WIRELESS COMMUNICATION ZIGBEE.

Contents:

Abstract:

The concept of zigbee is associated with controlling all electronic devices and communicating with themselves with the surrounding by using simple our mobile or pc by using this latest technology.The serious problem in this world is cables tremendous growth in science which is solved by this.

Zigbee is a set of specs built around the IEEE 802.15.4 wireless protocol. Zigbee devices are actively limited to a through-rate of 250kbps, operating on the 2.4GHZ ISM band, which is available throughout most of the world .This acts as co-ordinate and slave.This gives commands and receives commands from other electronic devices. This can connect upto 65,553 devices per unit.The important feature of Zigbee is provide with memory and logical unit for the first time.This helps in taking independent decisions by itself with need of coordinator,which help in sensor devices.There are technologies which already available in the market line BloothTooth.Their some ensured suides in that which lead to develop Zigbee.It has major advantage that it has low power consumption (30ma). Other advantages that it provide high security to all electronic devices.Another important thing is that it is of low cost.This can serve all purposes in industries and home appliancies ….It is very simple to operate by everyone . By all my statements I can conclude that in future we are going to a new world with cables, everything is done by single controls without using multi switches multi purposes.

Introduction

Zigbee is the name of a specification for a suite of high level communication protocols using small, low-power digital radios based on the IEEE 802.15.4 standard for wireless personal area networks (WPANs).

ZigBee operates in the industrial, scientific and medical (ISM) radio bands; 868 MHz in Europe, 915 MHz in the USA and 2.4 GHz in most jurisdictions worldwide. The technology is intended to be simpler and cheaper than other WPANs such as Bluetooth. The most capable ZigBee node type is said to require only about 10% of the software of a typical Bluetooth or Wireless Internet node, while the simplest nodes are about 2%. However, actual

code sizes are much higher, more like 50% of Bluetooth code size. ZigBee chip vendors have announced 128-kilobyte devices.

What is Zigbee?

Zigbee is a wireless networking standard that is aimed at remote control and sensor applications which is suitable for operation in harsh radio environments and in isolated locations. It builds on IEEE standard 802.15.4 which defines the physical and MAC layers. Above this, Zigbee defines the application and security layer specifications enabling interoperability between products from different manufacturers. In this way Zigbee is a superset of the 802.15.4 specification.

The 802.15.4 standard is primarily aiming at monitoring and control applications. Low power consumption is the most important feature that makes battery operated devices operates for a long time. The amount of data throughput (bandwidth) is relatively low compared to wireless LAN for example, but with 250kbps for many applications more than enough. The distance between 2 nodes can be up to 50 meters but be aware the each node can relay data to the next making a very big network, covering significant distances, possible.

Hardware (Physical and MAC layers)

The 2.4GHz frequency band is a license free band, so a ZigBee product may be used all over the world. All current products seem to be using the 2.4GHz band at the moment. Take a look at the next table for a few differences between the bands:

Frequency	868 MHz	915 MHz	2.4GHz
Bandwidth	20 kbps	40 kbps	250 kbps
Nr. of channels	1	10	16

In all bands DSSS (Direct sequence spread spectrum) is used. 868 and 915 MHz are using Binary Phase Shift Keying and 2.4GHz uses O-QPSK (Offset Quadrature Phase Shift Keying). Like in any network data is transmitted in packets. ZigBee's packets have a maximum size of 128 bytes including protocol overhead. In total there is room for a maximum of 104 bytes. For realtime features, ZigBee has the possibility to define high priority messages. This is achieved by use of a guaranteed timeslot mechanism so that the high priority messages can be send as fast as possible.

ZigBee uses 2 kinds of addressing. There is a 64 bit IEEE address that can be compared to the IP address on the internet. There is also a 16 bit short address. The short addresses are used once a network is setup so this makes a total of 2^16 = ~64000 nodes within one network possible. This is enough for almost anything imaginable.

