Probability of OFDM Signal Interception in eHealth Applications

Valerică Bîndar[1], Mircea Popescu[1], Valentin Grecu[1], Răzvan Crăciunescu[2], and Simona Halunga[2(✉)]

[1] The Special Telecommunications Service, Bucharest, Romania
mpopescu@sts.ro
[2] University Politehnica of Bucharest, Bucharest, Romania
shalunga@elcom.pub.ro

Abstract. The main purpose of the research conducted in this field is to improve senior's Quality of Life using remote monitoring systems. One of the main problems of these remote systems is the sensitive personal/medical data security. As in different field of e-Health, like telemedicine, where a high data rate is requested, OFDM systems represent a suitable candidate for these areas. This paper focus is to analyze the probability of intercept (POI) for OFDM (Orthogonal Frequency Division Multiplexing) communication systems. A number of measurements are performed using a WiMAX communication signal. The measurements were conducted using two broadband spectrum analyzers and the conclusions are that the POI, for these systems, is proportional with the number of parallel receiver channels and the scanning speed of the receivers.

Keywords: Interception · Wimax · e-Health · Telemedicine · OFDM

1 Introduction. Security Issues in E-Health

The ICT domain, especially the wireless communications applications offers new possibilities for elderly people to be monitored without intruding in their day to day activities. The increase of the possible data rates that are to be transmitted over the network allows the caregivers to communicate and to address the medical/social issues in real-time. But one of the most important aspects of remote monitoring using wireless communications is the data security.

Depending on the diseases concerned and on their level, the elders may choose to store and exchange with the caregiver a lot of personal data (health information, personal preferences and habits), that may be accessible through a wireless communication network. Consequently, depending on the data transmitted through the wireless network, different levels of security need to be provided. A radio communications link can be considered to be secure if a number of technical measures have been implemented in order to minimize the probability of detection and interception probability. In the last decade, a large number of researches have been developed and their results have been published, presenting different solutions that, on the one hand, secure the radio communication link, and on the other hand, defines the threshold parameters

V. Atanasovski, L.-G. Alberto (Eds.): Fabulous 2015, LNICST 159, pp. 83–90, 2015.
DOI: 10.1007/978-3-319-27072-2_11

for interception receivers. In [1] the authors refers to eHealth video communications that needs to be responsive and reliable, OFDM techniques offer, at the physical layer a scalable, resilient and reliable transmission technique. In [2] the authors study the most suitable wireless technologies for eHealth applications, from WiMAX (Worldwide Interoperability for Microwave Access) to GSM/GPRS to the latest 4G networks, while in [3, 4] the authors try to evaluate the most efficient solution for implementing a reliable health service based on the 4G networks. In [5] a special emphasis is put on the security of eHealth wireless networks based on OFDM techniques. In [6] is shown that OFDMA allows a large number of users share the system by assigning each of them a subset of subcarriers or tones, while in [7] the subcarrier allocation in OFDMA is studied. In [8] a number of considerations are made regarding a CDMA-OFDMA system and its performances obtained in different propagation conditions. Researchers are continuously seeking for the best trade-off between functionality, interoperability and security of the developed systems [9].

This paper presents the interception probability for systems that uses OFDM techniques. These threats are important especially for systems that are dealing with sensitive personal or medical data. The paper is organized as follows. In Sect. 2 is evaluated the probability of interception of a WiMAX OFDM signal with a search receiver that has a number of parallel receivers that performs several scans of the received signal while in Sect. 3 are presented some practical measurements. Finally, Sect. 4 presents the eWall project as a possible implementation of such an eHealth system that uses WiMAX OFDM and a number of conclusions are highlighted.

2 Probability of Intercept for OFDM Signals

In order to intercept and detect OFDM signals the first we assume that the bandwidth of the WiMAX radio channel and the OFDMA subcarrier spacing are known. The “search” receiver has the same instantaneous bandwidth as the signal and includes a number of parallel receiver channels (denoted by M_{sc}) whose center frequency coincides with the subcarriers frequency (denoted by M_{fh}). Moreover, in order to detect an OFDMA signal its frame duration, T_s, must be larger than the receiver dwell time, T_d.

