MLME-SAP). These two services provide an interface between the SSCS or another LLC and the PHY layer. The MAC management service has 26 primitives. Compared to 802.15.1 (Bluetooth™), which has about 131 primitives and 32 events, the 802.15.4 MAC is of very low complexity, making it very suitable for its intended low-end applications, albeit at the cost of a smaller feature set than 802.15.1 (e.g., 802.15.4 does not support synchronous voice links).

4.4 The General MAC Frame Format

The MAC frame structure is kept very flexible to accommodate the needs of different applications and network topologies while maintaining a simple protocol. The general format of a MAC frame is shown in **Figure 4**. The MAC frame is called the MAC protocol data unit (MPDU) and is composed of the MAC header (MHR), MAC service data unit (MSDU), and MAC footer (MFR). The first field of the MAC header is the frame control field. It indicates the type of MAC frame being

transmitted, specifies the format of the address field, and controls the acknowledgment. In short, the frame control field specifies how the rest of the frame looks and what it contains. The IEEE 802.15.4 MAC has four different frame types. These are the beacon frame, data frame, acknowledgment frame, and MAC command frame. Only the data and beacon frames actually contain information sent by higher layers; the acknowledgment and MAC command frames originate in the MAC and are used for MAC peer-to-peer communication.

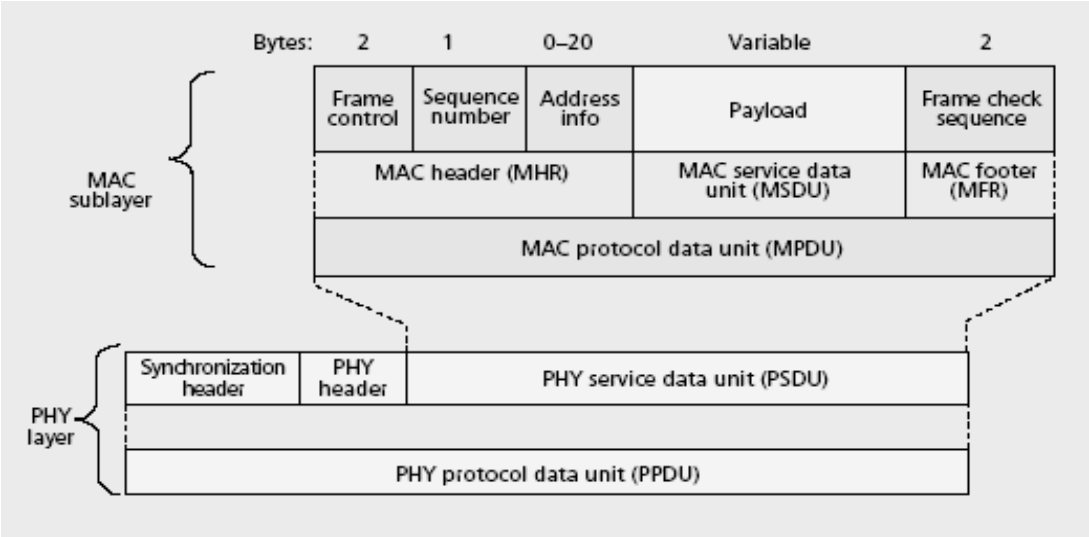

Figure 4: The general MAC frame format [7].

The size of the address field may vary between 0 and 20 bytes. For instance, a data frame may contain both source and destination information, while the return acknowledgment frame does not contain any address information at all. On the other hand, a beacon frame may only contain source address information. In addition, short 8-bit device addresses or 64-bit IEEE device addresses may be used. This flexible structure helps increase the efficiency of the protocol by keeping the packets short. The payload field is variable in length; however, the complete MAC frame may not exceed 127 bytes in length. The data contained in the payload is dependent on the frame type. Other fields in a MAC frame are the sequence number and frame check sequence (FCS). The sequence number in the MAC header matches the acknowledgment frame with the previous transmission. The transaction is considered successful only when the acknowledgment frame contains the same sequence number as the previously transmitted frame. The FCS helps verify the integrity of the MAC frame. The FCS in an IEEE 802.15.4 MAC frame is a 16-bit International Telecommunication Union — Telecommunication Standardization Sector (ITU-T) cyclic redundancy check (CRC).

