EDA 390 - Computer Communication and Distributed Systems

An Paper on ZigBee

Adis Vojvodić

1. Introduction

There are a multitude of standards that address mid to high data rates for voice, PC LANs, video, etc. and until recently there has not been a wireless network standard that meets the unique needs of devices such as sensors and control devices. Sensors and control devices which are mostly used in industry and home distinguish themselves with low data rates and in needs of very low energy consumption. There is multitude of proprietary wireless systems manufactured today which meet these requirements but they create significant interoperability problems with each other and with newer technologies. What is needed, is a standards-based wireless technology having the performance characteristics that closely meet the requirements for reliability, security, low power and low cost.

Feature(s)	IEEE 802.11b	Bluetooth	ZigBee
Power Profile	Hours	Days	Years
Complexity	Very Complex	Complex	Simple
Nodes/Master	32	7	64000
Latency	Enumeration upto 3 seconds	Enumeration upto 10 seconds	Enumeration 30ms
Range	100 m	10m	70m-300m
Extendability	Roaming possible	No	YES
Data Rate	11Mbps	1Mbps	250Kbps
Security	Authentication Service Set ID (SSID)	64 bit, 128 bit	128 bit AES and Application Layer user defined

Fig. 1 - Comparison of key features of complementary wireless technologies

A standard has been developed for such wireless applications 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". The scope of the task group is to define the physical layer (PHY) and the media access controller (MAC). A graphical representation of the areas of responsibility between the IEEE standard, the ZigBee™ Alliance [2], and the User is presented in Figure 1.

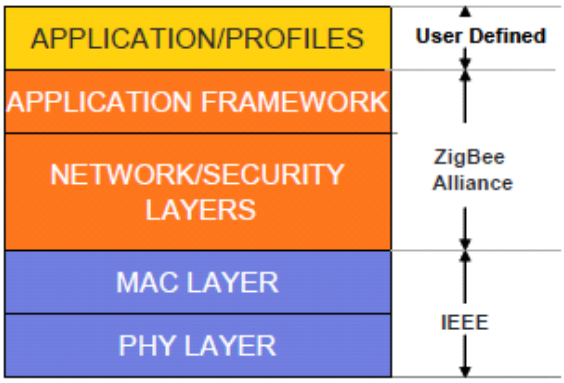

Fig. 2 - IEEE 802.15.4 Stack

di0voad@chl.chalmers.se

Since low total system cost is a main issue in 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.

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 group which is a non-profit industry consortium was organized to define and set the typical solutions for 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, ZigBee network topologies, application development procedure and some ZigBee applications will be presented. The name "ZigBee" is derived from the erratic zigging patterns many bees make between flowers when collecting pollen which can be said that connections in fully wireless environments look like.

2. IEEE 802.15.4 OVERVIEW

The IEEE 802.15.4 standard is optimized for low duty-cycle applications and low power consumption. It defines two physical layers (PHYs) representing three license-free frequency bands that include sixteen channels at 2.4 GHz (250 kbps maximum data rate), ten channels at 902 to 928 MHz (40 kbps), and one channel at 868 to 870 MHz (20 kbps). The 2.4 GHz band operates worldwide while the sub-1 GHz band operates in North America, Europe, and Australia/New Zealand.

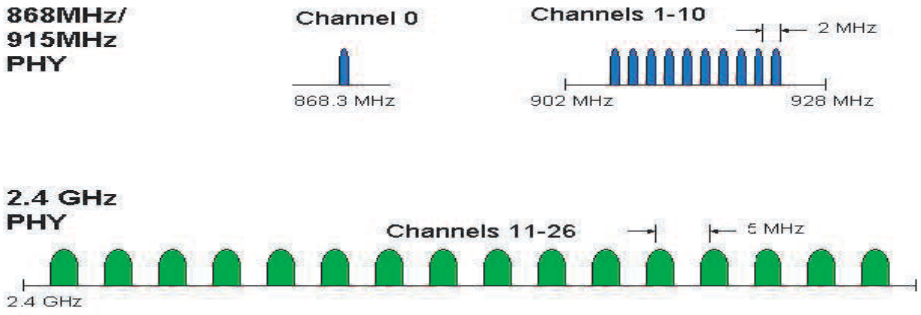

Fig. 3 - Operating frequency bands

Both PHYs use Direct Sequence Spread Spectrum (DSSS) which allows the analog circuitry to be very simple and very tolerant towards inexpensive implementations. The modulation type in the 2.4 GHz band is O-QPSK with a 32 Pseudo Number 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.