Detection of wideband signals requires a large amount of power, at least for the integration period of the receiver, T_i,(which is the sum of dwell time and the signal processing time). In addition, it and requires that the frequencies the receiver is tuned on are the subcarriers of the received signal. Assuming that at the receiver is implemented using K parallel detectors, each of them tuned on a different frequency, the probability that the wideband signal is detected in one of the K channels increases by a factor K. Thus, according to [10], the interception probability for an OFDMA signal, using a multichannel receiver in standby, is

$$P_1 = \frac{K}{M_{fh}}. \tag{1}$$

Next we assume that the receiver can perform several attempts to intercept the transmitted signal, during one frame duration T_s. Such an attempt can be considered valid only when the integration time, T_i, is less or equal then the OFDMA frame duration T_s. Therefore, the average number of valid interception attempts during T_s is given by [11]

$$\bar{n} = \frac{T_s - T_i}{T_d}. \tag{2}$$

The interception probability of wideband transmitted signals with $\bar{n}$ valid trials, during the time signal T_s, is [10]

$$P_{1n} = P_1 \cdot \bar{n} = \frac{K \cdot \bar{n}}{M_{fh}} = \frac{K}{M_{fh}}\left(\frac{T_s - T_i}{T_d}\right). \tag{3}$$

For OFDMA signals, if the total time of reception is T_t, such interception attempts can be repeated $N = T_t \cdot f_S$ times, where f_S is the frame rate. For each attempt, the interception probability is given by (3). Assuming that the receiver performs L complete scans, the probability that, in N repeated trials, we will have k correct interceptions (hits), with P success probability in each trials, is determined based on the binomial distribution and cumulative distribution function, given by [10]

$$P_N(k) \approx 1 - \sum_{l=0}^{k-1} C_N^k P^l (1-P)^{N-l} \tag{4}$$

resulting an average number of hits

$$\bar{k} = N \cdot P_N. \tag{5}$$

The relationship between the number of repeated attempts to intercept (N), the dwell time (T_d), the number of complete scans at the receiver (L), the number of reception channels (M_{sc}) the number of parallel filters (K) and frame rate (f_s) is given by [11]

$$N = \frac{M_{sc} T_d f_s L}{K} \tag{6}$$

3 Practical Estimation of OFDMA Signals Probability of Intercept

In the following we will analyze the probability of interception for WiMAX 802.16e transmissions using OFDMA signals. The following parameters are used for the transmitted signal: central frequency = 3660.5 MHz, bandwidth BW = 10 MHz, FFT size = 512, number of used carriers = 426, subcarrier spacing = 11.16 kHz, OFDMA symbol time = 100.8 µs, frame length T_s = 5 ms (for 49 symbols). A received signal containing a multiburst PUSC (partial usage of subchannels), FUSC (full usage of subchannels) zone with BPSK pilots and signals with QPSK, 16QAM, and 64QAM modulation types has been used for test purposes.

Regarding the receiver part we consider two different spectrum analyzers, with incorporated Vector Signal Analyzer, namely Agilent E3238 s system with Agilent 89600 system software and Anritsu MS2722 system. The receivers parameters are: instantaneous bandwidth = 36 MHz (for Agilent) /10 MHz (for Anritsu), dwell time = 1 ms (for Agilent) /3 ms (for Anritsu), frequency span = signal bandwidth × 1.1, center frequency = 3660.5 MHz, RBW = 1 kHz, triggering on the signal (to obtain good spectrum and time measurements on a burst signal), demodulator selected = 802.16e OFDMA -10 MHz, parallel channels $K = 32$ channels (for Agilent) /20 channels (for Anritsu), with IFBW = 10 kHz.

With (1) the detection probabilities for a single burst using a multichannel receiver are $P_1 = 6.2$ % for Agilent and $P_1 = 4$ % for Anritsu. According to (2) and (3) the detection probabilities of wideband transmitted signals, with $\bar{n} = 4$ for Agilent and $\bar{n} = 2$ for Anritsu, the probabilities of valid trials are $P_{1n} = 24.8$ % for Agilent and $P_{1n} = 8$ % for Anritsu. Assuming that the receiver performs a number $L = 1$ full scans and, according to (6), the number N of repeated attempts to intercept during L scans is $N = 132$. Then, the probability P_N of at k successes in N trials, where success probability in each trialis P_{1n}, can beestimated using (4).

