# ZIGBEE IN MICROCONTROLLER APLICATIONS

**Tomáš Krzák**
Doctoral Degree Programme (1), FEEC BUT
E-mail: xkrzak00@stud.feec.vutbr.cz

Supervised by: Tomáš Frýza
E-mail: fryza@feec.vutbr.cz

## ABSTRACT

ZigBee is a standard for the wireless communication based on IEEE 802.15.4. It is characterized by low power consumption what is good for a long life in battery powered systems. It is build as low data rate device and speed is only up to 250 Kb/s. ZigBee devices can be used for communication in wireless sensor networks and it finds its use in home, industry and many other applications.

## 1. INTRODUCTION

Many companies want to investigate and replace long wires which handling data transfer by inexpensive and low power RF devices. Texas Instruments produces low cost ZigBee IEEE 802.15.4 compatible RF transceiver Chipcon CC2520. This PAN (Personal Area Network) works in the ISM band 2,4 GHz (16 channels, 2400 MHz – 2483,5 MHz), same as WLAN, Bluetooth and some other systems. This paper considers possibility of connection Chipcon CC2520 and microcontroller ATMega128. There is used a modified Z-Stack programmed into microcontroller. Main objective of this project is design of two wireless devices which communicate with each other. Research will be oriented on controlling and data transfer over RS-232 standard between modules.

## 2. IEEE 802.15.4-2006 MODULATION FORMAT

The technology is based on implementation of access method CSMA/CA into physical layer. The modulation used in IEEE 802.15.4 is illustrated at block level in Figure 1. First, each is byte divided into 2 symbols and least significant symbol is transmitted first. Each symbol (4 bits) is mapped to one of 16 pseudorandom sequences, 32 chips ($C_0 – C_{31}$) each.

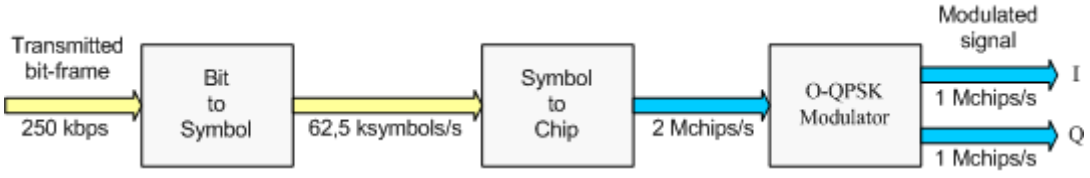


Figure 1: Modulation

The chip sequence is then transmitted at 2 Mchips/s. Format of the modulation is Offset - Quadrature Phase Shift Keying (O-QPSK). Each chip is shaped as a half-sine and transmitted alternately in I and Q channels with one half chip period offset.

For example transmitting packet that was captured in Sony Tektronix 3086 spectrum analyzer with I and Q phases is on Figure 2. Here, ZigBee device transmits with central frequency 2,44 GHz and span 5 MHz.

