# TECHNICAL ANALYSIS OF THE WIRELESS LOCAL AREA NETWORK SIGNALS

**Pawel Skokowski, Jerzy Lopatka**
Military University of Technology
Electronics Faculty, Warsaw, Poland
{skokos@wp.pl, jlopatka@wel.wat.edu.pl}

In this paper we present methods enabling the analysis of the wireless local area network (WLAN) signals. Presented procedures enable estimation the basic parameters of the signal, identification of the standard and provide knowledge concerning essential information about the working network. Efficiency tests of proposed method of analysis are also introduced in the work. The *Bit Error Rate* (BER) is accepted as the basic merit of the transmission quality.

## 1. Introduction

Demands on the wireless digital systems are constantly growing. Systems are expected to be faster, safer, interferences resistant and should effectively use available frequency band. It causes development and introduction of new extensions of the 802.11standard. They guarantee better quality of services (802.11e), the assurance of the safety (802.11i) and dynamic management of radio frequencies and power of the transmitter (802.11h). To provide proper operation of such systems, sometimes it is necessary to have a possibility to monitor wireless networks work, detect potential threats, study compatibility with other systems and identify the sources of interferences.

## 2. Problems of WLAN signals analisys

At present there is a lot of standards used for the wireless transmission. In ISM (*Industry, Science, Medicine*) and U-NII (*Unlicensed National Information Infrastructure*) band the following systems are the most popular: HIPERLAN, HIPERLAN2, 802.11a/b/g, Wi-Max 802.16a and Bluetooth. They use different techniques of modulation and exploit channels with various bandwidths that give variable throughput. Table 1. contains basic parameters of quoted above systems. Some of them use the shareable sets of frequency channels that require an effective recognition of the working system. At present, to analyze such signals specialized devices (e.g. spectrum analyzers) or dedicated software are used [1][4][5][6][7][8]. However they have many limitations resulting from the need of general purpose construction. Devices or software dedicated to a specific set of standards would be more useful. To identify WLAN standard it seems to be most important to estimate parameters like: carrier frequency, bandwidth of the channel, Signal to Noise Ratio (SNR), throughput, type of the applied modulation, number of stations in the network, format of transmitted frame and mode of the network operation [2].

| **System** | **Bluetooth** | **802.11b** | **802.11g/ 802.11a** | **HIPERLAN** | **HIPERLAN2** | **WiMax 802.16a** |
|---|---|---|---|---|---|---|
| **Band** | ISM | ISM | ISM/ U-NII | U-NII | U-NII | 2-11 GHz |
| **Channel bandwidth** | 1 MHz | 22 MHz | 20 MHz | 23,5 MHz | 20 MHz | 1,5-20 MHz |
| **Modulation type** | FHSS (GFSK) | DSSS (DBPSK, DQPSK, CCK) | OFDM (BPSK, QPSK, 16QAM, 64QAM) | GMSK | OFDM (BPSK, QPSK, 16QAM, 64QAM) | OFDM (QPSK, 16QAM, 64QAM) |
| **Number of subcarriers** | | | 52 | | 52 | 256 |
| **Number of pilots** | | | 4 | | 4 | 4-24 |
| **Throughput** | Up to 3 Mb/s | Up to 11 Mb/s | Up to 54 Mb/s | Up to 23 Mb/s | Up to 54 Mb/s | Up to 70 Mb/s |

Tab. 1. Wireless systems in ISM and U-NII band

## 3. Proposed Method

The advantage of the proposed method is that it realize full analysis using software application, which means that additional devices (like WLAN receiver) are not required. Elaborated method, contrary to commonly available programs, enables also despreading of the 802.11b signal and its demodulation.

The analysis is based on the data in complex IQ form, representing recorded real signal WLAN, with known center frequency. To conduct the analysis we assumed that studied signal is a signal in the digital form, with the predetermined length of record and known sample frequency. Program MATLAB Simulink is a tool used to the analysis of the signal, and tests are conducted in the „off-line” mode.

We can mark out the following stages of analysis (Fig.1.):

- definition of carrier frequency and working channel number,
- estimation of channel bandwidth and SNR,
- identification of WLAN standard,
- correlation signal with the spreading sequence - despreading signal,
- determination of frame format,
- demodulation and descrambling of preamble and header of PLCP frame,
- determination of demodulated signal parameters: frame defragmentation and specifying characteristic fields content,
- demodulation and descrambling the data field,
- decoding the MAC frame,
- recognition of the network mode of operation,
- determination of number of users, network's addresses and physical MAC card's addresses.

