Proc. of IEEE ISPLC 2013

Physical Layer Security in PLC Networks: Achievable Secrecy Rate and Channel Effects

Alberto Pittolo and Andrea M. Tonello
WiPli Lab – Wireless and Power Line Communications Lab – University of Udine
33100 Udine, Italy
Email: {alberto.pittolo, tonello}@uniud.it
Website: http://www.diegm.uniud.it/tonello/wiplilab

***Abstract*—We consider confidential data communication over power line communication (PLC) networks. In particular, rather than analyzing cryptographic techniques, we focus on the security provided at the physical layer, named physical layer security (PLS). Although physical layer security is widely discussed for wireless systems, we can not say the same for the PLC context. As a starting point, the wireless case will be examined. Then, we highlight the differences with PLC and we compare the average secrecy rate that can be achieved in typical wireless and PLC fading channels. Both optimal and uniform power distributions are considered. The theoretical results show that wireless fading channels provide higher secrecy rate than PLC channels. This is due to different channel statistics and propagation scenario. To provide experimental evidence, we consider channel measures obtained in a in-ship and in a in-home measurement campaign. While log-normal fading fits well the former channels, the latter channels are not strictly log-normal. Furthermore, the considered in-home network topology introduces correlation among channels, and it is subject to the keyhole effect introduced by branches that depart from the same node. These effects can reduce the secrecy rate.**

I. Introduction

In recent years, the use of the electricity network as a means of communication has gained increasing popularity and interest. The PLC allows us to exploit the existing power lines for data transmission. Consequently there is a considerable saving in costs and time for the infrastructure creation. Similarly to the wireless case, the PLC channel is intrinsically broadcast, namely it is shared by the users who access it. Therefore, data security is of crucial importance. To this end, we can provide security by applying cryptographic protocols to the high levels of the ISO/OSI stack model, as the data encryption standard (DES) does. However, there are techniques that allow us to manage security even at the physical level. This concept is known as physical layer security (PLS) [1]. PLS can complement and extend the concept of security implemented by other layers.

There are essentially two schools of thought concerning the PLS: the information-theoretic security and the complexity-based security. The information-theoretic approach was first formulated by Shannon in 1949 [2], where the adversary is assumed to have unlimited computational resources and the objective is to ensure that absolutely no information is released to the adversary (see Fig. 1). Complexity-based cryptography, on the other hand, discards the notion that the adversary has infinite computation capabilities. Thus, it assumes the adversary to have limitations on how much computation can be performed. Now, when an adversary witnesses an encrypted message (the ciphertext), the necessary computations render it practically unfeasible for the adversary to deduce the corresponding original message (the plaintext). The difficulty to decipher the encrypted message determines the quality of a given security protocol (such as DES). The information-theoretic approach to confidential communications offers advantages in wireless scenarios when compared with conventional complexity-based cryptography. In fact its basic principle is widely accepted as the strictest notion of security. This approach, which builds on Shannon's notion of perfect secrecy [2], was first studied by Wyner [3] for the classical wiretap channel. It is also interesting to note that the optimal power allocation problem with secrecy constraints, from an information-theoretic point of view, is similar to the more common resource allocation problem in multicarrier systems analyzed in [4].

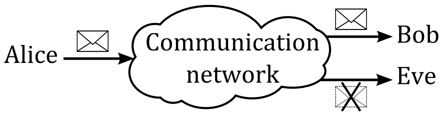


Fig. 1. Wiretap channel scheme.

The purpose of this paper is to provide a first investigation of the achievable secrecy rate in typical PLC channels and to highlight the differences with respect to the wireless communication case. Although the achievable rate has been studied in PLC channels both with experimental data and with the use of statistical simulators, e.g., in [5], [6], to our knowledge, PLS and the secrecy rate has not been evaluated yet. We show that PLS is possible in PLC. However, since PLC channels are not characterized by Rayleigh fading (which is typical of wireless channels), lower secrecy rates can be achieved compared to the wireless context. Furthermore, channel correlation introduced by signals propagating in a shared tree structure network, can reduce further the secrecy rate.

