Compromising Radiated Emission from a Power Line Communication Cable

Virginie Degardin, Pierre Laly, Martine Lienard, and Pierre Degauque

Abstract: **This contribution presents a preliminary investigation on the possibility of eavesdropping, i.e., of extracting information by exploiting the electromagnetic field radiated in the vicinity of a power line communication (PLC) network. This kind of problem is usually known in the electromagnetic compatibility area under the codename TEMPEST. Electromagnetic field measurements were carried out in a laboratory environment, both inside and outside a building, and the main statistical characteristics of the compromising channel are presented. A software tool simulating a PLC communication has been developed and used to draw a preliminary conclusion on whether the radiated emissions can be exploited or not.**

Index terms**: Power line communication, TEMPEST, Transmission line, Interference**

I. INTRODUCTION

Power Line Communication (PLC) is now a growing technology usually applied for in-house high bit rate communication. For most of the commercial systems, the transmitting frequency band extends up to 40 MHz. To ensure the Electromagnetic Compatibility (EMC) of such a system with its environment, the electromagnetic (EM) field radiated by the PLC network must remain below prescribed limits. Standardization aspects dealing with the maximum level of the transmit power spectral density (PSD) are thus under development.

When the transmitting (Tx)/receiving (Rx) modem is connected between two wires, the excitation is usually called a differential mode (DM) excitation. Since the main source of radiated emission is the common mode (CM) current flowing on the lines, extensive analyses have been made on the DM to CM current conversion mechanism and radiation phenomena. Results on these two aspects are described, for example, in [1] – [5]. The emission levels of existing PLC systems are compared to EMC standards in [6] – [10], while aspects dealing with crosstalk and conducted interference or radiated interference between systems are studied in [11] – [12]. Lastly, some in-situ measurements in various rooms of the radiated emission of an indoor network are presented in [13], a numerical modelling of a typical wiring configuration being investigated in [14]. It must be also outlined that notching is a useful technique to avoid interference with existing services [15].

However, even if the level of the radiated emissions remains low, e.g. if the PLC system fulfils the EMC requirements, the question of confidentiality may still arise. Indeed, if a PLC link is established within a building, one can wonder if the EM field radiated in the vicinity of the network can be used to decode with success the transmission or at least to extract some information from the measured signal.

It is thus important to quantify this risk and to know if PLC links must be avoided in certain cases for security reasons. As an example, let us consider an in-house PLC. To reach a certain degree of confidentiality, one can put filters to strongly decrease conducted emissions outside the area to be covered. Nevertheless, the radiation of the PLC lines may be detected by putting a loop antenna in adjacent room/houses. This problem of eavesdropping is very broad and the results will strongly depend on many parameters as the network architecture, the structure of the building and the relative position of the receiving antenna. Nevertheless, to have an idea of the possibility of signal detection, we consider in this paper a PLC link between two terminals situated in a room, the additional receiving sensor being a loop antenna placed in nearby rooms or outside the building.

This paper is organized as follows: Section II describes the configuration and the principle of the measurements. Section III details the statistical analysis of the field distribution radiated by the PLC line. Furthermore, the time domain channel characteristics of the wireless compromising channel are also given. Section IV first presents ambient noise measurement. By introducing noise and channel characteristics in a simulation tool, the bit error rate (BER) when demodulating the signal received by the loop is calculated. In this study, we do not consider the way of recovering information or part of it, using more advanced techniques as blind deconvolution techniques.

II. PRINCIPLES OF THE MEASUREMENTS

In addition to the actual power distribution network, a 3-wire power line was successively installed in two rooms situated at the first floor of a building at the University of Lille. The 3 wires were put in a cylindrical plastic tube as usual for in-house power network, at least in France. The relative position of these wires within the tube randomly varies with distance. One can expect that this will lead to a rather high DM to CM mode conversion, which thus

Manuscript received January 11, 2011, revised March 23, 2011.

The material in this paper was presented in part at the 18th International Conference on Software, Telecommunications and Computer Networks (SoftCOM 2010) Split-Bol, Croatia, Sept. 2010.

Authors are with the University of Lille, IEMN/TELICE, Villeneuve d'Ascq, France (email:{virginie.degardin, pierre.laly, martine.lienard, pierre.degauque}@univ-lille1.fr).

corresponds to a favourable configuration for detecting the EM field radiated by this structure. The 3 wires, namely phase, neutral and ground, are connected to the mains of the building.