## 4. Identification of 802.11a/b/g standards

To distinguish standards 802.11b/g from 802.11a, it is sufficient to know carrier frequency of the signal. If the carrier frequency belongs to U-NII band, it means that working network is compliant with 802.11a standard.

One way to distinct 802.11b and 802.11g standard is determination of signal bandwidth. If bandwidth of the signal equals 22 MHz, this means that network works using 802.11b standard. If bandwidth equals 20 MHz it can be assumed that network works using OFDM technology, so it is 802.11g standard.

The calculation of signal constellation is the next method of WLAN standard identification. If signal is transmitted using 802.11b standard, then constellations have form like DBPSK modulation (in variant A) or DQPSK. When transmitted signal belongs to 802.11g standard then can be use one from four modulations methods: BPSK, QPSK, 16 QAM or 64 QAM. Fig. 2. presents algorithm of WLAN standard identification.

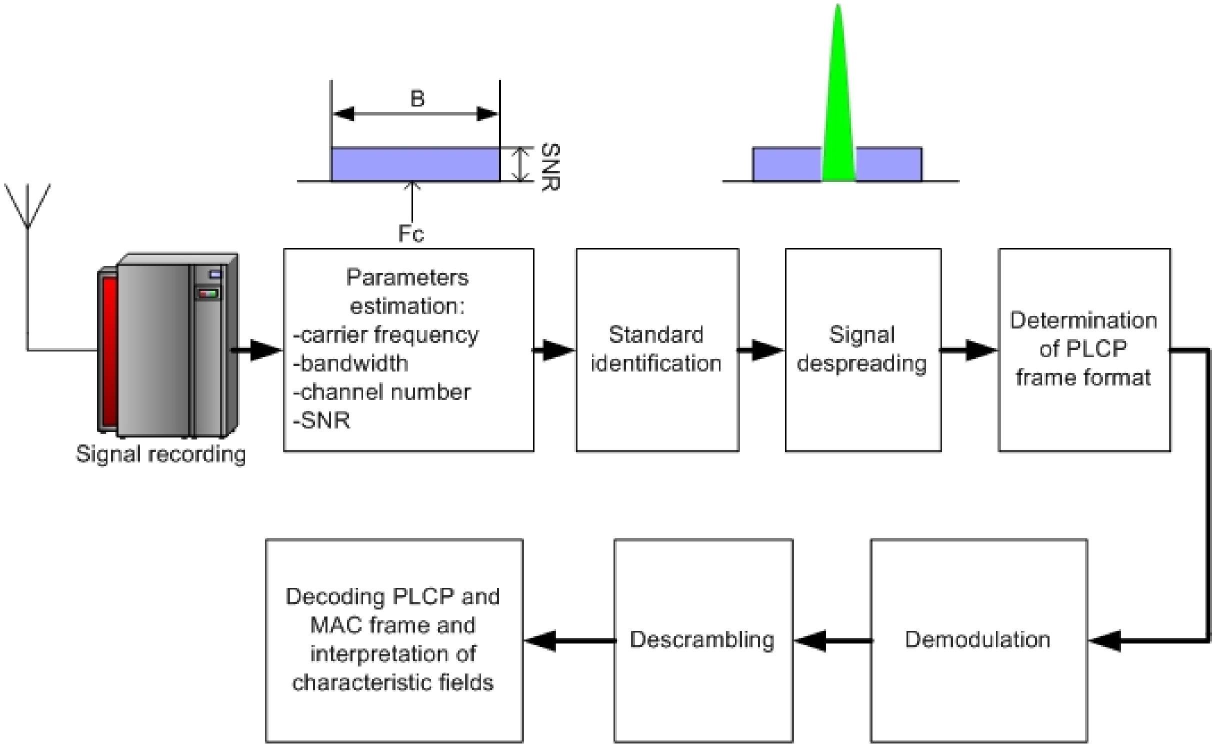


Fig. 1. Steps of analyze

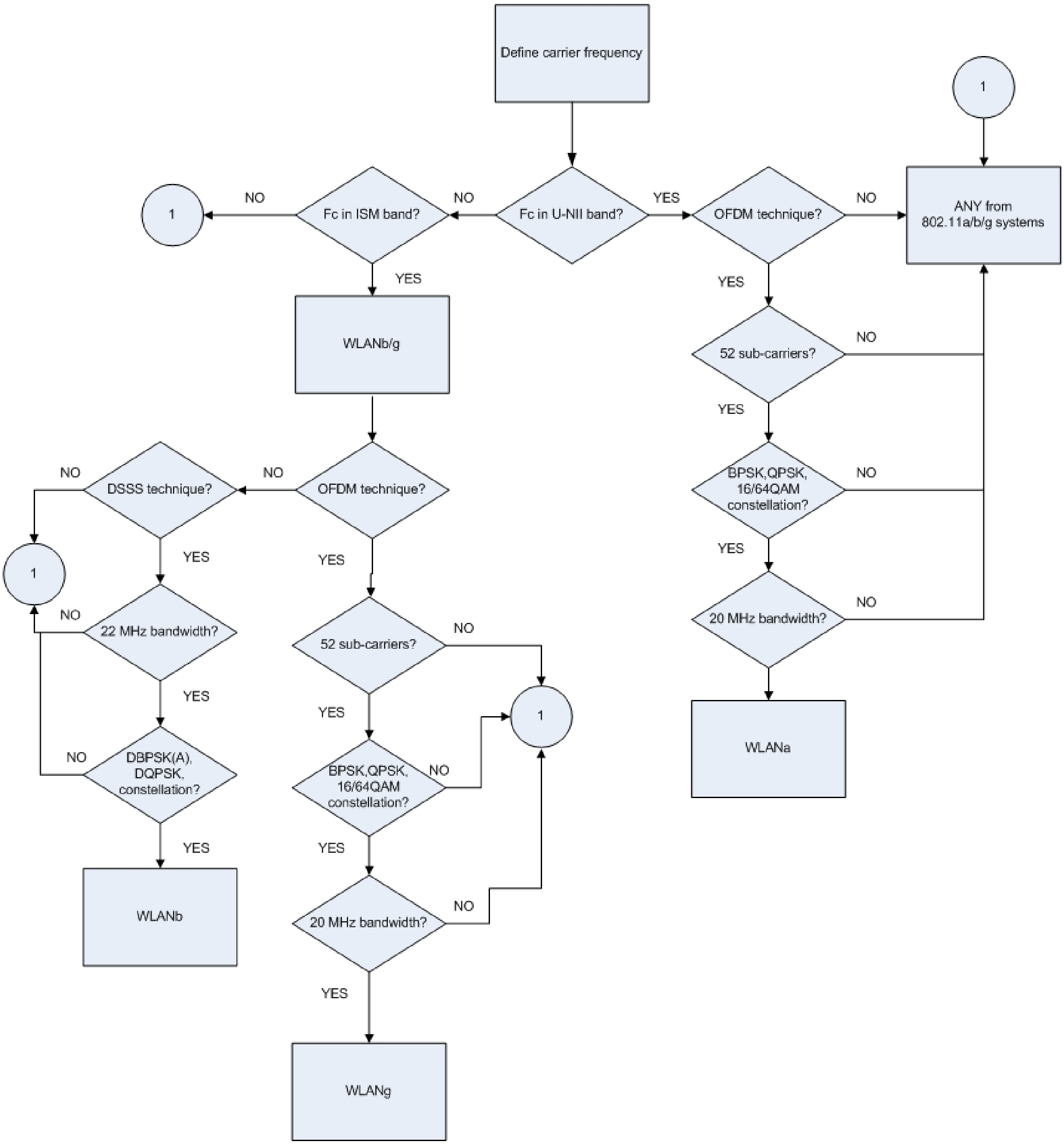


Fig. 2. Algorithm of WLAN standard identification

### 5. Analysis results for 802.11b standard

The carrier frequency equals to 2.437 GHz, corresponds channel number 6. Bandwidth of the channel is 22 MHz, and SNR ≈ 9 dB. Parameters were defined on the basis of spectrum analysis of the signal. The most exact results were obtained using the Yule-Walker's parametric method [3].

In the next step standard of the recorded signal was identified. The defined autocorrelation function shown on Fig. 3. shows, that the signal has the noise character, so the most probably it was spreaded using the direct sequence spread spectrum (DSSS) method.

