Published in IET Communications
Received on 6th June 2013
Revised on 5th September 2013
Accepted on 23rd September 2013
doi: 10.1049/iet-com.2013.0472

Special Issue: Secure Physical Layer Communications

ISSN 1751-8628

Physical layer security in power line communication networks: an emerging scenario, other than wireless

Alberto Pittolo, Andrea M. Tonello

Department of Electrical, Mechanical and Management Engineering (DIEGM) University of Udine, Via delle Scienze 208, Udine 33100, Italy
E-mail: tonello@uniud.it

Abstract: The authors consider the secure transmission of information over power line communication (PLC) networks. The focus is on the secrecy guaranteed at the physical layer, named physical layer security (PLS). Although PLS has been deeply investigated for the wireless case, it is not the same for the PLC environment. Thus, starting from the knowledge in the wireless context, the authors extend the results to typical PLC scenarios. In particular, the PLC channel statistics is evaluated and a performance comparison among PLC and wireless channels is performed, in terms of secrecy rate distribution. For the PLC case, the secrecy rate distribution, under a total power constraint, is evaluated for both optimal and uniform power distributions in broadband channels. To provide experimental evidence, the authors consider channel measures obtained in an in-home measurement campaign. The underlying network presents a tree topology, which introduces frequency and spatial correlation among channels, and suffers from the keyhole effect, generated by branches that depart from the same node. As shown by the numerical results, these effects can reduce the secrecy rate. Finally, the authors evaluate the secrecy rate region for the multi-user broadcast channel considering both simulated channel realisations and experimental channel measures.

1 Introduction

The communication over the power delivery infrastructure is known as power line communication (PLC). PLC exploits the existing power lines to convey high-speed data content. This leads to a considerable saving in costs and time. Also, for this reason PLC has gained increasingly momentum and popularity in recent times. There are many applications of PLCs, for example, extension or deployment of local area networks, home networking, home automation, remote metering and applications in the Smart Grid context. Essentially, the PLC devices can be grouped into two categories, that is, narrow-band and broadband PLC devices, according to the bit-rate they can achieve. Typically, broadband PLC devices adopt multi-carrier modulation in the form of orthogonal frequency division multiplexing (OFDM) at the physical layer. These devices have been developed with the aim of offering multimedia services to domestic or small office environments. A relevant example of commercial devices is the one compliant with the HomePlug AV (HPAV) specifications [1]. HPAV has been used as a baseline for the physical layer specification of the IEEE P1901 standard [2].

As in wireless cellular communications, PLCs are intrinsically broadcast, thus the channels are shared between the users in the network. In this scenario, the secrecy plays a crucial role in order to ensure information confidentiality, since, for instance, a transmitter wishes to send confidential information to different users, as Fig. 1 shows. The secrecy can be provided in two main ways: at the high levels of the ISO/OSI stack model or at the physical layer. The first method concerns a cryptographic approach based on algorithms such as the data encryption standard (DES) or the RSA. Whereas, the second exploits the physical medium, its time/frequency diversity and the differences between the user's links in order to provide security. This concept, known as physical layer security (PLS) [3], can complement and enhance the secrecy provided by other layers.

Basically, the approaches concerning the PLS are: the information-theoretic security and the complexity-based security. The information-theoretic approach [4] assumes the adversary to have unlimited computational resources, ensuring that absolutely no information is released to him. Otherwise, complexity-based cryptography assumes the adversary to have limitations on how much computation can be performed. Thus, when an adversary witnesses an encrypted message (the ciphertext), the necessary computational resources to decode the original message (the plaintext) render the disclosure of the information practically unfeasible. The principle underlying the information-theoretic approach to confidential communications is widely accepted as the strictest notion of security. Moreover, the optimal power allocation problem with secrecy constraints, from an information-theoretic viewpoint, resembles the general resource allocation problem in multi-carrier systems [5].

PLS exploits the time/frequency/spatial diversity offered by the medium to enhance the transmission security. The highly uncorrelated channel assumption holds in wireless networks, but it is no longer valid when PLC networks are considered. Indeed, PLC networks have a tree topology where part of the wires are shared among communication links, see Fig. 1. In this configuration, the links share part

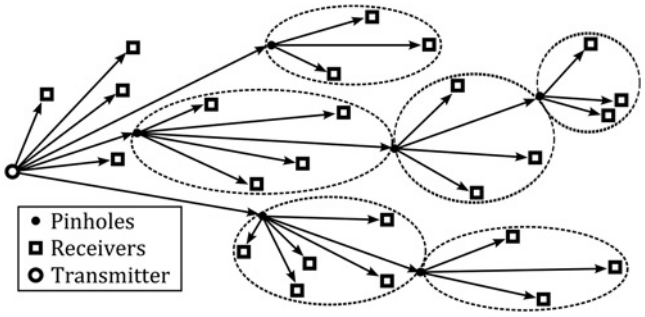

Fig. 1 *Scheme of a generic PLC network topology*

of the wires up to a node (pinhole) where branches are attached, giving rise to what is known as keyhole effect [6–8]. The keyhole effect in cooperative multi-hop PLCs has been recently studied in [9]. This phenomenon and the underlying PLC network topology introduce frequency and/or spatial correlation among the channel responses (mainly due to cross-talks and coupling effects). Furthermore, the sub-channel frequency responses (in multi-carrier transmission) are correlated and affected by fading which does not have a Rayleigh amplitude distribution, rather it is log-normal. Consequently, the achievable performance may differ from that achieved in wireless channels, which are usually affected by uncorrelated Rayleigh fading.

Although PLS has been deeply investigated for the wireless case, it is not the same for the PLC case. The maximum achievable secrecy rate (secrecy capacity) over a quasi-static Rayleigh fading channel (wireless case) is analysed in [10, 11]. Furthermore, [12] provides an analytic formulation of the secrecy rate and derives the optimal power allocation for multi-carrier, multi-antenna and multiple users scenarios. However, these studies focus on the wireless scenario, where the channel statistics is not the same as in PLC networks and the negative effects of spectral/spatial correlation, due to the network configuration, are less noticeable. The achievable rate in PLC networks, without secrecy constraints, for both experimental and statistical data, is investigated in [13, 14]. Instead, a preliminary analysis of the achievable secrecy rate in narrow-band PLC networks is presented in [15].

The purpose of this paper is to address fundamental and practically relevant questions related to many challenges arising from secure physical layer communications in PLC scenarios. More specifically, the aim is to investigate PLS in multi-carrier and multi-user broadcast systems. The effect of the channel statistics on the achievable secrecy rate is analysed. A comparison with the wireless scenario is made and enlightening results are reported by using a statistical PLC channel model as a tool to infer the effect of certain phenomena, as the spatial/frequency correlation and the keyhole structure, and to explain the performance degradation achieved with a set of measured channels.

