***PREPRINT 2015***
***Physical and Data-Link Security Techniques for Future Communication Systems***
**Springer Lecture Notes in Electrical Engineering**, ed.s *M. Baldi, S. Tomasin*

# Physical Layer Security in Power Line Communication Networks

Alberto Pittolo and Andrea M. Tonello

**Abstract** This chapter digs into the secrecy provided and guaranteed at the physical layer, named physical layer security (PLS), over power line communication (PLC) channels for in-home networks. The PLC scenario peculiarities are briefly discussed in terms of channel characteristics and noise features. The effects of the channel properties on the performance are evaluated, in terms of the achievable secrecy rate, starting from the single-input single-output (SISO) scheme with additive white Gaussian noise. The results are also compared to the more common wireless scenario, namely a scenario where the channels are independent and experience Rayleigh fading as a consequence of rich scattering. Furthermore, the performance improvement attainable with the use of multiple-input multiple-output (MIMO) transmission is discussed. The effect of increasing the transmission band 2–30 MHz to 2–86 MHz and the effect of colored spatially correlated noise is also investigated. Moreover, a non uniform power allocation strategy, provided by the application of an alternating optimization (AO) approach is evaluated. A comparison with the channel capacity, achieved without secrecy constraints, is also performed. The experimental results are provided relying on measured noise and channel responses.

## 1 Introduction

In recent years we have witnessed a fast and worldwide increase of data connectivity demand. This is due to the widespread use of social media services and multimedia content access. In order to satisfy this continuously growing amount of data

Alberto Pittolo
University of Udine, Via Delle Scienze 206 – 33100 Udine – Italy, e-mail: alberto.pittolo@uniud.it

Andrea M. Tonello
Alpen-Adria-Universität, Universitätsstraße 65-67 – 9020 Klagenfurt am Wörthersee – Austria, e-mail: andrea.tonello@aau.at

transfer needs, new wireless and wireline technologies and standards have been developed. Among the no-new-wires technologies, power line communication (PLC) has gained momentum due to its ability to offer high data rates exploiting the existing power delivery infrastructure. Broadband PLC operates in the band 2–30 MHz, e.g., the HomePlug AV (HPAV) compliant modems [7]. The latest HomePlug AV2 (HPAV2) [24] devices use orthogonal frequency division multiplexing (OFDM), together with multiple-input multiple-output (MIMO) transmission over multiple wires, and an extended band of 2–86 MHz. They can reach data rate in excess of 500 Mbit/s.

However, it is important not only to offer high data rates but also to grant security, especially in a multiuser network context where confidential communications and transactions are exchanged. Although cryptographic mechanisms are generally used, physical layer security can strengthen security by implementing strategies at the physical layer. As the wireless communication medium, the PLC scenario is intrinsically broadcast. Hence, the communication channel is shared among the users in the network so that a transmitted signal can reach each node belonging to the network.

There are essentially two ways to think and provide secrecy in a communication system. At the high levels of the ISO/OSI stack, named complexity-based security, and at the physical layer (the lowest of the ISO/OSI stack levels), known as physical layer security (PLS) [19] or information-theoretic security. The main differences are summarized below.

*Complexity-based* — It is the most common and deployed approach. It includes all the methods and the cryptographic techniques such as the data encryption standard (DES) or the RSA. This cryptographic approach assumes the adversary to have limitations on the computational power and/or available resources. Thus, the computational resources required to extract and decrypt the original message (the plaintext) from the encrypted one (the ciphertext) render it practically infeasible for the adversary in a reasonable time.

*Information-theoretic* — This approach was formulated by Shannon [18] and it is widely accepted as the strictest notion of security. Indeed, in this case, the adversary has unlimited resources, nevertheless no information has to be released. This concept underlies the formulation of the PLS, which exploits the physical medium time, frequency and spatial diversity in order to complement and enhance the security provided by other layers.

Although PLS has been deeply investigated and analyzed for the wireless scenario, little effort has been spent for the PLC case. A preliminary discussion about PLS on PLC has been made by the authors in [15]. Then, the study has been extended in [17] considering the effects of the PLC channel, as well as analyzing the multi-user case. Subsequently, a study about PLS over MIMO PLC channels, in the

2–28 MHz frequency range and with additive white Gaussian noise (AWGN), has been carried out in [25].

In order to perform an analysis of PLS in PLC, it is important to firstly understand the properties of the PLC network and the channel properties. As it will be clear in the following description, the PLC context significantly differs from the wireless context.

## *1.1 Properties of the PLC Channel and Network*

Even though wireless and PLC communication scenarios have some similarities, such as the broadcast nature, they significantly differ in channel statistics and properties, background noise and achievable performance. For example, the highly uncorrelated channel assumption, which usually holds in wireless networks, is no longer valid for PLC networks. This is, since wireless networks are essentially based on a star-style structure, while PLC ones deploy a tree topology, with multiple branches departing from the same node, see Fig. 1. In this configuration, the

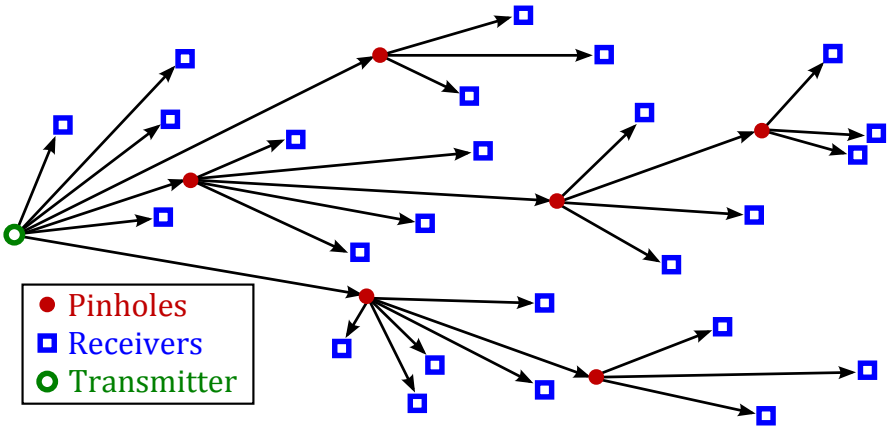


**Fig. 1** Tree structured scheme of a typical PLC network topology.

links to the end nodes share part of the wires up to a particular node, named pinhole or keyhole, where branches depart. This network topology leads to what is known as keyhole effect [1, 3], which typically affects PLC scenarios. The keyhole effect in cooperative multi-hop PLCs has been recently studied in [11]. As later clarified, this phenomenon causes spatial correlation among the channels and limits the performance.

Another prominent characteristic is the frequency correlation between the subchannels of a multi-carrier transmission scheme, mainly due to cross-talks and coupling effects. Furthermore, the PLC channels are affected by fading which exhibits

different statistics from the wireless channels. Indeed, while wireless fading has a well-known Rayleigh amplitude distribution [20], the PLC scenario shows log-normal fading statistics [6, 21], as demonstrated in the following.

