IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 5, 2017, accepted June 23, 2017, date of publication July 24, 2017, date of current version August 8, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2729784

Physical Layer Security Over Correlated Log-Normal Cooperative Power Line Communication Channels

ABDELHAMID SALEM, (Student Member, IEEE), KHAIRI ASHOUR HAMDI, (Senior Member, IEEE), AND EMAD ALSUSA, (Senior Member, IEEE)

School of Electrical and Electronic Engineering, The University of Manchester, Manchester M13 9PL, U.K.

Corresponding author: Abdelhamid Salem (abdelhamid.salem@manchester.ac.uk)

ABSTRACT Power line communication (PLC) has enabled many smart grid applications and functionalities over the past few years. Secure communications over such links however remain a crucial aspect for further development. Due to their shared nature, akin to wireless, PLC channels can benefit from many wireless-type security techniques, including physical layer security. To this end, and in contrast to existing studies, which focus on non-cooperative PLC systems, this paper considers the application of physical layer security in cooperative PLC networks in the presence of passive eavesdropping. We analyze the performance of such systems using log-normal correlated channel models considering background and impulsive noise components. Furthermore, the impact of PLC/wireless coding diversity on the system secrecy capacity is evaluated. The results include accurate mathematical expressions for providing an insight into the secrecy capacity and outage probability performance of such systems under various network scenarios.

INDEX TERMS Coding diversity, average secrecy capacity, jamming, correlated log-normal channels, physical layer security, power line communications, relaying, secrecy outage probability, smart grids.

I. INTRODUCTION

The rising demand for electricity, in both the domestic and industrial sectors, coupled with the need to enhance power efficiency and control made it necessary to modernize the aging electricity grid. This is commonly accomplished using power line communication (PLC), which is often preferred over the other alternatives, such as WiFi, fiber optics, because PLC exploits existing power cables and hence can be efficiently deployed. In general, PLC is divided into narrow-band (NB) and broad-band (BB) systems with frequency bands of 500 KHz and above 2 MHz, respectively [1], [2]. The former remains the main enabler of numerous smart grid applications and hence it will be the main focus of this paper.

Although it can be argued that PLC channels pose a more hostile medium, compared to the wireless counterparts, due to several inherent impairments, such as, impedance mismatching and non-Gaussian noise, the two channels have many similarities such as frequency selective fading and path loss. Moreover, the broadcast nature of these links allows different users to share the same channel, hence confidential messages become susceptible to eavesdropping [3], [4]. Such commonalities have encouraged researchers in the PLC community to build on many wireless-based advances for PLC systems including multiple-input multiple-output (MIMO) schemes [5], [6], MAC protocols, cryptography [7], as well as relaying and cooperative techniques, [8]–[11]. For instance, distributed space-time coding, as well as decode and forward relaying over PLC channels were studied in [12] and [13]. Also, cooperative multi-hop transmission has been applied for PLC in [14] and [15]. Recently, physical layer security techniques, have also been considered for PLC. The physical layer security is primarily characterized by the secrecy capacity metric, which is defined as the maximum transmission rate that can be achieved without leaking information to an eavesdropper [16], [17]. The authors in [18] and [19] considered physical layer security for a single-input single-output PLC system and compared its performance with the wireless counterpart. Motivated by this, the authors of [20] were the first to extend such idea to MIMO PLC networks and managed to demonstrate that multi-conductor PLC networks can be manipulated to provide more secure communications in comparison to the single-conductor case. In addition, in order to enhance the system security cooperative jamming technique has been

widely considered in wireless communications. In [21], several cooperation strategies have been proposed and the corresponding achievable performance bounds were derived; in this work the novel noise-forwarding (NF) strategy was proposed, where the relay node sends codewords independent of the source message to confuse the eavesdropper. Different relaying schemes were studied in [22] and [23] to maximize the secrecy capacity, while minimizing the total transmit power. The authors in [24], exploited physical layer security to provide secure cooperative communication for wireless networks, where security enhancement was achieved by cooperative relaying and cooperative jamming.

To the best of our knowledge, no existing work has considered physical layer security in cooperative PLC systems. Thus, in this paper we focus on investigating the performance of PLC physical layer security with amplify-and-forward (AF) relaying and cooperative jamming over correlated channels and provide accurate results in terms of the average secrecy capacity and outage probability. To seek further security improvements, we extend this work by exploring the impact of joint PLC/wireless coding diversity. The results are based on the assumption that PLC channels have Log-normal distribution as concluded in [19] and [25], and the noise is characterized with a two-term Gaussian noise model in which impulsive noise is modeled as a Bernoulli-Gaussian random process [26]–[28].

