Reliability of ZigBee transmission in agriculture production

I. Mašík

Department of Electrical Engineering and Automation, Faculty of Engineering, Czech University of Life Sciences Prague, Prague, Czech Republic

Abstract

Mašík I., 2013. **Reliability of ZigBee transmission in agriculture production**. *Res. Agr. Eng., 59: 153–159.*

Currently, the unlicensed ISM (Industrial Scientific and Medical) band 2.4 GHz has become saturated due many standards used at once. In agricultural production ZigBee has a lot of applications, from wireless sensors networks to complicated automation applications. This paper deals with improving the coexistence properties of ZigBee (IEEE 802.15.4), while keeping compatibility with the basic standard. This paper describes principles and application of forward error correction above the physical layer, consisting of block data interleaver and Hamming code, and also the effect of improvements in coexistence with variously loaded WiFi 802.11g.

Keywords: dependability; Hamming; wireless; communication

Currently, the unlicensed ISM band (Industrial Scientific and Medical) 2.4 GHz has become saturated due many standards used at once. Beginning with all WLAN network standards, through Personal Area Networks such as Bluetooth or ZigBee and last but not least, a lot of non-standardized wireless transmissions, such as wireless phones, PC peripherals etc. The coexistence of different wireless networks in the ISM band is inevitable, and it is also very probable that there will be carrier frequencies overlapping. In agricultural production, as at any other area with people traffic, a lot of interference situations caused by mobile devices hanged by persons can occur. Mobile phones, tablets, etc. are very usual at present time and WiFi or Bluetooth are used very frequently. The method described in this paper was built for anemometer data logger units, used for parameters measurement of new type windbreak at the Research Institute of Soil and Water Conservation, Prague, Czech Republic. An anemometer data logger (with ZigBee wireless data download) was positioned in the field with the aim to get long-term capabilities of windbreak units. When the data was downloaded, the collection unit has sometimes problems with interference from coexistent standards, caused by the equipment handled by the person who operates the collection unit. The aim of this paper is to describe main characteristics for coexistence improvement.

WiFi (802.11). WiFi 802.11g is currently being slowly replaced by 802.11n, but is still very frequently used. Theoretical transfer speed of 802.11g is 54 Mbit/s. Channels, their width, spacing and overlapping is identical with 802.11b, but with increased throughput, which is achieved using the Orthogonal Frequency Division Multiplex (OFDM) modulation. OFDM is a method, which allows operation of adjacent channels with overlap, without causing interference. It is a method that allows better utilization of given range, which increases noise immunity against the simple data transmission. Given channel is divided into sub channels and these are used as parallel separate links of communication, of course, with lower throughput. 802.11g allows channel

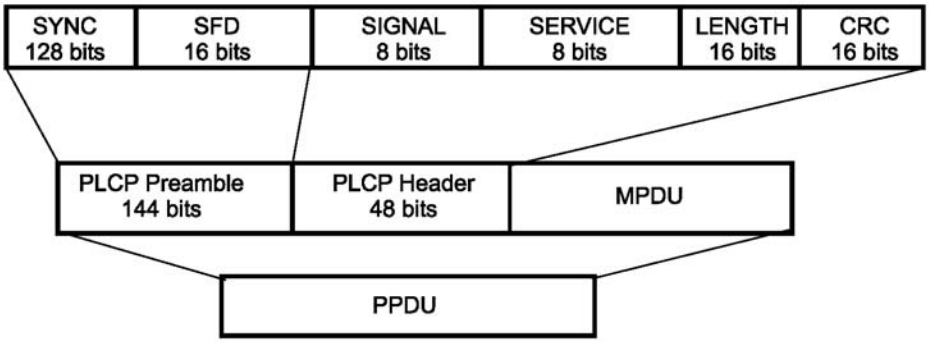

Fig. 1. Frame format of 802.11g (Institute of Electrical and Electronics Engineers, Inc., 2000)
SYNC – synchronisation; SFD – Sync Frame Delimiter; CRC – Cyclic Redundancy Check; PLCP – Physical Layer Convergence Protocol; MPDU – Medium Protocol Data Unit; PPDU – Presentation Protocol Data Unit