4.4.1 The Superframe Structure

The MAC protocol in IEEE 802.15.4 can operate on both beacon enable and non-beacon modes. In the beacon less mode the protocol is essentially a simple

CSMA-CA (Carrier Sense Multiple Access – Collision Avoidance) protocol. In beacon mode, the IEEE 802.15.4 uses a super frame structure as shown in **Figure 5.**

Some applications may require dedicated bandwidth to achieve low latencies. To accomplish these low latencies, the IEEE 802.15.4 LR-WPAN can operate in an optional superframe mode. In a superframe, a dedicated network coordinator, called the PAN coordinator, transmits superframe beacons in predetermined intervals. These intervals can be as short as 15 ms or as long as 245 s. There are both active and inactive period in superframe. Devices communicate with their PAN only during the active period and enter a low power mode during inactive period. The parameter mac Beacon Order (BO) decides the length of beacon interval (BI= 2^{BO} x a Base Super Frame Duration) and parameter mac Super Frame Order (SO) decide the length (2^{SO} x a Base Super Frame Duration) of active portion of the superframe [2].The time between two beacons is divided into 16 equal time slots independent of the duration of the superframe. A device can transmit at any time during a slot, but must complete its transaction before the next superframe beacon.

The Active portion of superframe is further divided in to 16 equal time slots and consists of three parts: the beacon, a Contention Access Period (CAP) and Contention Free Period (CFP). The channel access in the time slots is contention-based; however, the PAN coordinator may assign time slots to a single device requiring dedicated bandwidth or low-latency transmissions. These assigned time slots are called *guaranteed time slots* (GTS) and together form a contention-free period located immediately before the next beacon (Figure 5). The size of the contention-free period may vary depending on demand by the associated network devices; when GTS are employed, all devices must complete their contention-based transactions before the contention-free period begins. Each GTS consists of some integer multiple of CFP slots and up to 7 GTS are allowed in CPF [2]. The beginning of the contention-free period and duration of the superframe are communicated to the attached network devices by the PAN coordinator in its beacon [11].

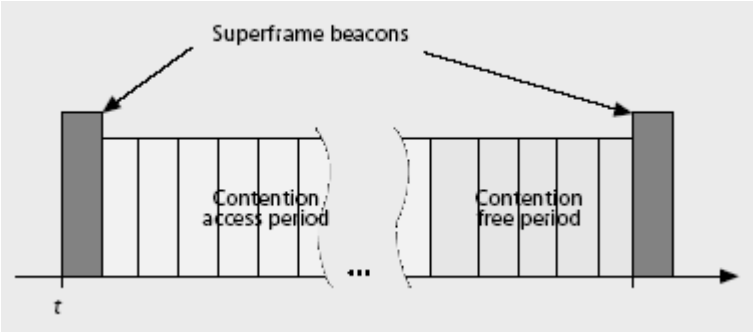

Figure 5: The LR-WPAN superframe structure [7]

5 MAC Protocol Overview in IEEE 802.15.4 [2]

Depending on network configuration, an LR-WPAN may use one of two channel access mechanisms. In a beacon-enabled network with superframes, a slotted

carrier sense multiple access with collision avoidance (CSMA-CA) mechanism is used. In networks without beacons, unslotted or standard CSMA-CA is used. This works as follows. When a device wishes to transmit data to PAN in a non-beacon-enabled network, it first checks if another device is currently transmitting on the same channel. If so, it may back off for a random period, or indicate a transmission failure if unsuccessful after some retries. Acknowledgment frames confirming a previous transmission do not use the CSMA mechanism since they are sent immediately following the previous packet. The PAN coordinator announces the superframe structure to PAN devices periodically through beacon frames. By changing active and inactive portion via parameter SO and BO, WPAN can operate under low duty cycle to conserve energy [2].