di0voad@chl.chalmers.se

3. RF DESIGN

A representative sub-1 GHz transceiver is shown in Fig. 4. The integrated chip 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. The transmission range varies with the environment all from 10 to 75 meters. Longer range can be obtained with smarter antennas, smart network designs or one can add power amplifiers to the transceiver.

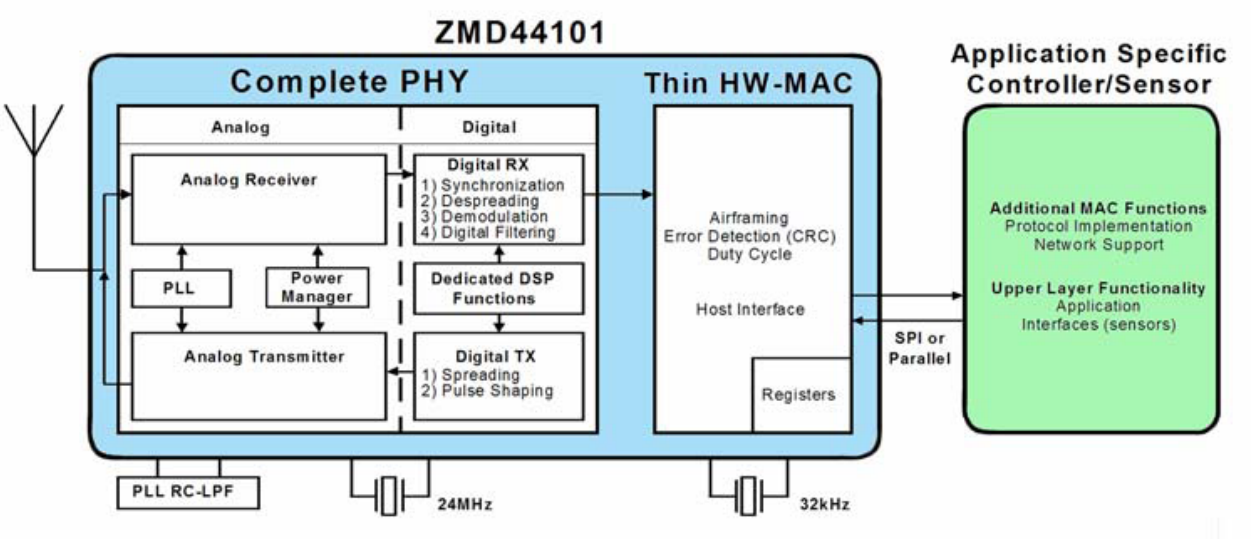

Fig.4 - Sub-1 GHz transceiver block diagram

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 choice of the receiver architecture is mainly a compromise of functional performance, power consumption, ease-of-integration, silicon area, and requirement of external components. Both analog receiver and transmitter architectures are direct-conversion "DCR" (or Zero-IF architecture). More on RF design considerations can be found in [3].

4. IEEE 802.15.4 PHY/MAC and ZigBee's layers

The IEEE 802.15.4 PHY layer includes features such as receiver energy detection (ED), link quality indication (LQI) and clear channel assessment (CCA).

The network addressing follows 64-bit IEEE and 16-bit short addressing, supporting over 65,000 nodes per network. The IEEE 802.15.4 MAC sublayer controls the access to the radio channel using unslotted CSMA-CA (Carrier Sense Multiple Access with Collision Avoidance) method. It is also responsible for flow control via acknowledgement and retransmission of data packets, frame validation, and network synchronization as well as support to upper layers for robust link operation. The MAC frame structure has been designed to keep the complexity to a minimum while making the system sufficiently robust for transmissions on a noisy channel.

di0voad@chl.chalmers.se

The IEEE 802.15.4 MAC defines four frame structures:

- A beacon frame, used by a coordinator to transmit beacons.
- A data frame, used for all transfers of data.
- An acknowledgment frame, used for confirming successful frame reception.
- A MAC command frame, used for handling all MAC peer entity control transfers.