width 22 MHz, divided into 52 subchannels, where 48 are data channels and 4 pilot channels used to synchronize transmission. In order of best band utilization, the channels are defined with an overlap. This overlap is then eliminated by orthogonality of adjacent frequencies. Therefore no inter-channel interferences occur there, because when one channel transmits a particular character, neighbouring channels are zero. OFDM actually converts the serial data transmission to parallel information transfer. Direct Sequence Spread Spectrum (DSSS) method uses redundant data to spread information to the spectrum and thereby interference resistance is increased. In practice, bits to transmit are replaced by chip sequences longer than the original data. This causes data redundancy, which can be used at the receiver side to correct errors resulting from noise in transmission channel. The 802.11g standard allows the use of both OFDM and DSSS modulation. Fig. 1 is a frame structure of 802.11g, where in relation to coexistence between ZigBee and WiFi, is interesting timing. Physical Layer Convergence Protocol (PLCP) Preamble sequence is 16 μs long, followed by PLCP Header with 4 μs length independently on current transfer speed, after that follows the data. Timing of data part depends on the speed and coding rate (Institute of Electrical and Electronics Engineers, Inc. 2000).

ZigBee (802.15.4). ZigBee is commercial wireless technology based on standard IEEE 802.15.4, which, like Bluetooth, belongs to the category of Personal Area Networks (PAN). ZigBee can operate in three bands to ensure usability on a global scale. Namely it is band 868 MHz, 915 MHz and 2.4 GHz. Each band has different max. baud rate, at 868 MHz it is 20 kbit/s, at 915 MHz it is 40 kbit/s and at 2.4 GHz the baud rate is 250 kbit/s (Gislason 2008). In order to increase the reliability of transmission, ZigBee physical layer uses the forward error correction DSSS, where each four bits to send are substituted with sequences of 32 chips. At this stage, the signal is transmitted with offset quadrature phase-shift keying (O-QPSK) modulation, which allows sending four bits per symbol with symbol timing 16 μs. At the receiver, when O-QPSK demodulation is done, for each 32 chip sequence microcontroller will evaluate the probability of compliance with each of the 2^4 variants of 32 chip originals, and then replace with appropriate 4 information bits, based on the best fit. Instead of 4 bits, 32 bits are transmitted, which means the channel bandwidth is reduced to 1/8. The benefit is the ability to statistically detect and "fix", or rather "ignore" errors caused by noise in the transmission channel. The efficiency of this forward error correction depends on the choice of chip sequences, their mutual dissimilarity being mainly important. That determines the number of bit errors necessary for wrong substitution and consequential error (Institute of Electrical and Electronics Engineers, Inc. 2006).

MATERIAL AND METHODS

Experimental hardware and software. In development process hardware by Texas Instruments (Dallas, USA) was used – SmartRF05 that uses SoC CC2530F256. This microcontroller has an integrated RF part directly on the chip, and therefore requires only a min. of external components. ZigBee Stack in C language is provided by the microcontroller manufacturer. Method described below was built on Zstack version 2.5.1. (Texas Instruments, Dallas, USA). Stack is not completely editable, large

part is prebuilt in libraries. The following method uses function "macMemReadRxFifo" for data access at physical layer.

Hamming Code. The following forward error correction method consists of two main parts, interleaver and Hamming encoder (7.4.) and interleaver are included in the system to protect the transmitted data against bit errors. Hamming code falls into the category of self-correction codes, and it also belongs to the group of perfect codes – that means with the lowest possible redundancy. The algorithm generating and decoding parity bits is easily implementable into 8-bit microcontroller. Encoding cycle costs are important especially in low power ZigBee wireless, because every incoming packet must be tested by FEC (Forward Error Correction) at receiving side. From this perspective Hamming code is the most suitable candidate. The principle of a Hamming code (7.4) is assigned from three parity bits (Eqs 1–3) for every four bits protected. Parity bits are located at positions of second power – 1, 2, 4 (Hamming 1950). Calculation of parity bits can be written:

$$p_1 = b_1 \oplus b_2 \oplus b_4 \quad (1)$$

$$p_2 = b_1 \oplus b_3 \oplus b_4 \quad (2)$$

$$p_3 = b_2 \oplus b_3 \oplus b_4 \quad (3)$$

where:

p_1, p_2, p_3 – parity bits, resulting from XOR addition of input bits b_1 to b_4

The result is written in format:

$$p_1\ p_2\ b_1\ p_3\ b_2\ b_3\ b_4$$

This 7-bit word allows to recognize and correct one single error. The detecting calculation is based in following three equations:

$$s_1 = b_1 \oplus b_2 \oplus b_4 \oplus p_1 \quad (4)$$

$$s_2 = b_1 \oplus b_3 \oplus b_4 \oplus p_2 \quad (5)$$

$$s_3 = b_2 \oplus b_3 \oplus b_4 \oplus p_3 \quad (6)$$

where the vector consisting of bits (s_1, s_2, s_3) represents an Error syndrome.