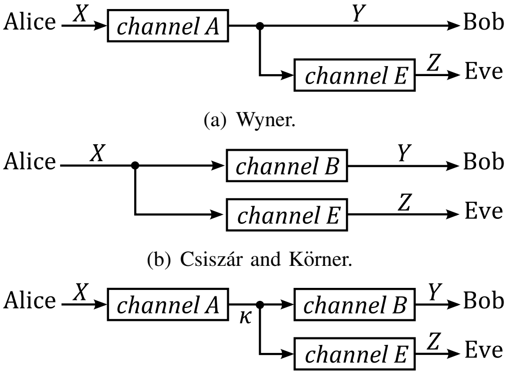
The rest of the paper is organized as follows. First, Section II offers an overview about the different channel configurations that have been considered in the PLS study framework. Then, Section III provides an information-theoretic formulation of the problem of secure communication over fading channels.

Herein, the secrecy capacity is defined, and the secrecy rate maximization problem is solved deriving the optimal power allocation. Section IV analyzes the differences between the secrecy rate of a Rayleigh fading channel (wireless case) and of a Log-normal fading channel. The latter model applies to certain PLC scenarios, as for instance the in-ship PLC scenario that we have measured. We also consider channels measured in a home network that do not strictly manifest log-normal fading and are correlated due to the different wiring topology that has a tree structure rather than a star structure as in the in-ship case. Finally, the conclusions follow.

II. The Wiretap Channel

The wiretap channel in Fig. 1 is a communication system where a transmitter (Alice) wants to send a private message to an intended or legitimate receiver (Bob), which should be kept perfectly secret from the eavesdropper (Eve). Eve listens and tries to decode the message that Alice sends to Bob.

There are mainly three types of channel configurations, each modeling a different scenario, as shown in Fig. 2.



(a) Wyner.

(b) Csiszár and Körner.

(c) Keyhole channel.

Fig. 2. Models of wiretap channel.

1) Wyner: In the wiretap channel proposed by Wyner [3], also referred to degraded wiretap channel, two legitimate users communicate over a main channel (*channel A*) and an eavesdropper has access to a degraded versions of the channel outputs that reach the legitimate receiver through the wiretapper channel (*channel E*), as depicted in Fig. 2(a). This fact simplifies the analysis and the derivation of secrecy limits because it assumes that Eve's received signal is always a degraded or noisier version of Bob's received signal. Wyner found that there is a trade off between the transmission rate of the main user and the equivocation at the wiretapper.

2) Csiszár and Körner: Later, Csiszár and Körner [7] extended Wyner's work to general broadcast scenarios, assuming the main and the eavesdropper channel independent from each other, as depicted in Fig. 2(b). This model can represent a typical star structure PLC topology as well as a typical wireless communication scenario. Furthermore, in this model the two channels can be statistically independent as it is the case for wireless communications with a high scattering environment.

3) Keyhole channel: The model depicted in Fig. 2(c) represents a tree or bus network configuration structure, which is very common in PLC networks. We refer to it as keyhole channel since the branch point κ is the keyhole through which the signals to Bob and Eve need to pass. The keyhole channel has been deeply investigated in the context of multiple-input multiple-output (MIMO) wireless channels [8]. In this propagation environment, the MIMO channel can exhibit a rank-deficiency or higher correlation, thereby reducing the MIMO channel capacity [9] and [10]. The keyhole channel effect in cooperative multihop PLCs has been recently studied in [11].

The model in Fig. 2(c) is sufficiently general to include both the model in Fig. 2(a) and in Fig. 2(b) by assuming *channel B* or *channel A* ideal, respectively.

III. Problem Formulation

Assuming the presence of additive noise, and narrow band transmission, the model in Fig. 2(c) can be mathematically written as

$$\begin{aligned} y_i &= h_{Mi} \cdot x_i + n_{Mi}, \\ z_i &= h_{Wi} \cdot x_i + n_{Wi}, \end{aligned} \tag{1}$$

where i is the time index, x_i is the channel input signal at the time instant i, and y_i and z_i are the channel outputs at the time instant i, respectively. Further, n_{Mi} and n_{Wi} represent the noise terms (assumed to be i.i.d. zero mean complex Gaussian in the following), whereas h_{Mi} and h_{Wi} are the channel gain coefficients for the main and the eavesdropper channel, respectively. This model is independently used n times to transmit the codeword of length n that is chosen for the message S.

