Vol. 5, No. 10 October 2014 ISSN 2079-8407
Journal of Emerging Trends in Computing and Information Sciences

http://www.cisjournal.org

A Methodical Approach to the Implementation of a Detection Method for Low-Power Wireless Sensors

Iztok Blazinšek
Margento R&D d.o.o., Gosposvetska cesta 84, 2000 Maribor, Slovenija
iztok.blazinsek@margento.com

ABSTRACT

This paper presents a methodical approach to the implementation of a robust and efficient method for detection of various radio frequencies wireless network sensors. A cluster of devices, which uses a radio network (RF) for communication between them, is used as an implementation example. The result of the methodical approach is a method which is used to upgrade existing wireless network to successfully detect other types of third-party add-on devices. The presented methodical approach includes the entire process from the selection of candidates for third-party devices, basic measurements and analyses to the implementation of the final communication method. The result of the presented approach is an efficient and robust method for capturing the data transmitted from third-party devices.

Keywords: *wireless sensor networks, wireless sensors, wireless sensor integration, wireless sensor data capture.*

1. INTRODUCTION

Various electronic devices are today increasingly pre-sent in our home environments. In general we can classify these devices in three main areas: devices designed to make our lives more comfortable, devices that make our homes safer, and devices meant to improve home security. In the lower price sector, each area of devices generally uses its own master communication interface, which is neither the most user-friendly nor energy- and cost-efficient solution. This is why the implementation of a method to integrate devices from different areas into one solution is of particular interest. In developing the method which would enable successful integration of several devices, a six step methodical approach was followed.

The first step of the approach requires careful selection of suitable third-party devices based on the parameters of the used radio transceiver. In the implementation, two types of devices are selected: temperature humidity sensors and burglar detection sensors. In the second step, the basic measurements to determine module carrier frequencies and modulation are performed. The results are then analysed to extrapolate the optimum carrier frequency for each type of selected modules. With optimum carrier frequencies and modulation, the third step in the proposed approach is to configure the receiving node accordantly, and to capture the data transmitted from the selected modules. In the fourth step, the optimum symbol definition is extrapolated from the captured data. With the optimum symbol definition extrapolated, an automatic capture method is synthesized and integrated in step five. In the final step, the robustness and the efficiency of the developed method are verified.

2. BASE COMMUNICATION NODE

The base communication node is equipped with short range radio-frequency link [1], which is implemented with the use of Texas Instruments' CC1101 chipset [2]. This is a versatile multiband transceiver that allows communication in ISM bands of 315, 433, 868 and 900 MHz. It also supports multiple modulation configurations, such as amplitude AM (amplitude modulation) or OOK (On/Off Keying) modulations, frequency 2FSK, 4FSK (Frequency-Shift Keying) modulation and GFSK (Gaussian Frequency-Shift Keying) modulation. As the device has multiple configuration options, it can be configured to work within both standards set by the FCC in the United States and the ECC in the European Union [3, 4 and 5]. The basic communication scheme between various devices is presented in Fig. 1:

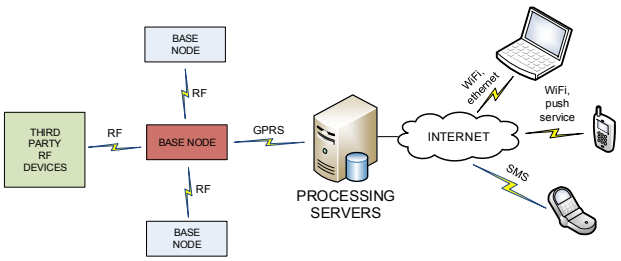

Fig 1: The basic communication scheme

The base node to base node communication use a 433 MHz frequency band and GFSK modulation. The frequency band is defined by the transceiver output stage and the implementation of the antenna [6, 7]. The transceiver fully utilizes the advanced CC1101 hardware options, such as digital SPI interface, packet data transfer mode, automatic hardware addressing, CRC calculation and data whitening. By using advanced features, such as hardware packet handling, the base node uses minimum resources to establish communication with other nodes. The base node can also support analogue data transceiver operation. In this mode, the signal detected on the input is directly proportional to the digital output, generated by the transceiver. This mode enables great flexibility, as it is independent from the data format. The data format can be later analysed and decoded by the processor unit.