When the Error syndrome is zero, the code word contains no errors, or more than one error. If there is one error in transmission, error syndrome corresponds to position of fault bit (Hamming 1950). It implies that when more than one error is given, the calculation may be correct, but the resulting syndrome does not correspond to reality. For this case extended Hamming code (8.4) can be used. This algorithm assigns one more parity bit to check the whole word. Then you can still fix one error, but also detect another. Because the following FEC method contains CRC (Cyclic Redundancy Check), there is no reason to use this parity bit.

Block Interleaver. Physical (PHY) layer of ZigBee uses spread spectrum method – replacing each four data bits by 32 chips. If a sufficient amount of bit errors occurs in transmission, backward process will not be able to replace chips with correct data bits and cluster error will occur. More than two separate errors in distance $n \leq 7$ affect wrong function of Hamming code. To prevent this case the Block data Interleaver is included in the processing.

Block interleaver is used to increase the distance between incorrect bits. Interleaving goal is to change the distribution of errors in the data block, spread clusters of errors to discrete errors. Discrete errors in distance $n > 7$ can be corrected by Hamming code (Křivánek 2008). Interleaver is built from the virtual table, where data are written in columns and output data are read by rows. Fig. 2 shows the principle for interleaving 4 × 4. The numbers in cells indicates the sequence position of input bits.

The design of interleaver is determined by ZigBee standard itself, and also from the measurement and simulation. Measurements show that the amount of the clusters highly depends on interfering element type, distance, and the signal strength. So chosen parameters of interleaver are not determined by measurement of cluster error rate only, but also with regard to the highest possible efficiency in the capabilities of ZigBee data packet and the acceptable load of the microcontroller. Size of the interleaver matrix was with respect to the max. interleaving

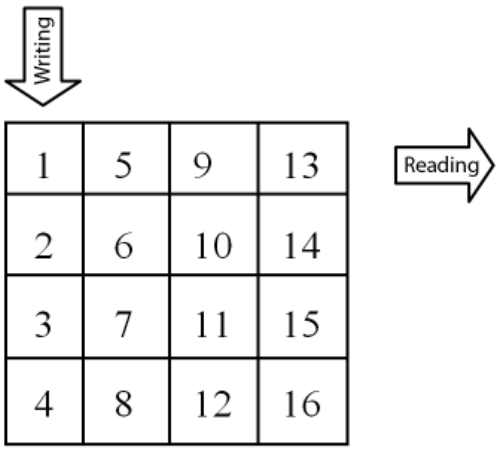

Fig. 2. Block interleaver matrix

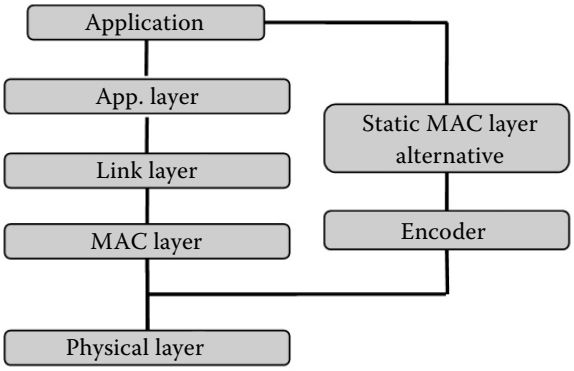

Fig. 3. Scheme of FEC data connection
MAC – Medium Access Layer; App. – Application

depth and a relatively large space in the data packets defined to 28 × 27. Matrix generates 756 bits, which corresponds to 108 code words of Hamming code. Final data capacity of one coded packet is 432 bits.

Efficiency of forward error correction above PHY layer. Because this method is located above the PHY layer, their impact does not cover all the transmission as show Fig. 3. To identify, which data can be covered by FEC and which cannot, a transmission structure summary follows (Fig. 4).