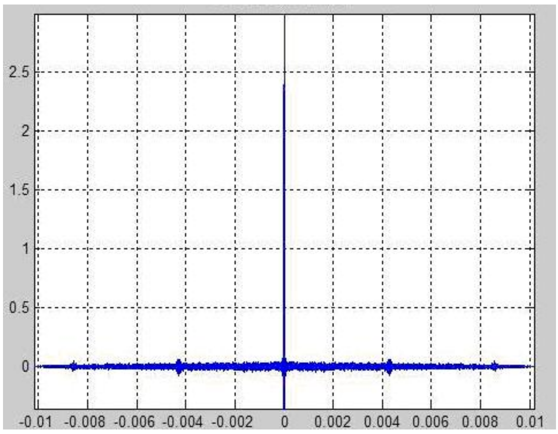


Fig. 3. Autocorrelation function of analyzed signal

Signal despreading is the next step of analysis. It is realized by correlating the signal with the 2 sliding windows containing the spreading Barker and complementary code.

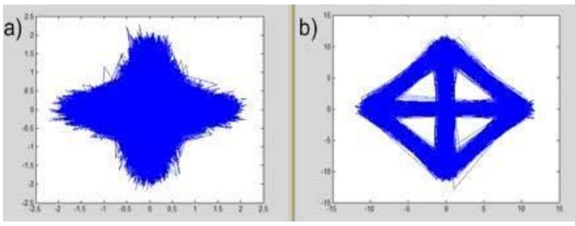


Fig. 4. IQ signals
a) before despreading
b) after despreading

Signal spectrum before and after despreading is shown on Fig. 5. On this basis we can see, that signal after despreading has power about 10 decibels higher than signal before despreading. It confirms that the despreading process is performed properly, because for WLAN 802.11b the processing gain is equal 10.4 dB.

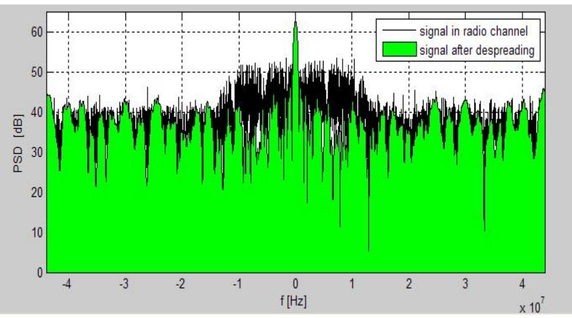


Fig. 5. Signal spectrum before and after despreading

Next, the header of PLCP frame was dealt out from the analyzed signal. Phase histogram created on the basis of the instantaneous phase samples shows that the modulation DBPSK (Fig. 6a.) was used. The maxima of the histogram appear for 0 and 180 degrees. Header constellation (Fig. 6b.) was done then and it shows a DBPSK constellation what confirms earlier considerations that the long format of frame was used. In the case of using short frame format, part of header would be modulated with DQPSK.

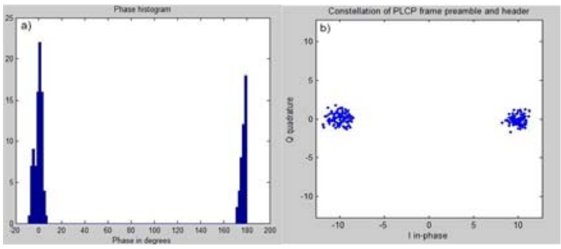


Fig. 6. PLCP frame header and preamble
a) phase histogram b) constellation

After determination of the frame format the process of demodulation of preamble and header of PLCP frame was performed. Because whole frame is scrambled in the transceiver side, to correctly decode fields of PLCP frame preamble and header, signal should be descrambled in the receiving side. Fig. 7a. presents fields of preamble and header before and Fig. 7b. after descrambling. White color represents logical one, and black logical zero.