In a preliminary step, this 3-wire PLC line was implemented in a room, called REU, situated at the extremity of the building, against a reinforced concrete wall. This configuration will allow comparing the electromagnetic field amplitude inside the building and outside the building at a distance of 1 m from the wall.

The PLC line was then installed in the so-called "room PLT" situated in the middle of the building. It is separated from room 118 by a reinforced concrete wall, from room 122 by a plaster wall and from the others by a corridor [16] - [18], as shown in Fig. 1.

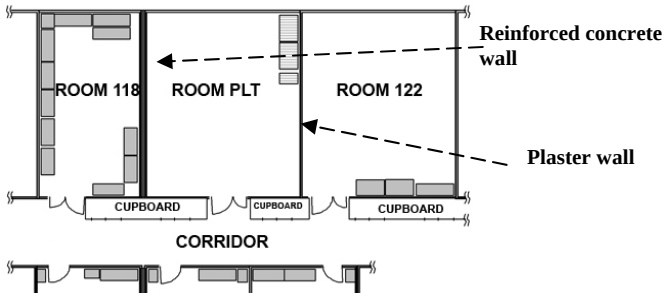

Fig. 1. Configuration of the rooms.

It must be emphasized that the building is powered by a three-phase cable but each room is fed by a single-phase current. Due to the architecture of the power network, the single-phase cable connected to the room PLT is not the same as for the other rooms presented in Fig. 1. This means that the high frequency PLC current injected on the wires in the room PLT will be strongly attenuated in the other rooms and this has been checked experimentally. As a first approximation, one can thus assume that the radiated field in the various rooms is due to the current flowing on the 3-wire line in the room PLT.

The configuration of the room PLT is given in Fig. 2. Various electrical items can be connected to the plugs of the additional power line. The complex channel transfer function was measured with a vector network analyzer (VNA) in a frequency range extending from 1 MHz up to 40 MHz. This transfer function corresponds to the S_{21} scattering parameter. The injection is made at point 1 (Fig. 2) between two wires owing to a capacitive coupler.

In the following, two transfer functions will be considered. The first one is the conventional PLC transfer function between two points on the line, numbered 1 and 6 in Fig. 2. The second one deals with the compromising channel or "wireless channel", i.e., for an injection at point 1 but a reception on a magnetic loop. This loop, having a diameter of 30 cm, can be placed either in the room PLT, as in Fig. 2, or in nearby rooms or outside the building.

It is important to emphasize that all results dealing with the received power on the loop antenna depend on the geometrical characteristics of this loop. This is the reason why, in the EMC approach, the antenna factor is taken into account, results being often presented in terms of magnetic field or equivalent electric field by introducing a wave impedance of 377 Ohms.

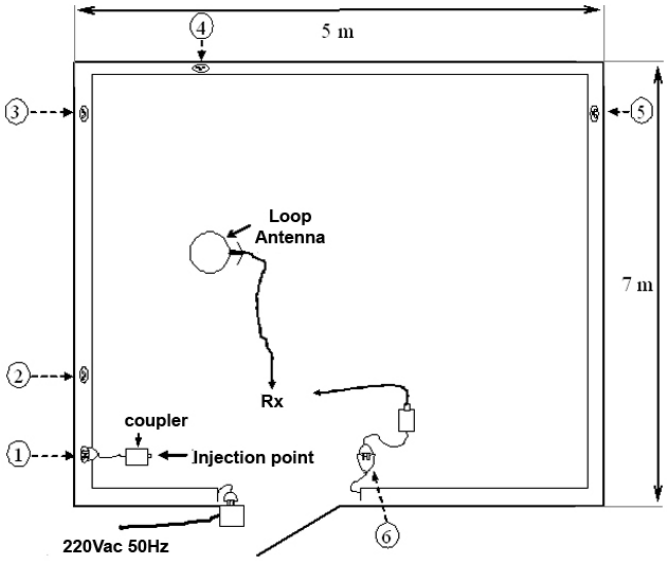

Fig. 2. Experimental set-up in the room PLT.

This approach is not needed in our application since the performances of the wireless channel, i.e., the possibility of detection, only depend on the signal to noise ratio and the antenna is the same both for signal and ambient noise.