Frame begins by the Preamble, SoF delimiter and Frame length value, total of 48 bits which cannot be covered by provided forward error correction method, because it is given by Physical layer and cannot be changed without incompatibility issue. If the compatibility with other ZigBee nodes is important, Medium Access Control (MAC) sublayer should be untouched too. Anyway, algorithm of this method shall decode all incoming packets, because alternative MAC header is included under FEC coding. That implies that the MAC header is not important from the perspective of probability of transmission at the end point. Coded frames will be compatible with all other ZigBee nodes, they will be able to route this frames as any other. From this perspective only PHY header cannot be covered by FEC and shall be error free in transmission. FEC method protection is 94% of PHY frame. If error occurs in covered part, MAC (Medium Access Layer) header or FCS (Frame Check Sequence), can be corrected, if error will occur in PHY header, frame will be lost.

Experimental measurement. The aim of this experiment was to verify efficiency of the described method in increasing reliability of transmission. As experimental hardware Development boards Texas Instruments SmartRF05 was used, where microcontrollers CC2530F256 (both Texas Instruments, Dallas, USA) are used. These modules have output power 4.5 dBm and receiving sensitivity 97 dBm. Experimental network consists of Coordinator and Router nodes, where Coordinator was a transmitter and Router receiver. Software in modules was upgraded with described FEC method and measurement application. When network establishment was done, application in Coordinator starts sending predefined amount of coded frames to Router. A coded frame contains random data, generated for each frame separately and alternative 16 bit checksum in coded area. Router is decoding all incoming frames with correct frame length, and checks CRC value. If CRC value is correct, router increments amount of "coded way" received packet. Simultaneously, application counts all incoming data frames received by sublayers of Z-Stack. Flow chart of receiver application is described by Fig. 5. ZigBee network was established at channel 11.

As coexistence partner WiFi 802.11g link was chosen. This network was built from two main parts, WiFi Router US Robotics USR8054 (US Robotics, Schaumburg, USA), and Tablet Samsung P3110 (Samsung, Suwon, South Korea) Packets were generated by PC connected into Router by unshielded twisted pair (UTP) cable at speed 100 Mbit/s,

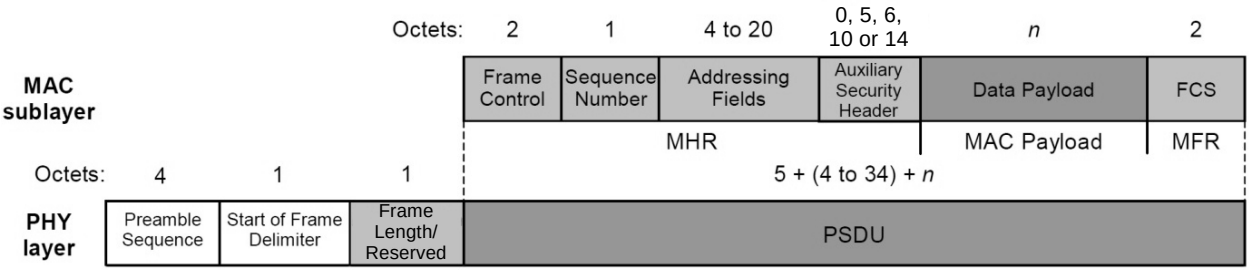

Fig. 4. Frame format of 802.15.4 (Institute of Electrical and Electronics Engineers, Inc. 2006)
PHY – physical; MHR – Mac Header; FCS – Frame Check Sequence; MFR – Mac Footer; MAC – Medium Access Layer; PSDU – Physical layer Service Data Unit

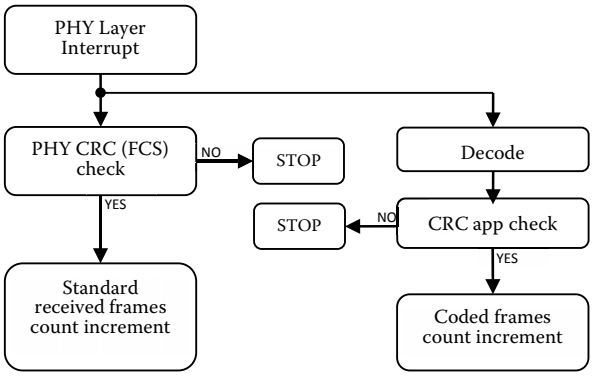

Fig. 5. Receiver application algorithm
CRC – Cyclic Redundancy Check; FCS – Frame Check Sequence; PHY – physical