A final key feature that should be taken into account is the type of background noise. Unlike the wireless case, the PLC scenario is subject to colored Gaussian noise with an exponential decreasing profile, as discussed in [22]. Consequently, all these channel and noise properties affect the performance achievable on PLC networks with respect to the wireless case, typically affected by uncorrelated Rayleigh fading under AWGN.

### *1.2 Main Contributions*

In the following, a brief description of the power line channel is provided, discussing its features and main properties, as well as the achievable performance in terms of maximum secrecy rate. To simplify the presentation first, a simpler single-input single-output (SISO) scenario in the 2–28 MHz frequency range and under AWGN, is considered. The specifications comply with the HPAV standard [7]. In this configuration set up, the effects of the PLC channel properties on the secrecy rate are evaluated and discussed, comparing the main results with a typical wireless case. In particular, independent and Rayleigh fading channels are assumed, as typically happens for rich scattering urban mobile channels.

Then, the multiple-input multiple-output (MIMO) transmission scenario is considered. The power allocation problem is assessed by applying an alternating optimization algorithm. The MIMO transmission considered exploits not only the differential transmission modes over three wires, but also an additional receiving mode, named common mode (CM). The analysis relies on real channel and noise measurements and fulfills the HPAV2 standard specifications [24]. These assumptions allow to provide results of practical relevance.

## 2 PLC Wiretap Channel

The communication channel configuration where a transmitter Alice wishes to send a secret or confidential message $x$ to an intended receiver Bob, so that no information can be inferred by an eavesdropper Eve, is known as wiretap channel, see Fig. 2. Eve represents the adversary which tries to detect and disclose the message $x$ having an arbitrarily high amount of available computational resources, as the information-theoretic secrecy foresees. The quantities $h_A$, $h_B$ and $h_E$ correspond to the channel state information (CSI) between Alice, Bob, and Eve, respectively; the two latter join at the same point, the keyhole $\kappa$, while, $y$ and $z$ are the received signals at Bob and Eve, respectively. Note that for the MIMO scheme discussed in Section 4 the

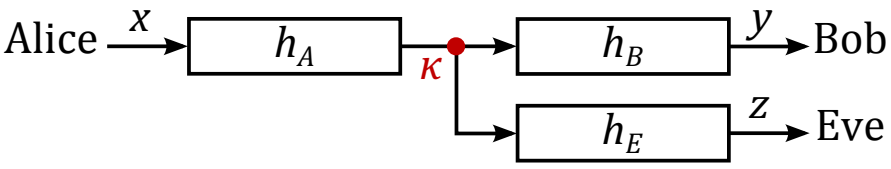


**Fig. 2** Overall wiretap channel scheme.

CSIs $h_A$, $h_B$ and $h_E$ are described by matrices, while the signals $x$, $y$ and $z$ become vectors.

The wiretap channel was firstly analyzed and introduced by Wyner in [23], where the secrecy rate was firstly found for a simple degraded wiretap channel. In this communication scenario, the channel to Bob ($h_B$) is considered less noisy than Eve's who receives a degraded, or noisier, version with respect to Bob. This assumption simplifies the analysis, enabling the derivation of the secrecy limits.

A more general broadcast scenario was considered by Csiszár and Körner [4]. The studied generic broadcast channel represents the case in which the channel from Alice ($h_A$) is assumed as ideal and the channels to Bob ($h_B$) and Eve ($h_E$) are statistically independent. This configuration is suitable to represent star-stile networks, such as rich scattering wireless scenarios.

The model depicted in Fig. 2 offers a sufficiently general setup by including a keyhole channel structure and can model other communication configurations with the proper assumptions. The branch node $\kappa$ represents the keyhole, or pinhole from which the links to Bob and Eve depart. Thus, the transmitted signal needs to cross the keyhole and travel an identical section, represented by $h_A$, before reaching the intended receiver and the eavesdropper. This introduces spatial correlation and a rank-deficiency of the communication channel, limiting the achievable secrecy rate performance [1, 3, 11]. The keyhole channel scheme in Fig. 2 resembles a tree-style network, which is the typical underlying structure of PLC networks.

## *2.1 Secrecy Capacity*

The secrecy capacity of the system in Fig. 2 represents the amount of information (e.g. bit/s) that can be reliably transmitted to the receiver. This means that the average decoding error probability approaches zero at the intended receiver, while the uncertainty at the eavesdropper, usually expressed by the equivocation rate, equals the secrecy rate. This way, no information is released to the eavesdropper, which cannot decode the messages from Alice at any positive rate lower than the secrecy capacity. For further details the reader is referred to [9]. In the following, a SISO scheme is considered, but all the results can be extended to the MIMO communication scenario. The secrecy capacity, namely the maximum achievable secrecy rate, is defined as [13]

$$C_S = \max_{f_X \in \mathscr{F}} [I(X;Y) - I(X;Z)]^+, \tag{1}$$

where $f_X$ and $\mathscr{F}$ represent the probability density function (pdf) of the channel input $X$ and the set of all the possible pdfs for $X$, respectively. Instead, $I(X;Y)$ and $I(X;Z)$ stand for the mutual information among $X$, $Y$ and $X$, $Z$, respectively. Note that $[q]^+ = \max(q,0)$. The mutual information terms $I(\cdot)$ are convex in $f_X$, this allows the formulation of a lower bound $R_S$ for the secrecy capacity in (1), given by [9]

$$C_S \geq \left[ \max_{f_X \in \mathscr{F}} [I(X;Y)] - \max_{f_X \in \mathscr{F}} [I(X;Z)] \right]^+ = R_S. \tag{2}$$

Since it is known how to maximize the mutual information terms, the lower bound in (2) is typically used for the calculation of the achievable secrecy rate.

As discussed in the following, the PLS turns out to be an optimization problem aiming at maximizing the information rate among the intended users, while keeping the eavesdropper completely ignorant about the message and unable to distill any information. As mentioned in Section 1, the PLS exploits all the available channel features in order to grant and enhance the secrecy of the system. In this regard, it is essential to investigate and study the main PLC channel features.

## *2.2 Channel Properties*

In order to assess the effect of the PLC channel properties on the performance, the statistical behavior of the channel is herein discussed. As mentioned in Section 1.1, the PLC networks, due to their underlying structure and to the physical medium, exhibit different phenomena with respect to the wireless scenario. In the following, the main features are individually analyzed relying on channel measurements carried out in three home sites [21]. The 2–86 MHz frequency range is considered.

### 2.2.1 Statistics

One of the most important properties to assess is the channel gain ($|h|^2$) statistics. Toward this end, the statistical analysis of the measurements is made relying on the likelihood function, defined as [14]

$$\Lambda(\theta) = \prod_{X \in \mathscr{X}} p(X|\theta), \tag{3}$$

where $X \in \mathscr{X}$ represents the set of measured samples, while $p(\cdot)$ and $\theta$ are the probability density function (pdf) and the parameters, obtained by the estimation, of the fitting distribution. The higher the value provided by the likelihood function, the better the tested distribution fits the measured data.