The rest of the paper is organised as follows: Section 2 analyses the wiretap channel under an information-theoretic viewpoint, defining the secrecy capacity. Then, in Sections 3 and 4, the secrecy rate optimisation problem is discussed and solved, deriving the optimal power allocation for the multi-carrier and multi-user scenarios, respectively. Section 5 provides an analysis of numerical results. Herein, the statistics, frequency and spatial correlation of the channel measures, as well as the effect of frequency correlation and keyhole effect on the secrecy rate, are evaluated. Afterwards, a comparison between the performance of wireless and PLC channels is made. Moreover, both the optimal and the uniform power allocation are considered assuming multi-carrier transmission. The secrecy region for the multi-user broadcast channel is discussed. Finally, the conclusions follow.

2 Wiretap channel

The scheme in Fig. 2 represents 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. This system is named wiretap channel [16].

There exist three main types of channel configurations; each models a different real scenario, which can be incorporated in a general representing scheme, depicted in Fig. 2. The three models and their features are listed below.

1. *Wyner:* This is the simplest model where the channel B in Fig. 2 is assumed ideal and Eve has access to a degraded (or noisier) version of the channel outputs that reach the legitimate receiver (Bob) through the main channel (channel A). Indeed, Wyner's wiretap channel [16] is also referred to degraded wiretap channel and this assumption simplifies the analysis and the derivation of the secrecy limits [17].
2. *Csiszár and Körner* [18]: It is a more general model that considers a broadcast scenario, assuming channel A as ideal, whereas the main (channel B) and the wiretapper (channel E) channels are independent from each other. This model is suitable for the representation of a star structure PLC topology as well as typical wireless communication networks where rich scattering is such that the two channels (channel B and channel E) are affected by statistically independent fading.
3. *Keyhole channel:* This model (Fig. 2) is the most general, since it includes both the above models by assuming channel B or channel A as ideal, as previously discussed. The signal x is transmitted over the channel A and reaches the receivers Bob and Eve (via channel B and channel E, respectively) moving through the branch point κ, named pinhole. We refer to this system configuration as keyhole channel since channel B and channel E depart from the same pinhole κ. This model well represents a tree or bus network configuration structure, which is very common in PLC. In multiple-input multiple-output (MIMO) transmission systems, the channels affected by the keyhole effect exhibit a rank-deficiency, which implies a MIMO channel capacity degradation [6–9].

2.1 Preliminaries

From an information-theoretic viewpoint, Alice's transmitted signal x and Bob's and Eve's received signals y and z,

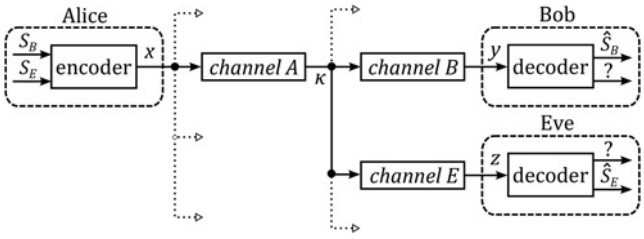

Fig. 2 *General wiretap channel model*

doi: 10.1049/iet-com.2013.0472

respectively, are modelled as random variables (see Fig. 2). In this system, Alice sends a secret message S_B to Bob or S_E to Eve (denoted generically with S) randomly chosen from the message set $\mathcal{S} = \{1, \ldots, M\}$, with $M = 2^{nR_S}$, over n channels uses, where R_S is the secrecy rate in bits per channel use.

An (M, n)-code consists of an encoder at the transmitter, which maps the secret message S into a codeword $\boldsymbol{x}^n$, and a decoding function at the legitimate receiver, which converts the received codeword $\boldsymbol{y}^n$ into the message $\hat{S}_B$. Eve overhears the output $\boldsymbol{z}^n$. Her residual uncertainty regarding S is generally expressed by the equivocation rate $R_e = H(S|\boldsymbol{z}^n)/n$, where $H(\cdot)$ denotes the entropy. The secrecy rate R_S is said to be achievable if for any $\varepsilon > 0$, there exists a sequence of $(2^{nR_S}, n)$ codes such that for any $n \geq n(\varepsilon)$, the average decoding error probability becomes arbitrarily small and the equivocation rate satisfies $R_e \geq R_S - \varepsilon$ [12, 19]. Perfect secrecy requires $R_e = R_S$, hence $\varepsilon = 0$. Thus, the secrecy capacity C_S is the maximum secrecy rate R_S such that the rate-equivocation pair $(R_S, R_e = R_S)$ is achievable.

For a general Gaussian wiretap channel (as well as for the keyhole channel), the secrecy capacity C_S is defined as [19]

$$C_S = \max_{f_x \in \mathcal{F}} [I(x; y) - I(x; z)]^+ \tag{1}$$

where f_x is the probability density function (pdf) of the channel input x, whereas $\mathcal{F}$ is the set of all pdfs at the channel input, under a power constraint. Instead, $[q]^+ = \max(q, 0)$, thus C_S is set to zero if Eve has a better channel realisation than Bob. The mutual information terms $I(x; y)$ and $I(x; z)$ are convex in f_x, hence, a lower bound R_S for the secrecy capacity in (1) can be formulated as [12]

$$C_S \geq \left[\max_{f_x \in \mathcal{F}} [I(x; y)] - \max_{f_x \in \mathcal{F}} [I(x; z)]\right]^+ = R_S \tag{2}$$

The lower bound R_S is often used for a simplified calculation of achievable secrecy rates since it is known how to maximise the mutual information terms. Furthermore, the PLS problem turns out to be an optimisation problem that aims to maximise the rate R_S between legitimate users, under a constraint on the maximum information R_e obtainable from unauthorised users.

3 Multi-carrier systems

The general system in Fig. 2 can be straightforwardly extended to a multi-carrier or to a multi-user scenario. In the following, the multi-carrier scenario is investigated, defining the system model, the optimisation problem formulation and its optimal solution. Afterwards, we discuss typical PLC application scenarios in which this optimal solution, deeply studied in the wireless case, can be applied.

3.1 System model

Consider a multi-carrier wiretap channel where Alice wants to send a confidential message to Bob in a system with N parallel sub-channels, keeping it secret from the eavesdropper Eve. This systems is equivalent to the scheme in Fig. 2 used N times in parallel, which can be mathematically written as

$$\begin{aligned} y_c &= h_{M,c} \cdot x_c + n_{M,c} \\ z_c &= h_{W,c} \cdot x_c + n_{W,c} \end{aligned} \tag{3}$$

where $c = 1, \ldots, N$ is the sub-channel index. On each sub-channel, Alice transmits the signal x_c, while Bob receives the signal y_c and Eve receives the signal z_c. The channels coefficients are identified by $h_{M,c}$ and $h_{W,c}$, whereas the noise variables by $n_{M,c}$ and $n_{W,c}$, for the main and the eavesdropper link, respectively.