In Fig. 1a is represented the probability P_N of at least k valid interception in N repeated attempts, for an ideal case using $K = 426$ parallel channels, with a variable mean number $\bar{n} = \{2; 4\}$ of valid attempts during one hop. The blue line (1) represents this probability achieved when the Agilent spectrum analyzer is used, while the red line (2) corresponds to the same probability when the Anritsu one is used, under the same conditions. Note that the probability of at least $k = 10$ valid interceptions in $N = 132$ attempts for the Anritsu analyzer is about 50 % while for the Agilent one is 100 %. This difference is due to the fact that the Agilent analyzer has a lower dwell time than the Anritsu analyzer and, implicitly, Agilent scanning speed is higher.

Figure 1b represents, the probability of at least k valid interception in N attempts, P_N, given in (4), with success probability in each trialis P_1, supposing only one valid detection attempt per hop interval, $\bar{n} = 1$, for receivers with different number of scanning filters, K. In the following, since the Agilent spectrum analyzer performs better than the Anritsu one, the first one will be used with different number of scanning filters, K, that may be enabled at the receiver. The blue line (3) represents probability P_N of at least k valid interception in $N = 132$ attempts when the central frequencies of the parallel receiver channels K, coincides with all the subcarriers of the WiMAX radio channel. In this case, the analyzer scans 512 consecutive subcarriers and uses $K = 32$ parallel channels. The red line (2) represents the interception probability of the WiMAX signal, with at least k valid interception in $N = 132$ attempts, when the spectrum analyzer scans consecutive WiMAX subcarriers. In this situation the interception receiver is using $K = 20$ parallel channels. Finally, the green line (1) represents the probability of achieving at least k valid interception in N attempts, for WiMAX signal, when the spectrum analyzer consecutively scans only one detection channel ($K = 1$). If we compare the performances obtained in the three cases above, one can see that for $k = 10$ valid interception performed by the intercept receiver, we obtainprobability $P_N = 20.4$ % when $K = 32$ parallel channels are used (similar to Agilent

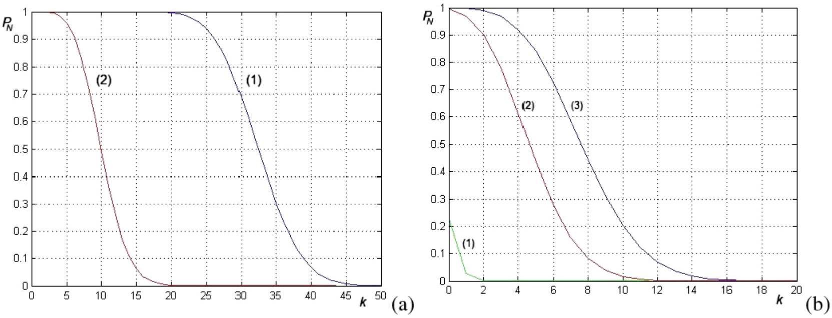

Fig. 1. **(a).** The probability P_N of at least k valid interception in N repeated attempts, with mean number of valid attempts by the receiver during one hop $\bar{n}$ = 4 (trace 1) and $\bar{n}$ = 2 (trace 2), for a ideal case using K = 426 parallel channels and **(b)** using using K = 32 parallel channels (trace 3), K = 20 parallel channels (trace 2) and single channel receiver (trace 1) (Color figure onlne)

spectrum analyzer), P_N = 1.8 % when K = 20 parallel channels are used (similar to Anritsu spectrum analyzer) and P_N = 0 % when only one scanning channel is used. Hence, as the receiver has more parallel channels enabled, the interception probability of the OFDMA signal is higher.