3. ADD-ON MODULES

Due to hardware limitations, such as antenna design, the base node is limited to a 433 MHz band. Two

Vol. 5, No. 10 October 2014 ISSN 2079-8407
Journal of Emerging Trends in Computing and Information Sciences

http://www.cisjournal.org

different types of add-on candidates are analysed in this section. The first type is a remote temperature and humidity sensor and the second type is a family of burglar detection sensors

3.1 Remote Temperature – Humidity Sensor

The remote temperature – humidity (H-B Instrument DURAC 81) sensor was selected as a first add-on device. It operates in the same 433 MHz band as required by the base node. We have also received the specifications for the sensor's default communication protocol, which are available on the internet [8].

3.2 Burglar Detection Sensors

In the product range of burglar detection sensors we can find proximity infra-red and microwave sensors for detecting movement, magnetic sensors, which can be used to detect window or door closing/opening, smoke sensors for fire detection, and many others types of sensors. The basic node transceiver operates within 433 MHz bandwidth frequency. Considering this basic requirement two types of wireless modules were selected. The first type of sensors was proximity infra-red or PIR sensors (MC-335R) and the second type was magnetic swipe sensors (MD-210R). Both modules come from the same family of devices, and should be supplied by the same manufacturer. Because these devices are usually used as a part of secure networks, they use at least partially encrypted transmission. This makes it difficult to find any data about the wireless connection link or the protocol used to transfer data [9-11].

4. BASIC MEASUREMENTS AND ANALYSIS

In this section the measurement environment, equipment and the basic results will be presented.

4.1 Environment Setup

To analyse the add-on modules, the environment for preforming critical measurements must be defined. The main tool used in analysing wireless communication is a spectrum analyser R&S FSH3. We have also used a software defined radio, controlled by the PC, which is used as a secondary measurement unit. To ensure that measurements are accurate, both instruments are placed exactly one meter from the measured device, as indicated in Fig. 2. Various number of each type of sensors are used in measurements to determine the average carrier frequency.

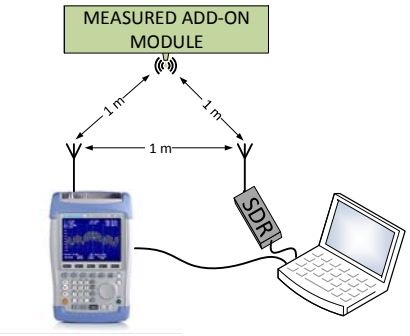

Fig 2: Environment configuration

4.2 Results of Remote Temperature and Humidity Sensors

Multiple measurements of each of the three samples of sensors were performed to help to determine the precise carrier frequency of temperature and humidity sensors. Results are gathered in Table 1:

Table 1: Results of the basic measurements of temperature and humidity sensors

Sensor	Sample 1	Sample 2	Sample 4
carrier frequency	433.884	433.916	433.890
Average carrier frequency: ~ **433.897 MHz ± 20 KHz**			

From the transmission protocol we already know that the modulation uses amplitude encoding. Measurements reveal the use of only two power levels. This suggests the use of the same OOK modulation as with burglar detection sensors.

4.3 Results of Burglar Detection Sensors

Multiple measurements of each of the four samples of sensors were performed to determine the precise carrier frequency. Samples one and two were PIR sensors and samples three and four were magnetic detection sensors. Results are gathered in Table 2:

Table 2: Results of the basic measurements of burglar detection sensors

Sensor	Sample 1	Sample 2	Sample 3	Sample 4
carrier frequency	433.957 MHz	433.959 MHz	433.960 MHz	433.959 MHz
Average carrier frequency: ~ **433.959 MHz ± 2 KHz**				

Transmission at a single carrier frequency can be an indication of amplitude modulation being used. Further analysis confirms that only two power levels are used. This suggests the use of on-off keying (OOK) modulation.