In reference to Fig. 2, $h_{M,c}$ can be viewed as the product of the gains of *channel A* and *channel B*, whereas $h_{W,c}$ as the product of the gains *channel A* and *channel E*. Thus, this model can describe each one of the three different models described in Section 2. For the sake of simplicity, we define

$$\alpha_c = |h_{M,c}|^2 \quad \text{and} \quad \beta_c = |h_{W,c}|^2 \tag{4}$$

where α_c and β_c are the channel power gains for the main and the eavesdropper channel, respectively.

Assumptions: For the rest of the paper, unless otherwise stated, we make the following assumptions: (i) For each sub-channel the variables x_c, $n_{M,c}$ and $n_{W,c}$ are statistically independent. (ii) The noise variables $n_{M,c}$ and $n_{W,c}$ are circular symmetric i.i.d. complex Gaussian with zero mean and variance σ^2. (iii) The power at the transmitter is constrained to $\sum_{c=1}^{N} |x_c|^2 \leq P_T$, where P_T is the total available power. Furthermore, we assume that Bob and Eve perfectly know their individual channel realisation and that Alice has a full channel state information (CSI) knowledge. Thus, Alice has access to the channel gains of both the legitimate receiver (Bob) and the eavesdropper (Eve). The CSI knowledge is gained via the insertion of training symbols in the transmitted signal, which enables the receiver to evaluate the channel attenuation (or gain). Hence, the channel information is sent back to the transmitter. This resembles the situation where Eve is not a hostile node, but simply another user of the network, which is not the intended user.

3.2 Optimisation problem formulation

In the system model described in Section 3.1, the secrecy rate can be computed according to (2) as [19]

$$R_S(\boldsymbol{P}_A) = B \sum_{c=1}^{N} \left[\log_2\left(1 + \frac{\alpha_c P_{A,c}}{\sigma^2}\right) - \log_2\left(1 + \frac{\beta_c P_{A,c}}{\sigma^2}\right)\right]^+ \tag{5}$$

where B is the sub-channel bandwidth, whereas $P_{A,c}$ is the power allocated by Alice on sub-channel c. The powers on each sub-channel are written in a vector $\boldsymbol{P}_A = [P_{A,1}, \ldots, P_{A,N}]$, which denotes the power allocation strategy adopted at the transmitter for a given channel realisation. It can be noted that for arbitrarily large powers $\boldsymbol{P}_A$, the secrecy rate is upper bounded by $\sum_{c=1}^{N} [\log_2(\alpha_c/\beta_c)]^+$, which can be small if the channel does not provide enough diversity.

The secrecy rate optimisation problem for the multi-carrier system under a total power constraint is given by

$$\max_{\boldsymbol{P}_A} R_S(\boldsymbol{P}_A) \quad \text{subject to} \quad \begin{cases} \sum_{c=1}^{N} P_{A,c} \leq P_T \\ P_{A,c} \geq 0 \end{cases} \tag{6}$$

This is a non-convex optimisation problem with the objective function R_S. It is shown in [20] that the optimal power allocation that solves (6) is to allocate zero power on the

doi: 10.1049/iet-com.2013.0472

sub-channels where the main channel is worse than the wiretapper (i.e. $\alpha_c \leq \beta_c$). The resulting problem is convex, hence it can be easily solved via the Karush–Kuhn–Tucker (KKT) conditions [21]. Consequently, the optimal power allocation that solves (6) is given by (7)

The parameter $\lambda > 0$ is chosen to satisfy the power constraint $\sum_{c=1}^{N} P_{A,c} \leq P_T$. In contrast to a generic optimisation problem (without secrecy constraints), the solution in (7) is not the water-filling solution.

3.3 PLC application scenarios

The computation of the secrecy rate formulated in (7) applies to a given channel realisation. Thus, this result can be applied to any communication system and in particular to the PLC scenario. It is however of interest to investigate the performance, considering a wide set of channels and therefore to carry out a statistical analysis of the secrecy rate. In a real PLC scenario, the solution in (7) can be averaged among the channel realisations providing the average secrecy rate, or more in general, the cumulative distribution function. In particular, this analysis is representative of three possible PLC 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 broadband time-variant (for instance, because of change in the loads); (ii) a scenario where we consider a given intended transmission link, that is, 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.

4 Multi-user broadcast systems

The results provided in Section 3 can be extended to the multi-user down-link case. In particular, in the broadcast channel that we consider, Alice wants to send K confidential messages to K receivers (users). The underlying PLC network can be represented as in Fig. 1. The basic network structure consists of a tree structure of star networks. Indeed, in Fig. 1, the arrows identify the communication links from the transmitter to the receiver through the different nodes. Whereas, the dashed circles highlight each of the star structure subnets, each one in cascade with another. Such a topology can be found in in-home PLC scenarios [22].

In the following, we consider a two-user (receivers) system as depicted in Fig. 2. In detail, Alice encodes the secret messages to Bob (S_B) and Eve (S_E) in a single transmitted signal x. Bob and Eve receive the signals, y and z, respectively, and they are able to decode only their intended message. The dashed arrows represent the possible presence of additional links in the considered network.

Assuming a multi-carrier system with N parallel sub-channels, the system model is equivalent to the model in (3), but in this case Bob and Eve can eavesdrop each other. All the assumptions listed in Section 3.1 still hold, but the constraint on the transmitted power translates into

$$\sum_{c=1}^{N} (P_{B,c} + P_{E,c}) \leq P_T \tag{8}$$

where $P_{B,c}$ and $P_{E,c}$ are the powers allocated by Alice for transmission to Bob and Eve on the cth sub-channel, respectively. Furthermore, in reference to Fig. 2, $h_{M,c}$ can be viewed as the product of the channel gains *channel A* and *channel B*, whereas $h_{W,c}$ as the product of the gains *channel A* and *channel E*.