With reference to Fig. 2(c), h_{Mi} can be viewed as the product of the *channel A* gain with the *channel B* gain. Similarly, h_{Wi} is obtained by the product of the *channel A* gain with the *channel E* gain. Thus, this model can describe each one of the three different models represented in Fig. 2.

From a system theoretic point of view, the channel input x and channel outputs y and z are random variables. The corresponding channel input or output alphabets are written as $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$. The secret S is a random integer from the set $\{1, \ldots, M\}$ with $M = 2^{nR_S}$ and it is transmitted in n channel uses. In this case, the secret has entropy $H(S) = nR_S$ bits and the secrecy communication rate is $R_S = H(S)/n$ bits per channel use. In this system, Alice encodes the message S into the codeword $\boldsymbol{x} = [x_1, \ldots, x_i, \ldots, x_n]$; Bob receives the channel output $\boldsymbol{y} = [y_1, \ldots, y_i, \ldots, y_n]$ and decodes $\hat{S}$ with error probability $P_e = Pr[S \neq \hat{S}]$. After Eve overhears the output $\boldsymbol{z} = [z_1, \ldots, z_i, \ldots, z_n]$, her residua uncertainty regarding the secret message S is given by the conditional entropy $H(S|\boldsymbol{z})$ which is generally expressed by an equivocation rate R_e.

From the perspective of confidential and reliable communication, the system performance depends on both the communication rate R_S (between Alice and Bob) and the equivocation rate R_e (between Alice and Eve). The physical layer security problem turns out to be an optimization problem that aims to maximize performance between legitimate users, under a constraint of maximum information obtainable from unauthorized users.

A secrecy rate R_S is said to be achievable over the wiretap channel if for any $\varepsilon >= 0$, there exists an integer $n(\varepsilon)$ and a sequence of (M, n)-codes of rate $R_S = \frac{1}{n}\log_2 M$, such that for all $n > n(\varepsilon)$, the average decoding error probability becomes arbitrarily small, i.e., $P_e^n \leq \varepsilon$, and the security constraint $R_e^n = H(W|\boldsymbol{z})/n \geq R_S - \varepsilon$ is fulfilled.

A. Secrecy Capacity

For perfect secrecy ($\varepsilon = 0$) the secrecy capacity C_S is the supremum of all achievable rates that guarantee the secrecy of the transmitted data $C_S = \max_{P_e^n \leq \varepsilon} R_S$. This means that it is the tightest upper bound on the amount of information that can be reliably transmitted to the receiver and perfectly kept secret from the eavesdropper.

For the degraded Gaussian wiretap channel, which was introduced in [12], where the main channel has an higher information rate than the eavesdropper channel, the secrecy capacity $C_{S,d}$ is given by the maximum difference of two channels mutual information, as follows:

$$C_{S,d} = \max_{f_x \in \mathcal{F}} [I(x;y) - I(x;z)], \tag{2}$$

where f_x is the probability density function (pdf) of the channel input x, instead, $\mathcal{F}$ is the set of all pdfs at the channel input under a power constraint. Instead, for the general Gaussian wiretap channel (as well as the keyhole channel) the secrecy capacity C_S has the same expression as in (2), but it is set to zero if Eve has a better channel realization than Bob.

$$C_S = \max_{f_x \in \mathcal{F}} [I(x;y) - I(x;z)]^+, \tag{3}$$

where $[q]^+ = \max(q, 0)$. The mutual information terms $I(x;y)$ and $I(x;z)$ are convex in f_x, so we can formulate a lower bound R_S for the secrecy capacity in (3) as follows.

$$C_S \geq \left[\max_{f_x \in \mathcal{F}} [I(x;y)] - \max_{f_x \in \mathcal{F}} [I(x;z)] \right]^+ = R_S. \tag{4}$$

This lower bound R_S is often used for a simplified calculation of achievable secrecy rates since it is known how to maximize the mutual information terms.

B. Secrecy Capacity in Fading Channels

Now, to model the effect of a fading channel, we can assume that the gain coefficients h_{Mi} and h_{Wi} in (1) are zero-mean proper complex random variables. The noise variables n_{Mi} and n_{Wi} are assumed zero-mean independent identically distributed (i.i.d.) complex Gaussian, having variances η^2 and ν^2, respectively. The input sequence $\boldsymbol{x}$ is subject to the average power constraint according to $\frac{1}{n}\sum_{i=1}^{n} E[x_i^2] \leq P_T$. Furthermore, we assume that the transmitter has a perfect knowledge of the channel state information (CSI), for both the intended (Bob) and the eavesdropper (Eve) links. This resembles the situation when Eve is not an hostile node, but simply another user of the network which is not the intended user.