Vol. 5, No. 10 October 2014 ISSN 2079-8407
Journal of Emerging Trends in Computing and Information Sciences

http://www.cisjournal.org

5. ADVANCED MEASUREMENTS AND ANALYSIS

The first step in capturing the data transmitted by sensors is to properly configure the receiving module with the data acquired in section 4. The main parameters include the operation mode of the transceiver, type of modulation, carrier frequency and the receive filter bandwidth. In both cases the operation mode of the transceiver is set to asynchronous mode. In this mode, the transceiver output directly reflects the state of the input RF signal, as demonstrated in Fig. 3.

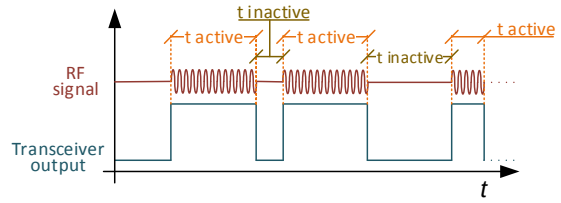

Fig 3: The transceiver operation mode representation

This mode is used to enable capturing of raw data, which can then be monitored either with a logic analyser or an oscilloscope, and processed by the main processor at a later stage.

5.1 Remote Temperature - Humidity Sensors

As the data transfer protocol for this type of device is known, the implementation of capturing data is easier. The captured data can be immediately compared to the transmission protocol of the device [8]. With the transceiver properly configured with data from subsection 4.3 and ready for reception, the frames from remote temperature and humidity sensors can be received. Fig. 4 shows on the right side the activation sequence captured with the SDR, and on the left side the data outputted by the receiver.

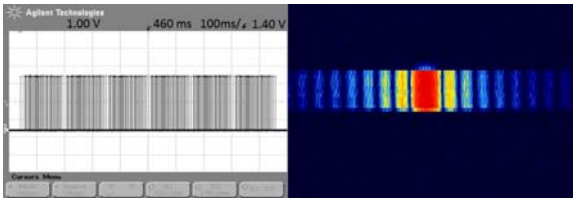

Fig 4: Successfully captured data from a remote temperature and humidity sensor

Each transmission from remote temperature and humidity sensors appears to be split in six identical frames. Fig. 5 represents one isolated frame.

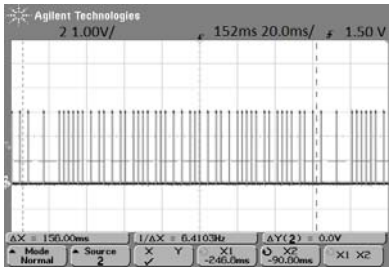

Fig 5: One isolated frame

As specified by protocol [8], the transmission appears to be divided in three distinct symbols, each defined by the same *t_active* followed by a different *t_inactive* (Fig. 3). These symbols are *sync_t*, symbol for bit '0' and symbol for bit '1'. To check if symbol times are consistent and in line with the specification, and to determine the best timeframes for each symbol, more than 50 sequences were captured and the values for each symbol extrapolated.

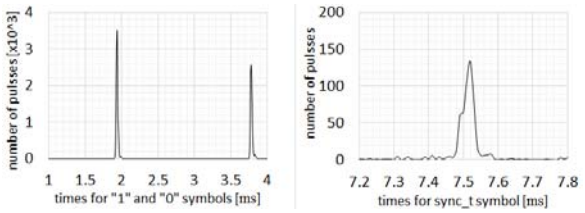

Fig 6: Symbols definitions: bits '0' and '1' (left) and *sync_t* (right)

Data from Fig. 6 can now be used to extrapolate optimum symbol definitions – Table 3.

Table 3: Optimum symbol definitions for remote temperature - humidity sensors

Symbol	*sync_t*	Bit '0'	bit '1'
Minimum timeframe	7300 µs	1.5 ms	3.5 ms
Maximum timeframe	7700 µs	2.5 ms	4.5 ms

5.2 Burglar Detection Sensors

Both detection sensors are from the same family of sensors, only one needs to be analysed. With the transceiver properly configured with data from subsection 4.2 and ready for reception of detection sensor frames, the capture efficiency is tested with the use of a digital oscilloscope (left image in Fig. 7) and an SDR (right image in Fig. 7).

