Compromising Electromagnetic Field Radiated by In-House PLC Lines

P. Degauque, P. Laly, V. Degardin, M. Lienard and L. Diquelou
IEMN/TELICE
University of Lille
Villeneuve d’Ascq, France
martine.lienard@univ-lille1.fr

Abstract—To limit the electromagnetic interference due to in-house PLC communication, standards on the emission levels of mains cables are now under elaboration. However, another additional aspect, not yet taken into account, deals with the possibility of exploiting the compromising radiated field to extract some information on the transmitted data. This problem of eavesdropping is known in the Electromagnetic Compatibility community, under the code name Tempest. The compromising propagation channel thus corresponds to the transmission by a modem between two wires of the power line and a reception on a loop antenna placed in adjacent rooms, apartments or houses. To evaluate this risk, a number of configurations are studied to determine the statistical properties of this channel. The influence of either the distance between the transmitting modem and the receiving loop, or of the walls between them, is investigated.

Keywords—Tempest, Radiated field, Power Line Communication

I. INTRODUCTION

PLC is now a growing technology usually applied for in-house high data rate communication. To ensure the Electromagnetic Compatibility (EMC) of such a system with its environment, the EMC approach is divided into two parts: First the susceptibility of the system in presence of noise, and especially of impulsive noise, and, secondly, the disturbing field radiated by the PLC lines which must not exceed a given limit, leading to a maximum power spectral density (PSD) at the injection point.

Since at large distance from the wires, the radiation is mainly due to the common mode current, extensive analyses have been published in the literature on the differential mode (DM) to common mode (CM) current conversion mechanism, due to network imbalance, and on the longitudinal conversion loss defined as the ratio of these two currents [1], [2]. Radiation phenomena are studied in [3]-[4], while the authors in [5] – [9] investigate the existing PLC/PLT systems to determine their emission levels in comparison to EMC standards FCC, EN55022 and NB30 and to proposed standards. With increasing market penetration of in-home PLC networks, it will occur more and more often, that two neighbouring apartments are equipped with PLC systems. Conducted interference and/or radiated interference between them may thus occur as outlined in [10], radiated levels deduced from a numerical modelling of a typical wiring configuration within a bungalow being presented in [11].

However, even if the PLC system fulfils the EMC requirements, the question of confidentiality may still arise. The possible detection of a conducted signal may be avoided by inserting a low pass-filter at the feeding point of the apartment or the house. However, 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. The objective of this paper is thus to quantify the risk and consequently to know if countermeasures based on adequate coding have to be implemented or if PLC must be avoided in certain cases for security reasons. The problem is of course very broad, and the results may strongly depend on a lot of parameters as the network architecture, the environment, the relative position of the receiving sensor, etc. Nevertheless, to have an idea of detection possibility, we consider a PLC link within a room, the receiving sensor being a loop antenna situated in adjacent rooms/apartments.

In Section II, the configuration of the measurement set-up is given. To have an idea of the received signal in various rooms, a qualitative approach is described in Section III. A commercial PLC modem connected on the power line is used as a transmitter, the field being measured in different rooms at the first floor of a building. It must be emphasized that this 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 PLT room 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 PLT room is strongly attenuated in the other rooms and no PLC link is possible from room PLT to the adjacent rooms. 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 PLT room. Since the signal to noise ratio appeared to be not prohibitive, extensive measurements were carried out to study the statistical characteristics of the compromising channel. Results are presented in Section IV. To conclude this approach, a software tool has been used to simulate a PLC transmission on the power line and to evaluate the bit error rate when demodulating the signal received by the Rx loop.