In summary, the contribution of this paper is threefold. First, we analyze the average secrecy capacity for cooperative PLC systems, with AF relaying protocol and cooperative jamming technique. Then, we derive an analytical expression for the corresponding secrecy outage probability. Finally, joint PLC/wireless coding diversity gain is analyzed in terms of the secrecy capacity metric. Monte Carlo simulations are included to verify the analysis.

The results reveal that the secrecy performance in the considered system is highly dependent on the jamming power level and relay gain. It is also found that the system security deteriorates when the correlation between the eavesdropper channels degrades. It is also shown that PLC/wireless diversity significantly improves the average secrecy capacity of the considered cooperative PLC system.

The rest of this paper is organized as follows. In Section II we describe the system model under consideration. Section III analyzes the average secrecy capacities at both the legitimate destination and eavesdropper nodes. The corresponding secrecy outage probability is evaluated in Section IV and Section V is dedicated to study the secrecy capacity of the PLC/wireless coding diversity. Numerical and simulation results are presented and discussed in Section VI. Finally, Section VII summarizes the paper and outlines the main conclusions.

II. SYSTEM MODEL

Fig. 1 depicts the system model considered in this study which consists of one source, one AF relay node and one destination node. Also, one illegitimate receiver node is assumed

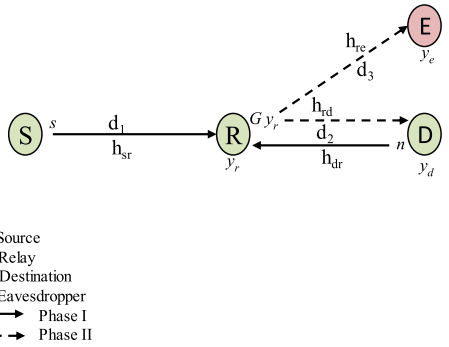


FIGURE 1. Basic PLC system model with cooperative AF relaying in the presence of an eavesdropper.

to eavesdrop the confidential messages from the relay-to-destination link. The source-to-relay, relay-to-destination, destination-to-relay and relay-to-eavesdropper channels are represented by the channel coefficients h_{sr}, h_{rd}, h_{dr} and h_{re}, respectively, all of which are modeled as correlated log-normal random variables [25]. As mentioned in the introduction, the noise signal consists of background and impulsive noise modeled by the two-component mixture-Gaussian noise model. In this model, the background component is considered complex Gaussian whereas the impulsive part is modeled as a Bernoulli-Gaussian random process [28]. Therefore, the additive noise samples at node m can be written as [29]

$$n_{pl_m} = n_{g_m} + n_{i_m}, \tag{1}$$

where $m\epsilon\{r, d, e\}$, n_{pl_m} is the total noise component at node m, n_{g_m} is the additive white Gaussian noise (AWGN) at node m with zero mean and variance σ^2_{gm}, $n_{im} = b_m A_m$ where A_m is complex white Gaussian noise at node m with mean zero and variance σ^2_{im}, and b_m is the Bernoulli process with parameter p_m and its probability mass function is given by

$$\begin{aligned} \Pr(b_m = 1) &= p_m, \\ \Pr(b_m = 0) &= 1 - p_m, \end{aligned} \tag{2}$$

where p_m denotes the impulsive noise probability of occurrence at node m. The variances σ^2_{gm} and σ^2_{im} denote the background and impulsive noise power which basically define the input signal-to-noise ratio (SNR) and signal-to-impulsive noise ratio (SINR) as $\text{SNR} = 10\log_{10}\left(1/\sigma^2_{gm}\right)$ and $\text{SINR} = 10\log_{10}\left(1/\sigma^2_{im}\right)$, respectively. This system model with independent log-normal channels and only Gaussian noise is considered in our previous work [30].

The overall secure source-to-destination transmission is accomplished over two phases referred to as phase I and phase II. During phase I, the source transmits its signal to the relay while the legitimate receiver transmits the artificial noise signal. In phase II, the relay combines and amplifies the two received signals and forwards it to the destination. Since the legitimate receiver has perfect knowledge of the artificial

$$G = \left(\frac{P_r}{P_s \mathbb{E}\left(A\left(d_1, f\right)^2 |h_{sr}|^2\right) + P_n \mathbb{E}\left(A\left(d_2, f\right)^2 |h_{dr}|^2\right) + \sigma_r^2} \right)^{\frac{1}{2}}. \tag{5}$$

$$\gamma_e = \frac{P_s A\left(d_1, f\right)^2 A\left(d_3, f\right)^2 |h_{sr}|^2 |h_{re}|^2 G^2}{P_n A\left(d_2, f\right)^2 A\left(d_3, f\right)^2 |h_{dr}|^2 |h_{re}|^2 G^2 + \sigma_r^2 A\left(d_3, f\right)^2 |h_{re}|^2 G^2 + \sigma_e^2}. \tag{9}$$

noise, this noise can be removed at the legitimate receiver but not at the eavesdropper node.