In this configuration set, it has been shown in [13] that the average secrecy capacity can be obtained from (3) as

$$\begin{aligned} C = \max_{\mathcal{P} \text{ s.t. } \overline{P} \leq P_T} E_U \Bigg[&\log_2 \left(1 + \frac{P(\boldsymbol{h})|h_M|^2}{\eta^2} \right) \\ &- \log_2 \left(1 + \frac{P(\boldsymbol{h})|h_W|^2}{\nu^2} \right) \Bigg], \end{aligned} \tag{5}$$

where $U = \left\{ \boldsymbol{h} : \frac{|h_M|^2}{\eta^2} > \frac{|h_W|^2}{\nu^2} \right\}$ and $\boldsymbol{h} = (h_M, h_W)$ is a random vector having the same distribution as the marginal distribution of the process $\boldsymbol{h_i} = (h_{Mi}, h_{Wi})$ at one time instant. Further, $P(\boldsymbol{h})$ denotes the power allocation for a given realization of one channel pair $\boldsymbol{h}$, whereas $\mathcal{P} = \{P(\boldsymbol{h}) : \boldsymbol{h} \in U\}$ and $\overline{P}$ is the average power allocated for the set of realizations $\boldsymbol{h} \in U$. This formulation provides a solution in terms of average performances, thus from a statistical viewpoint. It should be noted that for arbitrarily large power $P(\boldsymbol{h})$, the capacity is upper bounded by $E_U \left[\log_2 \left(\frac{|h_M|^2 \nu^2}{\eta^2 |h_W|^2} \right) \right]$, which may assume small values. To increase performances, it has been shown that higher secrecy rates are achievable by exploiting the degrees of freedom in a multiple antenna system or a wideband multicarrier system.

In order to find the optimal power allocation that maximizes (5) with the power constraint, we can exploit the fact that the argument in (5) is a concave function of $\mathcal{P}$. Therefore, the optimal power allocation $P^*(\boldsymbol{h})$ that provides the secrecy capacity in (5), for a given channel realization pair (h_M, h_W), can be obtained via the Karush–Kuhn–Tucker (KKT) conditions as follows

$$P^*(\boldsymbol{h}) = \begin{cases} \frac{1}{\lambda \ln 2} - \frac{\eta^2}{|h_M|^2}, & \text{if } |h_W|^2 = 0, \lambda < \frac{1}{\ln 2}\frac{|h_M|^2}{\eta^2}, \\ \frac{1}{2}\sqrt{\left(\frac{\nu^2}{|h_W|^2} - \frac{\eta^2}{|h_M|^2}\right)\left(\frac{4}{\lambda \ln 2} + \frac{\nu^2}{|h_W|^2} - \frac{\eta^2}{|h_M|^2}\right)} & \\ -\frac{1}{2}\left(\frac{\nu^2}{|h_W|^2} + \frac{\eta^2}{|h_M|^2}\right), & \\ & \text{if } |h_W|^2 > 0, \frac{|h_M|^2}{\eta^2} > \frac{|h_W|^2}{\nu^2}, \\ & \lambda < \frac{1}{\ln 2}\left(\frac{|h_M|^2}{\eta^2} - \frac{|h_W|^2}{\nu^2}\right), \\ 0, & \text{otherwise}, \end{cases} \tag{6}$$

where λ is chosen to satisfy the power constraint $\overline{P}(\boldsymbol{h}) = P_T$. It can be seen from (6) that the optimal power allocation is not the water filling solution and this is in contrast to what we find without the secrecy constraint. The solution in (6) will depend on the specific fading channel (h_{Mi} and h_{Wi}) statistics, where stationary and ergodic conditions are assumed.