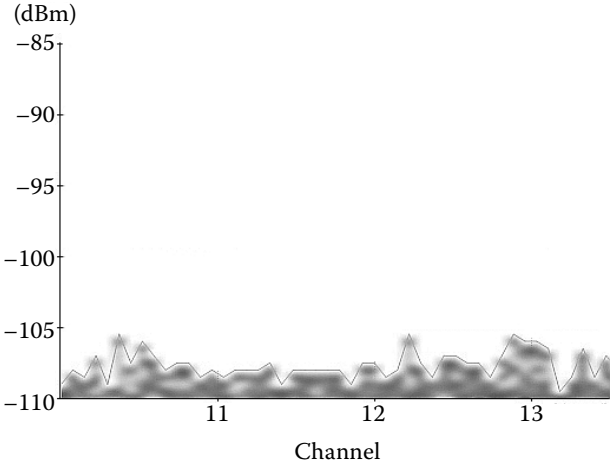

Fig. 7. Radio background at experiment area

and sent to IP address of tablet over WiFi. Various packet sizes were generated by Nping software (http://nmap.org/), where the following setting was used:

– 192.168.123.101 (IP address)
– data-length X (data length)
– delay 0 (delay between frames)
– c 2^{32} (total amount of frames)
– send-ip (compatibility setting parameter)

Parameter *X* is the length of user data, which was changed for each measurement.

Wireless connection between Router and Tablet was set to 1 channel and connection speed 54 Mbit/s. That implies that the Physical layer used 64-QAM modulation and data were coded with convolutional code in 3/4 ratio. Data stream was sent through 48 subchannels, where each symbol means 6 bits. Symbol duration is 4 μs. Over ZigBee network, only one type of packet was transferred, namely 108 Bytes of total length (13 B of ZigBee sublayers and 95 B of Data). That implies, since the symbol duration is 16 μs and DSSS coding (4/32) is used, 27.6 ms for each frame.

ZigBee nodes were mounted on tripod 1.5 m above ground, in 1 m distance. WiFi transceivers were in immediate distance, mounted on tripod in 1.5 m height. Distance between WiFi pair and ZigBee pair was gradually increased for each measurement. Distance was measured between ZigBee receiver and WiFi pair (Fig. 6). For each distance was sent defined amount of packets over ZigBee network, and registered values of correctly delivered packets on receiver. For each distance five measurements were done and then *PER* (Packet Error Rate) value was calculated according to the Eqs (7) and (8). Measurement was repeated for various packet length transmitted over WiFi.

$$PER_{ZigBee} = 1 - \frac{\text{amount of received frames with correct } CRC_{phy}}{\text{total of sent frames}} \quad (7)$$

$$PER_{fec} = 1 - \frac{\text{amount of received frames with correct } CRC_{app}}{\text{total of sent frames}} \quad (8)$$

where:

PER_{ZigBee} – Packet Error Rate of ZigBee transmission
PER_{fec} – Packet Error Rate with forward error correction
CRC_{phy} – Cyclic Redundancy Check of physical layer
CRC_{app} – Cyclic Redundancy Check of forward error correction

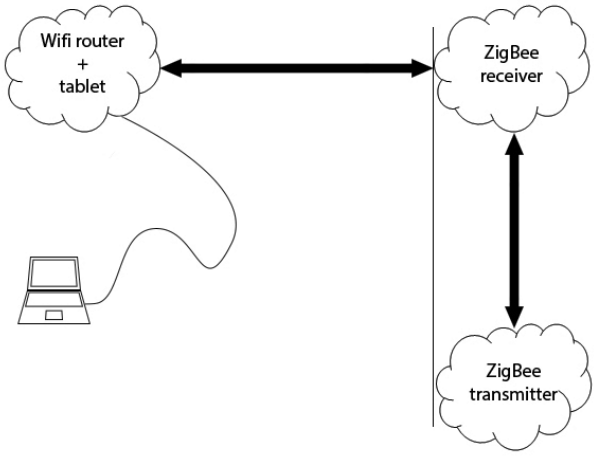

Fig. 6. Measurement equipment positioning

Experiment area. Measurement was done in open area, where no residential area or high-voltage lines were in 3 km radius. Before experiment radio back-

ground level was measured around 11 ZigBee channel, result is shown in Fig. 7. Measurement was done with WiSpy spectrum analyser and Chanalyzer Software (both MetaGeek, Boise, USA). As can be seen in Fig. 7, noise level was under –105 dBm.