To elaborate, the received signal at the relay, at a given frequency, in the first phase can be expressed as

$$y_r = \sqrt{P_s} A\left(d_1, f\right) h_{sr}\, s + \sqrt{P_n} A\left(d_2, f\right) h_{dr}\, n + n_r, \tag{3}$$

where P_s is the transmitted source power, $A\left(d_1, f\right)$ is the the power line attenuation, s is the information signal normalized as $\mathbb{E}\left[|s|^2\right] = 1$, P_n is the artificial noise power, n is the artificial noise signal $\mathbb{E}\left[|n|^2\right] = 1$, and n_r is the noise at the relay with variance σ_r^2 .

In phase II, the received signal at the destination node at a given frequency can be written as

$$\begin{aligned} y_d = {} & \sqrt{P_s} A\left(d_1, f\right) A\left(d_2, f\right) h_{sr}\, h_{rd}\, G\, s \\ & + \underbrace{\sqrt{P_n} A\left(d_2, f\right) A\left(d_2, f\right) h_{dr}\, h_{rd}\, G\, n}_{\text{Artificial Noise}} \\ & + n_r A\left(d_2, f\right) h_{rd}\, G + n_d, \end{aligned} \tag{4}$$

where n_d is the noise at the destination with variance σ_d^2 and G is the relay gain which can be considered either constant or variable as a function of the network channel coefficients. For simplicity, however, in this paper we assume a constant relay gain as given by (5), shown at the top of this page, where $|.|$ is the absolute value operator [31].

In this paper we assume that the destination has full state information of the main channel. Therefore, the second term in (4) can be removed and hence y_d can now be simplified as

$$\begin{aligned} y_d = {} & \underbrace{\sqrt{P_s} A\left(d_1, f\right) A\left(d_2, f\right) h_{sr}\, h_{rd}\, G\, s}_{\text{Signal Part}} \\ & + \underbrace{n_r A\left(d_2, f\right) h_{rd}\, G + \bar{n_d}}_{\text{Overall Noise}}, \end{aligned} \tag{6}$$

where $\bar{n_d} = n_d + n_{rs}$ and n_{rs} is the residual artificial noise resulting from imperfect cancellation of the artificial noise part at the destination, with variance σ_{rs}^2. Similarly, the received signal at the eavesdropper end in phase II at a given frequency can be written as

$$\begin{aligned} & y_e \\ & = \underbrace{\sqrt{P_s} A\left(d_1, f\right) A\left(d_3, f\right) G\, h_{sr}\, h_{re}\, s}_{\textit{Signal Part}} \\ & \quad + \underbrace{\sqrt{P_n} A(d_2, f) A(d_3, f) G h_{dr} h_{re} n + A(d_3, f) G h_{re} n_r + n_e}_{\text{Overall Noise}}, \end{aligned} \tag{7}$$

where n_e is the noise at the eavesdropper with variance σ_e^2. From (6) and (7), after some algebraic manipulations, we can write the SNR at the destination and eavesdropper nodes, respectively, as in (8) and (9), shown at the top of this page.

$$\gamma_d = \frac{P_s A\left(d_1, f\right)^2 A\left(d_2, f\right)^2 |h_{sr}|^2 |h_{rd}|^2 G^2}{\sigma_r^2 A\left(d_2, f\right)^2 |h_{rd}|^2 G^2 + \bar{\sigma}_d^2}, \tag{8}$$

where $\bar{\sigma}_d^2 = \sigma_d^2 + \sigma_{rs}^2$.

III. AVERAGE SECRECY CAPACITY

It is known that the secrecy capacity, C_s, is given by the maximum difference between the mutual information of the main and eavesdropper channels as follows [32], [33]. Assuming that the channel state information is unknown at the transmitter, the average secrecy capacity in this case can be obtained as [33, p. 4692] [34, eq. (4)],

$$\bar{C}_s = \left[\mathbb{E}\left[C_d\right] - \mathbb{E}\left[C_e\right]\right]^+, \tag{10}$$

where $[l]^+ = \max\left(0,\, l\right)$, C_d and C_e are the destination and eavesdropper capacities, respectively. Full derivation of the average secrecy capacity expressions in different scenarios are provided in [32] and [33].