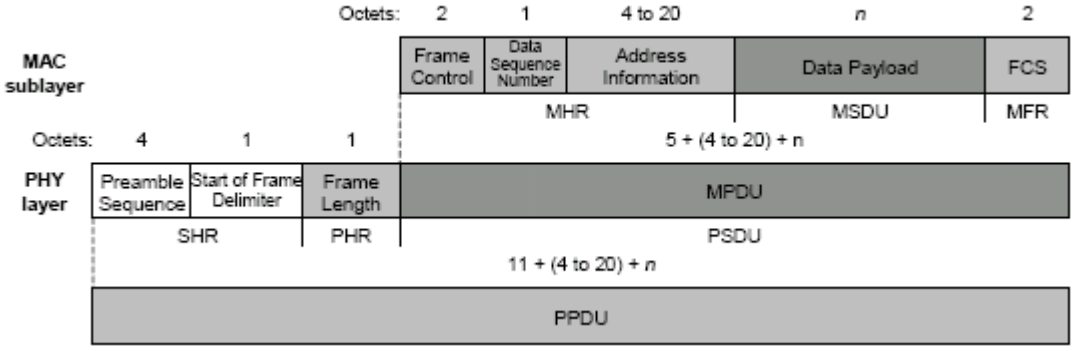

Fig. 5 - Data frame

The LR-WPAN standard allows the superframe structure with beacons for time synchronization, and a guaranteed time slot (GTS) mechanism for high priority communications.

MAC Primitives

MAC Data Service

- MCPS-DATA – exchange data packets between MAC and PHY
- MCPS-PURGE – purge an MSDU from the transaction queue

MAC Management Service

- MLME-ASSOCIATE/DISASSOCIATE – network association
- MLME-SYNC / SYNC-LOSS - device synchronization
- MLME-SCAN - scan radio channels
- MLME- COMM-STATUS – communication status
- MLME-GET / -SET– retrieve/set MAC PIB parameters
- MLME-START / BEACON-NOTIFY – beacon management
- MLME-POLL - beaconless synchronization
- MLME-GTS - GTS management
- MLME-RESET – request for MLME to perform reset
- MLME-ORPHAN - orphan device management
- MLME-RX-ENABLE - enabling/disabling of radio system

ZigBee defines the Security in form of MAC layer security that secures MAC command, beacon, and acknowledgment frames. ZigBee may secure messages transmitted over a single hop using secured MAC data frames, but for multi-hop messaging ZigBee relies upon upper layers (such as the NWK layer) for security. The MAC layer uses the Advanced Encryption Standard [4] (AES-128) as its core cryptographic algorithm and describes a variety of security suites that

di0voad@chl.chalmers.se

use the AES algorithm. These suites can protect the confidentiality, integrity, and authenticity of MAC frames. The NWK layer also makes use of the Advanced Encryption Standard (AES-128).

The responsibilities of the ZigBee Network Layer include starting a network, joining and leaving a network, configuring a newly attached device, addressing, synchronization within a network, security, routing. The protocols build on recent algorithmic research on Ad-hoc On-demand Distance Vector [5]. Three networking topologies are supported; star, mesh, and cluster tree as shown in Figure 6. Star networks (network + device identifier) are common and provide for very long battery life operation. Mesh, or peer-to-peer, networks (source/destination identifier) 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.