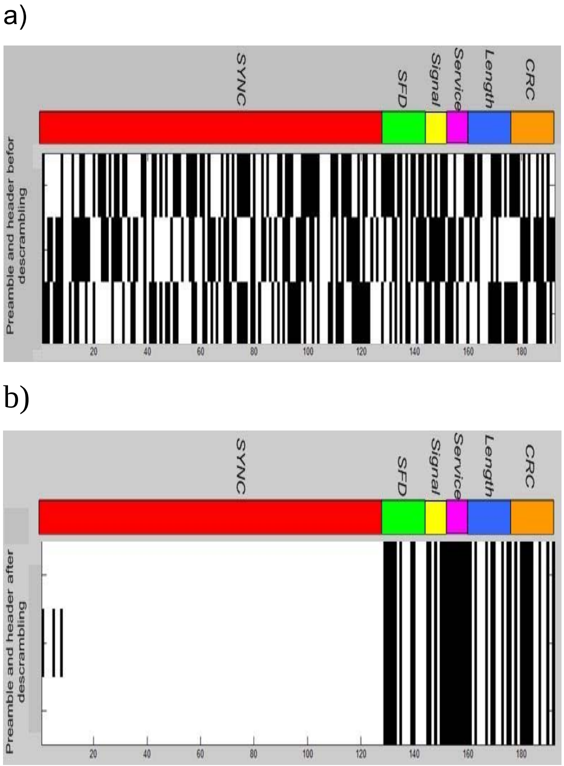


Fig. 7. Preamble and header of PLCP frame
a) before descrambling
b) after descrambling

After proper despreading, demodulation and descrambling it is possible to recognize content of fields in the preamble and the header of PLCP frame. They show that the long format of frame was applied for all three decoded frames of the value *SYNC* (all zeros) and *SFD* (0000 0101 1100 1111).

*Signal* field (0010 1000) indicates that data is transmitted with data rate 2 Mbps. Added MAC frames are transmitted with the data rate 2Mbps, using DQPSK modulation. Constellation for the data field of analyzed signal after despreading is shown on Fig. 8.

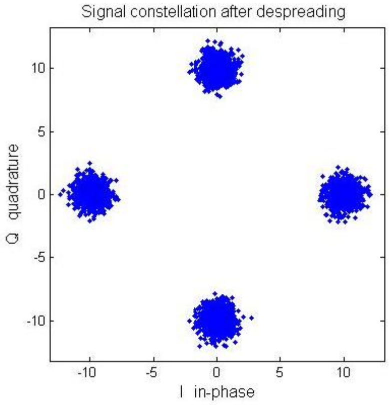
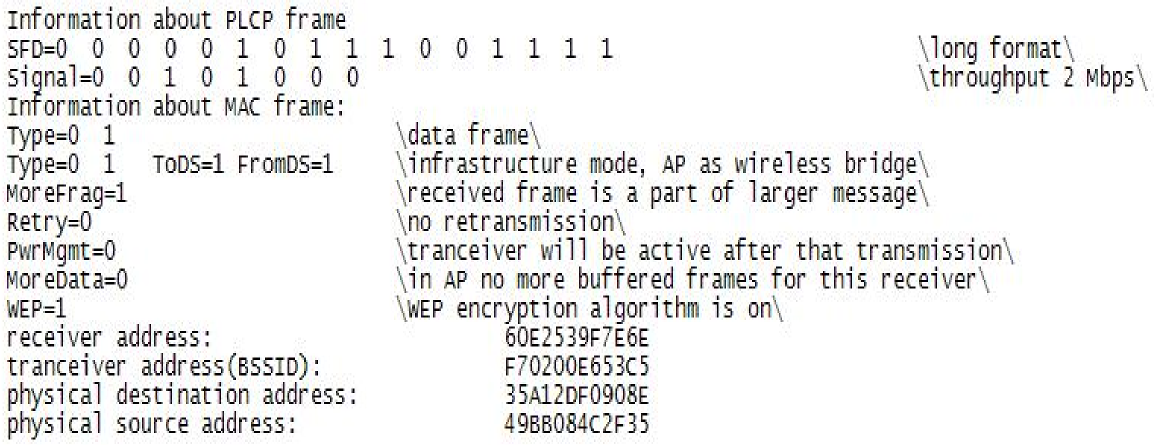


Fig. 8. Signal constellation after despreading

Then the field of data was demodulated using DQPSK demodulator and descrambled, to decode characteristic fields from the MAC frame header. The decoded information shows that received frames are data frames and recorded part of transmission is an exchange of data between two stations via access point. The network works in the infrastructure mode. The field of the given MAC frames is encrypted according to the WEP algorithm, and each frame is a fragment of the larger message and it isn't a retransmission of a previous one. Additionally it can be confirm that the station will be in the active mode after the completion of current transmission. Decoded addresses fields have following form:

- address of receiver set as the network address:
  60-E2-53-9F-7E-6E;
- address of transmitter, representing network identifier (BSSID):
  F7-02-00-E6-53-C5;
- address of destination, that is receiver physical address of MAC card:
  35-A1-2D-F0-90-8E;
- address of source, that is transmitter physical address of MAC card:
  49-BB-08-4C-2F-35.