In the PLC context, the formulation above for the computation of the average secrecy rate, applies in three possible scenarios: (i) a scenario where we consider a given triplet of nodes X (Alice), Y (Bob) and Z (Eve) and the channels X–Y and X–Z are narrow band time variant (for instance because of a change in the loads); (ii) a scenario where we consider a given intended transmission link, i.e., a given pair (X, Y), and the eavesdropper Z changes with time; (iii) a scenario where we want to compute the average secrecy rate with an average power constraint over the ensemble of possible triplets (X, Y, Z) in a certain network.

The results in (5) and (6) are also computed in [13]. Further, the secrecy capacity and the optimal power allocation, when transmission occurs over M orthogonal additive white Gaussian noise (AWGN) sub-channels or over a discrete-time memoryless fading channel, are derived in [14]. In [15], the secrecy capacity of a quasi-static Rayleigh fading channel in terms of outage probability is investigated. Lastly, [16] provides an analytical formulation of the secrecy capacity and derives the optimal power allocation for multi-carrier, multi-antenna and multiple users scenarios.

IV. Numerical Results and Comparisons

As stated in section III-B, the solution in (6) applies to a general fading channel. To make a comparison between the wireless channel and the PLC channel, we assume for the former Rayleigh fading, while for the latter Log-normal fading. It has been shown that the Log-normal distribution fits well the statistics of the channel gain in some scenarios [6].

A. Effect of Channel Statistics

In this section, we consider two different types of wiretap channel. First a Rayleigh fading wiretap channel, where h_M and h_W are zero mean proper complex Gaussian random variables with variances 1. Hence, $|h_M|^2$ and $|h_W|^2$ are exponentially distributed with parameter 1. Then, we consider a Log-normal fading wiretap channel, where $|h_M|^2$ and $|h_W|^2$ have a Log-normal distribution with parameters μ and σ^2: $h_M, h_W \in \text{Log-}\mathcal{N}(\mu, \sigma^2)$. In order to perform a comparison between these two types of fading channels (Rayleigh and Log-normal), we choose μ and σ^2 so that the Log-normal fading shows the same mean and variance of the Rayleigh fading channel. Thus, knowing that the exponential distribution has mean λ^{-1} and variance λ^{-2} and that the Log-normal distribution has mean $e^{\mu+\sigma^2/2}$ and variance $(e^{\sigma^2}-1)e^{2\mu+\sigma^2}$, we obtain $\mu = -\ln(\lambda\sqrt{2})$ and $\sigma^2 = \ln(2)$. The AWGN is assumed to have unit variance.

Fig. 3 shows the comparison between the average channel capacity, achieved without the secrecy constraints, and the average secrecy capacity, in [bit/symb/Hz], w.r.t. the total power constraint P_T in decibel assuming Log-normal fading. The average channel capacity exponentially increases with the increase of the total available power P_T and so with the increase of the signal-to-noise ratio (SNR). Conversely, the secrecy capacity is upper bounded by a certain value, as pointed out in section III-B. Thus, the gap goes to infinity as the SNR increases.

A performance comparison between the two types of fading channels aforementioned is depicted in Fig. 4 where we analyze the secrecy rate achieved by the optimal power allocation and the secrecy rate achieved by the uniform power allocation (i.e., allocating the same power for all channel states $\boldsymbol{h} \in U$) for both the Rayleigh and Log-normal wiretap channels. It can be seen that the uniform power allocation provides worse performances than the optimal power allocation for both fading statistics. However, for the SNRs of interest, while the gap between these two power allocation strategies remains almost constant for the Rayleigh fading case, for the Log-normal case the gap decreases. Note that in the Rayleigh fading channel without the secrecy constraint, the uniform power allocation can be close to optimum even for moderate SNRs. The secrecy rate goes to zero as the available power decreases, instead, for high power constraints, the secrecy rate is upper bounded (as seen in Fig. 3) by the same value for both power allocations, i.e., optimal and uniform. Finally and importantly, it should be noted that the secrecy rate for the Log-normal fading channel is always lower than the secrecy rate for the Rayleigh fading channel. This also applies to the secrecy rate bound achieved for high SNR. Therefore, this result makes us to believe that the secrecy rate of typical PLC channels characterized by a Log-normal fading statistics is lower than the one achievable in wireless channels.

