Exploitation of the PLC channel properties to enable secure communications

Federico Passerini and Andrea M. Tonello

Alpen-Adria-Universität Klagenfurt, Klagenfurt, Austria
{federico.passerini, andrea.tonello}@aau.at

I. Introduction

In physical broadcast networks (PBN), such as power line networks (PLNs), a malicious user can perform attacks on all the stacks of the ISO/OSI model, including the MAC and physical layer. In particular, the physical layer comes to play an important role in both planning attacks to the network and defensive strategies. In fact, since the physical medium is shared, every input into the network has an effect on the whole system. If the network system can be modeled, then its properties can be used with both malicious or aiding intent.

In the context of power line transmission and distribution networks, attacks and defensive strategies are normally based on system theory. In this case, the network is modeled as a dynamic system that describes the power flow. Attacks of different kind aim at altering the perception of the state of the network, which in turn might bring to a network failure [1]. In any case, informative signals need to circulate through the network, therefore a resilient communication architecture would enhance the PLN security. However, to our knowledge there is very few literature about physical-layer secure communications in PLNs [2][3][4][5].

In this regard, Power Line Communications (PLC) is a well established communication technology in PLNs [6]. This technology already provides a form of security in the fact that it uses a communication mean, the power line cables, that is owned by the utility and therefore not accessible to everybody. However, an unauthorized user might be able to get physical access to the network, or the utility might not want to share some information with part of the network. Therefore, additional security measures have to be provided. Since the PLC physical channel has some properties in common with that of wireless communications, it might make sense to directly apply the physical-layer security (PLS) techniques developed for wireless [7][8] to the case of PLC. However, it has been shown that the PLC channel, conversely from the wireless one, is in general not symmetric [9] and, moreover, has different statistical properties [10].

In this paper, we propose an analysis of the properties of the PLC channel in order to investigate under which conditions PLS techniques developed for wireless apply also to PLC. However, since the PLC channel is in general non symmetric, most of the known PLS algorithms cannot be applied to it. In order to overcome this limit, we make use of the fact that the PLC channel is reciprocal to investigate which channel state information (CSI) is known to both the transmitter and the receiver independently at any given time. The CSI obtained with the proposed method can be consequently used to generate common cryptographic keys separately at the two communication ends. Although our investigation focuses on PLN, the proposed data sources are common to every reciprocal network, including any kind of passive wired network and wireless networks.

II. Proposed Approaches

It has been shown in [9] that the power line channel is symmetric if the impedance Z_T at the transmission side is equal to the load impedance Z_L (see Fig. 1). Similarly, this condition applies to the wireless channel and to any other kind of passive network. However, while in wireless systems both Z_T and Z_L are set to the same value (usually 50Ω) to maximize the power transmitted and received, there are different cases in PLC. Considering in-band full duplex PLC, the transmitted and the received signal are referred to the same impedance [11]. This allows to optimize the bi-directional communication

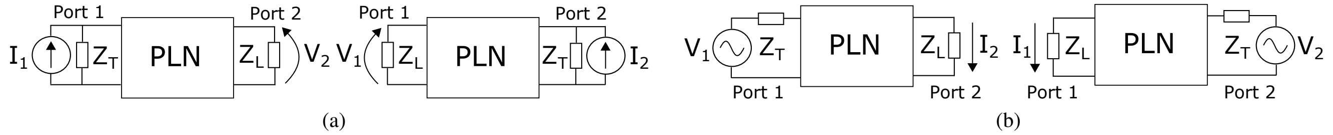

Fig. 1: Sketch of trans-resistance a) and trans-conductance b) communication schemes.

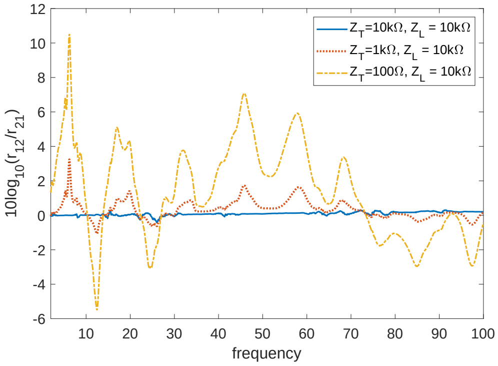

Fig. 2: Symmetry of r for different values of Z_T, with Z_L =10kΩ

output. Besides, it also means that if the two communication ends are equipped with modems that use an output impedance with the same value, we have $Z_T = Z_L$ and the channel is symmetric.