5.1 Contention Access Period (CAP)

In a beacon-enabled network, any device wishing to transmit during the contention access period, it enables its receiver and waits for the beginning of the next time slot and then determines if another device is currently transmitting in the same slot. If another device is already transmitting in the slot, the device backsoff for a random number of slots (up to 2^{BE}-1 period) and determines if channel is clear or indicates a transmission failure after some retries.

Three variables are maintained at each device for a channel access: NB, CW and BE. NB is the number of times the CSMA-CA backoffs while attempting the current transmission, and is reset to 0 for each new data transmission. CW is contention window length, which is reset to 2 either for a new data transmission or when the channel is found to be busy. BE is backoff exponent, which is related to backoff periods a device should wait before attempting carrier sensing. In addition, in a beacon- enabled network, acknowledgment frames do not use CSMA [2].An important function of the MAC is confirming successful reception of a received frame. Successful reception and validation of a data or MAC command frame is confirmed with an acknowledgment. If the receiving device is unable to handle the incoming message for any reason, the receipt is not acknowledged. The frame control field indicates whether or not an acknowledgment is expected. The acknowledgment frame is sent immediately after successful validation of the received frame. Beacon frames sent by a PAN coordinator and acknowledgment frames are never acknowledged.

In CSMA-CA, a lot of energy is generally consumed by long backoff period during high traffic to avoid collisions. As IEEE 802.15.4 supports a Battery Life Extension (BLE) mode, backoff exponent is limited to 0-2.This reduces the period of ideal listening in low offered traffic applications. A network device can put its radio to sleep to conserve energy immediately after the reception of acknowledgement packet if there is no more data to be sent or received.

5.2 Contention Free Period (CFP)

The IEEE 802.15.4 standard allows the optional use of CFP for devises those required dedicated bandwidth to achieve low latencies. Device requiring dedicated bandwidth and low latencies transmission can be assigned GTS in CFP by PAN coordinator. When device whishes to transmits the frame during GTS, it first check a list on the beacon frame to see whether it has been allocated a valid GTS. If a valid GTS is found, the device enables its receiver at a time prior to start of the GTS and transmits the data during the GTS period. The MAC of the PAN coordinator ensure that its receiver is enabled for all allocated guaranteed time slots All contention based actions must be completed before the CFP begins.

5.3 Synchronization

The PAN coordinator transmits beacon frames periodically to announce the superframe structure in a PAN. Devices need to synchronize with coordinator by receiving and decoding the beacon frames before any data transmission. There are two methods of synchronization: tracking and non-tracking [2].

With tracking, the device receives the first beacon, gets current superframe structure, known when to active its receiver for the next beacon and keep track of it. To transmit a frame, the device can enable its receiver just a little earlier before the beacon arrival. With non-tracking, the device attempts to acquire the beacon only once. The device needs to enable its receiver and searches for a specific period until it receives a beacon from its associated coordinator, when it attempts to transmit a frame.

6 The Physical Layer

IEEE 802.15.4 offers two PHY options that combine with the MAC to enable a broad range of networking applications. Both PHYs are based on direct sequence spread spectrum (DSSS) methods that result in low-cost digital IC implementation, and both share the same basic packet structure for low-duty-cycle low-power operation. The fundamental difference between the two PHYs is the frequency band. The 2.4 GHz PHY specifies operation in the 2.4 GHz industrial, scientific, and medical (ISM) band, which has nearly worldwide availability, while the 868/915 MHz PHY specifies operation in the 868 MHz band in Europe and 915 MHz ISM band in the United States [8].While mobility between countries is not anticipated for most home networking applications, the international availability of the 2.4 GHz band does offer advantages in terms of larger markets and lower manufacturing costs. On the other hand, the 868MHz and 915 MHz bands offer an alternative to the growing congestion and other interference (microwave ovens, etc.) associated with the 2.4 GHz band, and longer range for a given link budget due to lower propagation losses.