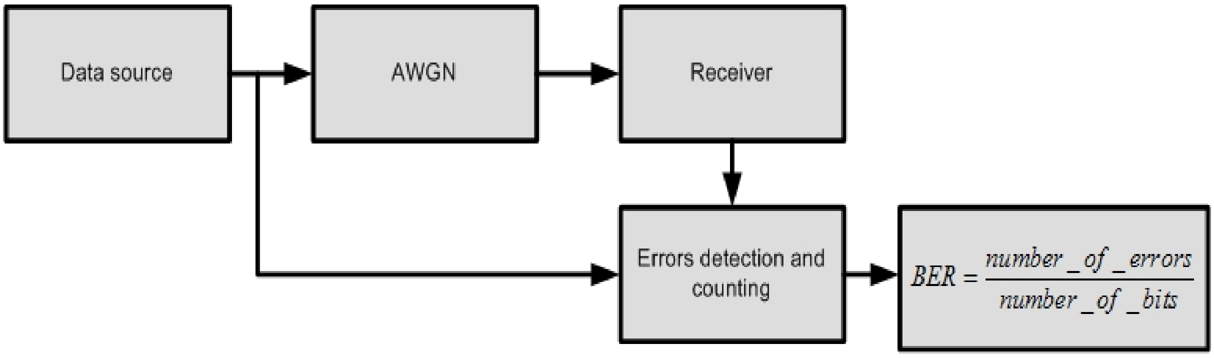
```
Information about PLCP frame
SFD=0  0  0  0  0  1  0  1  1  1  0  0  1  1  1  1                  \long format\
Signal=0  0  1  0  1  0  0  0                                         \throughput 2 Mbps\
Information about MAC frame:
Type=0  1                    \data frame\
Type=0  1   ToDS=1 FromDS=1  \infrastructure mode, AP as wireless bridge\
MoreFrag=1                   \received frame is a part of larger message\
Retry=0                      \no retransmission\
PwrMgmt=0                    \tranceiver will be active after that transmission\
MoreData=0                   \in AP no more buffered frames for this receiver\
WEP=1                        \WEP encryption algorithm is on\
receiver address:                      60E2539F7E6E
tranceiver address(BSSID):             F70200E653C5
physical destination address:          35A12DF0908E
physical source address:               49BB084C2F35
```

Fig. 9. Results from decoding procedure

## 6. Efficiency of the proposed method

To verify robustness of the proposed method against noise, a complex white Gaussian noise was added to the recorded signal. A number of tests were carried out for various values SNR. As a merit of demodulation quality a whole frame bit error rate (BER) was assumed. The measurement of BER was made according to the scheme presented on Fig. 10.

Recorded signal after demodulation and descrambling was used as the source of data (reference signal). Complex white Gaussian noise was added to recorded signal for SNR values -12, -11, -10 … 9 dB. Then for all values of SNR operations of despreading, demodulation and descrambling were performed. The number of bits used in tests was 19792 that correspond to 3 frames of signal. Results BER for various values of signal to noise ratio are shown on Fig. 11. The theoretical curve for the DQPSK system is marked additionally. It can be seen that despreading process gives processing gain about 10 dB.