To show the accordance between analytical expression for the interception probability and the experimental results, we conducted tests to detect a real WiMAX transmission using a spectrum analyzer Agilent E3238 s including Vector Signal Analyzer Agilent 89600. The test signal was an IEEE 802.16e-compliant downlink subframe, based on a WiMAX 10 MHz profile. It contains a PUSC zone of 12 symbols followed by a FUSC zone of 10 symbols, with BPSK pilots and signals with QPSK, 16QAM, and 64QAM modulationtypes. The spectrum analyzer settings for test were: central frequency f = 3660.5 MHz, span 11 MHz, resolution bandwidth 3 kHz, reference level −15 dBm, 32 parallel receiver channels, detector Peak, demodulation type = IEEE 802.16e OFDMA. Sweep time and trigger delay must be set so that the complete response signal of the tag is recorded. Displaying graphs station was to stop after 10 detections.

The measurement system receives the WiMAX signal represented in Fig. 2. In the top windows are displayed: the spectrum of the signal (a), time measurements on a burst signal (b) and table with the contents of the decoded FCH (Frame Control Header) and DL-MAP (c). In this table one can see that the spectrum analyzer with settings mentioned above, was performed detection and decoding of WiMAX signal. In the bottom windows are displayed: Probability Density Function - PDF for the received signal (d), Cumulative Distribution Function - CDF (e) and Complementary Cumulative Distribution Function - CCDF (f). From the PDF trace it can be deduced that the mean value of burst signal is 27.8 mV_{rms}, while using CDF trace, on can determine the probability corresponding to this average value of signal, resulting 47.9 %. In CCDF measurement the average power of the signal is −18.12 dBm and it can be seen that all signal's peaks with this level have probability of occurrence around 21 %. This probability of detection is very close to the theoretical value P_N = 20.4 %, obtained from simulations (Fig. 1b).

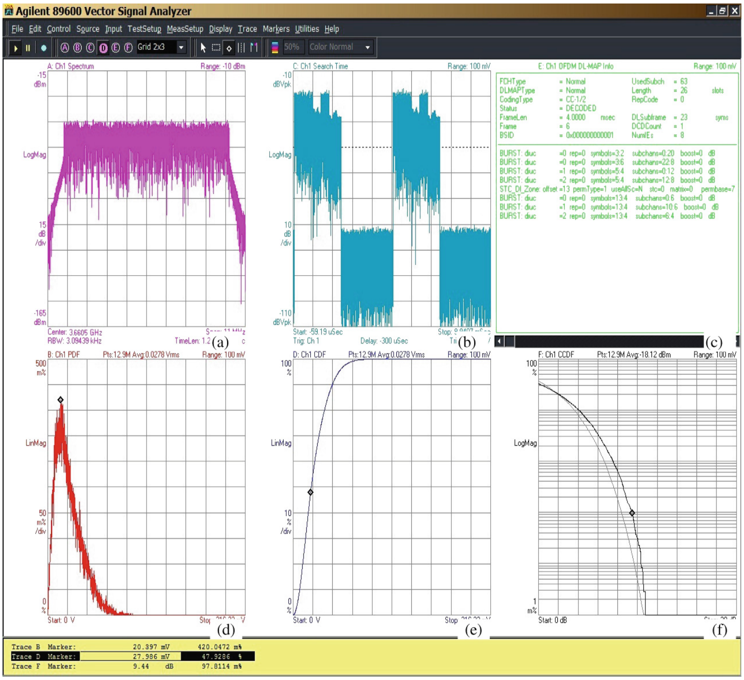

Fig. 2. Measurements of WiMAX signal in the frequency domain (a), in the time domain (b), burst analysis with DL-MAP (c) PDF (d), CDF (e) and CCDF (f) measurements of burst signal

From those results one can see that the interception probability of an OFDMA system is relatively high only if the interceptor has a relatively sophisticated dedicated measurement device. Such equipment should be multichannel receiverand with fastscan, which are characteristics that are difficult to obtain from a technical point of view. In this respect, WiMAX OFDMA proves to be a good candidate for implementing the physical layer in an eHealth system.

4 Possible Applications – the EWALL Project

The eWall for Active Long Living (eWALL) it's a project that intends to develop an architecture and appropriate methods for assisting the elderly that have health issues as Chronic Obstructive Pulmonary Disease or Mild dementia. As the quality of life has improved, the life expectancy also increased during the last years, fact that leads to an aging of the population [15]. It is well known that elderly people need special treatment and resources due to their decreasing capacity of self-caring. Thus, a high number of caregiver staff is trained for the challenge of assuring the suitable conditions, medicine, laboratory tests and - not less important – daily supervision.