A second distinguishing PHY characteristic of interest to network and application designers is transmission rate. The 2.4 GHz PHY provides a transmission rate of 250 kb/s, while the 868/915 MHz PHY offers rates of 20 kb/s and 40 kb/s for its two bands, respectively. The higher rate in the 2.4 GHz PHY is attributed largely to a higher-order modulation scheme, in which each data symbol represents multiple bits. The different transmission rates can be exploited to achieve a variety of different goals. For example, the low rate of the 868/915 MHz PHY can be translated into better sensitivity and larger coverage area, thus reducing the number of nodes required to cover a given physical area, while the higher rate of the 2.4 GHz PHY can be used to attain higher throughput, lower latency, or lower duty cycle. It is expected that each PHY will find applications for which its strengths are best suited.

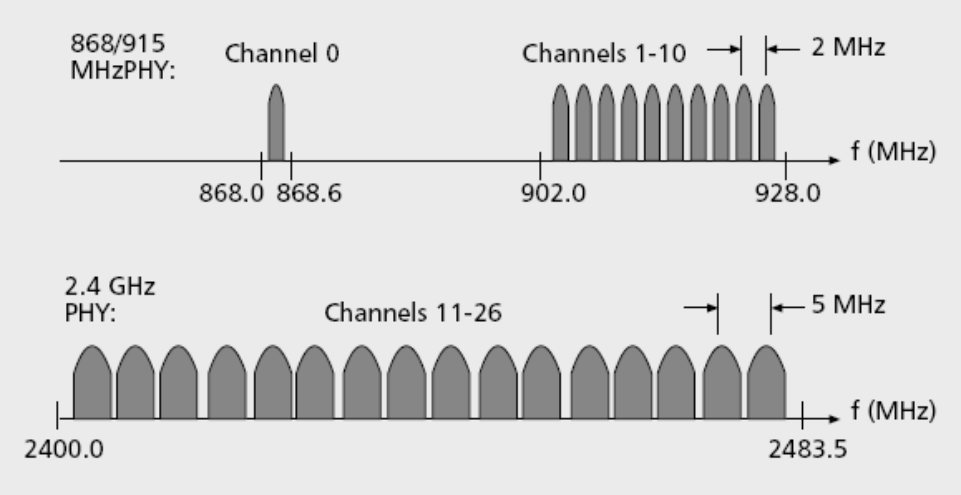

Figure 6: The IEEE 802.15.4 channel structure [7]

Table 2: IEEE 802.15.4 channel frequencies [7]

Channel number	**Channel center frequency (MHz)**
$k = 0$	868.3
$k = 1, 2, \ldots, 10$	$906 + 2(k - 1)$
$k = 11, 12, \ldots, 26$	$2405 + 5(k - 11)$

6.1 Channelization

Twenty-seven frequency channels are available across the three bands **(Figure 6** and **Table 2**). The 868/915 MHz PHY supports a single channel between 868.0 and 868.6 MHz, and 10 channels between 902.0 and 928.0 MHz. Due to the regional support for these two bands, it is unlikely that a single network would ever use all 11 channels. However, the two bands are considered close enough in frequency that similar, if not identical, hardware can be used for both, lowering manufacturing costs.

The 2.4 GHz PHY supports 16 channels between 2.4 and 2.4835 GHz with ample channel spacing (5 MHz) aimed at easing transmit and receive filter requirements [7].