III. Transfer Functions of the Wireless Channel

A. Current distribution and influence of the loads

First, it is interesting to know the influence of the loads connected to the power line at different points (2 to 5 in Fig. 2), on the CM current and thus on the radiated field. Curves in Fig. 3 show the variation of the CM current amplitude, expressed in dBA, versus frequency, if either no load is connected to the line or if 2 or 4 appliances are plugged. The input DM voltage is 1 V and the current probe was situated at mid-distance between the injection point 1 and the end of the line at point 6. Contrary to the case of the differential mode current which is strongly dependent on the load configuration, we see in Fig. 3 that the average variation of the CM current is not very sensitive to the loads.

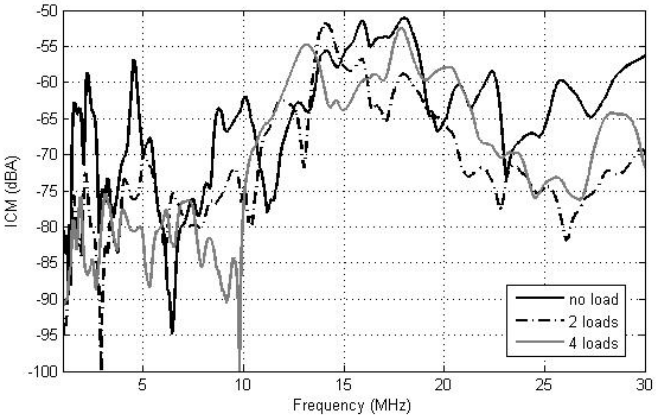

Fig. 3. Common mode current amplitude depending on the loads connected to the PLC line.

B. Field distribution in the various rooms

The loop antenna was moved in the various rooms and a map of the received power at 22 MHz is given in Fig. 4 for a 2-load configuration. The axis of the loop was always vertical since, statistically, this polarization corresponds to the maximum received power. The transmit (Tx) power on the PLC line being normalized to 0 dBm, the absolute value of the received (Rx) power corresponds to the path loss of the wireless channel.

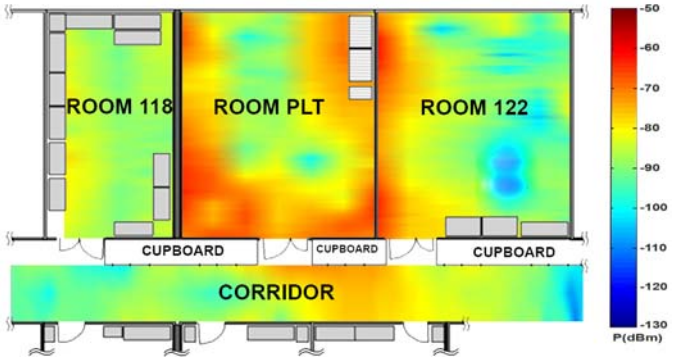

Fig. 4. The color scale gives the received power (P), expressed in dBm, at a frequency of 22 MHz and for a transmit power of 0 dBm.

This qualitative representation allows pointing out that the received power near the wall is nearly the same in rooms 122 and PLT, these two rooms being separated by a plaster wall. On the contrary, in presence of a reinforced concrete wall, the attenuation is rather important, as it appears between rooms 118 and PLT. It is also interesting to plot the received power versus frequency, at successive points within the same room. The curves in Fig. 5 were obtained from measurements at 8 locations situated in room 118 and at 1 m from the concrete wall. The increase in power with frequency is due partly to the increase of the radiated field, and partly to the response of the loop antenna. The average attenuation between the Tx power and the Rx power is about 70 - 90 dB for frequencies greater than 15 MHz, thus much higher than the path loss of a usual wire PLC communication, which is of the order of 20 - 40 dB, depending on the network architecture and the number of appliances connected to the mains. Such a path loss for the compromising channel may appear prohibitive but it will be partly compensated by a decrease of the noise power spectral density (PSD), as it will be outlined in Section IV.