The reverse link where the power line would work as an antenna receiving the signal transmitted from the loop antenna is not treated in this paper which only focuses on eavesdropping problems.
II. DESCRIPTION OF THE MEASUREMENT SET UP

The 3 wires of the power line, 24 m long, have been installed along the walls of a room, named “PLT room”, situated at the first level of a 3 store building at the University of Lille. The 3 wires being put in a cylindrical plastic tube, the relative position of the wires varies randomly along this tube. This configuration is quite usual in in-house power network, at least in Europe. Along this line, various electrical items can be connected or not, on various plugs, as shown in Fig. 1. To be in a realistic situation, this room contains usual furniture, shelves, etc. Furthermore, three wires of the line, namely phase, neutral and ground, are connected to the main power network of the building.

Figure 1. Configuration of the experimental set-up.

The injection is made at point 1 between the neutral wire and the phase wire, owing to a capacitive coupler. In the following, two propagation channels will be considered: The first one, called the “wire” channel, is the usual PLC channel and corresponds to the propagation along the power line. The second one deals with the compromising channel or “wireless channel”. In this case, the injection point is made, as previously, at point 1, but the receiving sensor is a calibrated shielded loop antenna, having a diameter of 10 cm.

This loop, set on a tripod, is placed at different locations in the PLT room and in the 5 other rooms mentioned in Fig. 2. Along the corridor, there is a series of reinforced concrete pillars. Between rooms PLT and 122 and between 117 and 119, the dividing walls are plaster walls, while reinforced concrete walls are between PLT and 118 and between 115 and 117.

The loop is connected to a 54 dB gain low noise amplifier (LNA), MITEQ AM1309, having a noise figure of 1.2 dB and battery powered. To avoid induced currents on connecting cables, coaxial cables with ferrite beads around their shield were chosen.

The coupler which includes a separate isolation transformer, is used either to inject a current on the PLC line or to measure the received signal on the various plugs. The measuring system is a spectrum analyser or a vector network analyser, as it will be explained in the next sections.

III. QUALITATIVE EXPERIMENTS WITH COMMERCIAL MODEMS

Experiments were first carried out with a commercial modem (85 Mbits/s) working in the 4 – 20.5 MHz band, plugged at point 1 (Fig. 1) and two electrical devices were plugged at points 3 and 5. The two ports of the modem are connected to the phase wire and the neutral wire. Firstly, the PLC systems are switched off to measure the noise floor. Then the modem is switched in a busy state to measure the radiated emission. Let us first consider a usual PLC communication. The power spectral density (PSD) of the transmitting (Tx) signal and of the received (Rx) signal at point 6, are shown in Fig. 3. Measurements are made with a spectrum analyzer with the following settings: Measurement range: 1-30 MHz, Resolution BW: 9.1 kHz, Measuring points 1200, peak holding time: 1 min. We see in this Figure that the maximum PSD of the injected signal is about -10 dBm in a 9 kHz bandwidth, and thus equal to -50 dBm/Hz. The notches are also clearly visible on the curve. At the receiving point 6 the signal is attenuated, mainly in the lowest and highest part of the frequency band, which is of course, in agreement with the results of direct measurements of path loss, carried out separately. The third curve plotted in Fig. 3 is the conducted noise PSD which presents a maximum value between 6 and 8 MHz and then keeps a nearly constant value of -100 dBm (-140 dBm/Hz).

Figure 2. Topology of the rooms.

Figure 3. PSD (in a 9.1 kHz bandwidth) of the input signal, of the received signal and of noise – “Wire channel”.

978-1-4244-5637-6/10/$26.00 ©2010 IEEE
The compromising channel or “wireless” channel assumes, as previously, an injection at point 1 but a reception on a loop antenna. The knowledge of the radiated field is important to compare its amplitude to the limits given by standards. However, in our case, we are interested by the feasibility of extracting information of the radiated signal. Therefore, only the signal to noise ratio (SNR) is of interest. Since both the signal and the ambient noise in the rooms were measured with the same loop, we have preferred to present the results in terms of received power, taking the gain of the receiving chain into account.