Since the LR-WAPN is likely to contain multiple types of wireless networks vying for the same frequency bands, as well as unintentional interference from appliances, the ability to relocate within the spectrum will be an important factor in network success. Accordingly, the standard includes the necessary hooks to implement dynamic channel selection, although the specific selection algorithm is left to the network layer. The MAC layer includes a scan function that steps through the list of supported channels in search of a beacon, while the PHY layers contain several lower-level functions, such as receiver energy detection, link quality indication, and channel switching, which enable channel assessment and frequency agility. These functions are used by the network to establish its initial operating channel and to change channels in response to a prolonged outage.

6.2 The Packet Structure

To maintain a common simple interface with the MAC, both PHY layers share a single packet structure as shown in **Figure 7**. Each packet, or PHY protocol data unit (PPDU), contains a synchronization header (preamble plus start of packet delimiter), a PHY header to indicate the packet length, and the payload, or PHY service data unit (PSDU). The 32-bit preamble is designed for acquisition of symbol and chip timing, and in some cases may be used for coarse frequency adjustment. Channel equalization is not required for either PHY due to the combination of small coverage area and relatively low chip rates. In particular, typical root mean square (RMS) delay spread measured in residential homes is reported to be 25 ns [10], which correspond to only 2.5 percent of the shortest spread spectrum chip period used in IEEE 802.15.4.

.

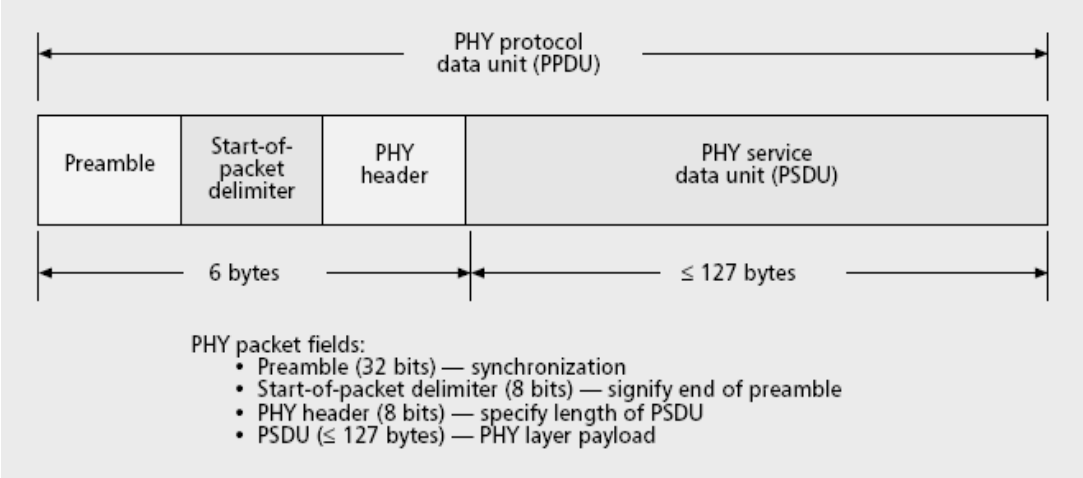

Figure 7: IEEE 802.15.4 physical layer packet structure [7].

Within the PHY header, 7 bits are used to specify the length of the payload (in bytes). This supports packets of length 0–127 bytes, although due to MAC layer overhead, zero-length packets will not occur in practice. Typical packets sizes for home applications such as monitoring and control of security, lighting, air conditioning, and other appliances are expected to be on the order of 30–60 bytes, while more demanding applications such as interactive games and computer peripherals, or multihop applications with more address overhead, may require larger packet sizes. Adjusting for the transmission rates in each band, the maximum packet durations are 4.25 ms for the 2.4 GHz band, 26.6 ms for the 915 MHz band, and 53.2 ms for the 868 MHz band [8].

7 System Design

7.1 Applications Areas

Zigbee protocol has been developed with the emphases on low cost battery powered application such as consumer electronics, industrial automation, home and building automation, PC peripherals, medical sensor applications, toys and games.