Thus, in order for the Sensing environment to communicate to the eWALL cloud a secure wireless or wired solution is required. In order to find the best solution multiple tests are being performed in order to determine the system with the best intercept-free percentage. As we demonstrated in Sect. 3, OFDMA with a large number of subcarriers proved to be a suitable solution for the eWALL system, and is now under testing. Measurements have shown that the signal can be intercepted with a high probability only by using sophisticated and expensive measurement devices, while for single channel receiver the interception probability is null, showing that, from security and privacy point of view, this technique offers increased data security. Based on those remarks the OFDMA technique is used in eWALLproject to communicate between the sensing environment and the cloud.

Acknowledgment. This work has been funded by European Commission by FP7 IP project no. 610658/2013 "eWALL for Active Long Living - eWALL" and the SfP-984409 ORCA project and by the SOPHRD Sectorial Operational Programme Human Resources Development 2007–2013 of the Ministry of European Funds through the Financial Agreement POSDRU/159/1.5/S/132397.

References

1. Panayides, A.S., Antoniou, Z.C., Constantinides, A.G.: An overview of mHealth medical video communication systems. In: Adibi, S. (ed.) Mobile Health. SSBN, vol. 5, pp. 609–634. Springer, Heidelberg (2015)
2. Keikhosrokiani, P., Zakaria, N., Mustaffa, N., Wan, T.-C., Sarwar, M.I., Azimi, K.: Wireless networks in mobile healthcare. In: Adibi, S. (ed.) Mobile Health. SSBN, vol. 5, pp. 687–726. Springer, Heidelberg (2015)
3. M., S.M., A., L.A., S., G.A.: Quality of service in wireless technologies for mHealth service providing. In: Adibi, S. (ed.) Mobile Health. SSBN, vol. 5, pp. 971–990. Springer, Heidelberg (2015)
4. Park, R.C., Hoill Jung, J., Shin, D., Cho, Y.H., Lee, K.D.: Telemedicine health service using LTE-Advanced relay antenna. Pers. Ubiquit. Comput. **18**(6), 1325–1335 (2014)
5. Song, J., Ding, W., Yang, F., Yang, H., Wang, J., Wang, X., Zhang, X.: Indoor hospital communication systems: An integrated solution based on power line and visible light communication. In: Faible Tension FaibleConsommation (FTFC), 2014 IEEE, pp. 1–6. IEEE (2014)
6. Craciunescu, R., Halunga, S., Fratu, O., Vizireanu, N.: Multi User Orthogonal Frequency division Multiple Access (MU-OFDMA) performances in AWGN and fading channels. In: 11th International Conference on Telecommunication in Modern Satellite, Cable and Broadcasting Services (TELSIKS), Nis, Serbia, vol. 01, pp. 229–232, 16–19 October 2013
7. Manea, C., Craciunescu, R., Halunga, S., Voicu, C., Preda, R.: Performance evaluation of subcarrier allocation methods for OFDMA. In: Proceedings of 21st Telecommunications Forum (TELFOR), Belgrade, Serbia, pp. 260–263, 26–28 November 2013
8. Craciunescu, R., Manea, O., Halunga, S., Fratu, O., Vizireanu, D.N.: Considerations on CDMA–OFDM system performances in different channel environments for different modulation and coding scenarios. Wireless Pers. Commun. J. **78**(3), 1667–1682 (2014)
9. Raychaudhuri, K., Pradeep, R.: Privacy challenges in the use of eHealth systems for public health management. Emerg. Commun. Technol. E-Health Med. **1**, 155 (2012)

10. Papoulis, Probability, Random Variables and Stochastic Processes. McGraw-Hill, Chap. 3, 1965
11. Wout, J., Martens, L.: Performance evaluation of broadband fixed wireless system based on IEEE 802.16. In: Wireless Communications and Networking Conference, 2006. WCNC 2006. IEEE, vol. 2, pp. 978–983. IEEE (2006)
12. eWALL Project Homepage, http://ewallproject.eu/ (accessed in March 2015)