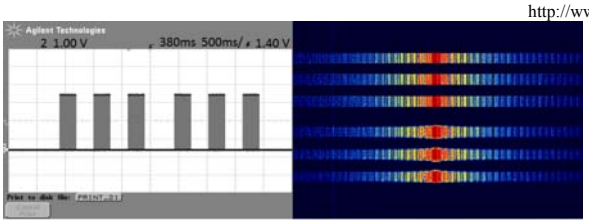

Fig 7: Successfully captured data from the burglar detection sensor

It can be seen in Fig. 7 that there are six data segments sent from the motion detection sensor. To extrapolate frames from segments, these segments are further analysed.

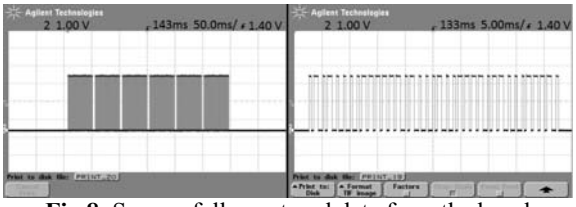

Fig 8: Successfully captured data from the burglar detection sensor

Further analysis shows that each data segment is composed of six frames (Fig. 8 - right), and each frame is composed of 37 pulses of two different lengths (Fig. 8 - left). The symbol encoding for this type of devices is believed to be either 33%/66% - start high or 33%/66% - end high [9]. In either case, data encoding is done on the basis of active pulse length. A longer active pulse (Fig. 3) is encoded as binary "1" and a shorter active pulse as binary "0". To ensure that data is captured in a sequence, we must first develop a method for symbol synchronisation. The easiest way to achieve symbol synchronisation is to implement a method which detects the minimum idle time between frames or sections (time *sync_d*). This way, the first symbol detected after *sync_d* time interval is the first symbol in a sequence. To get the most optimum symbol definition for each symbol, more than 100 sequences were captured, and idle time *snyc_d* and active times for each symbol "1" and "0" were extrapolated. Both types of sensors were measured to ensure that they use the same symbol definition.

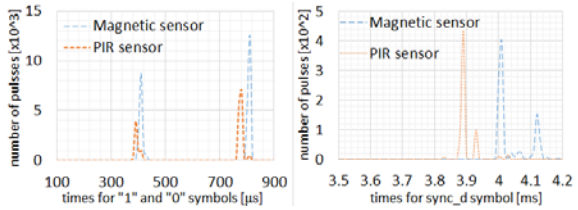

Fig 9: Symbol definitions: bits '0' and '1' (left) and d_sync (right)

Fig. 9 shows the results. As expected, symbol definitions for both sensors are almost the same. With this data as a base, an optimum timeframe for each symbol can now be defined - Table 4.

Table 4: Optimum symbol definitions for detection sensors

Symbol	*sync_d*	Bit '0'	bit '1'
Minimum timeframe	3500 µs	350 µs	750 µs
Maximum timeframe	4500 µs	450 µs	850 µs

These symbols can now be used to encode the received sequence in its digital representation. The digital representation is then sent to servers, where it is decoded and evaluated to determine if any further action is needed.

6. AUTOMATION AND INTEGRATION OF THE DATA CAPTURE METHOD

With the data gathered in tables I, II, III and IV, a universal method for automatic capturing of data can be synthesized. Because the carrier frequency of both modules differs slightly, the first step is to decide upon a method which would allow capturing transmission on both of the carrier frequencies. There are two methods available for achieving this goal:

- Either a wide receiver band filter is implemented, which allows for data to be received on both carrier frequencies simultaneously, or
- A channel scanning technique is implemented.

The advantage of the first method is its simplicity. The disadvantage of this method is higher error sensitivity. The second method (channel scanning) requires that the device divides the frequency bandwidth into specific channels, each having the optimum receive bandwidth. The advantage of this method is that it greatly reduces the error caused by sporadic transmissions due to a narrow band filter. The downside of this method is that the software must handle channel switching. This significantly increases the load of the microprocessor. In addition, the receiver and the software need time to switch between channels and to scan each channel for energy level, which in worst case could result in missed sequences. We have decided to implement and verify the first method. The method has been chosen because of a relatively small difference between both carriers and a clear difference between symbol definitions of each capturing method. The method also greatly benefits the system performance as the entire channel switching logic does not need to be implemented.