In order to simplify the analysis of the average secrecy capacity over the impulsive noise PLC channel, we consider the upper bound under the assumption that full knowledge of the noise state is available at the nodes. In this case with direct source to destination transmission, the channel capacity (in bits/sec/Hz) can be expressed by [30, eq. (35)] and [35]–[38]

$$C_d = \sum_{j=0}^{1} p_j \log_2\left(1 + \gamma_{d_j}\right), \tag{11}$$

where $p_0 = \left(1 - p_d\right)$, $p_1 = p_d$, γ_{d_0} is the instantaneous SNR under only AWGN and γ_{d_1} is the instantaneous SNR under both AWGN and impulsive noises. Therefore, with perfect knowledge of the noise states, (11) can be interpreted as the average of the capacities of two channels, one channel under only the AWGN with fraction $\left(1 - p_d\right)$, and the other under both AWGN and impulsive noises with fraction p_d.

In the relaying systems, each link (S-R, R-D) can either face impulsive noise and background noise or only background noise. Therefore, there are four possible sates of the additive noise at each node as shown in the table 1.

From this definition, it is clear that for one hop relay system, the capacity can be written as a sum of four

TABLE 1. Possible cases of the noises at the system nodes.

Impulsive noise in relay link	Impulsive noise in destination link	Noise variance at the relay	Noise variance at the destination	SNR
NO	NO	$\sigma^2_{r,0}=\sigma^2_{gr}$	$\sigma^2_{d,0}=\sigma^2_{gd}$	$\gamma_{d_{0,0}}$
NO	YES	$\sigma^2_{r,0}=\sigma^2_{gr}$	$\sigma^2_{d,1}=\sigma^2_{gd}+\sigma^2_{id}$	$\gamma_{d_{0,1}}$
YES	NO	$\sigma^2_{r,1}=\sigma^2_{gr}+\sigma^2_{ir}$	$\sigma^2_{d,0}=\sigma^2_{gd}$	$\gamma_{d_{1,0}}$
YES	YES	$\sigma^2_{r,1}=\sigma^2_{gr}+\sigma^2_{ir}$	$\sigma^2_{d,1}=\sigma^2_{gd}+\sigma^2_{id}$	$\gamma_{d_{1,1}}$

terms as

$$C_d = \frac{1}{2}\Big(p_{r,0}p_{d,0}\log_2\left(1+\gamma_{d_{0,0}}\right)+p_{r,0}p_{d,1}\log_2\left(1+\gamma_{d_{0,1}}\right) + p_{r,1}p_{d,0}\log_2\left(1+\gamma_{d_{1,0}}\right)+p_{r,1}p_{d,1}\log_2\left(1+\gamma_{d_{1,1}}\right)\Big), \tag{12}$$

where $\gamma_{d_{0,0}}$ is the instantaneous end-to-end SNR under only AWGN in S-R and R-D links, $\gamma_{d_{0,1}}$ is the instantaneous end-to-end SNR under only AWGN in S-R link and both AWGN and impulsive noises in R-D link, $\gamma_{d_{1,0}}$ is the instantaneous SNR under both AWGN and impulsive noises in S-R link and only AWGN in R-D link, $\gamma_{d_{1,1}}$ is the instantaneous SNR under both AWGN and impulsive noises in S-R and R-D links, $p_{r,0}=(1-p_r)$, $p_{r,1}=p_r$, $p_{d,0}=(1-p_d)$ and $p_{d,1}=p_d$., $p_{r,0}=(1-p_r)$, $p_{r,1}=p_r$, $p_{d,0}=(1-p_d)$ and $p_{d,1}=p_d$. The capacity in (12) can also be written as

$$C_d = \frac{1}{2}\sum_{i=0}^{1}\sum_{j=0}^{1} p_{r,i}p_{d,j}\log_2\left(1+\gamma_{d_{i,j}}\right). \tag{13}$$

The factor $\frac{1}{2}$ is due to the fact that two time slots are required for transmitter-to-receiver data transmission. Now, in order to find the average secrecy capacity $\bar{C}_s$, we need to calculate the average destination capacity $\bar{C}_d$ and the average eavesdropper capacity $\bar{C}_e$.