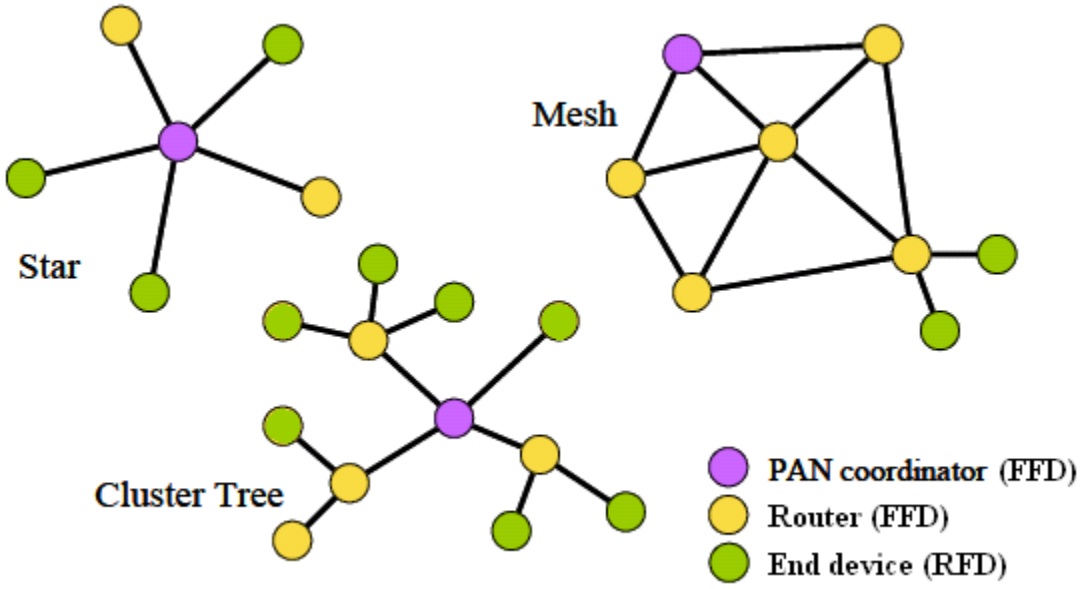

Fig. 6 - ZigBee supported network topologies

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 1.

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 1 - ZigBee physical device types

di0voad@chl.chalmers.se

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 Network Coordinator	The ZigBee Leaf Node
• Sets up a network • Transmits network beacons • Manages network nodes • Stores network node information •Routes messages between paired nodes • Typically operates in the receive state	•Designed for battery powered or high energy savings • Searches for available networks • Transfers data from its application as necessary • Determines whether data is pending • Requests data from the network coordinator • Can sleep for extended periods

Table 2 - ZigBee logical device functions

ZigBee application device types distinguish the type of device from an end-user perspective as specified by the Application Profiles Layer (APL) as seen in Fig. 7. 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.

ZigBee Application Profile Layer consists of the Application Profile Support (APS) sub-layer, the ZigBee Device Object (ZDO) and the manufacturer-defined application objects. The responsibilities of the APS sub-layer include maintaining tables for binding, which is the ability to match two devices together based on their services and their needs, and forwarding messages between bound devices. Another responsibility of the APS sub-layer is discovery, which is the ability to determine which other devices are operating in the personal operating space of a device. The responsibilities of the ZDO include defining the role of the device within the network (e.g., ZigBee coordinator or end device), initiating and/or responding to binding requests and establishing a secure relationship between network devices. The application objects that are "vendor-defined" implement the actual applications according to the ZigBee-defined application descriptions.