In Fig. 4, one can first compare the maximum values, given by the blue curves, of the OFDM signal received on a magnetic loop placed successively in the center of the following rooms: PLT, 122 and 118. The attenuation of the signal between rooms PLT and 122 is 5 to 10 dB, the plaster wall between these rooms not strongly attenuating the EM waves.

However, if we now compare the signals in rooms PLT and 118, the attenuation reaches sometimes 20 dB due to the reinforced concrete wall. One can mention that the attenuation effect of the walls of a building on the EM field generated by an indoor PLC system was numerically investigated in [12] but for a low frequency range, extending from 2 to 6 MHz. A theoretical attenuation of 30 dB was found, the main contributor being the rebar in the wall.

In Fig. 4, green curves refer to noise PSD.

IV. CHARACTERISTICS OF THE WIRELESS CHANNEL

The radiated field being strongly related to the common mode (CM) current flowing on the power line, we first study the influence of the loads connected to the network on the amplitude of this current. A comparison with the differential mode (DM) current amplitude will also be given. Ambient noise and transfer functions of the “compromising” (wireless) channel will then be studied.

A. Influence of the loads on the DM and CM current

Few results on the influence of the loads connected to the power line, on the DM and CM currents and on the transfer functions are successively presented. A voltage generator is connected to the PLC coupler whose voltage transfer function is nearly equal to 1 in the whole frequency range. The current flowing on the wires was measured with a current probe put either around the 3 wires (CM current), or around one of the two injection wires (DM current), the amplitude of the DM current being much larger than the CM one.

Curves in Fig. 5 give the amplitudes of the DM current, expressed in dBA, versus frequency, measured at about 10 m from the injection point and normalized to an injected voltage of 1 V. The point of measurement was situated nearly at mid-distance from the injection point and the terminal load, between two power sockets. To be able to put a current probe on a wire and thus to measure the DM current, the plastic tube containing the 3 wires was cut on a short distance.

![Figure 5. Amplitude of the DM current for various network loading conditions.](image)

For plotting the curve “no load”, no electric equipment was plugged on the line. The cases “2 loads” and “4 loads” correspond to appliances connected at points 3 and 5, and 2, 3, 4 and 5, respectively. If the number of loads increases, the fluctuations of the DM currents are more important and the channel becomes frequency selective. Curves in Fig. 6 represent the variation of the CM current measured at the same point as previously.

![Figure 4. PSD of the received signal in various rooms (blue curves) and noise PSD (green curves) – Wireless channel.](image)
Contrary to the case of the DM current, the global behavior of the CM current remains the same whatever the loads. For the network under test, the maximum value of the CM current occurs between 10 and 18 MHz, the difference in amplitude between the DM current and the CM current in this band is on the order of 15 dB. Since the loading condition does not strongly influence the amplitude of the radiated field, the “no load” configuration will be kept in the following. The two aspects of the wireless channel, namely ambient noise and transfer functions, are described in the next two paragraphs.

B. Ambient noise PSD

Some experimental data dealing with the level of the background noise measured in a room with a loop antenna, are described in [6]. In [13], radiated emissions associated with household appliances such as TV set, oven, personal computer are presented. For our application, the three noise components, x, y and z, were measured at about 50 location points situated in various rooms, at the first floor of the building (Fig. 2). The z axis is vertical, the x and y axis being parallel and perpendicular to the corridor, respectively. The upper part of Fig. 7 refers to the average noise PSD in a 9 kHz bandwidth. Excluding narrow band interferer, mainly due to radio broadcasting, average ambient noise can be estimated to be on the order or less than -115 dBm/9kHz i.e. -155 dBm/Hz. When using a software tool for simulating the communication link on the wireless channel, a drastic approximation would be to suppose that this noise is white and Gaussian. Curves in the lower part of Fig. 7 correspond to the electric field component deduced from the magnetic field, assuming plane wave impedance, as recommended in the standards, and taking the loop antenna factor into account. To evaluate the risk of detection, by using software tool simulating the communication link, the channel must be characterized in time domain. The channel impulse response can be deduced from the complex channel transfer function, as described in the next paragraph.