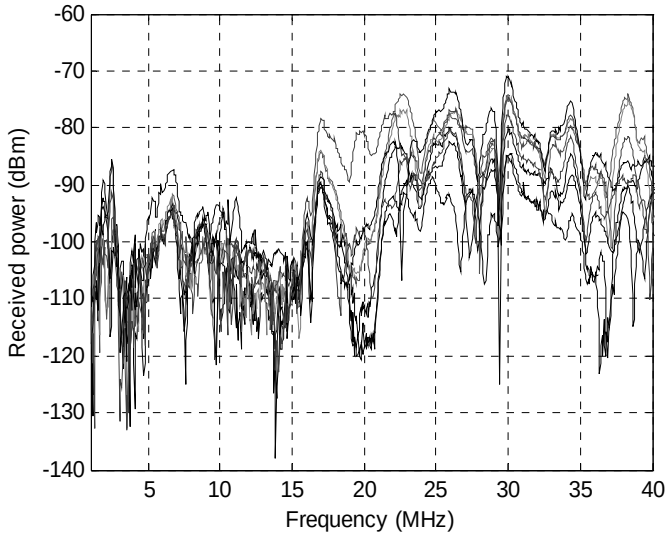

Fig. 5. Received power versus frequency at different locations in room 118, i.e., behind a reinforced concrete wall.

To determine the average attenuation due to a wall situated between the PLC network and the Rx loop antenna, it is not possible to compare the values of the Rx power at few points due to the large dispersion of these values. A statistical approach has thus been done [16], [17] and the distributions of the Rx power are presented in Fig. 6.

Each curve in Fig. 6 has been obtained from measurements at 1200 frequency points between 1 and 40 MHz, and for 8 to 10 location points inside each room or outside the building. In all cases, the distance between the loop antenna and the dividing wall along which the PLC line is installed, is 1 m.

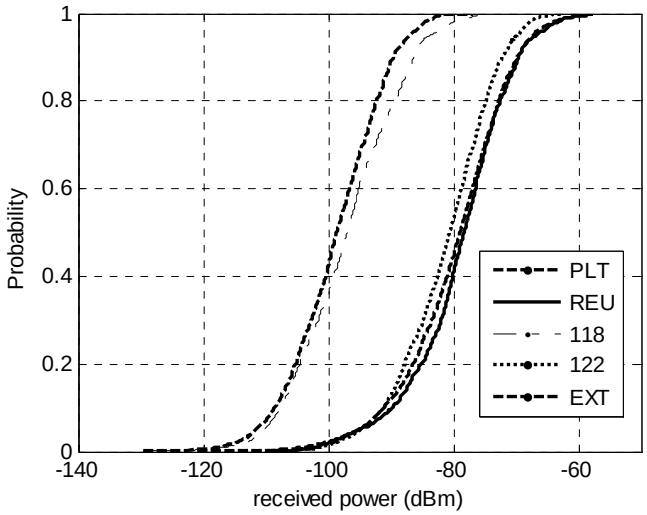

Fig. 6. Complementary cumulative distribution function of the received power in various rooms at 1 m from the PLC line.

Rooms PLT, 118 and 122 have already been defined in Fig. 1. Room REU, as mentioned in Section II, is also a room where the PLC 3-wire line was implemented but this room is situated at the end of the building. Lastly the curve “EXT” deals with measurements made outside the building.

As it can be expected, the Rx power in the 2 rooms PLT and REU are nearly identical, around – 80 dBm, considering a probability of 0.5. We also note that the attenuation due to the plaster wall (room 122) is negligible. Let us now consider the following case: the room in which the PLC transmission takes place is separated from the location of the loop antenna by a reinforced concrete wall. The comparison of curves PLT and 118 on one hand, and REU and EXT on the other hand, shows that the additional attenuation due to the concrete wall is 20 dB.

Lastly, impulse response and power delay profile of the compromising channel were deduced from measurements in the frequency domain through a Fourier transform. It appears that the delay spread of the wireless channel can reach 120 ns, instead of 40 ns for the usual wire channel. However, this value remains much smaller than the usual duration of the

Orthogonal Frequency Division Multiplexing (OFDM) guard interval inserted for eliminating inter-symbol interference in the PLC communication.

IV. Compromising Channel: Signal to Noise Ratio, Preliminary Experiments and Simulation of a PLC Link

A. Noise power spectral density

Ambient noise measurements have been carried out in various rooms of the building and for 3 orthogonal polarizations of the loop antenna, noted *x*, *y* and *z*. The *z* polarization corresponds to a loop whose axis is vertical. As an example, noise PSD in room 122 and measured in a 9.1 kHz bandwidth, as often mentioned in the EMC standards, is given in Fig. 7.