- Remote sensing: Water/sewage level monitoring, Temperature sensing.
- Industrial and commercial : Monitor, control and automation links
- Building automation : Security, light, thermostat, Air condition control
- Heath care : Patient monitoring, data logger, remote diagnosis
- Memory tagging : Automotive service record, maintenance logging, inventory control/tracing

7.2 Sensitivity and Range

IEEE 802.15.4 currently specifies receiver sensitivities of –85 dBm for the 2.4 GHz PHY and –92 dBm for the 868/915 MHz PHY. These values include sufficient margin to cover manufacturing tolerances as well as to permit very low-cost implementation approaches. In each case, the best devices may be on the order of 10 dB better than the specification. Naturally, the achievable range will be a function of the receiver sensitivity as well as transmit power. The standard specifies that each device shall be capable of transmitting at least 1 mW, but depending on the application needs, the actual transmit power may be lower or higher (within regulatory limits). Typical devices (1mW) are expected to cover a 10–20 m range; however, with good sensitivity and a moderate increase in transmit power, a star network topology can provide complete home coverage. For applications allowing more latency, mesh network topologies provide an attractive alternative for home coverage since each device needs only enough power (and sensitivity) to communicate with its nearest neighbor [7].

Table 3: A comparison of LR-WPAN with other wireless technology [5]

Market Name Standard	**GPRS/GSM 1xRTT/CDMA**	**Wi-Fi™ 802.11b WLAN**	**Bluetooth™ 802.15.1 WPAN**	**Zigbee™ 802.15.4 LR-WPAN**
Application Focus	Wide Area Voice & Data	Web, Email, Video	Cable Replacement	Monitoring & Control
System Resources	16MB+	1MB+	250KB+	4KB - 32KB
Battery Life (days)	1-7	1.5 - 5	1 - 7	100 - 1,000+
Network Size	1	32	7	255 / 65,000
Bandwidth (KB/s)	64 - 128+	11,000+	720	20 - 250
Transmission Range (meters)	1,000+	1 - 100	1 - 10+	1 - 100+
Success Metrics	Reach, Quality	Speed, Flexibility	Cost, Convenience	Reliability, Power, Cost

7.3 Energy

The main design consideration for LR-WPANs is low power consumption, and therefore long battery life. Some of the techniques that help achieve low average power consumption are:

- Reduction of the amount of data transmitted
- Reduction of the transceiver duty cycle and the frequency of data transmissions
- Reduction of frame overhead
- Implementation of strict power management mechanisms, such as power-down and sleep modes

As an example, a goal in a particular application may be to obtain two years of battery life, employing an alkaline AAA battery. Knowing that the typical capacity of a **AAA** battery is 750 mAh and that there are 8760 hours in a year, and assuming a 1V system design that employs a linear voltage regulator (so the supply current equals the load current), the required average current drain Iavg needed to meet this specification is [10].

$$Iavg = \frac{750mAh}{2year \times 8760hours} = 42.8\mu A$$

$Iavg$, of course, is the time average of the transmit, receive and standby currents:

$$Iavg = Trxon \cdot Irxon + Ttxon \cdot Itxon + (1 - Trxon - Ttxon) \cdot Istby \quad [1]$$

Where,

$Iavg$ = Required average current drain from the battery

$Irxon$ = Current drain from the battery when the receiver is on

$Itxon$ = Current drain from the battery when the transmitter is on

$Istby$ = Current drain from the battery when both receiver and transmitter are off
$Trxon$ = Fraction of time the receiver is on
$Ttxon$ = Fraction of time the transmitter is on

Interestingly, for low-power devices operating in the 2.4 GHz **ISM** band, the transmitter and receiver currents are often similar. If one assumes they are the same, and makes the additional simplifying assumption that the network communication links are symmetrical (meaning the average transmit and receive times of individual devices is the same), the average battery current equation reduces to

$$Iavg = Ton \cdot Ion + (1 - Ton) \cdot Istby \quad [2]$$

Ton = Fraction of time either receiver or transmitter is on
Ion = Current drain from the battery when either the receiver or transmitter is on. From this equation and as well from the estimates of the current consumption of practical hardware, the maximum acceptable Ton may be determined. Ton as a function of the device average battery current.
For example, if Ion = 10 mA,
$Istby$ = 10 μ A, and $Iavg$ = 43 μ A, Ton =0.0033
The network design must allow the device to remain asleep, on average, for 99.67 percent of the time it is operational for given current value..