To implement this method, the first step is to extrapolate from Tables I and II the new receiver bandwidth (Eq. 1) and the base carrier frequency (Eq. 2) for the RF transceiver, which would allow reception of transmission from both types of sensors simultaneously.

$$RX_{BW} = f_{MAX}\,(\text{Table I, Table II}) - f_{MIN}\,(\text{Table I, Table II}) \quad (1)$$

$$f_{carrier} = \frac{f_{MAX}(\text{Table I, Table II}) + f_{MIN}(\text{Table I, Table II})}{2} \quad (2)$$

The newly calculated receiver filter is ≥75 KHz, with the carrier frequency of 433.922 MHz. The next step is the implementation of an algorithm for automatic data collection.

The algorithm implements two modes: mode 1 enables reception of transmissions from temperature – humidity sensors, and mode 2 enables reception of transmissions from detection sensors. The algorithm in its idle state waits to either get the sync symbol from the temperature - humidity sensor or to detect the synchronization timeout between detection sensors' subsections. After this symbol is successfully received, the capture value and the current bit counter value are reset. Proper symbol definitions and the expected bit count are also loaded for future use. The algorithm then waits to receive the required number of symbols. If the algorithm is currently processing data in mode 1, the captured sequence is forwarded to the application for further processing. If the algorithm is operating in mode 2 and the bit count reaches the minimum bit count expected from the alarm sensors (39 bits), the alarm ID is extrapolated. If the extrapolated alarm ID matches any of the previously enrolled alarms, the alarm is forwarded to the application for further processing and the received bit count and the alarm value are reset. If the alarm does not match, the algorithm waits for the next bit and compares the values again. The algorithm is represented by Figure 10:

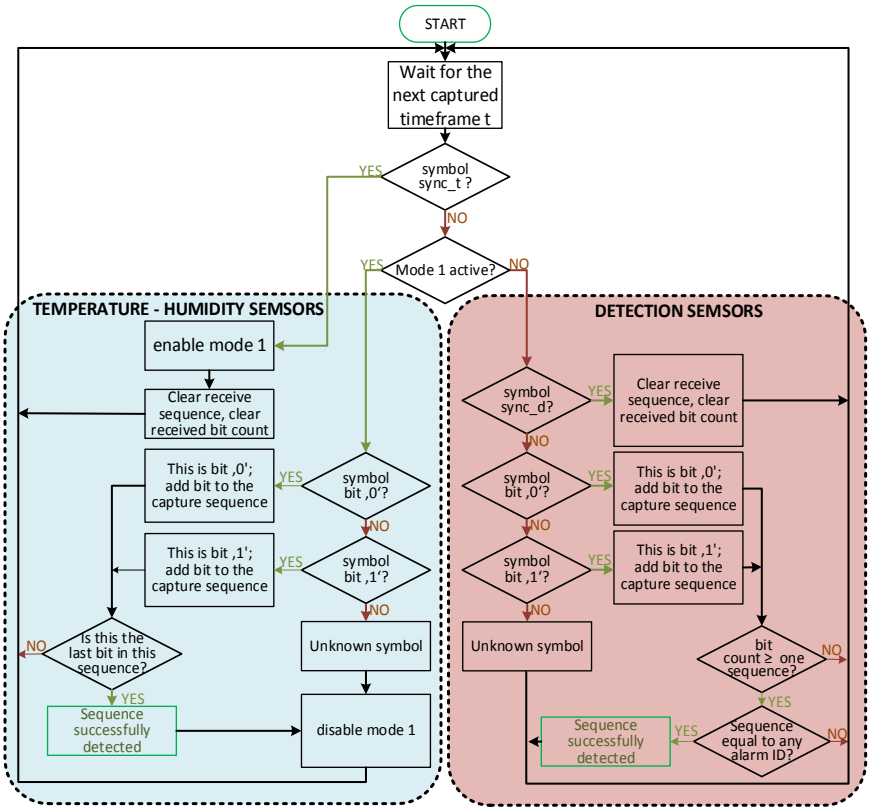

Fig 10: Automatic data capturing algorithm

7. VERIFICATION

This section presents the verification of the method developed in section 6. The performed tests measured how many sequences are detected in each transmission over at least one hundred transmission events. The test environment consists of a large room and two adjacent rooms. Ten random positions were chosen and from each position ten transmissions were made. Each sensor was manually triggered and transition reception was verified. In addition, a computer recorded every successfully detected frame. From the analyses preformed in sections 3 and 4 it can be calculated how many frames the receiver should receive that the reception would be 100 % successful. From this and from the count of captured frames, the success ratio for frame transmission can be calculated. The main and absolute requirement is to get at least one successfully detected and decoded frame per transmission as this guarantees 100 % reception success. The intention of the verification was to test the method efficiency in the environment without external interferences. This is why all other types of devices were turned off and only one sensor was used

during the measurements. This reduced the possibility of the results being inaccurate due to the interference from other devices.

7.1 Remote Temperature - Humidity Sensors

Remote temperature - humidity sensors were tested first. Results are presented in Fig. 11:

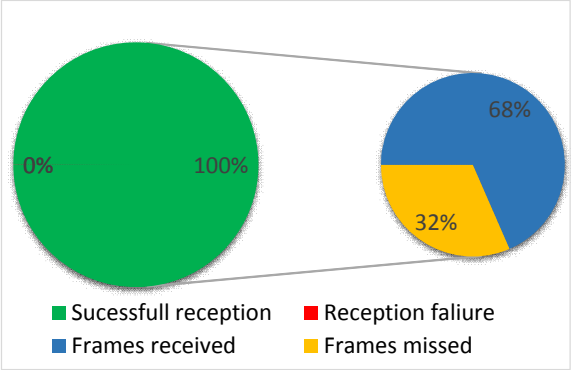

Fig 11: Test results from the remote temperature – humidity sensor

If at least one frame from each transmission is successfully received, then the event is successfully detected. This is indicated by a green circle (left side of Fig. 11). The right side of Fig. 11 shows that overall 68 % of all the data frames were successfully received on average. It can be concluded that in every transmission the master node on average successfully received and decoded four out of six frames. This indicates a good level of reception success.

7.2 Burglar Detection Sensors

Both types of detection sensors were tested: first the magnetic and then the proximity infra-red sensor.

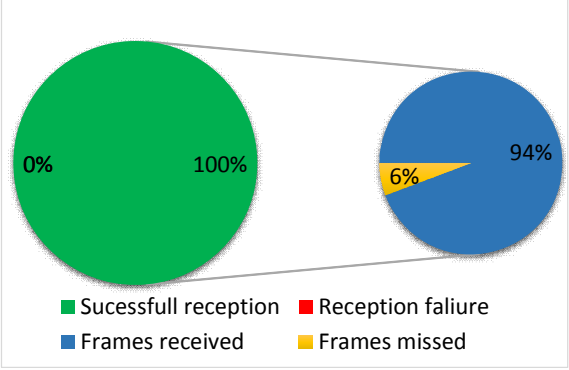

Fig 12: Test results from the magnetic detection sensor

If at least one frame in every data segment is successfully received, then the event is successfully detected. Fig. 12 (left side) shows 100 % reception success with a 94 % frame reception success (Fig. 12, right side). These are particularly good results as the sensors do not use the start up or preamble sequence to allow the receiver to settle before transmission. The first symbol already represents the data being sent.

Next the proximity-infra red sensors are tested. Results are displayed on Figure 13:

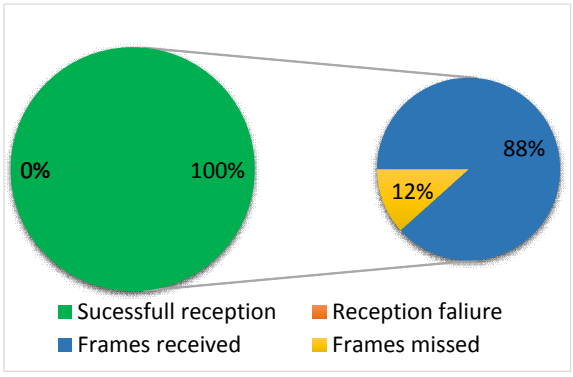

Fig 13: Test results from the proximity infra-red sensor

Test results in Fig. 13 (left side) indicate a 100 % reception success, which means at least one frame per every data packet was successfully decoded. Further analysis shows that each transmission is captured with an 88 % frame reception success (Fig. 13, right side).