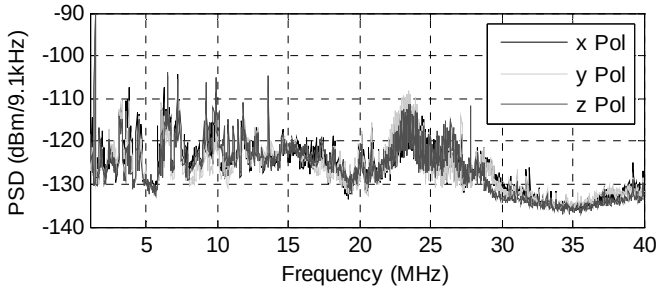

Fig. 7. Noise power spectral density for different antenna polarizations.

We note that, except narrow band interference due to broadcast transmitters, noise PSD is independent on the polarization of the receiving loop. One can estimate that the average PSD does not exceed or is on the order of -118 dBm in this 9.1 kHz band, i.e., – 158 dBm/Hz. This noise PSD value is about 20 dB lower than the conducted background noise usually measured on in-house power lines.

B. Preliminary experiments with commercial modems

Preliminary experiments were carried out with commercial modems (85 Mbits/s) and working in the 4-20.5 MHz band. The maximum value of the PSD of the injected signal, using the function “maxhold” of a spectrum analyzer, is given by the upper curve in Fig. 8. The resolution bandwidth is equal to 20 kHz, i.e., the spacing between two OFDM subcarriers. The lower curve shows the distortion of the signal received by the loop antenna in room 118 (See Fig. 1). Since it seems possible to be able to extract some information from this signal, a more extensive study based on a numerical simulation of an ODFM transmission has been carried out, the objective being to get quantitative values, as the bit error rate (BER), characterizing the wireless compromising channel.

C. Simulation of an OFDM link

For simulating the link, a software tool has thus been developed, the input data being the measured channel transfer functions. Among the various proposed PLC specifications as: HomePlugAV [19], OPERA [20], IEEE P1901 standard [21],

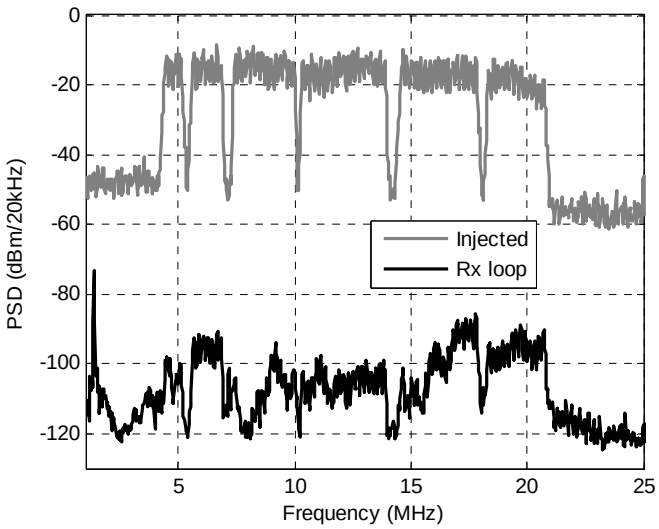

Fig. 8. PSD of the injected OFDM signal and of the signal received on a loop antenna behind a reinforced concrete wall (Room 118).

the OPERA specifications were chosen for our application. After a brief description of the main OPERA characteristics, the BER, which can be expected for the wireless link, is presented.

C.1 Summary of the OPERA specifications

In the OPERA specifications of the physical (PHY) layer, there are two separate bit streams, associated with data payload and delimiters, respectively [20], [22]. The transmission scheme for data payload is illustrated in Fig. 9.

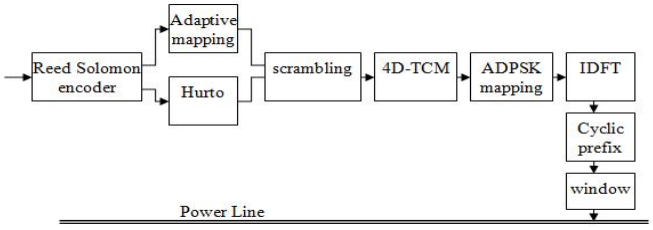

Fig. 9. OPERA transmission scheme, PHY layer for data payload

The data are first Reed Solomon encoded, the channel coding parameters depending on the forward error correction (FEC) redundancy, varying from 8 and 20 bytes. In case of low Signal to Noise Ratio (SNR) and of strongly frequency selective channels, the data stream is mapped through a HURTO (High performance ultra redundant transmission) block. Such a transmission will not be considered in our examples. In the other cases, an adaptive mapping is applied, the number of bits per subcarrier being related to the SNR in the frequency band and the data rate is up to about 200 Mbit/s.