7.4 Security

The IEEE 802.15.4 draft standard provides for three levels of security: no security of any type (e.g., for advertising kiosk applications); access control lists (noncryptographic security); and symmetric key security, employing AES-128. To minimize cost for devices that do not require it, the key distribution method (e.g., public key cryptography) is not specified in the draft standard but may be included in the upper layers of appropriate applications [7].

7.5 Network Coexistence Issue

The IEEE 802.15.4 devices are proposed to operate in the 2.4 GHz industrial, scientific and medical (ISM) band. The same operational band used by other IEEE 802 wireless devices, such as IEEE 802.11b (WLAN) and IEEE 802.15.1 (Bluetooth). IEEE 802.15.4 and IEEE 802.11b standards support complimentary applications; e.g., IEEE 802.15.4 devices used to support a wireless sensor array within a home or industrial complex could be collocated with IEEE 802.11b in order to provide WLAN support [8]. Wireless devices based on these two standards are likely to be collocated and therefore their ability to coexist needs to be evaluated [9].

7.6 Hardware

Different semiconductor vendors like Atmel, Chipcon, Ember, Freescale from Motorola are providing hardware and software support for embedded implementation of LR-WPAN [12] [13] [14]. As discusses earlier MAC and PHY are two major layer

of LR-WPAN. The RF transceiver is just one component in the Zigbee technology-ready platform solution. A processing device, such as an MCU or DSP, is required to complete the entire solution by housing the IEEE 802.15.4 MAC and Zigbee software (**Figure 8**).

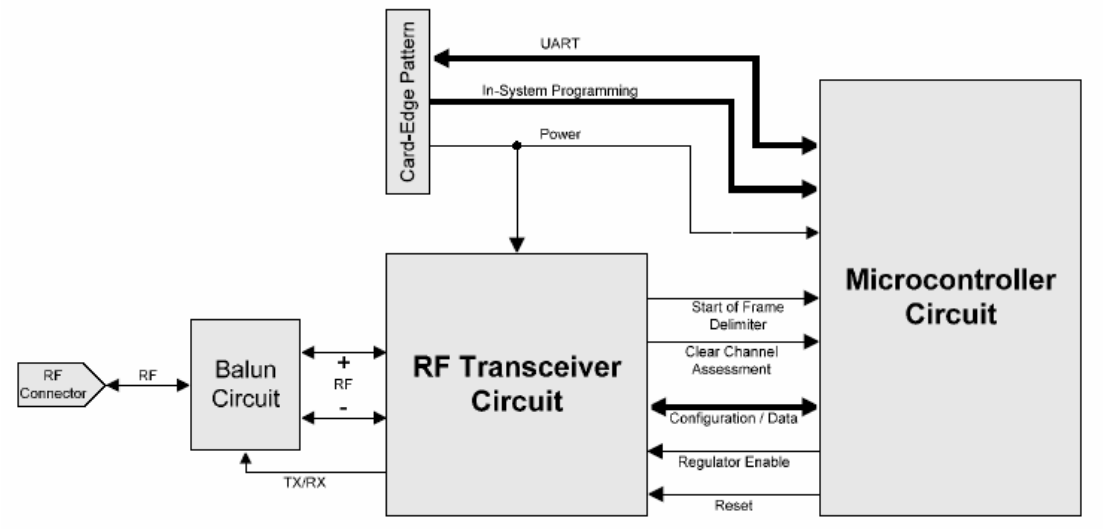

Figure 8: Zigbee device with RF transceiver and microcontroller

8. Conclusion

Extremely low duty cycle operation enables significant energy saving but at the cost of higher latency and lower data rate. The CSMA-CA algorithm reduces the energy cost due to ideal listening in the back-off period but increases the collision at higher rate and larger number of source. While the use of GTS in contention free period can allow dedicated bandwidth to a device to ensure low latency, the device needs to track beacon frame in this mode, which increases the energy cost.