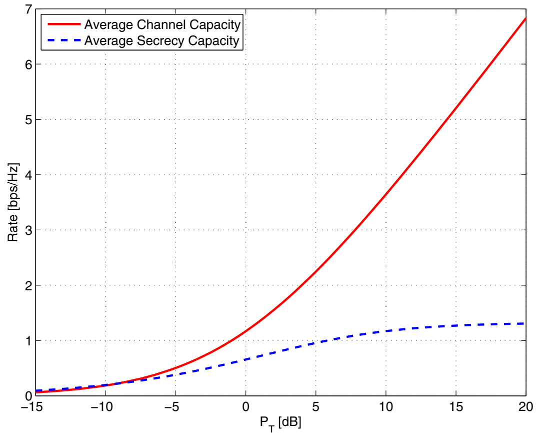


Fig. 3. Comparison between the average channel capacity (without secrecy constraints) and the average achievable secrecy capacity for transmission from Alice to Bob in a Log-normal fading wiretap channel.

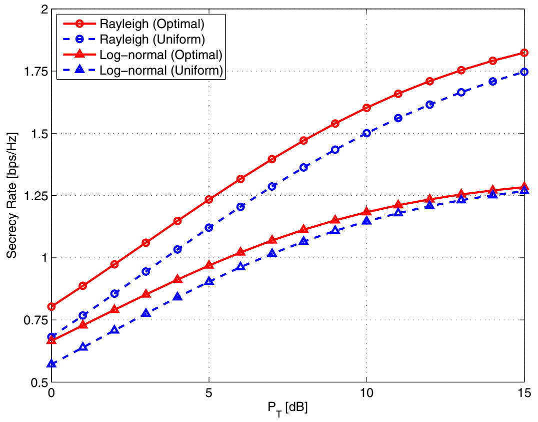


Fig. 4. Comparison between the achievable secrecy rate, for both optimal and uniform power allocation, for the two different types of analyzed fading channel statistics, Rayleigh and Log-normal.

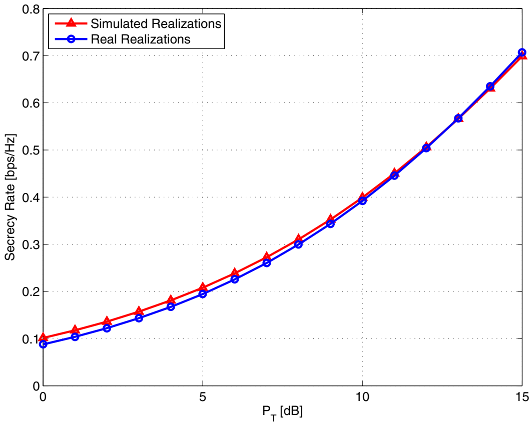


Fig. 5. Comparison between the average secrecy rate achieved when considering the channel measures (real realizations) versus the simulated channel realizations (generated with the same channel statistical parameters).

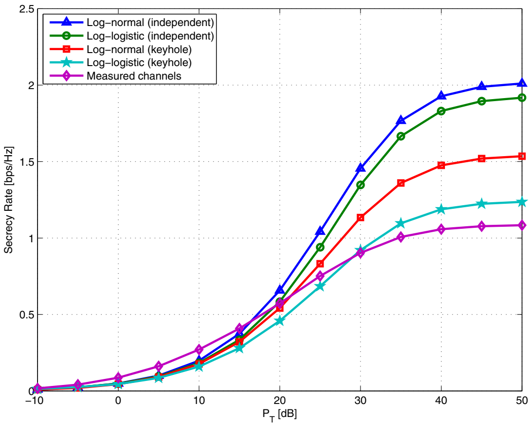


Fig. 6. Comparison between the average secrecy rate achieved when considering the channel measures (real realizations), the keyhole effect and the independent channels (with the same statistical parameters) for both the Log-logistic and the Log-normal fading channels.

To validate the above theoretical results and to dig further into the problem, in the next sections we will consider the data acquired in experimental channel measurement campaigns.

B. In-Ship Channel Measures

In this section we report numerical results obtained by using the channel measured in a cruise ship [17] in the frequency range $0-50$ MHz. The considered topology has a star structure, i.e., channels were acquired in the link from the substation switchboard to the distribution board, and from the distribution board to the room panel. Thus the model in Fig. 2(b) applies.