4.1 Optimisation problem formulation

In the system configuration above, the achievable secrecy rates for the transmission to Bob and Eve are the sum of the secrecy rates over all sub-channels, given by

$$\begin{aligned} R_{S,B}(\boldsymbol{P}_B, \boldsymbol{P}_E) &= B \sum_{c=1}^{N} \left[\log_2\left(1 + \frac{\alpha_c P_{B,c}}{\sigma^2 + \alpha_c P_{E,c}}\right) \right. \\ &\quad \left. - \log_2\left(1 + \frac{\beta_c P_{B,c}}{\sigma^2}\right)^{+} \right] \quad \text{and} \\ R_{S,E}(\boldsymbol{P}_B, \boldsymbol{P}_E) &= B \sum_{c=1}^{N} \left[\log_2\left(1 + \frac{\beta_c P_{E,c}}{\sigma^2 + \beta_c P_{B,c}}\right) \right. \\ &\quad \left. - \log_2\left(1 + \frac{\alpha_c P_{E,c}}{\sigma^2}\right) \right]^{+} \end{aligned} \tag{9}$$

This is a worst-case assumption (in terms of secrecy) since we assume that the wiretapper (Eve or Bob, respectively) performs successive interference cancellation [12]. Thus, the hostile user detects his own data, afterwards he subtracts it from the received signal and tries to decode the message for the intended user.

In this case, our goal is to maximise the sum of the individual secrecy rates, named sum secrecy rate, which is given by

$$R_S^{\text{sum}}(\boldsymbol{P}_B, \boldsymbol{P}_E) = R_{S,B}(\boldsymbol{P}_B, \boldsymbol{P}_E) + R_{S,E}(\boldsymbol{P}_B, \boldsymbol{P}_E) \tag{10}$$

where $R_{S,B}$ and $R_{S,E}$ are the secrecy rates from Alice to Bob and from Alice to Eve, respectively. The power allocation over the sub-channels for Bob and Eve are collected in the vectors $\boldsymbol{P}_B = [P_{B,1}, \ldots, P_{B,N}]$ and $\boldsymbol{P}_E = [P_{E,1}, \ldots, P_{E,N}]$, respectively. Since in this case there is more than one user, the secrecy rate becomes a secrecy rate region.

The corresponding optimisation problem is given by

$$\max_{\boldsymbol{P}_B, \boldsymbol{P}_E} R_S^{\text{sum}}(\boldsymbol{P}_B, \boldsymbol{P}_E) \quad \text{subject to} \quad \begin{cases} \sum_{c=1}^{N} (P_{B,c} + P_{E,c}) \leq P_T \\ P_{B,c} \geq 0 \\ P_{E,c} \geq 0 \end{cases} \tag{11}$$

$$P_{A,c} = \begin{cases} 0, & \text{if} \quad \alpha_c \leq \beta_c \\ \left[\sqrt{\left(\frac{\sigma^2(\alpha_c - \beta_c)}{2\alpha_c\beta_c}\right)^2 + \frac{1}{\lambda \ln 2} \frac{\sigma^2(\alpha_c - \beta_c)}{\alpha_c\beta_c}} - \frac{\sigma^2(\alpha_c + \beta_c)}{2\alpha_c\beta_c} \right]^{+}, & \text{otherwise} \end{cases} \tag{7}$$

doi: 10.1049/iet-com.2013.0472

It was shown in [20] that the optimal solution is to support only the best user per sub-channel. Thus, the power allocation per sub-channel $P_{A,c} = P_{B,c} + P_{E,c}$ becomes

$$P_{A,c} = \begin{cases} P_{B,c} & \text{if} \quad \alpha_c > \beta_c \\ P_{E,c} & \text{if} \quad \alpha_c < \beta_c \end{cases} \tag{12}$$

The case $\alpha_c = \beta_c$ is neglected since we assume a continuous distribution for the channel gain coefficients (in fading scenarios), thus $\Pr(\alpha_c = \beta_c) = 0$. The optimal power allocation which solves the optimisation problem in (11) can be derived from the formulation in (7) by replacing $(\alpha_c - \beta_c)$ with $(\max(\alpha_c, \beta_c) - \min(\alpha_c, \beta_c))$.

The optimisation problem in (11) can be extended to the optimisation of the weighted sum secrecy rate [23] defined as

$$R_S^{\text{wgh}}(\boldsymbol{P}_B, \boldsymbol{P}_E, \eta) = \eta R_{S,B}(\boldsymbol{P}_B, \boldsymbol{P}_E) + (1-\eta) R_{S,E}(\boldsymbol{P}_B, \boldsymbol{P}_E) \tag{13}$$

where the variable $0 \le \eta \le 1$ can guarantee a certain quality of service (QoS) to the users. The optimal power allocation for this optimisation problem is shown in (14)

It can be noted that the optimal power allocation is basically the same computed in (7), but it is assigned to a user or another depending on the channel realisations at sub-channel c and on the QoS parameter η.

5 Secrecy rate in PLC channels

The aim of this section is to evaluate the performance in terms of achievable secrecy rate in single-user and multi-user PLC scenarios, and compare it with the wireless scenario. The purpose is to identify the physical phenomena that affect real PLC networks. As pointed out in Section 2.3, PLC networks have a tree topology where part of the wires are shared among communication links. This introduces frequency and spatial correlation among the channel responses. Furthermore, the sub-channel frequency responses (in multi-carrier transmission) are affected by fading which does not have a Rayleigh amplitude distribution, rather it is log-normal. Consequently, the achievable secrecy rate may differ from that achieved in wireless channels, which are usually affected by uncorrelated Rayleigh fading. The impact of these effects is evaluated providing a channel model which enables the generation of channel responses that are statistically equivalent to measured channels. To this end, we take into account the experimental channel measures carried out in the measurement campaign presented in [22].

System assumptions: In this section, we consider a total of 1300 channel realisations acquired with an experimental measurement campaign in a number of houses. More details can be found in [22]. The considered frequency range is 2–28 MHz, which is compliant with the HomePlug AV standard specifications [1]. Multi-carrier transmission is assumed and, unless otherwise stated, the following assumptions hold: (i) multicarrier transmission with optimal power allocation under a total power constraint; (ii) additive white Gaussian noise (AWGN) and average signal-to-noise ratio (SNR) equal to 80 dB in the absence of attenuation introduced by the channel. It should be noted that typical PLC systems transmit with a uniform power spectral density (PSD) of −50 dBm/Hz and a noise PSD of −130 dBm/Hz. This yields an average SNR equal to 80 dB. Moreover, the PLC networks are often subjected to a composition of Gaussian and impulsive noise. Nevertheless, only AWGN is assumed in our analysis, as often done in PLC work, since we are interested in evaluating the effects introduced by the channel response only.

First, the experimental channel features, such as statistics, frequency and spatial correlation are evaluated. Then, a comparison in terms of secrecy rate is done, assuming different channel distributions with and without frequency/spatial correlation. The gains provided by optimal power allocation w.r.t. uniform power allocation are also discussed. Finally, the secrecy rate region in multi-user PLC systems is investigated.