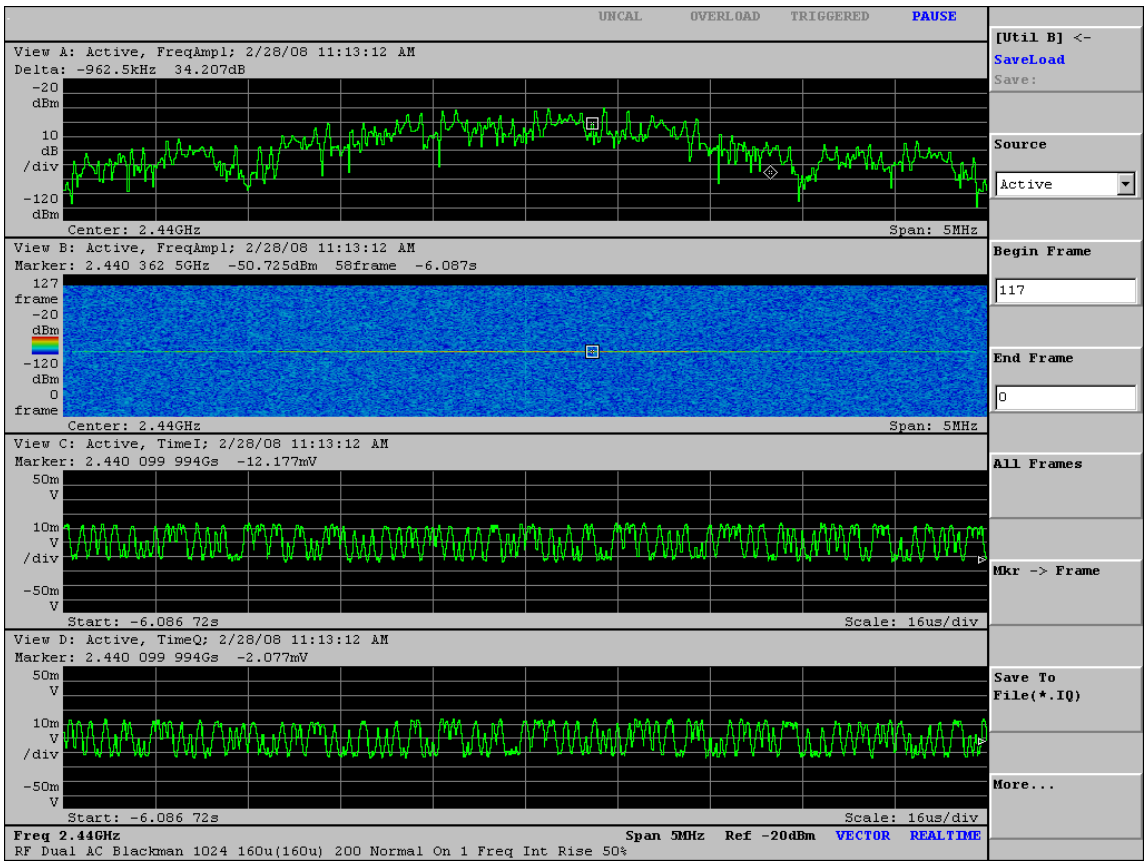


Figure 2: Packet capture in Sony Tektronix 3086 spectrum analyzer

## 3. PROTOCOL FRAME FORMAT AND SECURITY

Table 2 shows a view of the IEEE 802.15.4 frame format. Follow lines describing PHY PDU (Protocol Data Unit) layer, see more in [2].

Table 1: Format of PHY protocol data unit

| Bytes: 4 | 2 | 1 | | N |
|---|---|---|---|---|
| Preamble | SFD | Frame lenth (7 bits) | Reserved (1 bit) | PSDU |
| SHR | | PHR | | PHY payload |

**Synchronization Header (SHR)** - allows a receiving device to synchronize and lock onto the bit stream

**PHY Header (PHR)** - contains frame length information

**PHY Service Data Unit (PSDU)** - has a variable length and carries the data of the PHY packet, see below

The ZigBee protocols support beacon and non-beacon enabled networks. In non-beacon network is used unslotted CSMA/CA channel access mechanism. In this case some devices receive continuously, while others transmit only when an external stimulus is detected. In

beacon networks, ZigBee Full Functional Devices transmit periodic beacons to confirm their presence to other network nodes. Nodes may sleep between beacons and extending their battery life.

There are four types of communication frames :

**Data Frame** - frame used for transfer of useful information 104 bytes long

**Acknowledgement Frame** - frame used by MAC layer for communication with acknowledgement and is transmitted during "dead time" right after the packet

**MAC Command Frame** – frame is used for centralised configuration and control of client (host) devices in ZigBee network

**Beacon Frame** - frame used for synchronization of devices in network, allows host devices to go into sleep mode with very low power consumption

Security provided by AES (Advanced Encryption Standard) with 128 bit key is used to secure ZigBee communication and is implemented in the network layer. If security of MAC Command Frame is also required, Beacon Frame and Acknowledgement Frame are realized already in MAC layer by AES.

Network layer is secured by SSP (Security Services Provider). It provides security of outgoing frames and decoding and identity checking of incoming frames.

