Proceedings of Workshop on Communication Security, Ancona, Italy, Sept. 11-12, 2014

Physical Layer Security in MIMO-ME PLC Networks with Alternating Optimization

Alberto Pittolo and Andrea M. Tonello

University of Udine, {alberto.pittolo, tonello}@uniud.it

I. Introduction and Problem Statement

This paper deals with the secrecy guaranteed at the physical layer, namely physical layer security (PLS). The aim is to evaluate the achievable rate on the power delivery infrastructure, or power line communication (PLC) networks, under secrecy constraints. The focus is on the multiple-input, multiple-output and multiple eavesdropper (MIMO-ME) wiretap communication channel. The system consists of a transmitter (Alice), which wishes to securely transmit a confidential message to the intended receiver (Bob), avoiding any leakage of information to the eavesdropper (Eve), which tries to detect the message.

In order to provide actual and fair results, the intent is to evaluate the performance of the MIMO-ME wiretap channel achieved on real channel measurements and under a realistic background noise assumption. Moreover, the exploitation of an additional receiving mode, named common mode (CM), together with all the available wires (phase, neutral and protective earth), is considered. Furthermore, a different power allocation strategy, provided by an alternating optimization (AO) approach, is discussed and implemented. Towards this end, also the extended frequency band in the 2–86 MHz is taken into account, as required by the HomePlug AV2 (HPAV2) standard for the next generation devices. This assumptions and strategies could lead to a performance increase in terms of achievable secrecy capacity.

II. Proposed Solution Outline

It has already been proved in [1] how the exploitation of the multiple conductor, phase (P), neutral (N) and protective earth (E), at the transmitter and at the receiver side, could noticeably increase the physical layer security of a PLC network. However, the analysis carried out in [1] considers a maximum of 2 spatial transmission and reception modes, a white Gaussian background noise and a 2–28 MHz frequency band. Furthermore, the performance is evaluated relying on a numerically generated network topology based on a bottom up model approach. Otherwise, the purpose of this paper is to consider two Δ-style transmitting modes (P-N and N-E) and four star-style receiving modes (P, N, E and CM) for both the legitimate and hostile nodes. The common mode is given by the current that flows in the three conductors, with the same intensity and direction. It has been proven in [2] as this additional mode could improve performance, without secrecy constraints. This strategy could also result in an improvement of the channel capacity with secrecy constraints, or secrecy capacity.

The performance is evaluated on 353 MIMO channel realizations obtained through an experimental measurement campaign across Europe. The measurements were collected by the ETSI special task force 410 (STF-410) [3] considering the 2–86 MHz frequency band extension and according to the latest HPAV2 standard [4]. Furthermore, a colored (with an exponential decreasing profile along frequency) and correlated (between the different receiving modes) Gaussian background noise (for details see [2]), which typically affects real PLC networks, is considered. These assumptions allow to obtain actual and fair results in performance evaluation for today's and future PLC devices. Moreover, the noise correlation could lead to a performance improvement w.r.t. the same network affected by independent noise (among different modes), with equivalent statistical parameters. This is because the noise correlation could be exploited to aid its cancellation at the receiver side. The "spatial" correlation of the noise (off diagonal elements of the covariance matrix) is modeled according to the procedure discussed in [2].

Last but not least, unlike the uniform power allocation assumed in [1], the novel approach discussed in [5] is adopted to compute the "best" power resource allocation at the transmitter side. The solution provided in [5] is adopted to tackle the non-trivial and non-convex secrecy optimization problem in MIMO wiretap channels. Furthermore, the proposed algorithm is computationally efficient and guarantees the convergence to a Karush-Kuhn-Tucker (KKT) point of the secrecy capacity maximization problem. Also this strategy could lead to an increase of the performance in terms of achievable secrecy capacity.

III. Preliminary Numerical Results and Conclusions

We take into account 353 channel measurements performed in the 0–100 MHz frequency band, according to the measurement procedure followed by the STF-410, detailed in [3]. The experimental MIMO channels where divided equally among the legitimate and the unintended receiver ($176 = \lfloor 353/2 \rfloor$ realizations for both the Alice to Bob and Alice to Eve communication channels).