5.1 Statistical analysis and correlation evaluation

Herein, we study the statistics of the channel frequency response. The measured channel gain statistics is assessed by comparing it with the major known distributions. In order to find the best fitting, the comparison is made in terms of likelihood function [24]. Moreover, the frequency and the spatial correlation among the channel measures is evaluated.

5.1.1 Statistics: The statistical analysis is performed by fitting the distribution of the absolute square value of the channel frequency response in linear scale (i.e. of the gains α_c, β_c). We fit the distribution of the measured gains with the well-known distributions: Exponential, Gamma, Log-normal, Normal, Rayleigh, Weibull and Log-logistic. Basically, for each distribution, we find the maximum likelihood estimates of the parameters that enable for the best fitting of the measured channel gains. We compute the likelihood function as follows [24]

$$\Lambda(\theta) = \prod_{x \in \mathbb{X}} f(\theta | x) \tag{15}$$

where $x \in \mathbb{X}$ is the set of measured samples, $f(\cdot)$ is the probability density function (pdf), while θ represents the parameters (mean and variance) of the fitting distribution. The higher the likelihood function, the better the parameters fit the measured distribution. The analysis is performed as a function of frequency. Fig. 3 shows the values of the logarithmic version of (15). We note that the log-normal distribution provides the highest likelihood value in the entire frequency range. Therefore, we can confirm the conclusion in [22], that is, the gain (in linear scale) of the measured data is log-normally distributed with good

$$P_{A,c} = \begin{cases} \left[\sqrt{\left(\dfrac{\sigma^2(\alpha_c - \beta_c)}{2\alpha_c\beta_c} \right)^2 + \dfrac{\eta}{\lambda \ln 2} \dfrac{\sigma^2(\alpha_c - \beta_c)}{\alpha_c\beta_c}} - \dfrac{\sigma^2(\alpha_c + \beta_c)}{2\alpha_c\beta_c} \right]^+ & \text{if} \quad \alpha_c > \beta_c \\ \left[\sqrt{\left(\dfrac{\sigma^2(\beta_c - \alpha_c)}{2\alpha_c\beta_c} \right)^2 + \dfrac{1-\eta}{\lambda \ln 2} \dfrac{\sigma^2(\beta_c - \alpha_c)}{\alpha_c\beta_c}} - \dfrac{\sigma^2(\alpha_c + \beta_c)}{2\alpha_c\beta_c} \right]^+ & \text{if} \quad \alpha_c < \beta_c \end{cases} \tag{14}$$

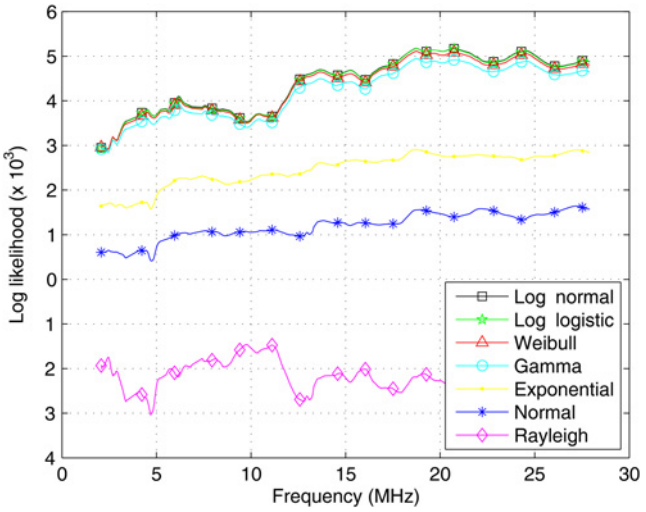

Fig. 3 *Log-likelihood value of the best fittings for the distribution of the measured amplitudes*

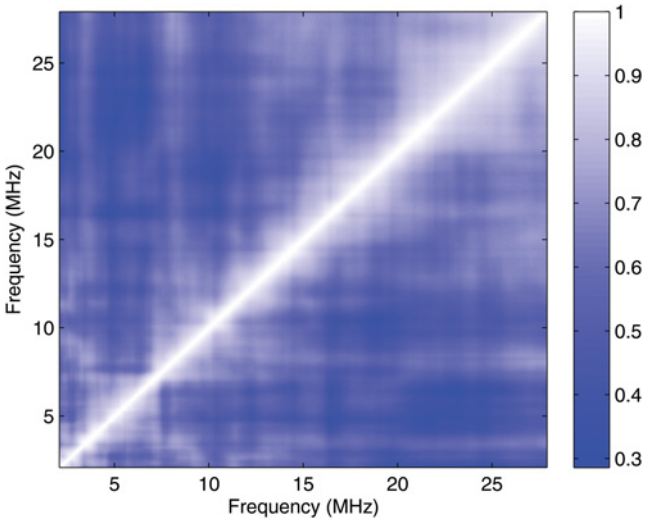

Fig. 4 *Representation of the frequency correlation matrix among sub-channels of the experimental channels in dB scale*

approximation. The log-logistic distribution performs similarly to the log-normal one. Furthermore, the Gamma and Weibull distributions are close as well. The reason is that these distributions exhibit similar shapes and the main differences are limited to the tails.

5.1.2 Frequency correlation: In reference to the frequency correlation, we evaluate the normalised co-variance matrix $\boldsymbol{R}_{gg}$ containing the pairwise co-variance coefficient between each pair of sub-channels (frequencies), as follows

$$R_{gg}(i,j) = \frac{C_{gg}(i,j)}{\sqrt{C_{gg}(i,i)C_{gg}(j,j)}} \tag{16}$$

where i, j are the sub-channel indexes and $\boldsymbol{C}_{gg}$ is the covariance matrix with elements given by

$$C_{gg}(i,j) = E\Big[(g(i) - \mu_i)(g(j) - \mu_j)\Big] \tag{17}$$

The operator $E[\cdot]$ denotes the expectation, $g(i)$, $g(j)$ are the channel gains and μ_i, μ_j their mean ($\mu = E[g]$), at the ith and jth frequency, respectively. The average is performed using the channel measures (realisations). In particular, we evaluate the correlation matrix of the logarithmic version of the channel gains which are with good approximation normally distributed. This allows us to easily generate a set of correlated log-normal random variables from the generation of a set of independent normal variables. The co-variance matrix for the channel measures in dB is depicted in Fig. 4. The figure shows how certain sub-channel frequencies are more correlated with all the others, such as those at 3, 8 MHz (horizontal and vertical white lines). Moreover, we can see a higher degree of correlation in the upper right regions, that is, at high frequencies. This is due to the crosstalk phenomena between wires, which becomes increasingly prominent at high frequencies.