A. AVERAGE DESTINATION CAPACITY

To find the average capacity at the destination, it is more convenient to rewrite γ_d in (8) as

$$\gamma_{d_{i,j}} = \frac{X}{Y_i+W_j}, \tag{14}$$

where $X = P_s A(d_1,f)^2 A(d_2,f)^2 |h_{sr}|^2 G^2$, $Y_i = \sigma^2_{r,i} A(d_2,f)^2 G^2$ and $W_j = \frac{\bar{\sigma}^2_{d,j}}{|h_{rd}|^2}$. Hence from (13), the capacity at the destination C_d can now be expressed as

$$C_d = \frac{1}{2}\sum_{i=0}^{1}\sum_{j=0}^{1} p_{r,i}p_{d,j}\log_2\left(1+\frac{X}{Y_i+W_j}\right). \tag{15}$$

Lemma 1: It is found in [39] that for any u, $v>0$

$$\mathbb{E}\left[ln\left(1+\frac{u}{v}\right)\right] = \int_0^\infty \frac{1}{z}\left(\mathcal{M}_v(z)-\mathcal{M}_{v,u}(z)\right)dz, \tag{16}$$

where $\mathcal{M}_v(z)$ denotes the moment generating function (MGF) of v and $\mathcal{M}_{v,u}(z)$ is the MGF of $(v+u)$.

Using the definition in (16), and since X and W are correlated, the destination average capacity can be obtained as

$$\mathbb{E}[C_d] = \frac{1}{2\ln(2)}\sum_{i=0}^{1}\sum_{j=0}^{1} p_{r,i}p_{d,j} \times \int_0^\infty \frac{1}{z}\left(\mathcal{M}_{Y_i,W_j}(z)-\mathcal{M}_{X,Y_i,W_j}(z)\right)dz, \tag{17}$$

where $\mathcal{M}_{Y_i,W_j}(z)$ and $\mathcal{M}_{X,Y_i,W_j}(z)$ are the MGFs of the variables Y_i+W_j and $X+Y_i+W_j$, respectively. Now, since Y is constant, the MGF of Y_i+W_j can be written as [40]

$$\mathcal{M}_{Y_i,W_j}(z) = \mathcal{M}_{Y_i}(z)\,\mathcal{M}_{W_j}(z), \tag{18}$$

where

$$\mathcal{M}_{Y_i}(z) = e^{-z\sigma^2_{r,i}A(d_2,f)^2G^2}. \tag{19}$$

and

$$\mathcal{M}_{W_j}(z) = \mathcal{M}_{\frac{1}{|h_{rd}|^2}}\left(\bar{\sigma}^2_{d,j}z\right), \tag{20}$$

$$\mathcal{M}_{\left(\sum_{k=1}^{K}\Omega_k Y_k\right)}(z) \simeq \sum_{n_1=1}^{N_p}\sum_{n_2=1}^{N_p}....\sum_{n_K=1}^{N_p}\left(\prod_{k=1}^{K}\frac{H_{n_k}}{\sqrt{\pi}}\right)\times\exp\left(-\sum_{k=1}^{K}z\Omega_k\exp\left(\sqrt{2}\sum_{J=1}^{K}c_{kJ}x_{n_J}+\mu_k\right)\right)+R_N. \tag{23}$$

$$\mathcal{M}_{Y_iW_j}(z) \simeq \frac{\mathcal{M}_{Y_i}(z)}{\sqrt{\pi}}\sum_{i=1}^{N_p}H_{x_i}\exp\left(10^{\frac{-\sqrt{2}2\sigma_{h_{rd}}x_i+-\left(2\mu_{h_{rd}}\right)}{10}}\bar{\sigma}^2_{d,j}z\right). \tag{24}$$

$$\mathcal{M}_{X,W_j,Y_i}(z) \simeq \mathcal{M}_{Y_i}(z)\sum_{n_1=1}^{N_p}\sum_{n_2=1}^{N_p}\left(\prod_{k=1}^{2}\frac{H_{n_k}}{\sqrt{\pi}}\right)\times\exp\left(-\sum_{k=1}^{2}z\Omega_k\exp\left(\sqrt{2}\sum_{J=1}^{2}c_{kJ}x_{n_J}+\mu_k\right)\right). \tag{25}$$

where $\bar{\sigma}^2_{d,j} = \sigma^2_{d,j} + \sigma^2_{rs}$. Similarly, because X and W_j are correlated, the MGF of $X + Y_i + W_j$ can be expressed as [40]

$$\mathcal{M}_{X,\,Y_i,\,W_j}(z) = \mathcal{M}_{Y_i}(z)\,\mathcal{M}_{X,W_j}(z)\,. \tag{21}$$