## 4. CONNECTION CHIPCON CC2520 WITH MICROCONTROLLER ATMEGA128

The Chipcon CC2520 wireless transceiver is being used because it is a single, surface mount integrated circuit that operates at 2,4 GHz. The possibilities of using CC2520 in connection with microcontroller (MCU) ATMega128 [3] and different kind of peripheries (sensors, LCD, etc.) are shown on Figure 3. Microcontroller can transfer data by several type of bus (RS232/USB, CAN or TCP/IP) depending on target application.

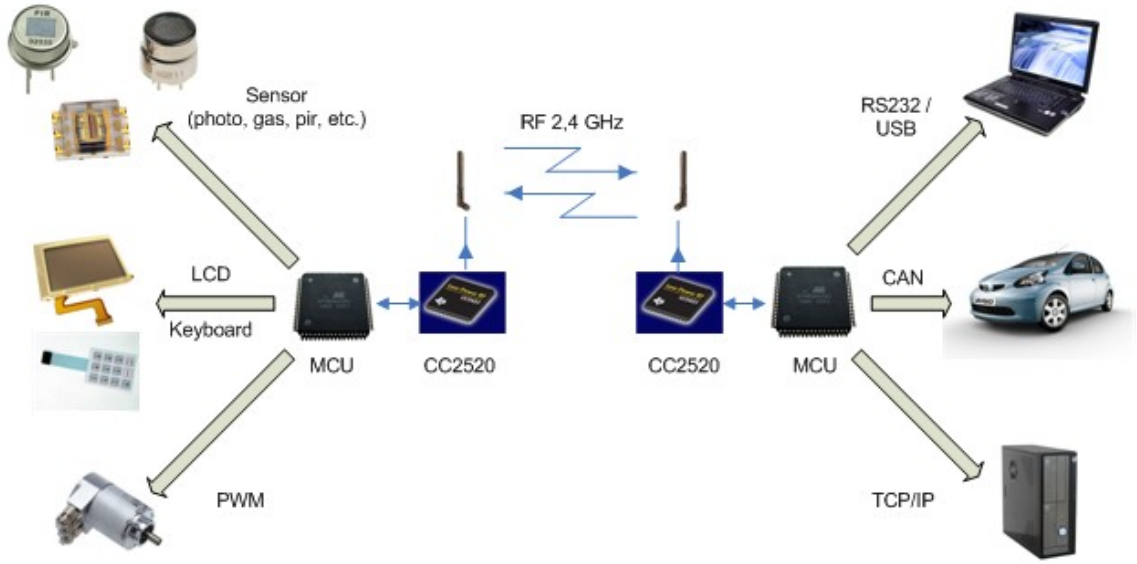


Figure 3: Communication between two ZigBee devices

The CC2520 is designed for low-power consumption at 18,5 mA when receiving and 25,8 mA when transmitting. This radio frequency transceiver is configured by a four wire serial peripheral interface (SPI). The microcontroller is designed with a hardware SPI interface.

Figure 4 shows that the SPI interface for the CC2520 consists of these four pins: CSn, SI, SO, and SCLK. The CSn pin is a digital input for SPI chip select. The SI pin is also a digital input for SPI Slave input. The last input pin on the serial peripheral interface of the wireless controller is SCLK. This pin is an SPI clock input. The final SPI connection is made with the SO pin of the CC2520. The SO pin is a digital output that is for the SPI slave output.