C. Wireless channel characteristics

The complex channel transfer function, corresponding to the S21 scattering parameter was measured with a vector network analyzer (VNA) in a frequency range extending from 1 MHz up to 40 MHz. The calibration of the VNA takes all interconnecting cables into account. The injection is made between two wires at point 1 (Fig. 1), the receiving loop antenna being put at different locations in the rooms. An example of the amplitude of S21 is shown in Fig. 8. The various curves correspond to different locations of the loop in room 122 (Fig. 1). As previously outlined, S21 is not an intrinsic channel characteristic since it will increase with the size of the loop, but as does received noise.

The increase of the insertion gain with frequency is due partly to the increase of the field radiated by the power line, and partly to the response of the magnetic loop. Above 15 MHz, the average path loss is about 85 dB. This very high attenuation, compared to the attenuation of a typical wire channel, is partly compensated by a low noise PSD. Indeed, the
PSD of the conducted background noise measured on the power line was -140 dBm/Hz, compared to -155 dBm/Hz for the ambient noise. To see the additional attenuation when the receiving loop is behind a reinforced concrete wall, a statistical approach must be made. In Fig. 9, the complementary cumulative distribution function of the insertion gain is plotted when the loop is located in 3 rooms. For plotting one curve, all values of insertion gain obtained for the 1200 frequency points and for 10 location points inside the room are considered. Comparing curves for rooms 118 and 122, an additional attenuation of 10 dB is observed in room 118. Rooms 118 and 122 are adjacent to the PLT room, but the dividing wall is a reinforced concrete wall and a plaster wall, respectively.

![Figure 9. CCDF of the insertion gain for the wireless channel when the Rx loop is situated in different rooms.](image-url)

We have also measured the common mode current on the power line in rooms 118 and 122 to check that their radiation in the room is negligible. If the PSD of the signal transmitted by a PLC modem is -50 dBm/Hz, and if the channel is characterized by an average insertion gain of –90 dB and a noise PSD of -155 dBm/Hz, this leads to a signal to noise ratio of 15 dB. One can mention that in the frame of “eavesdropping”, the location of the Rx loop in an adjacent apartment/house, may be chosen adequately to maximize the SNR. The impulse responses of the channel and the power delay profile were deduced from measurements of the complex transfer function in the frequency domain through a Fourier transform. The delay spread of the wireless channel reaches 120 ns but this value remains much smaller than the usual OFDM guard interval, equal to 20 μs in the OPERA specifications [14] and 7.56 μs for HomePlug AV.

### D. Simulation of the communication link

In the following, a link following the OPERA specifications was chosen [14]. The maximum theoretical bit rate is 200 Mbits/s, with 10 bits per subcarrier. A multi-dimensional trellis code modulation (TCM) is applied, followed by a M-PSK mapping. Details on the bit allocation algorithm are given in [14]. An ADPSK modulation is also specified. It is known that such a technique degrades the performance but facilitates the decoding process. A software tool simulating the OFDM link was developed partly in C language and partly under Matlab, to predict the performance of the link, assuming a perfect synchronization between transmitting and receiving modems. To give an example, let us assume a communication between two modems on the wire channel, at a rate of about 30 Mbits/s, the injected power being -50 dBm/Hz. By choosing the less attenuated transfer function in room 118, thus for a receiving point behind the reinforced concrete wall, the bit error rate on the detected signal, would be $2 \times 10^{-2}$. This gives an idea of the risk of extracting information, keeping in mind that, practically, advanced techniques based for example on blind deconvolution algorithms, could be used.

### V. CONCLUSION

The propagation channel associated with the radiation of a PLC network inside a building has been characterized. If a PLC link is established in a room, it seems that the exploitation of radiated emissions measured in an adjacent room of another apartment/house, could be possible, at least in some cases.

### REFERENCES