The test is performed on the measured channel gains for all the main and well known distributions, such as: exponential, gamma, log-normal, normal, Rayleigh, Weibull and log-logistic. For each distribution, the parameters that provide the best fit are found. The value obtained by each pdf is depicted in Fig. 3, which shows the logarithmic version of (3) as a function of frequency.

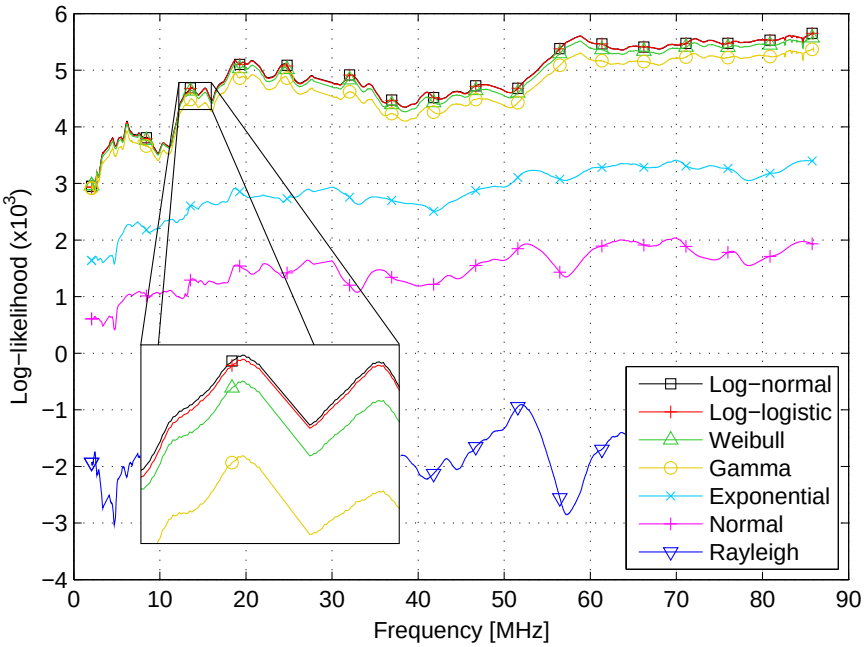


**Fig. 3** Best log-likelihood value of the measured channel gains for each tested distribution $\mathscr{X}$.

It is noted that the highest score is obtained by the log-normal distribution, along the entire frequency range. This means that, in this case, the measured PLC channel gains are log-normally distributed with good approximation [21]. However, also other statistical distributions, such as log-logistic, Weibull and gamma, obtain similar scores. This is due to the pdf shape of all these distributions, which is very similar, with the main difference limited to the tails. Since the network structure, the loads, and the reflections and propagation effects can be different in different scenarios, log-normality does not strictly apply in all contexts. However, it is noticeable that the PLC channels do not exhibit Rayleigh fading, contrariwise to what happens in the wireless case [20].

### 2.2.2 Frequency Correlation

Since broadband PLC is considered, multi-carrier modulation (OFDM) is adopted at the physical layer. This is the modulation scheme used by the HPAV and HPAV2 standards. In OFDM the broadband channel is partitioned in a number of parallel sub-channels whose responses can be correlated. The degree of this correlation is evaluated in terms of normalized covariance matrix between the sub-channel responses, defined as

$$R_{hh}(i,j) = \frac{C_{hh}(i,j)}{\sqrt{C_{hh}(i,i)C_{hh}(j,j)}}. \tag{4}$$

The normalized covariance matrix $\mathbf{R_{hh}}$ contains the pairwise covariance coefficient between each pair of sub-channels, identified by the indices $i$ and $j$. $\mathbf{C_{hh}}$ is the covariance matrix whose elements are defined as

$$C_{hh}(i,j) = E[(h(i)-\mu_i)(h(j)-\mu_j)], \tag{5}$$

where the operator $E[\cdot]$ denotes the expectation, $h(i)$, $h(j)$ the $i$-th and $j$-th sub-channel gains and $\mu_i$, $\mu_j$ their mean ($\mu = E[h]$), respectively. The expectation is performed on the channel measurements.

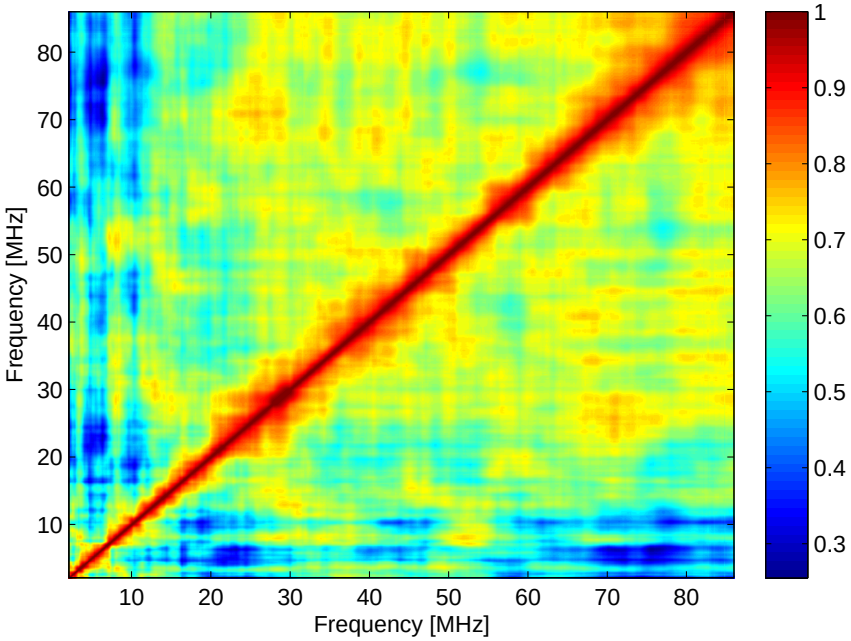


**Fig. 4** Normalized covariance matrix for the measured channel gains in dB scale.

The normalized covariance is evaluated on the logarithmic, or dB, version of the channels gains, which is normally distributed. Thus, it becomes easier to generate and simulate correlated log-normal random channels, starting from independent normally distributed realizations. Fig. 4 depicts the normalized covariance matrix between the measured sub-channels in dB scale. It can be noted as certain sub-channels are more related to some others, where the colors become warmer (yellow and red), as happens for the sub-channels in the upper right corner, which identifies high frequencies. This phenomenon is due to the crosstalk among the wires and to the coupling effects, which become prominent at higher frequencies.