With the standardization of the MAC and PHY almost complete, the focus is now on the upper protocol layers and application profiles. The Zigbee Alliance is taking the lead in this effort. In parallel, several leading semiconductor manufacturers are expected to announce integrated circuit support for implementation of Zigbee stack.

The focus of 802.15.4 development was on maintaining simplicity by concentrating on the essential requirements that will leverage a successful standard. The standard is targeting the residential and industrial market. It is expected that the industrial market will be the first to enable new products with focus on adding value through installation ease. The residential market will follow, taking advantage of lower cost due to the volume already driven by the industrial segment.

IEEE 802.15.4 has already caught the attention of other communities, such as IEEE 1451 with a focus in sensor networking. It is expected that several users of proprietary wireless technologies will shift toward the standard solution due to the expected lower cost and performance improvement.

References

[1] Sri Kolla, David Border and Erik Mayer, *"Fieldbus Networks for control system implementations," Proc IEEE,* pp.493-498, sept. 2003

[2] Gang Lu, Bhaskar Krishnamachari, Cauligi S. Raghavendra, *"Performance Evolution of the IEEE 802.15.4 MAC for Low-rate Low-Power Wireless Networks," Proc IEEE,* pp.701-706, April 2004

[3] Feng-Li Lian, *"Analysis, Design, Modeling and control of Networked control system," Ph.D Dissertation*, 2001

[4] Gunnar Stein and Klaus Kabitzsch, *"Concept for An architecture of a Wireless Building Automation," Proc IEEE,* vol. 1 ,pp.139-142, Oct. 2002

[5] Zigbee alliance. http://www.zigbee.org

[6] Mikhail Galeev, *"Home Networking With Zigbee,"* *www.embedded.com*

[7] Ed Callaway, Paul Gorday and Lance Hester, *"Home Networking with IEEE 802.15.4: A Developing standard for Low-Rate Wireless Personal Area Networks," IEEE Communication Magazine*, Vol.40,pp.70-77, Aug. 2002

[8] 802.15.4-2003 IEEE standard for Information Technology- *Part 15.4 : Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications for Low Rate Wireless Personal Area Networks (LR-WPANS)*, Oct 2003

[9] Ivan Howitt, Jose A.Gutierrez, *"IEEE 802.15.4 Low Rate- Wireless Personal Area Network Coexistence Issues," Proc IEEE,* vol.3,pp.1481-1486, March 2003

[10] Jose' A.Gutierrez, Marco Naeve, Ed callaway, Monique Bourgeois, Vinay Mitter, *"IEEE 802.15.4: A Developing Standard for Low-Power Low-Cost Wireless Personal Area Networks," Proc IEEE*,Vol.15,pp.12-19, Sept.-Oct. 2001

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

[12] www.ember.com

[13] Data sheet for 2.4GHz IEEE 802.15.4 Zigbee RF transceiver at http://www.chipcon.com/files/CC2420_data_sheet_1_0.pdf

[14] AT86RF210 Z-Link™ Transceiver 868/902–928 MHz Direct Sequence Spread Spectrum BPSK Transceiver at www.atmel.com

[15] S. Keshav ,*"An Engineering Approach to Computer Networking ATM Networks, the Internet, and the Telephone Network,"* Pearson Education,India,2004

[16] Cena, G.; Demartini, C.; Valenzano, A.,*"On the performances of two popular fieldbuses" Proc IEEE*,pp.177-186, Oct. 1997