After scrambling, the stream is encoded with a Four Dimensional Trellis Coded Modulation (4D–TCM) and mapped using an Adaptive Differential Phase Shift Keying (ADPSK) modulation. The differential phase encoding allows simplifying the Rx part by suppressing the phase channel equalization. A 2048 point – inverse discrete Fourier transform (IDFT) - is then applied and a 20 µs cyclic prefix is

added for generating the OFDM symbol of duration 71.2 μs. Finally, a raised cosine window is performed to limit the bandwidth. Among the 2048 sub carriers, equally spaced in a bandwidth either equal to 10, 20 or 30 MHz, only 1536 carriers are used for the transmission. The results presented in this paper were obtained by assuming a bandwidth of 30 MHz, called type 1 in OPERA specifications, the subcarrier spacing being equal to 19.5 kHz. Based on these specifications, the software tool was developed partly in C language and partly under Matlab [22].

C.2 Bit error rate of the compromising channel

In this preliminary study on the possibility of signal detection, a wire PLC communication is assumed to be established between plugs 1 and 6 (Fig. 2). The transmit PSD is – 50 dBm/Hz, the frequency band extends from 10 to 40 MHz and we set the useful throughput to 28 Mbits/s. The redundancy added to each OFDM symbol and introduced in the FEC previously mentioned is chosen equal to 20 bytes. An additional eavesdropper's receiver, supposed to be perfectly synchronized with the transmitter, is connected to the loop antenna placed in a nearby room.

In a first step we suppose, as in the OPERA specifications, that an adaptive bit loading is performed. The principle of this technique is that, from the knowledge of the wire channel characteristics, the transmitter optimizes the bit allocation to each subcarrier, according to a look-up table given in the OPERA specifications. The bit allocation thus strongly depends on the load configuration of the wire network. To see the role and the influence of this adaptive bit loading on the BER of the compromising channel, we have introduced in the software tool simulating the link, two different transfer functions measured between plugs 1 and 6. These transfer functions have been obtained when either 2 appliances or 4 appliances are connected to the power line on the different plugs noted 2 to 5 in Fig. 2.

In the second step, we assume that the bit allocation is uniform, i.e., is the same for all subcarriers. A Differential Quadrature Phase Shift Keying (DQPSK) modulation scheme was chosen, the bit rate being also set to 28 Mbits/s. In all cases, noise is supposed to be an additional white Gaussian noise (AWGN) whose PSD is equal to – 158 dBm/Hz, as indicated in Section IV.A. Interference due to broadcast emissions is not taken into account.

Curves in Fig. 10 give the BER for 8 successive positions of the receiving loop antenna in room 118, i.e., behind a reinforced concrete wall. This BER was obtained by also introducing in the software tool, the transfer functions of the compromising channel shown in Fig. 5. The 8 positions being quite arbitrary, they have been numbered in such a way that the BER continuously increases from locations 1 to 8.

The curve "DQPSK" corresponds to a uniform bit allocation. Curves 1 and 2 were obtained with an adaptive bit loading, when 2 loads or 4 loads are plugged on the PLC line, respectively. The worst performance of the signal extraction, occurring when the adaptive bit loading is applied, can be easily explained. Indeed, there is only a small probability that