### 2.2.3 Spatial Correlation

The spatial correlation represents the correlation coefficient, or degree of correlation, among the main channel and the wiretapper channel. With reference to Fig. 2, the main channel, denoted by $h_M$, refers to the communication link among Alice and Bob. Thus, it is given by the product of the two channels in cascade, as $h_M = h_A h_B$. The wiretap channel, denoted by $h_W$, instead, refers to the communication link between Alice and Eve, given by $h_W = h_A h_E$. Since the transmitting and receiving

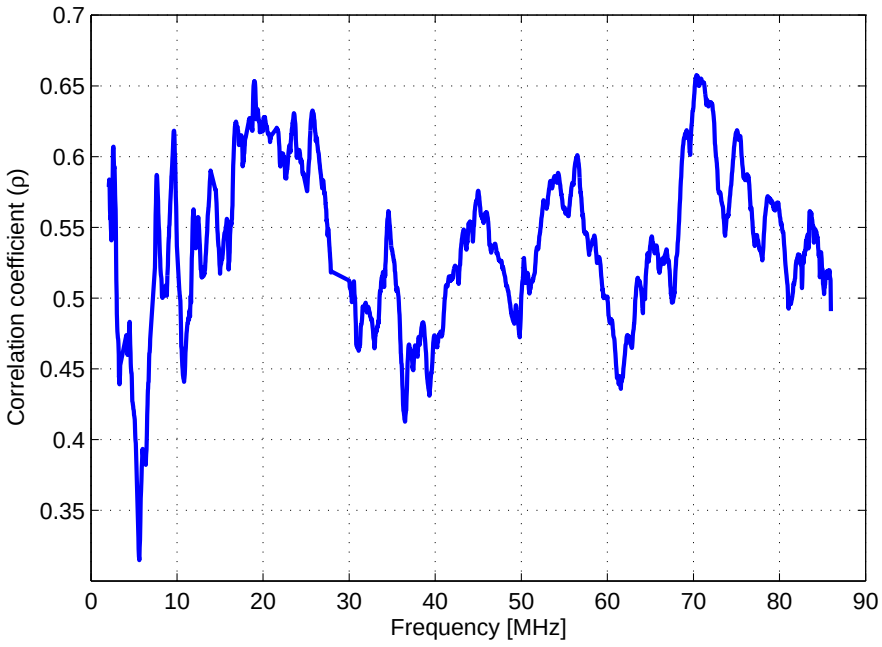


**Fig. 5** Spatial correlation coefficient between the main and the wiretapper channels in dB scale.

plugs are known, the measurements are carefully divided among the main and the

wiretapper channel so that the corresponding channels share the same transmitting plug. Therefore, the communication scheme resembles that depicted in Fig. 2.

The correlation coefficient $\rho$ among the main and the wiretapper channel, in dB scale, is depicted in Fig. 5 as a function of frequency. As can be seen, the value is quite high over the entire frequency range, with some peaks and minimums confined at certain carriers (frequencies). The spatial correlation herein shown is mainly due to the keyhole effect caused by the underlying network structure.

## *2.3 Noise Properties*

As mentioned in Section 1.1, not only the channel properties affect the PLC performance. Also the background noise must be taken into account. Contrariwise the wireless case, affected by white Gaussian noise, PLC networks are subject to colored Gaussian background noise. Depending on the PLC context, different noise floors and profiles have been documented [22]. A typical noise power spectral density (PSD) profile is depicted in Fig. 6. The displayed PSDs refers to the noise

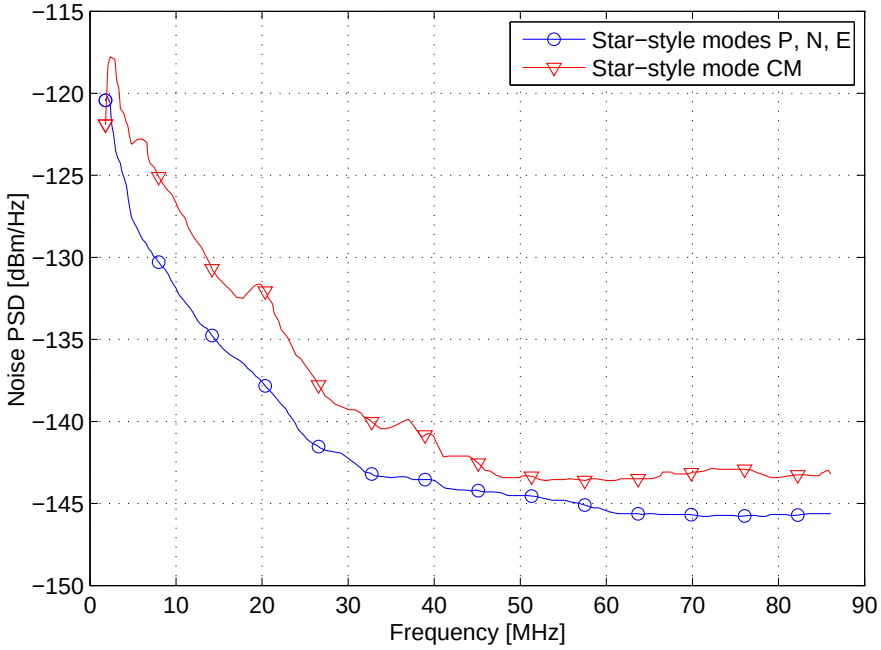


**Fig. 6** Typical background noise at the star-style receiving modes in a MIMO PLC network.

measured at the star-style receiving modes for the MIMO scheme described in Section 4.1. As can be noted, the common mode experiences a higher PSD with respect

to the other three modes. The effects on the channel performance of these colored noise PSD profiles, together with the spatial correlation between the modes, are discussed in Section 4. In the following, the effects of the PLC channel properties on the achievable secrecy rate are evaluated for the simpler SISO scheme under AWGN.

## 3 SISO Scheme under AWGN

As described in Section 2.2, PLC networks are subject to a variety of physical phenomena. In order to asses how these phenomena affect the PLS performance, different types of random channels are generated through a numerical model. In particular, the impact of the channel statistics, the frequency and spatial correlation, as well as the keyhole effect, is evaluated generating random channels responses with the appropriate statistics. Furthermore, this approach allows the PLC and the wireless scenario comparison, relying on channel responses with different distributions. To facilitate the comprehension, the SISO channel is considered first. Moreover, to fairly compare wireless and PLC scenarios, the same background AWGN noise is assumed.

### *3.1 Optimization Problem Formulation*

As discussed in Section 1, the evaluation of the secrecy capacity for the model depicted in Fig. 2 involves solving an optimization problem. Assuming OFDM transmission with $N$ carriers or sub-channels, the received signals by Bob and by Eve, at the $c$-th carrier, can be written as

$$y_c = h_{M,c}x_c + n_{B,c}, \tag{6}$$

$$z_c = h_{W,c}x_c + n_{E,c}, \tag{7}$$

respectively, where, the transmitted signal on carrier $c$ is $x_c$. Moreover, $h_{M,c}$ and $h_{W,c}$ are the main and the wiretapper channels, while $n_{B,c}$ and $n_{E,c}$ represent the effect of the additive Gaussian noise, with zero mean and variance $\sigma_n^2$. The transmitted signal and the noise are assumed to be statistically independent from each other and for each sub-channel $c$. Moreover, as usually happens, the power at the transmitter is limited by a total power constraint $\sum_{c=1}^{N} |x_c|^2 \leq P_T$, where $P_T$ is the total available power. Finally, perfect channel state information (CSI) is assumed at the transmitter side. Thus, Bob and Eve know their own channel, while Alice has access to both channel gains to Bob and Eve. This case resembles the situation in which Eve is not an adversary, but simply an unintended user of the same network.