The ZigBee upper layers

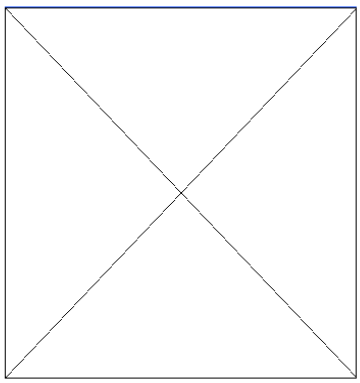


Figure 1: Layers in Zigbee

The layers above that what 802.15.4 specifies is what we call the ZigBee standard (look above for a graphical overview). Many aspect of the network are specified in this layer, like: Application profiles, security settings and the messaging.

ZigBee is known because of its mesh network architecture but it does also support a star topology or cluster tree or hybrid architecture. Depending on the application or situation each kind of topology has its own advantages and disadvantages. A star topology is very simple, all nodes directly communicate with one central node (like a star...). The mesh topology is more complicated, each node may communicate with any other node within range. It's easy to understand that this gives many possible routes through the network; this makes it a very robust topology because bad performing routes can be ignored. The cluster tree topology is basically a combination of star and mesh.

Software and hardware

The software is designed to be easy to develop on small, cheap microprocessors. The radio design used by ZigBee has been carefully optimized for low cost in large scale production. It has few analog stages and uses digital circuits wherever possible.

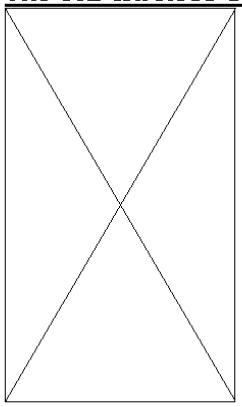
Even though the radios themselves are cheap, the ZigBee Qualification Process involves a full validation of the requirements of the physical layer. This amount of concern about the Physical Layer has multiple benefits, since all radios derived from that semiconductor mask set would enjoy the same RF characteristics. On the other hand, an uncertifed physical layer that malfunctions could cripple the Battery lifespan of other devices on a Zigbee Network. Where other protocols can mask poor sensitivity or other esoteric problems in a fade compensation response, ZigBee radios have very tight engineering constraints: they are both power and bandwidth constrained. Thus, radios are tested to the ISO-17025 standard with guidance given by Clause 6 of the 802.15.4-2003 Standard. Most vendors plan to integrate the radio and microcontroller onto a single chip.

• Why choose ZigBee?

Reliable and self healing
• Supports large number of nodes
• Easy to deploy
• Very long battery life
• Secure

• Low cost
• Can be used globally

The 802 Wireless Space



ZigBee specification

The ZigBee Alliance is an association of companies working together to enable reliable, cost-effective, low-power, wirelessly networked, monitoring and control products based on an open global standard.

Data Reliability

Reliable data delivery is critical to ZigBee applications. The underlying 802.15.4 standard provides strong reliability through several mechanisms at multiple layers. For example, it uses 27 channels in three separate frequency bands (see Figure 3).

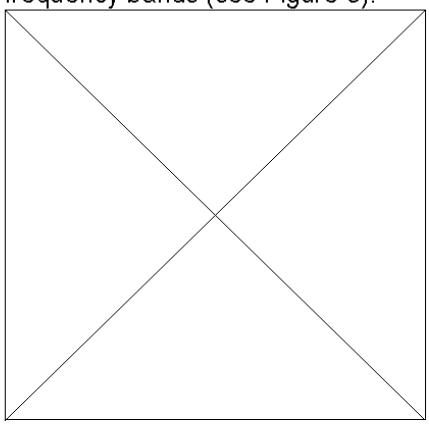


Figure - 3

IEEE 802.15.4 provides three frequency bands for communications. Global utility, propagation, path loss, and data rate differences let ZigBee profile developers optimize system performance

The 2.4 GHz band is used worldwide and has 16 channels and a maximum over-the-air data rate of 250 Kbps. Lower frequency bands are also specified.