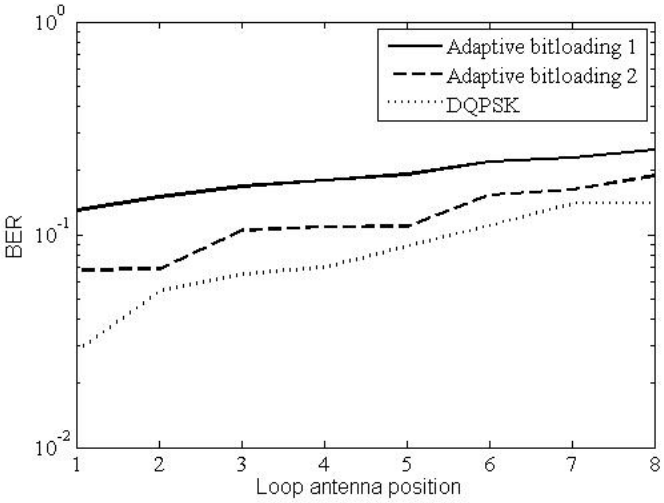

Fig. 10. Bit error rate assuming either an adaptive bit loading (curves 1 and 2) or a uniform DQPSK modulation scheme. The receiving loop antenna is situated behind a reinforced concrete wall.

either fading or a low attenuation of the wire channel occur in the same frequency band as for the wireless channel. The BER of the wireless channel is thus dependent on both channel characteristics. For example, in the case of a 2-load configuration (curve 1), the transfer function of the wire channel presenting a low attenuation between 11 and 19 MHz, the number of bit per subcarrier in this band is important. Unfortunately, a large part of this band is strongly attenuated in the wireless channel, as shown in Fig. 5.

Among the 8 positions of the loop antenna, the minimum value of the BER is on the order of 10^{-1}. If there is only a plaster wall between the PLC network and the loop antenna, other numerical simulations have shown that the BER of the wireless channel strongly decreases and can be as small as 10^{-4} when using the same adaptive bit loading as in the previous configuration.

It must be also mentioned that for such an eavesdropping application, an optimization of the position of the Rx loop and of its size would probably lead to better performances.

V. CONCLUSION

This study is a preliminary approach for characterizing the propagation channel associated with the radiation of a PLC network. The signal to noise ratio on the receiving loop being not prohibitive, at least in the tested configurations, the exploitation of radiated emissions to extract some information on the transmitted data based on advanced signal processing techniques seems possible. However, further works are needed, especially on exhaustive measurements of ambient noise and of path loss in various environments and on the optimization of the receiving sensor.

REFERENCES

[1] E. Marthe, F. Rachidi, M. Ianoz and P. Zweiacker: *Indoor radiated emission associated with power line communication systems*, in Proc. of IEEE Symp. on EMC, pp. 517 – 520, 2001

[2] A. K. M. Mahbub Ar Rashid, N. Kuwabara, M. Maki, and H. Yamane: *Evaluation of longitudinal conversion loss for indoor AC mains line*, in Proc. of IEEE Int. Symp. on EMC, vol. 2, pp. 771-776, Aug. 2003.

[3] Y. Watanabe and M. Tokuda: *Relation between balance-unbalance conversion factor and leaked electric field in power line with branch for PLC*, in Proc. of PIERS Conf., pp. 81-87, March 2006.

[4] Y. Minamitani, T. Okabe, and M. Wasaki: *Effect produced on electric leakage in PLC by indoor power line arrangements*, in Proc. of IEEE/ISPLC Conf., pp. 276-280, March 2003.

[5] C. Rodriguez- Morcillo, A. Rubinstein, M. Rubinstein, F. Rachidi, A. Vukicevic: *Experimental Verification of Common-Mode Current Generation in Home Electrical Wiring in the Powerline Communications Band*, in Proc. of IEEE/ISPLC Conf., March 29 – April 1, 2009.

[6] R. Vick: *Estimating the radiated emissions of domestic main wiring caused by power line communication systems*, in Proc. of Int. Symp. on EMC, Zurich, pp. 87-92, 2003.

[7] ETSI: *Powerline telecommunication; EMI review and statistical analysis*, Technical report, ETSI TR 102 259, Sept. 2003.

[8] B. Adebisi and B. Honary: *Comparisons of indoor PLC emissions measurement results and regulation standards*, in Proc. of IEEE/ISPLC Conf., pp. 319 – 324, 2006.

[9] Joong-Geun Rhee: *Korean rules and regulations on PLC*, in Proc. of IEEE/ISPLC Conf., April 2-4, 2008.

[10] E. Marthe, F. Rachidi and M. Ianoz: *Evaluation of indoor PLC radiation from conducted emission limits*, in Proc. of IEEE Int. Symp. on EMC, vol. 1, pp. 162-165, May 2003.