The secrecy rate of the system model discussed in Section 2 can be computed according to (2) [13], as

$$R_S(\mathbf{P_x}) = \sum_{c=1}^{N} \left[ \log_2 \left( 1 + \frac{\alpha_c P_{x,c}}{\sigma_n^2} \right) - \log_2 \left( 1 + \frac{\beta_c P_{x,c}}{\sigma_n^2} \right) \right]^+, \tag{8}$$

where $P_{x,c}$ is the transmitting power on the $c$-th sub-channel, whereas $\alpha_c = |h_{M,c}|^2$ and $\beta_c = |h_{W,c}|^2$ are the channel gains of the main and the wiretapper channels, respectively. The power allocated on each sub-channel is organized in a vector $\mathbf{P_x} = [P_{x,1}, \ldots, P_{x,N}]$, which corresponds to the transmitter power allocation strategy for a given channel realization. Note that the secrecy rate in (8) is upper bounded by $\sum_{c=1}^{N} [\log_2(\alpha_c/\beta_c)]^+$ for arbitrarily large power $\mathbf{P_x}$ and can turn out to be small if the channel does not provide enough diversity.

The secrecy rate optimization problem for the multi-carrier system aims at maximizing the quantity in (8), under a total power constraint, and it is formulated as

$$\max_{\mathbf{P_x}} [R_S(\mathbf{P_x})] \text{ subject to } \sum_{c=1}^{N} P_{x,c} \leq P_T \text{ and } P_{x,c} \geq 0. \tag{9}$$

To perform a fair analysis, the total power $P_T$ equals the sum of the HPAV PSD constraint over the used sub-channels. Although, as seen, this is a non-convex optimization problem, it has been shown in [8] that the optimal power allocation strategy is to not allocate power on the sub-channels in which Eve has a higher gain than Bob, i.e. when $\alpha_c \leq \beta_c$. Consequently, the resulting problem becomes convex and can be easily solved through the Karush-Kuhn-Tucker (KKT) conditions [2]. For a more complete and general treatment the reader is referred to [17, 9].

## *3.2 Effects of Channel Characteristics on Performance*

The typical PLC channel properties, discussed in Section 2.2, are herein evaluated in terms of achievable secrecy rates. Hence, the first step is to compute the statistical parameters and the degree of frequency and spatial correlation, starting from real channel measurements. The evaluation is performed relying on 1300 in-home channel measurements in the 2–28 MHz frequency range, carried out in different house sites, as specified in [21]. The specifications comply with the HPAV standard [7].

For the secrecy rate computation, a signal-to-noise ratio (SNR) of 80 dB has been assumed, without taking into account the channel attenuation. This SNR value is typical in PLC networks since, usually, the PSD at the transmitter is constrained at $-50$ dBm/Hz, while the noise PSD floor equals $-130$ dBm/Hz. The secrecy rate achieved over the channel measurements is compared to that of the numerically simulated channel realizations, generated taking into account different channel effects as follows. For further details the reader is referred to [17].

1. *Independent channels*: the main and the wiretapper channels are independently generated with a log-normal distribution.

2. *Keyhole effect*: three independent log-normal channel realizations are generated for the Alice's, Bob's and Eve's channels ($h_A$, $h_B$ and $h_E$, respectively), see Fig. 2. The parameters are imposed so that the mean and the variance of the main and wiretapper channels turn out to be equivalent to those of the channel measurements. This is made possible exploiting the properties of the product of log-normal variables.
3. *Spatial correlation*: in this case, the main and wiretapper channels are generated, with a log-normal distribution, according to the measured correlation coefficient discussed in Section 2.2.3. The frequency correlation is not considered.
4. *Frequency correlation*: the log-normally generated channels exhibit the same frequency correlation of the measured channels, analyzed in Section 2.2.2, but are spatially uncorrelated.
5. *Keyhole effect and frequency correlation*: the same procedure in 2 is applied to frequency correlated channels. Thus, the frequency correlation and keyhole effect are jointly considered.
6. *Spatial and frequency correlation*: the generated channel realizations are affected by both frequency correlation and spatial correlation, between the main and the wiretapper channels, as usually happens in real PLC networks.

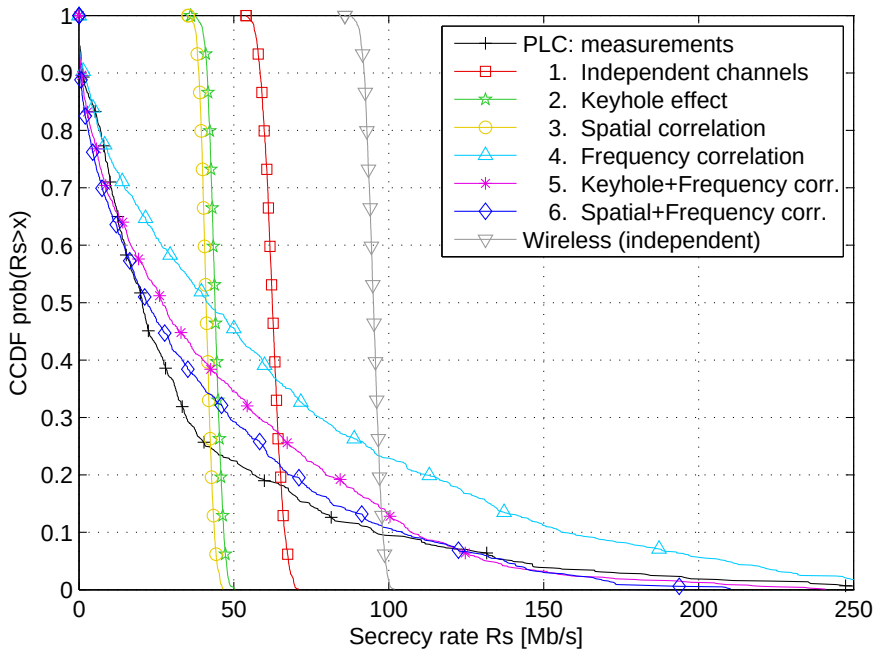


**Fig. 7** Secrecy rate CCDF comparison among measurements and simulated realizations with different phenomena. The secrecy rate for wireless independent channels is also depicted.

The secrecy rate, for all the above listed channel realizations, has been computed solving (9), as in [17]. The secrecy rate complementary cumulative distribution function (CCDF) is depicted in Fig. 7. It can be seen as the CCDF for the measured channels completely differs from that of the independent channels in both trend and average secrecy rate, summarized in Table 1. Also when considering the spatial correlation or the keyhole effect the trend does not change, although there is an average secrecy rate reduction. When the frequency correlation is introduced, the CCDF trend improves. Moreover, it closely approaches the measured one when also the keyhole effect or the spatial correlation are taken into account. The agreement can also be noted looking at the average secrecy rates summarized in Table 1. This analysis demonstrates that the channel statistics, together with the frequency and spatial correlation, constrain and limit the PLC channel performance. As a final remark, the results in Fig. 7 validate the implemented numerical model for the channel generation.