di0voad@chl.chalmers.se

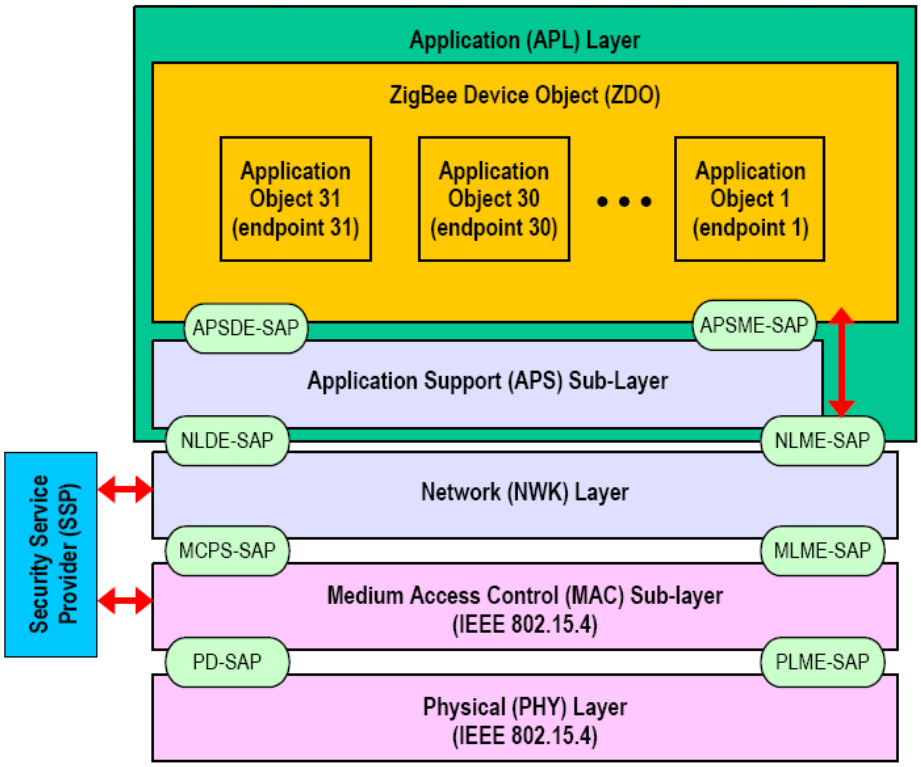

Fig. 7 - ZigBee stack

8. Application Development procedure

Developing user applications or extending MAC features like protocol implementation and network support is usually done with help of various development kits. The kits typically consist of a microcontroller on a board which connects to an computer, some switches/LEDs and other peripherals. The transceiver is connected to the board in form of a self contained radio module. As low system cost is the main issue, developers are integrating microcontrollers into transceivers with direct memory access (for cycle reduction and thus power reduction). The MCUs are usually 8-bit with integrated features like A/D converters and such. The MCU memory size varies as well. In this system-on-chip model a compatible test board directly connects to a computer. For rapid application development a costly ZigBee stack can be added the kit. Microchip™ distributes a software stack for ZigBee free of charge without the security layer though. Various ZigBee-related computer development supportive software exists such as network sniffers, visual analyzers, IDEs and Application Profile constructors. Different reference designs, sample code and PCB layouts are also available.

di0voad@chl.chalmers.se

9. ZigBee Applications

ZigBee networks handle 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** – application defined rate (e.g. wireless sensor or meter). Data is typically handled using a beaconing system whereby the sensor wakes up at a set time and checks for the beacon from the PAN coordinator, it then requests to joint the network. If the coordinator accepts it, data is passed by the sensor before it goes to sleep again. This capability provides for very low duty cycles.

• **Intermittent data** – either application or external stimulus defined rate (e.g. 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 thus saving considerable energy.

• **Repetitive low latency data** – Allocations of time slots. (e.g. medical alerts and security systems). These applications may use the guaranteed time slot (GTS) capability when timeliness and critical data passage is required. 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.

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, accessing a channel and transmitting data takes about 15 ms respectively. ZigBee applications benefit from the ability to quickly attach information, detach, and go to deep sleep. These procedures occur much faster than with a Bluetooth technology.