5.1.3 Spatial correlation: Finally, we discuss the spatial correlation among the measured channels. To this end, we choose the channel measures assigning them to the main and to the wiretapper channel so that each channel pair has the same transmitting node (plug). Then, the correlation coefficient among these two channels in the frequency range 2–28 MHz is evaluated for each sub-channel, according to (16). Although not shown, we have observed how the channels are more correlated at certain frequencies, compared to other frequencies where they are practically uncorrelated.

5.2 Channel effects on the secrecy rate distribution

In this section, we investigate the effect of the channel statistics on secrecy rate. In particular, we compare the secrecy rate achieved in the measured channels with that achieved when the channels are generated according to a log-normal distribution under different assumptions, listed in the following. (a) *Independent channels:* The channels from Alice to Bob and to Eve are independently generated. (b) *Keyhole effect*: The channels are obtained by the product of log-normal channel realisations. That is, we generate three different log-normal channel realisations associated to the channels from Alice to the pinhole κ (*channel A*), from the pinhole to Bob (*channel B*) and from the pinhole to Eve (*channel E*), see Fig. 2. The processes are generated so that the cascade of the channels (Alice $-\kappa \Rightarrow \kappa-$Boband Alice$-\kappa \Rightarrow \kappa-$Eve) have the same statistical parameters of the measured channels. (c) *Spatial correlation*: The channels from Alice to Bob and to Eve are generated according to the measured correlation coefficient defined in Section 5.1.3. These channels do not exhibit frequency correlation. (d) *Frequency correlation*: The channels exhibit frequency correlation according to the measured links (see Section 5.1.2), but are spatially uncorrelated. (e) *Keyhole effect and frequency correlation*: The channels affected by the keyhole effect are generated starting from log-normal frequency-correlated channels. (f) *Spatially and frequency correlation*: We add to the channels realisations the correlation among frequencies and between the main and the wiretapper channels, which is what usually happens in real PLC networks.

The results of the comparison are shown in Fig. 5 in terms of complementary cumulative distribution function (CCDF). The figure shows that there is a high discrepancy between the measured channels and the independent log-normally

doi: 10.1049/iet-com.2013.0472

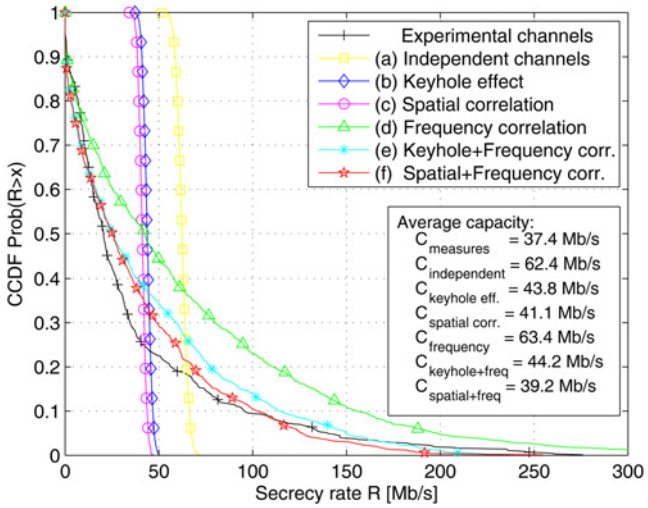

Fig. 5 *Comparison between the experimental channels and different types of numerically generated channels, in terms of secrecy rate distribution*

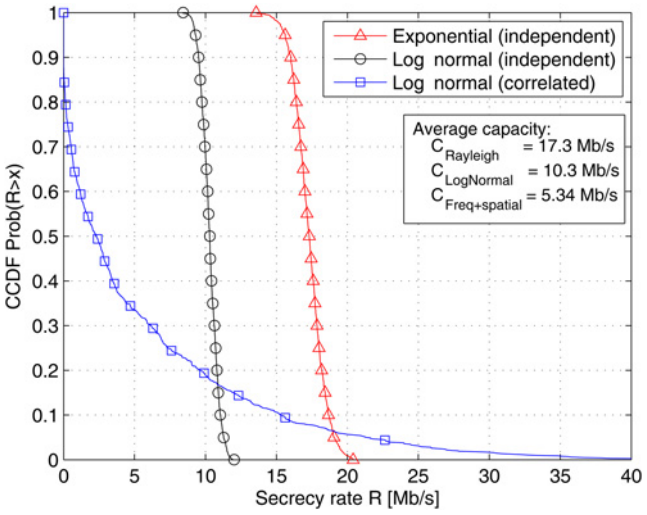

Fig. 6 *Comparison between exponential, log-normal and frequency and spatially correlated channels having the same statistics, in terms of secrecy rate distribution in multi-carrier systems*

distributed channels, both in terms of CCDF trend and average secrecy rate. When the channels are keyhole affected (case (b)) or spatially correlated (case (c)) similar performance in terms of secrecy rate distribution is achieved, although still far in terms of CCDF trend and average secrecy rate from the measured ones. When frequency correlation is considered (case (d)), the CCDF trend becomes more similar to the experimental one. Good matching is found when both the keyhole and frequency correlation (case (e)) or frequency and spatial correlation (case (f)) are considered. Therefore, we can conclude that the model with spatial correlation and the keyhole model can be used to represent the same physical phenomena.

Interestingly, although not shown due to figures restrictions, it has been found that the secrecy rate CCDF of the experimental channels depicted in Fig. 5 is well fitted by an exponential function given by $\text{CCDF} = e^{-\delta R}$, where the average secrecy rate satisfies $E[R] = 1/\delta$, with $\delta = 0.0252$ $(\text{Mb/s})^{-1}$.

5.3 Wireless against PLC

In this section, we investigate whether Rayleigh fading channels and log-normal channels provide different secrecy rate. Wireless links typically exhibit Rayleigh fading and are often independently faded. As shown in Section 3, the PLC channels are actually log-normally distributed and exhibit spatial and frequency correlation.

We consider two different types of wiretap channel. First, a Rayleigh fading channel, where $h_{M,\,c}$ and $h_{W,\,c}$ are zero mean proper complex Gaussian random variables. Hence, the gains $|h_{M,c}|^2$ and $|h_{W,c}|^2$ are exponentially distributed. Then, we consider a log-normal fading channel where the channel gains (α_c and β_c) have a log-normal distribution. In order to perform a fair comparison, we choose the parameters so that the log-normal channel gains show the same parameters (mean and variance) of the exponential channel gains.

Fig. 6 shows the comparison between the secrecy rate CCDF in [Mb/s] for the wireless (exponential) and the PLC (log-normal) channels. The SNR is set equal to 80 dB. The channel gains for both scenarios (wireless and PLC) are generated as independent random variables with the same statistics. Fig. 6 shows that PLC channels (log-normal) always achieve a lower secrecy rates than wireless channels (Exponential). If, in addition, we take into account spatial and frequency channel correlation, which typically affect PLC networks (as discussed in Section 5.2), the secrecy rate diminishes further.