8. CONCLUSION

The purpose of this article was to present a methodical approach to the implementation of an efficient and robust wireless communication interface between the base communication node and various third-party devices. The proposed approach consisted of six steps. In the first step, candidates for add-on modules (third-party devices) were selected. In the second step, both types of the modules were measured to determine the basic parameters. In the third step, the data received from the modules were captured and analysed. In the fourth step, a method was developed which enabled the receiver to automatically capture and decode the data and finally in the fifth step, the method was integrated in the existent communication scheme. Finally, in the last step, the efficiency of the developed communication method was verified.

Analysis of the test results shows that the results from the temperature - humidity type of devices are not as good as those from the detection type of deceives. The most obvious explanation for this is the method of communication. While the method for detection sensors extrapolates data from *t_active* time, the temperature – humidity type of devices use the *t_inactive* (Fig. 3). Because the symbol definition is very large, up to few milliseconds, there is a large chance of interference. This is even more obvious when the receiver due to weak signal uses a high gain. The results from detection sensors are encouraging. A very high frame reception rate suggests that the implemented method is robust, efficient and a good candidate to be implemented in future master device releases.

The obtained results demonstrated that with the use of the presented approach an efficient and robust method for communication with various types of wireless devices can be developed. The communication method,

developed with this methodical approach requires minimum investment in research time and development while providing a very significant increase in product value.

ACKNOWLEDGEMENT

This operation is partly financed by the European Union, European Social Fund. The operation is implemented in the framework of the Operational Programme for Human Resources Development for the Period 2007-2013, Priority axis 1: Promoting entrepreneurship and adaptability, Main type of activity 1.1.: Experts and researchers for competitive enterprises.

REFERENCES

[1] Electronic Communications Committee: The European table of frequency allocations and applications in the frequency range 8.3 kHz to 3000 GHz", (2013).

[2] CC1101 documentation: http://www.ti.com/product/cc1101 (2013).

[3] ISM-Band and Short Range Device Regulatory Compliance Overview: http://www.ti.com/lit/an/swra048/swra048.pdf (2005).

[4] ERC Recommendation: http://www.erodocdb.dk/docs/doc98/official/pdf/rec7003e.pdf (2013).

[5] Part 15 of Title 47 of the Code of Federal Regulations: http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&SID=991c4d4bdec8591ce7ef3ac259e87786&tpl=/ecfrbrowse/Title47/47cfr15_main_02.tpl (2014).

[6] W. Liu, Z. Zhang, J. Zheng, Z. Feng, "A novel miniaturized antenna for ISM 433MHz wireless system", Electrical Design of Advanced Packaging and Systems Symposium (EDAPS), pp. 1-4, 2011

[7] A. Babar, L. Ukkonen, M. Soini, L. Sydanheimo, "Miniaturized 433 MHz antenna for card size wireless systems", Antennas and Propagation Society International Symposium, pp. 1-4, 2009

[8] Temperature – humidity sensor transmission protocol: http://www.doc88.com/p672304442567.html (2012).

[9] NM95HS01/NM95HS02 HiSeCTM High Security Rolling Code Generator: http://www.engineering.uiowa.edu/sites/default/files/ees/files/NI/pdfs/01/23/DS012302.pdf

[10] J. Zhou, A. Mason "Communication Buses and Pro-tocols for Sensor Networks." Sensors, pp. 244-257, 2002

[11] Protocol Examples for ISM Band Applications: http://www.infineon.com/dgdl/PMA71xx_PMA51xx_AN_RF_Protocol_Examples_V1.0.pdf?folderId=db3a3043191a246301192dd3ee2c2ae4&fileId=db3a3043243b5f17012452f9c8a0548c (2009