[11] H. Dalichau: *EMC aspects of inhome PLC: crosstalk between neighbouring apartments and increase of disturbance due to a large number of simultaneously transmitting PLC systems*, in Proc. of IEEE/ISPLC Conf., pp. 73-79, March 2002.

[12] M. Zhang and W. Lauber: *Evaluation of the interference potential of in-home PLC systems*, in Proc. of IEEE/ISPLC Conf., pp. 291-296, March 26-29, 2006.

[13] J. P. Rouzaud, F. Issa and E. Perrier de la Bathie: *Some in-situ measurements of the radiated emission in an indoor network*, in Proc. of IEEE/ISPLC Conf. Proc., pp. 79-87, March 2002.

[14] I. Wu, S. Ishigami, K. Gotoh, and Y. Matsumoto: *Dependence of attenuation of common mode radiation from indoor power line communication systems on structure of reinforced concrete wall*, IEICE Trans. Commun., vol. E92B, n°9, pp. 2931-2938, 2009

[15] A.Vukicevic, A. Rubinstein, M. Rubinstein, F. Rachidi: *On the efficiency of notching technique to reduce EM radiations from PLC networks*, in Proc. of IEEE/ISPLC Conf., pp. 253-258, April 2008.

[16] L. Diquelou, *Propagation des signaux sur les lignes d'énergie électrique : Etude des risques de compromission par rayonnement*, Ph. D. Thesis, Univ. of Lille, 20 May 2010

[17] P. Degauque, P. Laly, V. Degardin and M. Lienard: *Power Line Communication and Compromising Radiated Emission*, 5th Symp. on Environmental Electromagnetic Compat., Split, Croatia http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5623680, 23-25 Sept. 2010.

[18] P. Degauque, P. Laly, V. Degardin, M. Lienard and L. Diquelou, *Compromising Electromagnetic Field Radiated by In-House PLC Lines*, in Proc. of GLOBECOM Conf., Dec. 6-10, 2010.

[19] http://www.homeplug.org/, 2010.

[20] http://www.opera.org, 2008.

[21] http://grouper.ieee.org/groups/1901/, 2010.

[22] V. Degardin, E. P. Simon, M. Morelle, M. Lienard, P. Degauque, I. Junqua and S. Bertuol: *On the possibility of using PLC in aircraft*, in Proc. of IEEE/ISPLC Conf.., pp. 337-340, 28-31 March 2010.

Virginie Degardin received the engineer degree from the Ecole Universitaire d'Ingenieurs de Lille, France in 2000 and the Ph.D degree from the University of Lille, France in 2002. She is currently an Associate Professor at the University of Lille. Her current research at TELICE (Telecommunications, Interference and Electromagnetic Compatibility) Group of the Institut d'Electronique, Microelectronique et de Nanotechnologies (IEMN) deals with the optimization and performances of modulation and channel coding for power line communications.

Pierre Laly was awarded from the Institut Universitaire de Technologies (IUT) de Lille in 1991 and received a Licence's degree in Telecommunication network in 2002. From 1991 to 1999, he was with Micropuce Inc. He joined the University of Lille, Lab IEMN/TELICE in 2000, where he is presently an engineer. His main field of interests is on measurement techniques for wire or wireless communication systems.

Martine Lienard received the M.S and Ph.D. degrees from the University of Lille, Lille, France in 1988 and 1993, respectively.

In 1990, she joined the TELICE group of IEMN. She is presently a Professor at the University of Lille and head of TELICE.

Her current research deals with both the theoretical and experimental prediction of propagation characteristics in confined areas, as in tunnels, and the optimization and performances of modulation and diversity schemes, such as MIMO and OFDM techniques, for wireless local area network and power line communications. She is also studying new wireless localization techniques in indoor environment.

Pierre Degauque received the M.S and Ph.D. degrees from the University of Lille, Lille, in 1966 and 1970, respectively. He also received the engineer degree from the Institut Superieur d'Electronique du Nord, Lille, in 1967. Currently, he is a Professor at the University of Lille. Since 1967, he has been working in the field of electromagnetic wave propagation and radiation from various antenna configurations for geophysical applications. His primary interest is now in radio propagation in confined areas, mines and tunnels. He is also active in research on Electromagnetic Compatibility, including wave penetration into structures and coupling to transmission lines.

He was Vice Chairman of URSI Commission E, Electromagnetic Noise and Interference, from 1999 to 2002 and Chairman from 2002 to 2005.