5.4 Optimal and uniform power allocation

Herein we discuss the secrecy rate achieved in multi-carrier broadband PLC channels comparing uniform and optimal power allocation strategies. Uniform power allocation involves the allocation of the same power across the used sub-channels, that is, where the main channel gain is greater than the wiretapper gain ($\alpha_c > \beta_c$). Uniform power allocation is what is done, for instance, in the HPAV specifications. In order to make a fair comparison, the total power constraint for the optimal power allocation, evaluated according to (7), equals the sum of the PSD values over the used sub-channels (−50 dBm/Hz for HPAV).

A comparison between optimal and uniform power allocation strategies, in terms of secrecy rate CCDF and for a SNR = 0 dB, is depicted in Fig. 7*a*. We can observe an upwards shift for the secrecy rate CCDF with optimal power allocation w.r.t. uniform power allocation. On the contrary, when the SNR = 80 dB as in Fig. 7*b*, optimal and uniform power allocations are almost equal in terms of secrecy rate distribution. This is due to the fact that the SNR is so large that the differences among the channel gains are negligible compared to the available power per sub-channel. It follows that optimal power allocation can provide gains in bad channel environments.

5.5 Multi-user systems

In this section, we consider the two users system described in Section 4. The effects of frequency and spatial correlation on the secrecy rate region, obtained with an exhaustive search, and on the average secrecy rate under a QoS constraint are depicted in Figs. 8*a* and 8*b*, respectively. Optimal power allocation, under a total power constraint (defined in

doi: 10.1049/iet-com.2013.0472

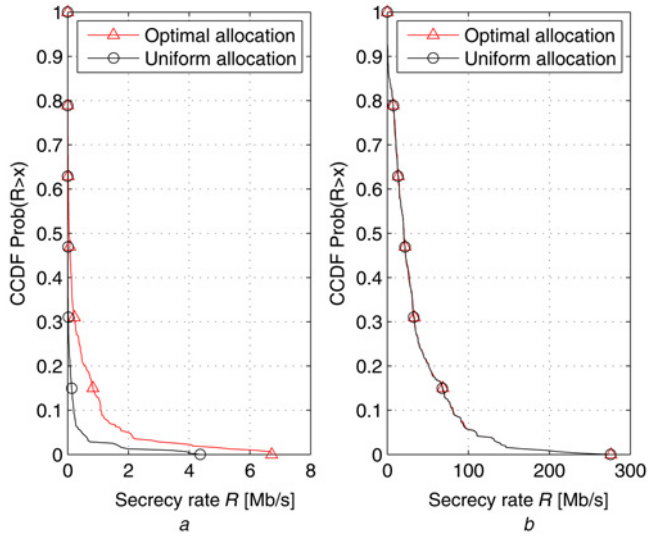

Fig. 7 *Comparison between optimal and uniform power allocation in terms of secrecy rate distribution with:*

a SNR equal to 0 dB
b SNR equal to 80 dB

Section 5—*System assumptions*), and SNR = 80 dB are considered. The curves delimit the achievable region obtained by interconnecting the outermost secrecy rate points, jointly achieved by the pair of links from Alice to Bob and from Alice to Eve, evaluated as discussed in Section 4.1. These lines represent an upper bound for the secrecy rate region.

When independent and log-normally distributed channels are assumed, the uncorrelated nature of the channels (from Alice to Bob and from Alice to Eve) is such that the rates are almost equal between the two links. Thus, the upper bound has a convex trend (curve with cross markers). Instead, the secrecy rate region for the experimental channels (curve with circles), as well as for the channels affected by correlation (curve with stars), is confined along the axes, with many rate pairs in the middle low rate region (among the axes). This gives to the region bound a concave (hyperbolic) trend. This is due to the detrimental effects of the frequency and spatial correlation. In fact, there is a good match between these two secrecy region bounds (curves with circles and stars). The correlation implies that the channels of Bob and Eve have nearly the same gain, thus a small secrecy rate is achieved. A high secrecy rate is achieved only when the channels are highly unbalanced, this is the reason for which the large rate values are concentrated along the axes. The few points exceeding the independent channels region bound (crosses) are due to the tails of the secrecy rate CCDF (beyond 70 Mb/s), depicted in Fig. 5.

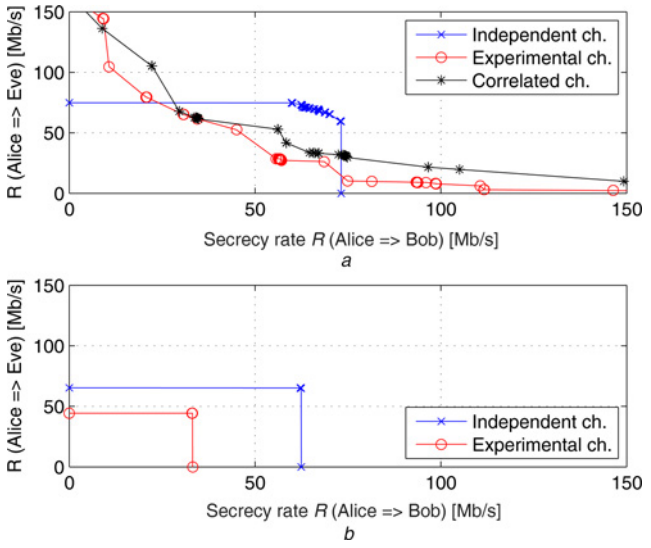

Fig. 8 *Two users multi-carrier broadcast channel for experimental and statistically independent channels:*

a Secrecy rate region for uncorrelated channels and channels affected by spatial and frequency correlation
b Average secrecy rate under a QoS constraint

The average secrecy rate pair (averaged over channel realisations) under a QoS constraint (for $0 \leq \eta \leq 1$), discussed in Section 4.1, is depicted in Fig. 8*b*. As expected the independent channels outperform the experimental ones (affected by frequency and spatial correlation). Such a high SNR (80 dB) involves the rate pairs to lay on a rectangle, due to the secrecy rate upper bound (see Section 3.2). Instead, although not shown, low SNRs lead to rate pairs laying on a convex curved line.

6 Conclusions

We have discussed PLS in PLC networks. The secrecy rate heavily depends on the channel statistics. The statistical analysis of a set of measured channels acquired with an in-home measurement campaign has highlighted that the PLC channel frequency response (gain at a certain frequency) is not Rayleigh distributed, rather it is better fitted by a log-normal distribution. Furthermore, the channels exhibit frequency and spatial correlation. This is due to the fact that the network topology has a tree structure, where the signals to different users share portions of the wires (similarly to the keyhole effect in wireless) and suffer from mutual coupling and cross-talks.