Since we are considering a narrow band channel model, we use the average channel gain (ACG) as a representation of the channel. The ACG for the r-th acquisition has been computed as follows

$$ACG(r) = \frac{1}{N}\sum_{c=0}^{N-1}|H(r,c)|^2, \qquad (7)$$

where $H(r,c)$ identifies the channel frequency response at the c-th measured frequency.

The analysis of the ACG reveals that it can be well fitted by a Log-normal distribution with parameters $\mu \cong -5.7$ and $\sigma^2 \cong 2.1$. A comparison between the achievable secrecy rate that is obtained with the Log-normal fit and with the real channels is shown in Fig. 5. The figure shows a good match between theoretical and experimental results. The slight discrepancy at low SNRs is amenable to the fact that the Log-normal fit is an approximation and the measured channels exhibit some small correlation. The effect of channel correlation is discussed in the next section.

C. In-Home Channel Measures

As pointed out in Section II-3, in a PLC network the channels are correlated as the result of sharing the same tree structure grid. In fact some users may share the same section of wires. To investigate this, we consider the in-home measures that were presented in [18] from the results of an experimental measurement campaign. The considered frequency range is $2-100$ MHz, as done in [19]. Also in this case we compute the ACG for each realization as in (7). Then, we evaluate the probability density function (pdf) of the ACG fitting different types of distributions (i.e. normal, exponential, gamma, ...) to our data. Interestingly, in this case the best fit is not the Log-normal but rather the Log-logistic distribution with parameters $\mu \cong -6.22$ and $\sigma^2 \cong 0.46$. This confirms that Log-normal fading is not always a good representation of the PLC channel.

The comparison in terms of secrecy rate with optimal power allocation among the real and simulated Log-logistic channel realizations is depicted in Fig. 6. In particular, in this first comparison the simulated channels are assumed to be independent. The comparison shows that there is a large discrepancy between experimental data and simulated channels. The discrepancy would be even higher if we assume a Log-normal fading distribution as Fig. 6 shows.

To make another comparison we also generate channels according to the keyhole model. That is, we generate three different Log-logistic fading processes associated to the channels from Alice to the branch point κ (*channel A*), from the branch point to Bob (*channel B*) and from the branch point to Eve (*channel E*), see Fig. 2(c). The processes are generated so that the cascades of the channels (Alice$-\kappa \Longrightarrow \kappa-$Bob and Alice$-\kappa \Longrightarrow \kappa-$Eve), have the same statistical parameters of the measured ACGs. Interestingly, with this channel model there is a better agreement between the experimental and simulated secrecy rates.

For comparison we also consider a keyhole channel obtained from the product of Log-normal segments. In such a case, as Fig. 6 shows, there still exists a discrepancy with the experimental data. It should be noted that in the low and mid power range, the rate achieved for the channel measures outweighs the others. This may be due to correlation phenomena which are not taken into account in our simple keyhole channel model.

As a final remark, the secrecy rate obtained with the Log-

logistic channel model (and with the experimental data) is lower than that achieved assuming a Log-normal distribution.

V. Conclusion

We have discussed physical layer security in terms of average secrecy rate in a wiretap channel. We have presented some results obtained in the wireless communication context and we have shown how they can be applied in the PLC context. We have highlighted that in PLC, channel fading is not Rayleigh distributed, rather it is Log-normal or it can have other statistics. In fact we have shown that measured channels in a cruise ship have a Log-normal average channel gain, while the measured channels in a house are better fitted by a Log-logistic distribution. As a consequence, the average secrecy rate (under AWGN and with an average power constraint) is lower than that attainable in Rayleigh fading. This is not all, since the secrecy rate is influenced by the correlation between the intended and the eavesdropper channels. In-home power line networks exhibit a tree structure, so that the communication links may share part of the same wires giving rise to a keyhole channel effect and moreover to channel correlation. Consequently, the secrecy rate can diminish further. Our analysis has been done assuming narrow band transmission and perfect CSI knowledge. It is expected that improved secrecy rates are attainable in wide band channels by the exploitation of the frequency diversity. However, a performance loss may be introduced by partial or imperfect CSI knowledge at the transmitter. The analysis of this paper can be extended to the case of periodically time variant channels. Herein, the channels have been considered time invariant since in the scenarios where measures were made, this assumption holds true.