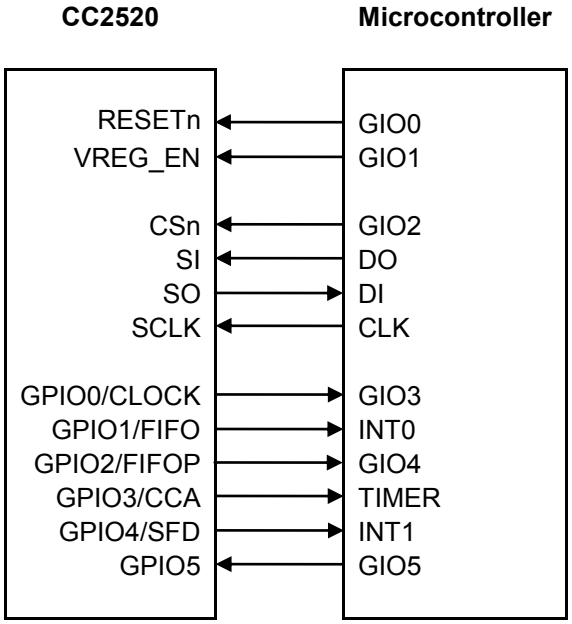


Figure 4: Connection between wireless Chipcon CC2520 and microcontroller

Figure 4 also shows six more pins that need to be connected between the wireless interface and the microcontroller. These additional six pins interface the data between two circuits. Each pin can be configure as input, output and activate pull-up resistor. After the reset GPIO pins are configured as shown in the Figure 4. The CLOCK, FIFO, FIFOP, CCA, and SFD pins are all outputs connected to inputs on the microcontroller. The CLOCK pin generate 1 MHz clock signal with 50/50 duty cycle. The FIFO and FIFOP pins are status pins used to interface to the receiver and transmit FIFOs. The CCA pin and the SFD pin are used for clear channel assessment and for timing information related to the start of frame delimiter. Last GPIO7 input pin can be used to trigger one of 16 commands strobes (see more in [1]).

## 5. ZIGBEE STACK

Chipcon CC2520 contains only physical layer and a part of link layer of the network. Other layers are components of ZigBee stack [4]. Firmware for microcontroller must include Z-stack and code for control of connected peripheries. There are three types of ZigBee devices:

**Coordinator** – There is only one in each network which after start chooses optimal topology (star, tree or mesh) depending on local environment and establish wireless connection with all devices in network. This FFD (Full Functional Device) component have whole protocol frame implemented. Coordinator stores information about the network and might bridge to other networks.

**Router** – This is FFD component passing data from other components.

**End-device** – This RFD (Reduced Functionality Device) have implemented only necessary protocol library. Device can communicate only with coordinator and can be put in sleep mode. The RAM memory requirements are lower for end-devices.

The stack profile is set of stack parameters that needs to be configured to specific values. All devices must have the stack profile parameters configured to the same values. Z-stack is free to download from official web pages of Texas Instruments. Stack code is written in ANCI-C using the development environment from IAR Embedded workbench [5].

## 6. CONCLUSION

RF modems brings possibility of implementation ZigBee wireless standard to user applications with microcontroller. User also doesn't have to take care about error detection, correction, just simply watch bad frames or hamming code corrections. Chipcon CC2520 has hardware modulation (demodulation), synchronization, coding (decoding), auto acknowledgements and supports MAC security. Texas Instruments offers Z-stack for free that saves a lof of development time. There's no need to use microcontroller in protocol processing so it can be run on lower frequencies. It's very important because microcontroller running on 8 MHz has little current consumption. Chipcon CC2520 works with wide supply range 1,8 V – 3,8 V with no need for DC-DC converter. Now is being worked on circuit design and implementation on PCB as small as possible. In next step modification of Z-stack and creation of service application for simulation and testing ZigBee modules will be required.

## ACKNOWLEGEMENT

This research has been supported by the Research programs of Brno University of Technology MSM21630513.

## REFERENCES

[1] CC2520 Datasheet v1.0 SWRS068 December 2007
http://focus.ti.com/lit/ds/symlink/cc2520.pdf, 2007-11-19

[2] IEEE Standards 802.15.4 1:st October 2003
http://standards.ieee.org/getieee802/download/802.15.4-2003.pdf, 2006-04-10

[3] ATMega128(L) Datasheet Rev. 2467N-AVR March 2006
http://www.atmel.com/dyn/resources/prod_documents/doc2467.pdf, 2006-07-28

[4] Texas Instruments, Inc. Z-Stack v1.4.3 2006 http://www.ti.com, 2007-12-21

[5] IAR Embedded workbench for MCS-51 evaluation v7.30B September 2007
http://www.iar.com, 2007-12-21