As the PLC channel is generally represented with log-normal distribution [18], the MGF of channel (h) is [41, eq. (2.28)]

$$\mathcal{M}_h(z) \simeq \frac{1}{\sqrt{\pi}}\sum_{i=1}^{N_p} H_{x_i} \exp\left(10^{\frac{\sqrt{2}\sigma_h x_i + \mu_h}{10}} z\right), \tag{22}$$

where H_{x_i} and x_i are the weight factors and zeros of the N_p-order Hermite polynomial, respectively, and $\mu_h, \sigma_h$are the mean and the standard deviation of the channel h. Furthermore, the MGF of K lognormal correlated channels are given by (23), shown at the bottom of the previous page, [42], [43], where Ω_k is arbitrary non negative constants, c_{kJ} is the $(k.J)^{th}$ element of the square root of the correlation matrix R_M, i.e elements of $R_{sq}$where $R_M = R_{sq}R^{\dagger}_{sq}$, and the reminder R_N is sufficiently small when $N_p > 10$ [42], [43].

Using these definitions, for $|h_{sr}|^2 \overset{d}{\sim}$ lognormal $\left(2\mu_{h_{sr}},\, 4\sigma^2_{h_{sr}}\right)$ and $\frac{1}{|h_{rd}|^2} \overset{d}{\sim}$ lognormal $\left(-2\mu_{h_{rd}},\, 4\sigma^2_{h_{rd}}\right)$, we can express the MGFs of $W_j + Y_i$ and $X + W_j + Y_i$, respectively, as in (24) and (25), shown at the bottom of the previous page, where $\Omega_1 = P_s A(d_1,f)^2 A(d_2,f)^2 |h_{sr}|^2 G^2$ and $\Omega_2 = \bar{\sigma}^2_{d,j}$.

Finally, the average capacity at the destination can be obtained by simply substituting (24) and (25) into (17).

B. AVERAGE EAVESDROPPER CAPACITY

Similarly as in the previous section, the average capacity at the eavesdropper can be derived here. We begin by rewriting (9) as

$$\gamma_{e_{i,l}} = \frac{\chi}{S + \Upsilon_i + C_l}, \tag{26}$$

where $\chi = P_s A(d_1,f)^2 A(d_3,f)^2 |h_{sr}|^2 G^2$, $S = P_n A(d_2,f)^2 A(d_3,f)^2 |h_{dr}|^2 G^2$, $\Upsilon_i = \sigma^2_{r,i} A(d_3,f)^2 G^2$ and $C_l = \frac{\sigma^2_{e,l}}{|h_{re}|^2}$. Now, using (13) and (16) and based on the fact that χ , S and C are correlated, the average capacity at the eavesdropper can be expressed as

$$\mathbb{E}[C_e] = \frac{1}{2\ln(2)}\sum_{i=0}^{1}\sum_{l=0}^{1} p_{r,i}\,p_{e,l} \times \int_0^{\infty}\frac{1}{z}\left(\mathcal{M}_{S,\,\Upsilon_i,\,C_l}(z) - \mathcal{M}_{\chi,S,\,\Upsilon_i,\,C_l}(z)\right)dz, \tag{27}$$

where $p_{e,0} = (1 - p_e)$, $p_{e,1} = p_e$. The $\mathcal{M}_{S,\,\Upsilon_i,\,C_l}(z)$ can be given by

$$\mathcal{M}_{S,\,\Upsilon_i,\,C_l}(z) = \mathcal{M}_{\Upsilon_i}(z)\;\mathcal{M}_{S,C_l}(z)\,, \tag{28}$$

where

$$\mathcal{M}_{\Upsilon_i}(z) = e^{-z\sigma^2_{r,i}A(d_3,f)^2G^2}, \tag{29}$$

As in (25), $\mathcal{M}_{S,\,\Upsilon_i,\,C_l}(z)$ can be given by

$$\mathcal{M}_{S,\,\Upsilon_i,\,C_l}(z) \simeq \mathcal{M}_{\Upsilon_i}(z)\sum_{n_1=1}^{N_p}\sum_{n_2=1}^{N_p}\left(\prod_{k=1}^{2}\frac{H_{n_k}}{\sqrt{\pi}}\right) \times \exp\left(-\sum_{k=1}^{2} z\Omega_k \exp\left(\sqrt{2}\sum_{J=1}^{2} c_{kJ}x_{n_J} + \mu_k\right)\right), \tag{30}$$