On the other hand, in half-duplex PLC systems optimal communication rate is obtained by maximizing the transferred voltage [12]. Therefore, PLM are usually equipped with Z_T $\sim$1Ω and Z_L $\sim$10kΩ. This renders the channel highly non symmetric. Nevertheless, the PLC channel is reciprocal and this property can be exploited to get symmetric CSI using particular transmission schemes. In fact, in any reciprocal network the following holds true:

- referring to Fig. 1a, the ratio $r = V_2/I_1$ remains constant when the two ports are inverted, under the condition $Z_T = Z_L = \infty$,
- referring to Fig. 1b, the ratio $g = I_2/V_1$ remains constant when the two ports are inverted, under the condition that $Z_T = Z_L = 0$.

This means that it is possible to obtain symmetric transmission of signals considering the trans-resistance r or the trans-conductance g of the network instead of the classical voltage transfer function. However, the values of the impedances under which this property holds are ideal and far from the common values of Z_T and Z_L. Nevertheless, it comes out from our simulations that a good degree of symmetry is hold also with $Z_T = Z_L$ $\sim$10kΩ or $Z_T = Z_L$ $\sim$1Ω for the trans-resistance and trans-conductance cases, respectively (see Fig. 2). Trans-resistance communication would be practically implementable in power line modems, by piloting the line with a current instead of a voltage and using a classical voltage receiver. On the other end, trans-conductance communication would imply to send a voltage signal using a classical transmitter and to receive a current signal over a very small impedance.

References

[1] Y. Mo, T. H. J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber-physical security of a smart grid infrastructure," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195–209, Jan 2012.

[2] A. Salem, K. M. Rabie, K. A. Hamdi, E. Alsusa, and A. M. Tonello, "Physical layer security of cooperative relaying power-line communication systems," in *2016 International Symposium on Power Line Communications and its Applications (ISPLC)*, March 2016, pp. 185–189.

[3] A. Pittolo and A. M. Tonello, "Physical layer security in power line communication networks: an emerging scenario, other than wireless," *IET Communications*, vol. 8, no. 8, pp. 1239–1247, May 2014.

[4] A. Pittolo and A. M. Tonello, "Physical layer security in mimo-me plc networks with alternating optimization," in *Proc. of Workshop on Communication Security, Ancona*, September 2014.

[5] A. Pittolo and A. M. Tonello, "Physical layer security in plc networks: Achievable secrecy rate and channel effects," in *2013 IEEE 17th International Symposium on Power Line Communications and Its Applications*, March 2013, pp. 273–278.

[6] C. Cano, A. Pittolo, D. Malone, L. Lampe, A. M. Tonello, and A. G. Dabak, "State of the art in power line communications: From the applications to the medium," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 7, pp. 1935–1952, July 2016.

[7] W. Henkel, O. Graur, and U. Pagel, "Wireline physical-layer key generation," in *11th Workshop on Power Line Communications*, Prague, (CZ), Sept 2017.

[8] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*, 1st ed. New York, NY, USA: Cambridge University Press, 2011.

[9] M. D. Piante and A. M. Tonello, "Characteristics of the plc channel: Reciprocity, symmetry and port decoupling for impedance matching," in *2016 International Symposium on Power Line Communications and its Applications (ISPLC)*, March 2016, pp. 93–97.

[10] A. Pittolo and A. M. Tonello, "Physical layer security in power line communication networks," in *Physical and Data-Link Security Techniques for Future Communication Systems*, ser. Book: Lecture Notes in Electrical Engineering, M. Baldi and S. Tomasin, Eds. Cham: Springer International Publishing, 2015, vol. 358, pp. 125–144.

[11] F. Passerini and A. M. Tonello, "Adaptive hybrid circuit for enhanced echo cancellation in full duplex PLC," in *2018 IEEE International Symposium on Power Line Communications and its Applications (ISPLC)*, April 2018, pp. 1–5.

[12] M. De Piante and A. M. Tonello, "On impedance matching in a power-line-communication system," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 63, no. 7, pp. 653–657, July 2016.