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).