where $\Omega_1 = P_n A(d_2,f)^2 A(d_3,f)^2 G^2$, $\Omega_2 = \sigma^2_{e,l}$, $\sigma^2_{e,0} = \sigma^2_{ge}$ and $\sigma^2_{e,1} = \sigma^2_{ge} + \sigma^2_{ie}$. Similarly, the $\mathcal{M}_{\chi,S,\,\Upsilon_i,\,C_l}(z)$ can be written as

$$\mathcal{M}_{\chi,S,\,\Upsilon_i,\,C_l}(z) = \mathcal{M}_{\Upsilon_i}(z)\,\mathcal{M}_{\chi,S,C_l}(z)\,, \tag{31}$$

where

$$\mathcal{M}_{\chi,S,C_l}(z) = \sum_{n_1=1}^{N_p}\sum_{n_2=1}^{N_p}\sum_{n_3=1}^{N_p}\left(\prod_{k=1}^{3}\frac{H_{n_k}}{\sqrt{\pi}}\right) \times \exp\left(-\sum_{k=1}^{3} z\Omega_k \exp\left(\sqrt{2}\sum_{J=1}^{3} c_{kJ}x_{n_J} + \mu_k\right)\right), \tag{32}$$

while $\Omega_3 = P_s A(d_1,f)^2 A(d_3,f)^2 G^2$.

$$\mathbb{E}[C_d] \approx \sum_{i=0}^{1}\sum_{j=0}^{1} p_{r,i}p_{d,j}\frac{1}{2\ln(2)\,Y_i}\sum_{\epsilon=1}^{n}\omega_\epsilon\frac{Y_i}{z_\epsilon}\left(\frac{1}{\sqrt{\pi}}\sum_{i=1}^{N_p}H_{x_i}\exp\left(10^{\frac{-\sqrt{2}2\sigma_{h_{rd}}x_i + -\left(2\mu_{h_{rd}}\right)}{10}}\frac{\bar{\sigma}^2_{d,j}z_\epsilon}{Y_i}\right) - \sum_{n_1=1}^{N_p}\sum_{n_2=1}^{N_p}\left(\prod_{k=1}^{2}\frac{H_{n_k}}{\sqrt{\pi}}\right) \times \exp\left(-\sum_{k=1}^{2}\frac{z_\epsilon\Omega_k}{Y_i}\exp\left(\sqrt{2}\sum_{J=1}^{2}c_{kJ}x_{n_J} + \mu_k\right)\right)\right). \tag{33}$$

$$\mathbb{E}[C_e] \approx \sum_{i=0}^{1}\sum_{l=0}^{1} p_{r,i}\,p_{e,l}\,\frac{1}{2\ln(2)\,\Upsilon_i}\sum_{\epsilon=1}^{n}\omega_\epsilon\frac{\Upsilon_i}{z_\epsilon}\left(\sum_{n_1=1}^{N_p}\sum_{n_2=1}^{N_p}\left(\prod_{k=1}^{2}\frac{H_{n_k}}{\sqrt{\pi}}\right) \times \exp\left(-\sum_{k=1}^{2}\frac{z_\epsilon\Omega_k}{\Upsilon_i}\exp\left(\sqrt{2}\sum_{J=1}^{2}c_{kJ}x_{n_J} + \mu_k\right)\right)\right. - \sum_{n_1=1}^{N_p}\sum_{n_2=1}^{N_p}\sum_{n_3=1}^{N_p}\left(\prod_{k=1}^{3}\frac{H_{n_k}}{\sqrt{\pi}}\right) \times \exp\left(-\sum_{k=1}^{3}\frac{z_\epsilon\Omega_k}{\Upsilon_i}\Omega_k\exp\left(\sqrt{2}\sum_{J=1}^{3}c_{kJ}x_{n_J} + \mu_k\right)\right)\Bigg). \tag{34}$$

$$P_{out} = \Pr\left[\left(\frac{1}{2}\sum_{i=0}^{1}\sum_{j=0}^{1} p_{r,i}p_{d,j}\,\log_2\left(1+\gamma_{d_{i,j}}\right) - \frac{1}{2}\sum_{i=0}^{1}\sum_{l=0}^{1} p_{r,i}\,p_{e,l}\,\log_2\left(1+\gamma_{e_{i,l}}\right)\right) < R\right]. \tag{36}$$

$$P_{out} = 1 - \Pr\left[X > \frac{\upsilon - 1}{\frac{1}{W+Y} - \frac{\upsilon\,\Theta}{C+Y\,\Theta+S}} \mid C = c,\ S = s,\ W = w\right]. \tag{41}$$