**Table 1** Average secrecy rate for different simulated PLC channel phenomena.

| Scenario | Channel type | Average secrecy rate (Mb/s) |
|---|---|---|
| Wireless | Independent | 95 |
| PLC | Independent | 62.5 |
| PLC | Keyhole effect | 44 |
| PLC | Spatial correlation | 41.1 |
| PLC | Frequency correlation | 62.9 |
| PLC | Keyhole + frequency correlation | 43.7 |
| PLC | Spatial + frequency correlation | 38.9 |
| PLC | Measurements | 37.4 |

### 3.2.1 Wireless versus PLC

It is interesting to compare the secrecy rate attainable in wireless channels characterized by statistically independent Rayleigh fading and in PLC channels that exhibit correlated log-normal fading. As above specified, in order to perform a fair comparison, an equal SNR of 80 dB (without considering the channel attenuation) is assumed for both scenarios. The secrecy rate CCDF is reported in Fig. 7 where it is shown that the wireless case outperforms the PLC one. The difference is noticeable also in terms of average secrecy rate, displayed in Table 1.

## 4 MIMO Scheme under Colored and Correlated Noise

The limits on the secrecy rate, due to the PLC channel characteristics, can be mitigated exploiting the spatial domain end extending the used bandwidth. The perfor-

mance improvements provided by the MIMO transmission scheme with an additional receiving mode, namely the common mode (CM), the bandwidth extension up to 86 MHz and a novel alternating optimization (AO) approach are herein assessed. It has already been proved in [25] that MIMO transmission can increase PLS performances on PLC. However, the work considers numerically generated channels with two transmitting and receiving modes in the 2–28 MHz frequency band, under AWGN. In this section, the analysis is further extended relying on real channel and noise PSD measurements. As specified by the HPAV2 [24],the 2–86 MHz bandwidth is considered, and the maximum number of possible transmitting and receiving modes are exploited, as described in the following. These assumptions provide actual performance results that can be viewed as a target for future devices development.

## *4.1 MIMO structure*

In today's houses, power supply networks usually consist of three different wires, namely the phase (P), the neutral (N) and the protective earth (E). Hence, due to Kirchhoff's laws, only two $\Delta$-style modes can be exploited at the same time. Where $\Delta$ mode means to inject the differential signals between pair of wires, see Fig. 8 for details. Instead, at the receiver side, the signals can be observed between one con-

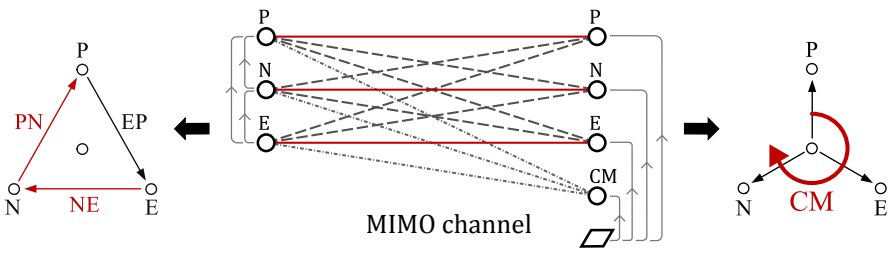


**Fig. 8** MIMO $\Delta$-style transmitting and star-style receiving modes according to STF-410.

ductor and a reference plane, referred to star-style mode. Beyond the three available star-style modes, one additional mode, given by the coupling between the wires and the physical earth, can be exploited, namely the common mode (CM) [5]. The CM is given by the current that flows in the three conductors, which has the same intensity and direction. Thus, a $2 \times 4$ MIMO transmission scheme can be implemented between the transmitter and the receiver side.

### *4.2 Alternating Optimization Algorithm*

The secrecy rate maximization belongs to the family of non-convex optimization problems, which are non-trivial and not easily solvable. This is because the secrecy capacity is obtained by the maximization of the difference of two convex terms, as shown in (1). The optimization becomes even more difficult when considering MIMO wiretap channels, with one or multiple eavesdroppers. Anyway, to provide a solution, an alternating optimization (AO) approach has been proposed in [12]. The secrecy capacity optimization problem has been reformulated with an equivalent expression which can be brought back to two convex optimization problems, alternatively solved, as briefly described in the following.

For each used sub-channel, the secrecy rate maximization in (9) can be reformulated for the MIMO transmission scheme as follows

$$C_S = \max_{\mathbf{X}} \left[\log_2 |\mathbf{I} + \mathbf{H_M}^H \mathbf{X} \mathbf{H_M}| - \log_2 |\mathbf{I} + \mathbf{H_W}^H \mathbf{X} \mathbf{H_W}|\right], \quad \text{subject to } \mathrm{Tr}(\mathbf{X}) \leq P_c,\ \mathbf{X} \succeq 0, \tag{10}$$

where $\mathbf{X}$ is the covariance matrix of the transmitted signal $x$, while $\mathbf{H_M}$ and $\mathbf{H_W}$ represent the main and wiretapper MIMO channel matrices, respectively. Furthermore, $P_c$ is the PSD constraint on the $c$-carrier and $\mathbf{X} \succeq 0$ means that $\mathbf{X}$ must be positive semidefinite. The identity matrix is represented as $\mathbf{I}$. The optimization problem in (10) is properly reformulated exploiting the following lemma [10].

**Lemma 1.** *Let $\mathbf{E} \in \mathbb{C}$ be any $N \times N$ positive definite matrix ($\mathbf{E} \succ 0$). Consider the function $f(\mathbf{S}) = -\mathrm{Tr}(\mathbf{SE}) + \log_2 |\mathbf{S}| + \mathbf{N}$, then*

$$\log_2 |\mathbf{E}^{-1}| = \max_{\mathbf{S} \succeq 0} f(\mathbf{S}), \tag{11}$$

*and the optimal solution to the right-hand side of (11) is $\mathbf{S}^* = \mathbf{E}^{-1}$.*

Hence, applying Lemma 1 via setting $\mathbf{E} = \mathbf{I} + \mathbf{H_W}^H \mathbf{X} \mathbf{H_W}$, the problem in (10) can be reformulated as

$$\max_{\mathbf{X},\mathbf{S}} \left[\log_2 |\mathbf{I} + \mathbf{H_M}^H \mathbf{X} \mathbf{H_M}| - \mathrm{Tr}\left(\mathbf{S}(\mathbf{I} + \mathbf{H_W}^H \mathbf{X} \mathbf{H_W})\right) + \log_2 |\mathbf{S}|\right], \quad \text{subject to } \mathrm{Tr}(\mathbf{X}) \leq P_c,\ \mathbf{X} \succeq 0,\ \mathbf{S} \succeq 0, \tag{12}$$

where $\mathbf{S}$ denotes a Hermitian positive semidefinite matrix. For simplicity the constant $\mathbf{N}$ has been dropped. The problem in (12) is still non-convex with respect to (w.r.t.) both $\mathbf{X}$ and $\mathbf{S}$. However, it can be verified that the problem is convex w.r.t. either $\mathbf{X}$ or $\mathbf{S}$, fixing the other decision variable. This property motivated the use of an AO approach. Defining $\mathbf{X}^n$, $\mathbf{S}^n$ the solutions for the $n$-th iteration, the following two optimization problems are alternatively solved

$$\mathbf{S}^n = \arg\max_{\mathbf{S} \succeq \mathbf{0}} \left[\log_2 |\mathbf{S}| - \mathrm{Tr}\left(\mathbf{S}(\mathbf{I} + \mathbf{H_W}^H \mathbf{X}^{n-1} \mathbf{H_W})\right)\right], \tag{13}$$

$$\mathbf{W}^n = \arg\max_{\mathbf{W}} \left[\log_2 |\mathbf{I} + \mathbf{H_M}^H \mathbf{X} \mathbf{H_M}| - \mathrm{Tr}(\mathbf{H_W}^H \mathbf{S}^n \mathbf{H_W} \mathbf{X})\right], \quad \text{subject to } \mathrm{Tr}(\mathbf{X}) \leq P_c,\ \mathbf{X} \succeq 0. \tag{14}$$