The information is coded onto the carrier with direct sequence spread spectrum (DSSS), an inherently robust method of improving multipath performance and receiver sensitivity through signal processing gain. The receiver sensitivity and selectivity is well suited for inexpensive silicon processes, with most vendors promising to meet or

beat the standard. The size of the data payload ranges from 0 to 104 bytes, more than enough to meet most sensor needs. Figure 4 shows the construction of the data frame, also called a *data packet*.

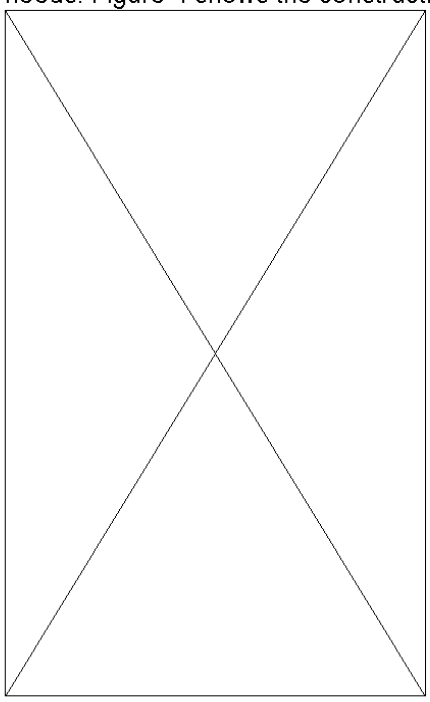


Figure 4.

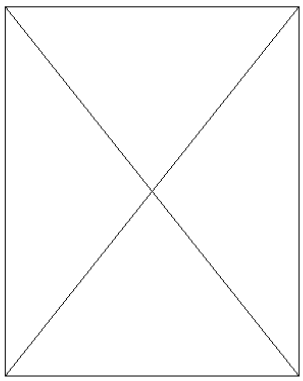
The data packet is one of four packet structures provided in 802.15.4/ZigBee. In the MAC protocol data unit, the data payload is appended with source and destination addresses, a sequence number to allow the receiver to recognize that all packets transmitted have been received, frame control bytes that specify the network environment and other important parameters, and finally a frame check sequence that lets the receiver verify that the packet was received uncorrupted. This MAC frame is appended to a PHY synchronization and PHY header, which provides a robust mechanism for the receiver to quickly recognize and decode the received packet.

After receiving a data packet, the receiver performs a 16-bit cyclic redundancy check (CRC) to verify that the packet was not corrupted in transmission. With a good CRC, the receiver can automatically transmit an acknowledgement packet (depending on application and network needs), allowing the transmitting station to know that the data were received in an acceptable form. If the CRC indicates the packet was corrupt, the packet is dropped and no acknowledgement is transmitted. When a developer configures the network to expect acknowledgement, the transmitting station will retransmit the original packet a specified number of times to ensure successful packet delivery. If the path between the transmitter and receiver has become less reliable or a network failure has occurred, ZigBee provides the network with self-healing capabilities when alternate paths (if physically available) can be established autonomously.

Battery Life

In many applications, you can't afford to make regular trips back to a sensor to change the battery. Ideally, the sensor is good for the life of the battery.

The basic 802.15.4 node is fundamentally efficient in terms of battery performance. You can expect battery lifetimes from a few months to many years as a result of a host of system power-saving modes and battery-optimized network parameters, such as a selection of beacon intervals, guaranteed time slots, and enablement/disablement options.



Transmission Range

The standard specifies transmitter output power at a nominal –3 dBm (0.5 mW), with the upper limit controlled by the regulatory agencies of the region in which the sensor is used. At –3 dBm output, single-hop ranges of 10 to more than 100 m are reasonable, depending on the environment, antenna, and operating frequency band.