RESULTS AND DISCUSSION

Fig. 8a shows results of coexistence measurement with the length of WiFi packet 76 B (31.2 μs). Mean time between WiFi packets was 3 ms. From this parameters it can be deduced that in each ZigBee packet (27.6 ms) 9 collisions with WiFi packet can occur. Each collision may take up to 31.3 μs. That implies interference can persist for 3 consecutive ZigBee symbols (16 μs each). Three symbol errors can result into 12 mistaken chips in row, and it means cluster of errors in length of 8 bits.

Fig. 8b shows the effect of FEC under 802.11g coexistence with packet size 188 B (47.9 μs). Mean time between WiFi packets was 1 ms. Under this circumstances an error can occur in three consecutive ZigBee symbols like in the previous case, max.

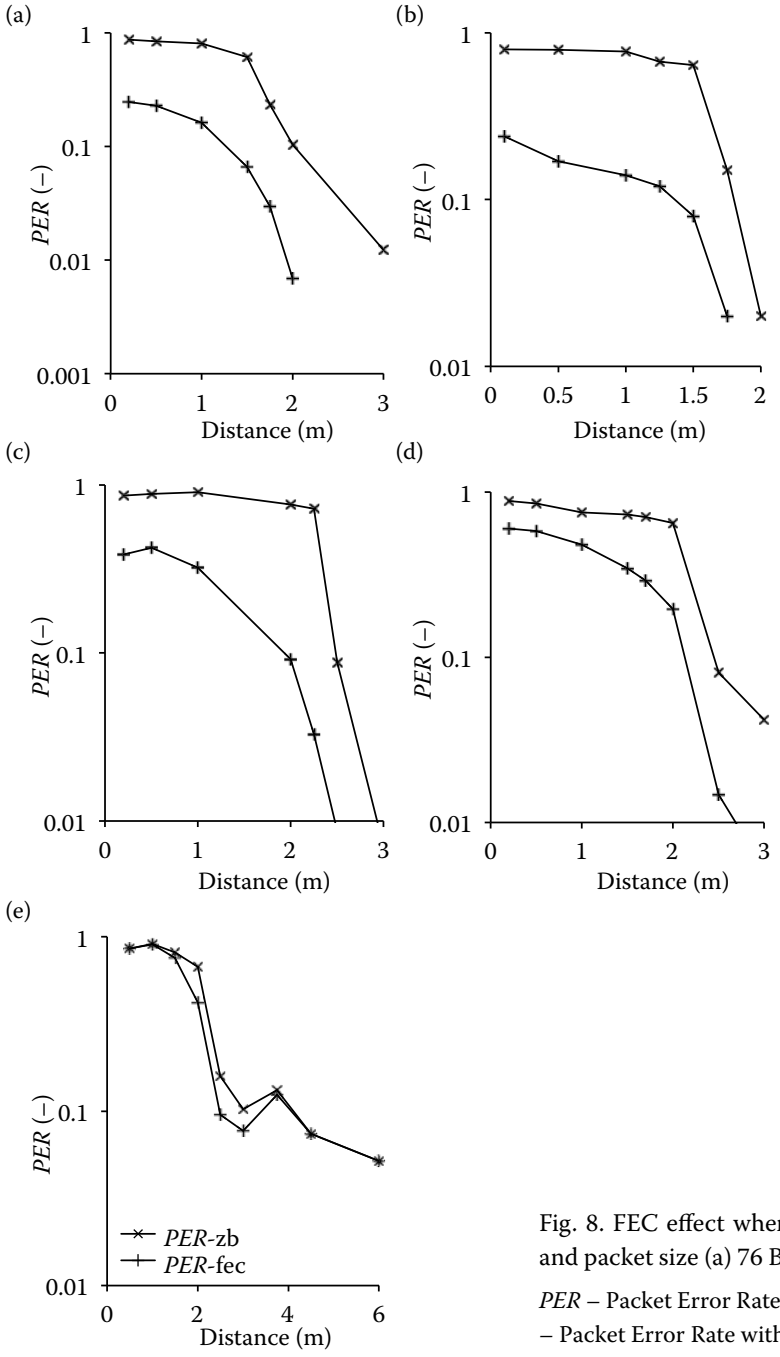

Fig. 8. FEC effect when operating under WiFi 802.11g coexistence and packet size (a) 76 B; (b) 188 B; (c) 316 B; (d) 572 B and (e) 1532 B