We evaluate the secrecy capacity (shown as C_s) achieved on the $2 \times 4 \times 4$ MIMO-ME wiretap channel for all the channel measurements, under uniform and "best" power allocation strategy (provided by the iterative algorithm discussed in [5]). Two different background Gaussian noise models are considered in Fig. 1, white and independent (on the left side), colored and correlated (on the right side). As a term of comparison, the capacity (shown as C) of the MIMO communication channel (without secrecy constraints), under optimal power allocation, is displayed for both the different noise models.

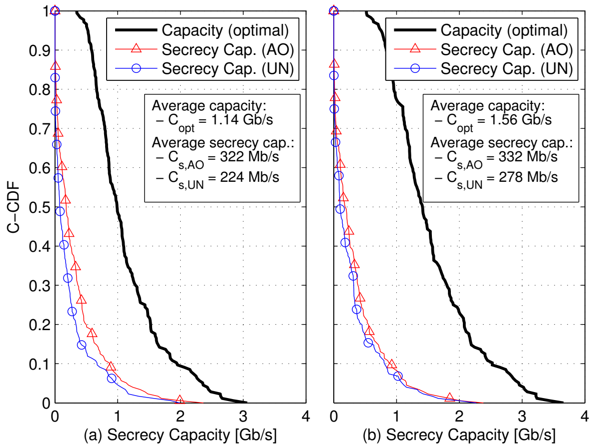

Fig. 1. Capacity C-CDF comparison among uniform and the AO algorithm approach for both white independent (a) and colored and correlated (b) Gaussian background noise.

The complementary cumulative distribution function (C-CDF) for the channel capacity and secrecy capacity, achieved with the power allocation provided by the AO algorithm and with uniform allocation (shown as AO and UN), are depicted in Fig. 1. It can be noted as the performance without secrecy constraint (capacity), for the transmission from Alice to Bob, outperforms the secrecy capacity for any power allocation and considered scenario (different background noise), as expected. Furthermore, concerning the secrecy capacity, the use of the alternating optimization (AO) algorithm proposed in [5] (for a power allocation other than uniform), leads to a performance improvement for both the considered background noise models. In fact, the AO approach provides an average secrecy capacity (averaged over the realizations) increase of about 30% for the white independent noise, and by approximately 20% for the colored and correlated noise, w.r.t. the uniform power allocation. Obviously, the average channel capacity outperforms the average secrecy capacity (approximately 4 times greater). Finally, note as the secrecy capacity (for both the AO algorithm and uniform allocation), as well as the channel capacity, increases when the network is affected by colored and correlated noise, w.r.t. white and independent noise. This is because, as previously stated, the noise correlation aids its cancellation at the receiver side.

References

[1] Y. Zhuang and L. Lampe, "Physical Layer Security in MIMO Power Line Communication Networks," in *Proc. of 2014 18th IEEE International Symposium on Power Line Communications and its Applications (ISPLC)*, March 2014, pp. 272–277.

[2] A. Pittolo, A. M. Tonello, and F. Versolatto, "Performance of MIMO PLC in Measured Channels Affected by Correlated Noise," in *Proc. of 2014 18th IEEE International Symposium on Power Line Communications and its Applications (ISPLC)*, March 2014, pp. 261–265.

[3] ETSI TR 101 562-1 V 1.3.1, "PowerLine Telecommunications (PLT); MIMO PLT; Part 1: Measurement Methods of MIMO PLT," European Telecommunication Standardization Institute, Tech. Rep., 2012.

[4] L. Yonge, J. Abad, K. Afkhamie, L. Guerrieri, S. Katar, H. Lioe, P. Pagani, R. Riva, D. Schneider, and A. Schwager, "An Overview of the HomePlug AV2 Technology," *Journal of Electrical and Computer Engineering*, vol. 2013, 2013.

[5] Q. Li, M. Hong, H.-T. Wai, Y.-F. Liu, W.-K. Ma, and Z.-Q. Luo, "Transmit Solutions for MIMO Wiretap Channels using Alternating Optimization," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1714–1727, 2013.