Data Rate

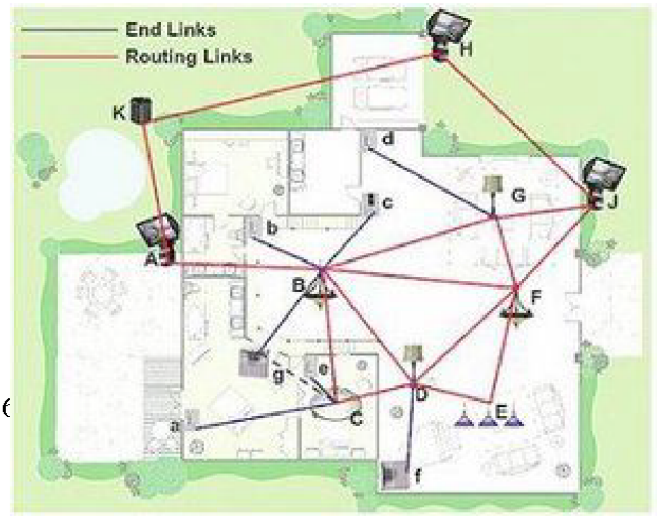
Higher data rates at a given power level mean there's less energy per transmitted bit, which generally implies reduced range. But both 802.15.4 and ZigBee value battery life more than raw range and provide mechanisms to improve range while always concentrating on battery life.

Data Latency

Sensor systems have a broad range of data-latency requirements. If sensor data are needed within tens of milliseconds, as op-posed to dozens of seconds, the requirement places different demands on the type and extent of the intervening network. For many sensor applications, data latency is less critical than battery life or data reliability.For simple star networks (many clients, one network coordinator), ZigBee can provide latencies as low as ~16 ms in a beacon-centric network, using guaranteed time slots to prevent interference from other sensors. Data latency can also affect battery life.

Size

As silicon processes and radio technology progress, transceiver systems shrink in physical size. . In the case of ZigBee systems, the radio transceiver has become a single piece of silicon, with a few passive components and a relatively non critical board design.



Data Security

It's important to provide your sensor network with adequate security to prevent the data

from being compromised, stolen, or tampered with. IEEE 802.15.4 provides authentication, encryption, and integrity services for wireless systems that allow systems developers to apply security levels as required. The ZigBee security toolbox consists of key management features that let you safely manage a network remotely.

APPLICATIONS

Zigbee protocols are intended for use in embedded applications requiring low data rates and low power consumption. ZigBee's current focus is to define a general-purpose, inexpensive, self-organizing, mesh network that can be used for industrial control, embedded sensing, medical data collection, smoke and intruder warning, building automation, home automation, etc.

ZigBee standard addresses the unique needs of most remote monitoring and control applications:

- Enables the broad based deployment of simple, reliable, low cost wireless network solutions
- Provides the ability to run for years on inexpensive primary batteries
- Provides the ability to inexpensively support robust mesh networking technologies .
- Home Automation
- Building Automation
- Industrial Automation

Figure 6: ZigBee Home Automation

Conclusion

Zigbee is all set to provide the consumers with ultimate flexibility, mobility, and ease of use by building wireless intelligence and capabilities into every day devices. ZigBee technology will be embedded in a wide range of products and applications across consumer, commercial, industrial and government markets worldwide. For the first time, companies will have a standards-based wireless platform optimized for the unique needs of remote monitoring and control applications, including simplicity, reliability, low-cost and low-power.

References

1. INTRODUCTION - Z:\wireless com-zig\wireless-zigbee\ZigBee - Wikipedia, the free encyclopedia.htm
2. WHAT IS ZIGBEE - Z:\wireless com-zig\wireless-zigbee\What is ZigBee.htm- Z:\wireless com-zig\wireless
3. UPPER LAYERS - zigbee\ZigBee, a wireless mesh network (hasse_nl).htm
4. SPECIFICATIONS - Z:\wireless com-zig\wireless-zigbee\zig.htm
5. APPLICATIONS - Z:\wireless com-zig\wireless-zigbee\ZigBee - Wikipedia, the free encyclopedia.htm