References

[1] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical Layer Security in Wireless Networks: A Tutorial," *IEEE Wireless Communications*, vol. 18, no. 2, pp. 66–74, April 2011.

[2] C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, October 1949.

[3] A. D. Wyner, "The Wire-Tap Channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, October 1975.

[4] I. Kalet, "The Multitone Channel," *IEEE Transactions on Communications*, vol. 37, no. 2, pp. 119–124, February 1989.

[5] A. M. Tonello and F. Versolatto, "Bottom-Up Statistical PLC Channel Modeling – Part I: Random Topology Model and Efficient Transfer Function Computation," *IEEE Transactions on Power Delivery*, vol. 26, no. 2, pp. 891–898, April 2011.

[6] ——, "Bottom-Up Statistical PLC Channel Modeling – Part II: Inferring the Statistics," *IEEE Transactions on Power Delivery*, vol. 25, no. 4, pp. 2356–2363, October 2010.

[7] I. Csiszár and J. Körner, "Broadcast Channels with Confidential Messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[8] D. Chizhik, G. J. Foschini, M. J. Gans, and R. A. Valenzuela, "Keyholes, Correlations, and Capacities of Multielement Transmit and Receive Antennas," *IEEE Transactions on Wireless Communications*, vol. 1, no. 2, pp. 361–368, April 2002.

[9] D. Chizhik, G. J. Foschini, and R. A. Valenzuela, "Capacities of Multi-Element Transmit and Receive Antennas: Correlations and Keyholes," *Electronics Letters*, vol. 36, no. 13, pp. 1099–1100, 22 June 2000.

[10] D. Gesbert, H. Bölcskei, D. Gore, and A. J. Paulraj, "Outdoor MIMO Wireless Channels: Models and Performance Prediction," *IEEE Transactions on Communications*, vol. 50, no. 12, pp. 1926–1934, December 2002.

[11] L. Lampe and A. J. H. Vinck, "Cooperative Multihop Power Line Communications," in *Proc. of 16th IEEE International Symposium on Power Line Communications and Its Applications (ISPLC 2012)*, Vancouver, BC, Canada, 27-30 March 2012, pp. 1–6.

[12] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian Wire-Tap Channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, July 1978.

[13] Y. Liang and H. V. Poor, "Secure Communication over Fading Channels," in *Proc. of 44th Annual Allerton Conference on Communication, Control and Computing*, University of Illinois, Monticello, IL, 27-29 September 2006. [Online]. Available: http://arxiv.org/abs/0708.2733v1

[14] Z. Li, R. Yates, and W. Trappe, *Securing Wireless Communications at the Physical Layer*. Springer US, 2010, ch. 1: Secrecy Capacity of Independent Parallel Channels, pp. 1–18. [Online]. Available: http://dx.doi.org/10.1007/978-1-4419-1385-2_1

[15] J. Barros and M. R. D. Rodrigues, "Secrecy Capacity of Wireless Channels," in *Proc. of IEEE International Symposium on Information Theory*, July 2006, pp. 356–360.

[16] E. A. Jorswieck, A. Wolf, and S. Gerbracht, *Trends in Telecommunications Technologies*. InTech, March 2010, ch. 20: Secrecy on the Physical Layer in Wireless Networks, pp. 413–435. [Online]. Available: http://sciyo.com/articles/show/title/secrecy-on-the-physical-layer-in-wireless-networks

[17] M. Antoniali, A. M. Tonello, M. Lenardon, and A. Qualizza, "Measurements and Analysis of PLC Channels in a Cruise Ship," in *Proc. of IEEE International Symposium on Power Line Communications and Its Applications (ISPLC 2011)*, Udine, Italy, 3-6 April 2011, pp. 102–107.

[18] F. Versolatto and A. M. Tonello, "PLC Channel Characterization up to 300 MHz: Frequency Response and Access Impedance," in *Proc. of IEEE Global Telecommunications Conference (GLOBECOM 2012)*, Anaheim, California, USA, 3-7 December 2012.

[19] ——, "On the Relation Between Geometrical Distance and Channel Statistics in In-Home PLC Networks," in *Proc. of 16th IEEE International Symposium on Power Line Communications and Its Applications (ISPLC 2012)*, Beijing, China, 27-30 March 2012, pp. 280–285.