As mentioned, both the problems (13) and (14) are convex, and can be alternatively solved, as done by the AO algorithm. The solution is guaranteed to converge at a KKT point. For further details the reader is referred to [12].

The solution reported in [12] assumes AWGN. Herein, it is extended to the more complicated colored and correlated Gaussian noise scenario. A non-uniform power allocation solution is found. The results rely on real channel and noise assumptions.

### *4.3 Results for the MIMO Scenario*

The focus is on the MIMO wiretap channel. The transmitter exploits the two $\Delta$-style transmitting modes, while both Bob and Eve use all the four star-style receiving modes, as discussed in Section 4.1. The performance is evaluated exploiting 353 MIMO channel measurements, carried out through an experimental measurement campaign across Europe and collected by the ETSI special task force 410 (STF-410) [5]. The considered frequency range is 2–86 MHz, and the PSD constraint at the transmitter is $-50$ dBm/Hz in the 2–30 MHz, while $-80$ dBm/Hz in the 30–86 MHz, according to the latest HPAV2 standard [24]. Moreover an AWGN and a colored and correlated Gaussian background noise are considered. For the colored noise the exponential profile is taken from the STF-410 noise PSD measurements, while the spatial correlation is implemented between the modes as discussed in [16]. The white noise, instead, has been generated so that it exhibits a total power equivalent to the colored one in the considered bandwidth. The channels are equally divided and assigned to the intended receiver and to eavesdropper, respectively.

Under the above system specifications, the secrecy rate achieved over the $2 \times 4$ MIMO wiretap channel is evaluated and depicted in Fig. 9. As a term of comparison, two different noise models are taken into account, white and independent in Fig. 9a, and colored and correlated in Fig. 9b. Furthermore, the performance achieved with the allocation strategy provided by the AO algorithm is compared to that achieved under uniform power allocation (identified by the subscripts AO and UN, respectively).

The comparison is made in terms of secrecy rate CCDF. It can be noted as the AO algorithm translates into a performance improvement for both considered background noise models. This is even more evident looking at the average secrecy rate displayed in the boxes. In practice, an increase of about 30% and 20% has been noticed for the AWGN and the colored and correlated noise, respectively. When considering colored and correlated noise the performance increases further. This happens since the noise correlation makes easier its cancellation at the receiver side. As a further term of comparison, the channel capacity, achieved without any secrecy constraint, is also computed and depicted in Fig. 9. It can be noted as its average value is almost four times higher than the average secrecy rate. This consideration gives the idea on the cost in granting and providing secrecy and confidentiality, in terms of PLS performance.

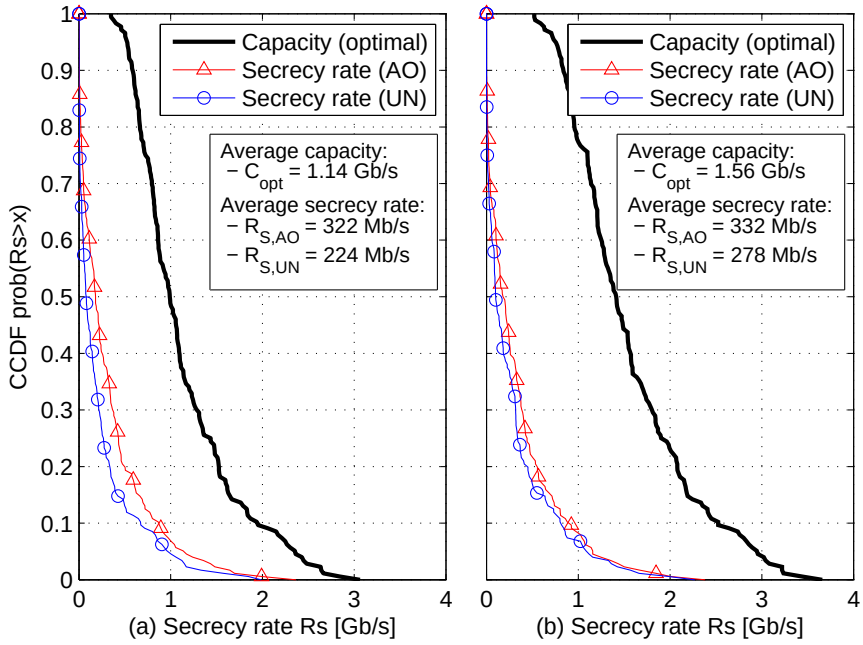


**Fig. 9** Secrecy rate CCDF for uniform and AO approach power allocation under AWGN (a) or colored and correlated (b) Gaussian background noise. The channel capacity is also depicted.

### 4.3.1 Overall Comparison

A comparison between the SISO and MIMO scenarios is reported in this section. The average secrecy rate, averaged over the channel realizations, of the two transmission schemes for different frequency ranges and background noise models, is summarized in Table 2. As a term of comparison, both the SISO database (DB), discussed in Section 3.2 (identified by 'our DB'), and the ETSI measurements, described in Section 4.3, are considered. Moreover, various power allocation strategies are assumed.

**Table 2** Average secrecy rate comparison for different transmission schemes, frequency ranges, power allocation strategies and background noise. Two distinct databases are considered.

| Transmission scheme | Frequency range (MHz) | Background noise | Power allocation | Measurements database | Secrecy rate (Mbit/s) |
|---|---|---|---|---|---|
| SISO | 2–28 | AWGN | Optimal | Our DB (same Tx) | 37.4 |
| SISO | 2–28 | AWGN | Uniform | Our DB (all) | 52.8 |
| SISO | 2–28 | AWGN | Uniform | ETSI (all) | 62.9 |
| MIMO | 2–28 | AWGN | Uniform | ETSI (all) | 90.4 |
| MIMO | 2–86 | Measured | AO | ETSI (all) | 332 |

The results show that when considering the 2–28 MHz frequency range and the keyhole effect, with the same transmitting plug for the main and the wiretapper channels, the average secrecy rate for the SISO scheme is not very high. This, even though the optimization problem is subject to a total power constraint, as detailed in Section 3.1. However, the SISO channel performance for the house sites (our DB) almost doubles when considering the entire database, irrespectively of the transmitting plug. Indeed, with this choice, the channels used in the simulation are more uncorrelated. For comparison purposes, in this case a uniform power constraint, equal to the HPAV PSD limit, is considered. However, this assumption does not significantly affect the achievable performance, as detailed in [17].