Data source
AWGN
Receiver
Errors detection and counting
$BER = \frac{number\_of\_errors}{number\_of\_bits}$

Fig. 10. Scheme of BER measurement set

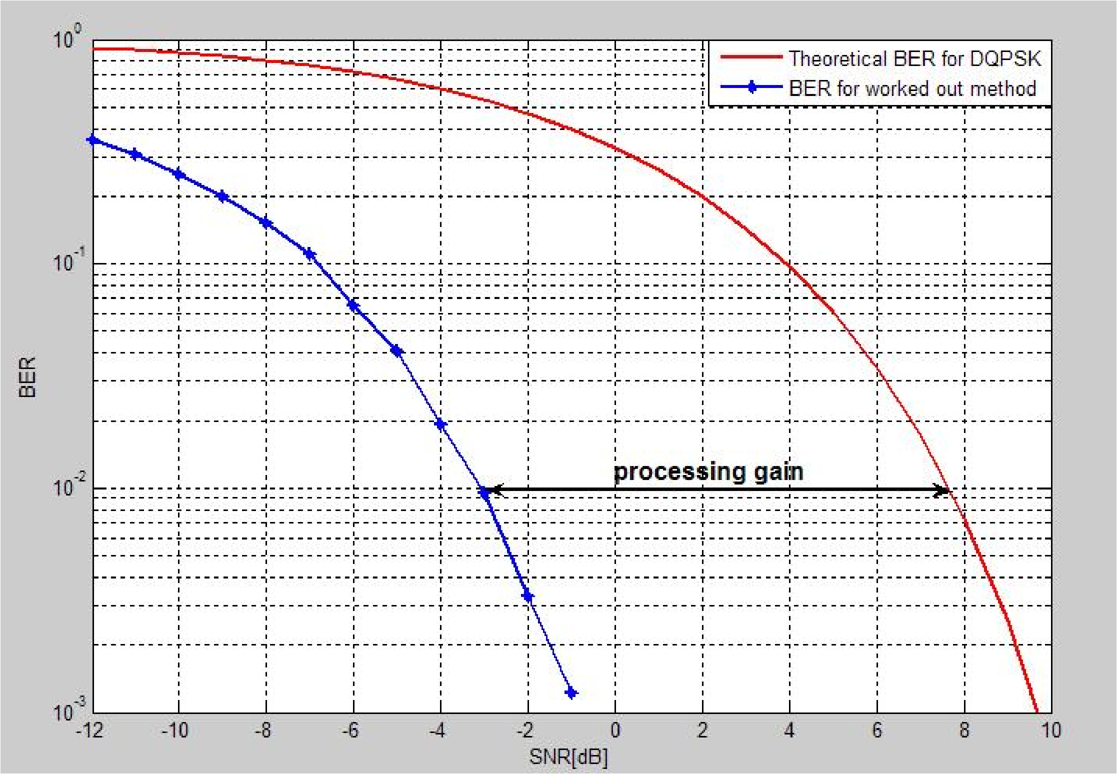


Fig. 11. Processing gain between worked out method and DQPSK system

Performed test also showed that correct descrambling and demodulation is possible for SNR ≥ -7 dB. For signals with such SNR it was possible to identify standard and specify throughput. For SNR ≥0 dB correct MAC frame decoding is also possible. The Fig. 12. shows result of analysis for SNR -6 dB.