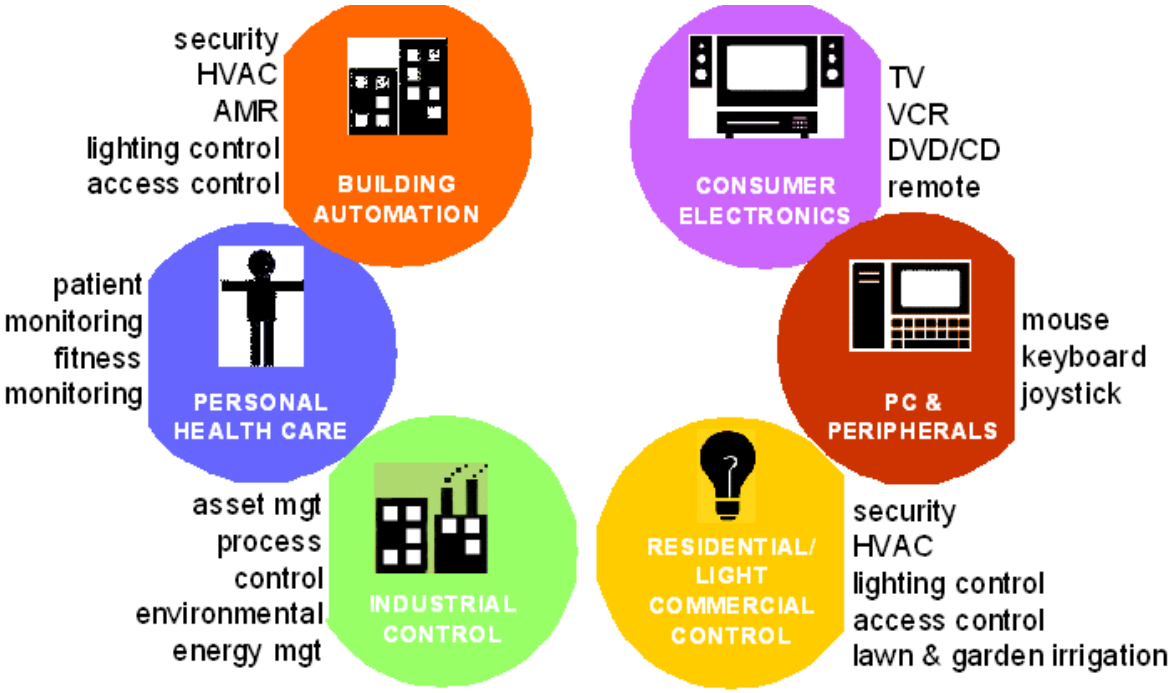

Fig. 8 - ZigBee Applications overview

di0voad@chl.chalmers.se

Some examples where short-range, low-data, cheap wireless networks can be used are:

- Automatic Meter Reading provides the usage statistics for Power Management and Energy Conservation whether it is electric, natural gas, water or other utilities.
- Controlling the environment in HVAC systems. Lighting, temperature and other building controls help save utility usage and maintenance costs. Wireless monitoring and control systems remove expensive installation costs where wiring is difficult, extensive or part of a retrofit design.
- ZigBee network can help in collecting the information necessary for an effective Inventory and Logistics Management. In fleet management, vehicles can automatically transmit logged information or receive updates when inside the fleet yard.
- Various control and automation scenarios are possible both for homes and industries using cheap wireless communication including security systems and access control.

10. Discussion

This area of wireless networks is tough for the engineers since the specification is ever-changing and as the pervasiveness grows a true comprehension of the communication paths will be difficult.

Currently the interoperability between ZigBee implementations is an issue. There are no standards governing mesh networks. Bridges must be constructed between the different mesh networks or one also could hold on to one mesh vendor.

There is no efficient data broadcasting protocol for ZigBee networks. It is needed to prune out redundant retransmissions since ZigBee uses a best effort flooding based broadcasting mechanism in which every node forwards each broadcast message they receive. The also missing multicasting protocol for ZigBee networks will be probably developed after a successful broadcasting protocol.

Many positive factors are driving the market growth for ZigBee. There are new solutions in the automobile industry, health care, homeland security, manufacturing, and asset management. New opportunities both for systems integrators and network engineers will appear. It has been predicted that the market for low-power, low-cost radio frequency integrated circuits will grow to 730 million units by 2007 or $4.8B where ZigBee by will be accounted for $1.7B. By 2009 it is expected that 150 million devices will be taking advantage of the ZigBee.

di0voad@chl.chalmers.se

11. References

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

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

[3] Designing a ZigBee-ready IEEE 802.15.4-compliant radio transceiver,
http://rfdesign.com/mag/radio_designing_zigbeeready_ieee/

[4] The archive of the old official AES website,
http://csrc.nist.gov/CryptoToolkit/aes/

[5] The Ad hoc On Demand Distance Vector,
http://moment.cs.ucsb.edu/AODV/aodv.html/

di0voad@chl.chalmers.se