A comparison between Rayleigh (wireless) and log-normal (PLC) channels has shown that the average secrecy rate (under AWGN and with a total power constraint) for PLCs is lower than that attainable in wireless networks. Furthermore, the spatial and frequency correlation can reduce the secrecy rate further. Moreover, we have compared optimal and uniform power allocation in multi-carrier transmission systems, under a total power constraint. The results suggest that optimal power allocation can lead to a performance improvement in low SNR scenarios.

Finally, the secrecy rate region, when considering a multi-user broadcast channel, has been studied. Simulation results have shown that the secrecy rate region bound has a shape that completely changes if independent channels (convex trend) or correlated channels (concave trend), according to the experimental measures, are considered. The hyperbolic trend degenerates into two straight lines, corresponding to the axes, when strongly correlated channels and low SNRs are experienced. This shows that in some situations the PLC channels can be detrimental in terms of achievable secrecy rate.

Future work may broaden the analysis by taking into account the composition of Gaussian and impulsive noise, which typically affects PLC networks.

7 References

1 HomePlug AV System Specifications, HomePlug Powerline Alliance, Version 1.0.09, February 2007

doi: 10.1049/iet-com.2013.0472

2 Galli, S., Logvinov, O.: 'Recent developments in the standardization of power line communications within the IEEE', *IEEE Commun. Mag.*, 2008, **46**, pp. 64–71

3 Shiu, Y.-S., Chang, S.Y., Wu, H.-C., Huang, S.C.-H., Chen, H.-H.: 'Physical layer security in wireless networks: a tutorial', *IEEE Wirel. Commun.*, 2011, **18**, (2), pp. 66–74

4 Shannon, C.E.: 'Communication theory of secrecy systems', *Bell Syst. Tech. J.*, 1949, **28**, (4), pp. 656–715

5 Kalet, I.: 'The multitone channel', *IEEE Trans. Commun.*, 1989, **37**, (2), pp. 119–124

6 Chizhik, D., Foschini, J., Valenzuela, R.A.: 'Capacities of multi element transmit and receive antennas: correlations and keyholes', *Electron. Lett.*, 2000, **36**, (13), pp. 1099–1100

7 Almers, P., Tufvesson, F., Molisch, A.F.: 'Keyhole effect in MIMO wireless channels: measurements and theory', *IEEE Trans. Wirel. Commun.*, 2006, **5**, (12), pp. 3596–3604

8 Chizhik, D., Foschini, G.J., Gans, M.J., Valenzuela, R.A.: 'Keyholes, correlations, and capacities of multielement transmit and receive antennas', *IEEE Trans. Wirel. Commun.*, 2002, **1**, (2), pp. 361–368

9 Lampe, L., Vinck, A.J.H.: 'Cooperative multihop power line communications'. Proc. 16th IEEE Int. Symp. Power Line Communications and its Applications (ISPLC 2012), Vancouver, BC, Canada, 27–30 March 2012, pp. 1–6

10 Liang, Y., Poor, H.V.: 'Secure communication over fading channels'. Proc. 44th Annual Allerton Conf. Communication, Control and Computing, University of Illinois, Monticello, IL, 27–29 September 2006. [Online]. Available at: http://arxiv.org/abs/0708.2733v1

11 Barros, J., Rodrigues, M.R.D.: 'Secrecy capacity of wireless channels'. Proc. IEEE Int. Symp. Information Theory, July 2006, pp. 356–360

12 Jorswieck, E.A., Wolf, A., Gerbracht, S.: 'Trends in telecommunications technologies'. InTech: Secrecy on the Physical Layer in Wireless Networks, March 2010, pp. 413–435, chap. 20 [Online]. Available at: http://sciyo.com/articles/show/title/secrecy-on-the-physical-layer-in-wireless-networks

13 Tonello, A.M., Versolatto, F.: 'Bottom-up statistical PLC channel modeling – Part i: Random topology model and efficient transfer function computation', *IEEE Trans. Power Deliv.*, 2011, **26**, (2), pp. 891–898

14 Tonello, A.M., Versolatto, F.: 'Bottom-up statistical PLC channel modeling – Part ii: Inferring the statistics', *IEEE Trans. Power Deliv.*, 2010, **25**, (4), pp. 2356–2363

15 Pittolo, A., Tonello, A.M.: 'Physical layer security in PLC networks: achievable secrecy rate and channel effects'. Proc. 17th IEEE Int. Symp. Power Line Communications and its Applications (ISPLC 2013), Johannesburg, South Africa, 24–27 March 2013, pp. 273–278

16 Wyner, A.D.: 'The wire-tap channel', *Bell Syst. Tech. J.*, 1975, **54**, (8), pp. 1355–1387

17 Leung-Yan-Cheong, S.K., Hellman, M.E.: 'The Gaussian wire-tap channel', *IEEE Trans. Inf. Theory*, 1978, **24**, (4), pp. 451–456

18 Csiszár, I., Körner, J.: 'Broadcast channels with confidential messages', *IEEE Trans. Inf. Theory*, 1978, **24**, (3), pp. 339–348

19 Li, Z., Yates, R., Trappe, W.: 'Securing wireless communications at the physical layer'. *Secrecy Capacity of Independent Parallel Channels*, Springer US, 2010, pp. 1–18, chap. 1 [Online]. Available at: http://dx.doi.org/10.1007/978-1-4419-1385-2_1

20 Jorswieck, E.A., Wolf, A.: 'Resource allocation for the wire-tap multi-carrier broadcast channel'. Proc. Int. Conf. Telecommunications (ICT 2008), 2008, pp. 1–6

21 Boyd, S., Vandenberghe, L.: Convex optimization, (Cambridge University Press, 2004). [Online]. Available at: http://www.stanford.edu/ boyd/cvxbook/bv_cvxbook.pdf

22 Versolatto, F., Tonello, A.M.: 'PLC channel characterization up to 300 MHz: frequency response and line impedance'. Proc. IEEE Global Telecommunications Conf. (GLOBECOM 2012), Anaheim, California, USA, 3–7 December 2012, pp. 3525–3530

23 Jorswieck, E.A., Gerbracht, S.: 'Secrecy rate region of downlink OFDM systems: efficient resource allocation'. Proc. 14th Int. OFDM-Workshop (InOWo 2009), Hamburg, Germany, 2009

24 Myung, I.J.: 'Tutorial on maximum likelihood estimation', *J. Math. Psychol.*, 2003, **47**, (1), pp. 90–100 [Online]. Available at: http://www.sciencedirect.com/

doi: 10.1049/iet-com.2013.0472