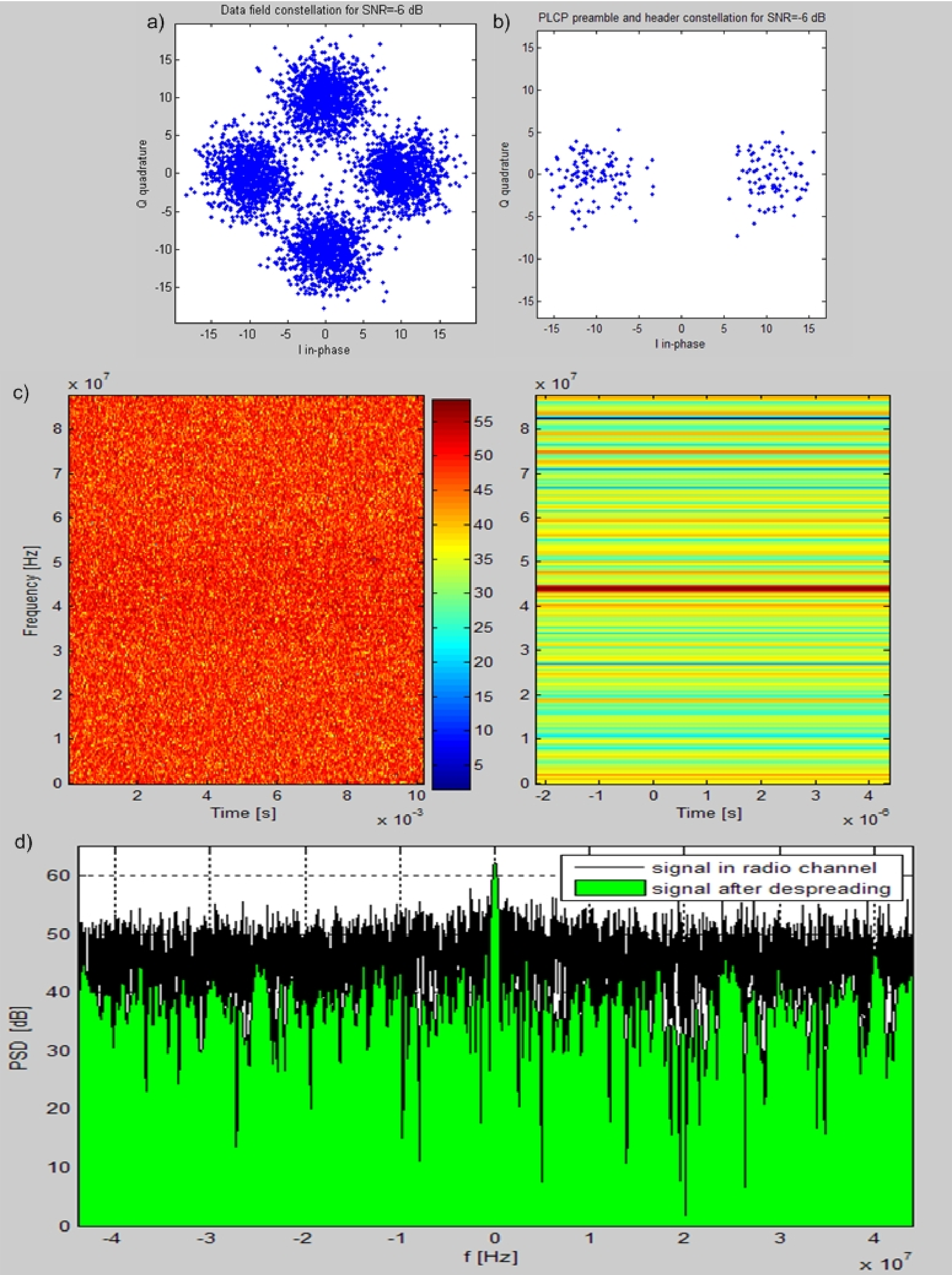


Fig. 12. 802.11b signal for SNR=-6 dB
a) constellation for data field,
b) constellation for header PLCP frame field,
c) spectrogram before and after despreading,
d) spectrum before and after despreading

## 7. Conclusions

Proposed methods enable estimation of the following signal parameters: carrier frequency and channel number, bandwidth of the signal, signal to noise ratio SNR, data rate, type of used modulation scheme, PLCP frame format and size of the added MAC frame (data size).
It allows WLAN standard identification.
The procedures may be used for „off-line" monitoring of wireless local area networks. They also make possible qualification if the transmitted frame is data, management or control frame and which unit of network sent it. It is also possible to get information about the network operation: mode of work, number of stations, number of available networks on the given area, network identifier (BSSID), destination and source addresses of transmitted frames and used of encryption WEP algorithm.

Proposed methods can be also used to design device working in a real time, enabling the analysis of WLAN in the „on-line" mode.

## References

1. Ch. Olgaard, *Using advanced signal analysis to identify sources of WLAN transmitter degradations,* LitePoint Corporation
2. J. Lopatka, *Effective methods of identification and demodulation of the selected radio communication signals,* Warsaw: Military University of Technology, 2006
3. P. Skokowski, *The technical analysis of the wireless local area network's signals,* Warsaw: Military University of Technology, 2007
4. *RF Testing of WLAN Products*, Application Note 1380-1, Agilent Technologies
5. *Spectrum Analyzer R 3681 from Advantest with the WLAN modulation analysis module,* News from Rohde & Schwarz Number 180 (2003 / IV)
6. T. Rappaport, *Wireless Communications, Principles and Practices,* Prentice Hall
7. *Testing and Troubleshooting Digital RF Communications Receiver Designs*, Application Note 1314, Agilent Technologies
8. *Using Error Vector Magnitude Measurements to Analyze and Troubleshoot Vector-Modulated Signals*, Product Note 138-1, Agilent Technologies