PER – Packet Error Rate; *PER-zb* – Packet Error Rate of ZigBee; *PER-fec* – Packet Error Rate with forward error correction

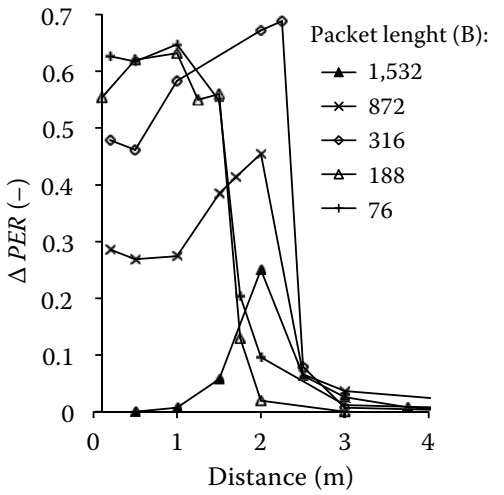

Fig. 9. Difference between standard ZigBee and FEC covered transmission

Δ*PER* – Delta Packet Error Rate

is 8 burst errors in a row. Due to the packet spacing, 26 clusters can occur in each ZigBee frame.

Fig. 8c shows FEC impact when WiFi packet is set to 316 B (66.8 μs), and mean time between packets is 1 ms. Compared to the previous case, now 5 consequent ZigBee symbols can occur, which results into 20 wrong chips and, as before, two error clusters in a row. As before, interference can occur 26 times for each ZigBee frame.

Next case (Fig. 8d) shows FEC impact when WiFi packet length is set to 572 B (104.7 μs). At this time 8 ZigBee symbols can occur in a row, which means 32 chips, and again two clusters of errors with length of 8 bits. As before, interference can occur 26 times for each ZigBee frame.

Fig. 8e shows results with the length of WiFi packet 1532 B (247 μs) and mean time between packets 450 μs. Effect of FEC method under this coexistence variant is very low. An error can occur in 17 ZigBee symbols in a row, which means 68 chips and cluster of 12 bits. For each ZigBee frame 40 collisions can occur, 12 bits each maximum.

As can be seen in Fig. 9, a significant benefit of described FEC method is when coexisting WiFi is lowly loaded, mainly with packets below 512 B of length. With interfering packets 316 B of length or lower, difference between standard ZigBee transfer and FEC covered method is at the same conditions about Δ*PER* 0.6, that means the "FEC packet" error probability is 60% lower.

CONCLUSION

Hamming code (7.4) has information rate 0.57, that results in a decrease of packet capacity from 95 B to 54 B. However, this amount shall be decreased for 2 bytes of CRC and the same alternative address of destination 1 or 2 bytes, so the final frame capacity will be lowered of 7 bytes (4 bytes coded by Hamming code). It implies that described Forward Error correction method decreases frame capacity of 50.5%. Experimental measurement in open area demonstrates benefits of this method under WiFi 802.11g coexistence. When WiFi is loaded with shorter packet lengths, FEC method can increase probability of successful transmission of 50–70% at same position.

References

Gislason D., 2008. Zigbee Wireless Networking. Oxford, Newnes: 425.

Hamming R.W., 1950. Error detecting and error correcting codes. The Bell System Technical Journal, *29*: 147–160.

Institute of Electrical and Electronics Engineers, Inc., 2000. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band. New York, Institute of Electrical and Electronics Engineers, Inc.: 89.

Institute of Electrical and Electronics Engineers, Inc., 2006. Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Network (WPANs). New York, Institute of Electrical and Electronics Engineers, Inc.: 305.

Křivánek V., 2008. Systémy realizace protichybového kódování. [Systems design of correction coding.] [Ph.D. Thesis.] Brno, Brno University of Technology: 1–93.

Received for publication February 2, 2013
Accepted after corrections May 27, 2013

Corresponding author:

Ing. Ilja Mašík, Czech University of Life Sciences Prague, Faculty of Engineering,
Department of Electrical Engineering and Automation, Kamýcká 129, 165 21 Prague 6, Czech Republic
phone: + 420 224 383 315, e-mail: ilja.masik@gmail.com