Now, the ETSI measurements are considered under the same uniform power constraint and AWGN. Focusing on the reduced 2–28 MHz frequency range and converting the $2 \times 4$ $\Delta$-style to star-style MIMO scheme into a $\Delta$-style to $\Delta$-style SISO channel, it can be seen as the average secrecy rate is only slightly higher compared to that achieved on the whole DB of the other measurement campaign. Thus, the two different scenarios can be compared. If the spatial dimension is exploited through MIMO transmission, the performance increases further. Moreover, the bandwidth extension up to 86 MHz, the real background noise assumption, together with the AO algorithm, provide a drastic increase in the achievable secrecy rate.

It can be concluded that the keyhole effect significantly limits the achievable secrecy rate. However, the performance improves through MIMO transmission, bandwidth extension, real noise assumption and non uniform power allocation.

## 5 Final Remarks

It has been shown that PLS over PLC is possible, although constrained and limited by the channel properties and the network characteristics. The results show that PLC channels exhibit log-normal fading, with frequency correlation, due to coupling and cross-talk, and spatial correlation, mainly caused by the underlying network structure. The typical tree-structured PLC network topology gives rise to what is known as keyhole effect, which causes spatial correlation and rank deficiency. As showed, these effects, together with the channel statistics, limit the PLS performance. Furthermore, the comparison among wireless (characterized by Rayleigh fading) and PLC scenarios (characterized by correlated log-normal fading) shows that the former outperforms the latter in terms of secrecy rate, under the same SNR assumption. However, the performance can be improved through the exploitation of the spatial dimension, via the use of MIMO transmission, extending the transmission band 2–28 MHz to 2–86 MHz, and exploiting the power allocation provided by the AO algorithm. The performance improves further when colored and spatially correlated background noise is considered. The results have been obtained with measured channels and noise PSD. Therefore, they have practical value and provide an indication of the achievable level of secrecy if physical layer mechanisms are considered.

## References


1. P. Almers, F. Tufvesson, and A. F. Molisch, "Keyhole Effect in MIMO Wireless Channels: Measurements and Theory," *IEEE Trans. on Wirel. Commun.*, vol. 5, no. 12, pp. 3596-3604, 2006.
2. S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004. [Online]. Available: http://www.stanford.edu/ boyd/cvxbook/bv cvxbook.pdf
3. D. Chizhik, G. J. Foschini, M. J. Gans, and R. A. Valenzuela, "Keyholes, Correlations, and Capacities of Multielement Transmit and Receive Antennas," *IEEE Trans. on Wirel. Commun.*, vol. 1, no. 2, pp. 361-368, Apr 2002.
4. I. Csiszár and J. Körner, "Broadcast Channels with Confidential Messages," *IEEE Trans. on Inf. Theory*, vol. 24, no. 3, pp. 339-348, May 1978.
5. 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.
6. S. Galli, "A Novel Approach to the Statistical Modeling of Wireline Channels," *IEEE Trans. Commun.*, vol. 59, no. 5, pp. 1332-1345, May 2011.
7. *HomePlug AV System Specifications*, HomePlug Powerline Alliance, Version 1.0.09, Feb 2007.
8. E. A. Jorswieck and A. Wolf, "Resource Allocation for the Wire-tap Multi-carrier Broadcast Channel," in *Proc. of Int. Conf. on Telecommun. (ICT)*, 2008, pp. 1-6.
9. E. A. Jorswieck, A. Wolf, and S. Gerbracht, *Trends in Telecommunications Technologies*. InTech, Mar 2010, ch. 20: Secrecy on the Physical Layer in Wireless Networks, pp. 413-435.
10. J. Jose, N. Prasad, M. Khojastepour, and S. Rangarajan, "On Robust Weighted-Sum Rate Maximization in MIMO Interference Networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun 2011, pp. 1-6.
11. L. Lampe and A. J. H. Vinck, "Cooperative Multihop Power Line Communications," in *Proc. of 16th IEEE Int. Symp. on Power Line Commun. and Its Appl. (ISPLC)*, Vancouver, BC, Canada, 27-30 Mar 2012, pp. 1-6.
12. 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 J. on Sel. Areas in Commun.*, vol. 31, no. 9, pp. 1714-1727, 2013.
13. Z. Li, R. Yates, and W. Trappe, "Secrecy Capacity of Independent Parallel Channels," in *Securing Wireless Communications at the Physical Layer*, R. Liu and W. Trappe, Eds. Springer US, 2010, pp. 1-18.
14. I. J. Myung, "Tutorial on maximum likelihood estimation," *J. of Math. Psychol.*, vol. 47, no. 1, pp. 90-100, Feb 2003.
15. A. Pittolo and A. M. Tonello, "Physical Layer Security in PLC Networks: Achievable Secrecy Rate and Channel Effects," in *Proc. of 17th IEEE Int. Symp. on Power Line Commun. and Its Appl. (ISPLC)*, Johannesburg, South Africa, 24-27 Mar 2013, pp. 273-278.
16. A. Pittolo, A. M. Tonello, and F. Versolatto, "Performance of MIMO PLC in Measured Channels Affected by Correlated Noise," in *Proc. of 18th IEEE Int. Symp. on Power Line Commun. and its Appl. (ISPLC)*, Mar 2014, pp. 261-265.
17. A. Pittolo and A. M. Tonello, "Physical layer security in power line communication networks: an emerging scenario, other than wireless," *IET Commun.*, vol. 8, no. 8, pp. 1239-1247, 22 May 2014.
18. C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656-715, Oct 1949.
19. 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 Wirel. Commun.*, vol. 18, no. 2, pp. 66-74, Apr 2011.
20. G. Stüber, *Principles of Mobile Communication*. Kluwer Academic, 2001. [Online]. Available: http://books.google.it/books?id=65 fF83bja0C
21. A. M. Tonello, F. Versolatto, and A. Pittolo, "In-Home Power Line Communication Channel: Statistical Characterization," *IEEE Trans. on Commun.*, vol. 62, no. 6, pp. 2096-2106, Jun 2014.

22. A. M. Tonello, A. Pittolo, and M. Girotto, "Power Line Communications: Understanding the Channel for Physical Layer Evolution Based on Filter Bank Modulation," *IEICE Trans. Commun.*, vol. E97-B, no. 8, pp. 1494-1503, Aug 1, 2014.
23. A. D. Wyner, "The Wire-Tap Channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355-1387, Oct 1975.
24. 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," *J. of Electr. and Comput. Eng.*, vol. 2013, 2013.
25. Y. Zhuang and L. Lampe, "Physical Layer Security in MIMO Power Line Communication Networks," in *Proc. of 18th IEEE Int. Symp. on Power Line Commun. and its Appl. (ISPLC)*, Glasgow, Scotland, Mar 30-Apr 2 2014, pp. 272-277.