$$\bar{F}_X(r) = 1 - \frac{1}{2}\left(1 + \mathrm{erf}\left(\frac{\ln(r) - \left(2\mu_{h_{sr}} + \ln\left(P_s A\,(d_1,f)^2\,A\,(d_2,f)^2\,G_r^2\right)\right)}{2\sigma_{h_{sr}}\sqrt{2}}\right)\right). \tag{44}$$

$$f(s,c,w) = \frac{\exp\left(-\left(\frac{1}{2}\right)(\ln(\mathbf{h}) - \boldsymbol{\mu_h})^T\,\mathbf{K_h^{-1}}\,(\ln(\mathbf{h}) - \boldsymbol{\mu_h})\right)}{(2\pi)^{\frac{3}{2}}\,|\mathbf{K_h}|^{\frac{1}{2}}\prod_{l=1}^{3} h_l}. \tag{45}$$

Now by substituting (30) and (31) into (27), we get the average eavesdropper capacity. Finally, substituting (17) and (27) into (10) yields the average secrecy capacity of the proposed system.

According to the best of the authors knowledge, these expressions of $\mathbb{E}[C_d]$ and $\mathbb{E}[C_e]$ are the simplest expressions for the average capacities. Furthermore, to more clearly highlight the effect of various system parameters, Gaussian Quadrature rule can be straightforwardly applied. For instance we can write (17) and (27) as in (33) and (34), respectively, shown at the bottom of the previous page, where z_ϵ and ω_ϵ are the ϵ^{th} abscissa and weight, respectively, of the *nth* order Laguerre polynomial, tabulated in [44, eq. (25 .4 .45)].

IV. SECRECY OUTAGE PROBABILITY

The secrecy outage probability is defined basically as the probability that the secrecy capacity falls below a certain threshold value, R, and can be mathematically given as

$$P_{out} = \Pr[C_s < R]. \tag{35}$$

The secrecy outage probability can be written as in (36), as shown at the top of this page.

It should be stressed that the secrecy outage in this work means that in an ensemble of networks we do not offer a certain secrecy rate. In this section, for simplicity we assume that, the source relay channel h_{sr} is independent of the other channels, as adopted in [29] and [37]. In addition, in order to make the analysis clearer we study one case, when there is no impulsive noise.[1] Therefore,

$$P_{out} = \Pr\left[\frac{1+\gamma_d}{1+\gamma_e} < \upsilon\right] = \Pr[\gamma_d - \upsilon\gamma_e < \upsilon - 1], \tag{37}$$

[1]Numerical results for the exact secrecy outage probability will be presented in the numerical results section.

where $\upsilon = 2^{2R}$. Substituting (14) and (26) into (37) yields

$$P_{out} = \Pr\left[\frac{X}{Y+W} - \frac{\upsilon\,\chi}{C+\Upsilon+S} < \upsilon - 1\right]. \tag{38}$$

By substituting $\chi = X\Theta$ and $\Upsilon = Y\Theta$, where $\Theta = \left(\frac{A(d_3,f)^2}{A(d_2,f)^2}\right)$, we can write the secrecy outage probability now as

$$P_{out} = \Pr\left[\frac{X}{Y+W} - \frac{\upsilon\,\Theta X}{C+Y\,\Theta+S} < \upsilon - 1\right]. \tag{39}$$

$$= \Pr\left[X < \frac{\upsilon - 1}{\frac{1}{W+Y} - \frac{\upsilon\,\Theta}{C+Y\,\Theta+S}}\right]. \tag{40}$$

By conditioning on C, S and W, P_{out} can be written as in (41), as shown at the top of this page, which can also be expressed as

$$P_{out} = 1 - \int_0^\infty\int_0^\infty\int_0^\infty \bar{F}_X(r)\,f(s,c,w)\,ds\,dc\,dw, \tag{42}$$

where $\bar{F}_X(.)$ is the complementary cumulative distribution function (CCDF) of the random variable X, $f(s,c,w)$, is the joint PDF and

$$r = \frac{\upsilon - 1}{\frac{1}{w+Y} - \frac{\upsilon\,\Theta}{c+Y\,\Theta+s}}. \tag{43}$$

Since X, S, C and W have log-normal distributions, i. e., $X \overset{\mathrm{d}}{\sim} \mathrm{lognormal}\left(2\mu_{h_{sr}} + \ln\left(P_s A\,(d_1,f)^2\,A(d_2,f)^2 G_r^2\right), 4\sigma_{h_{sr}}^2\right)$, $S \overset{\mathrm{d}}{\sim} \mathrm{lognormal}\left(2\mu_{h_{rd}} + \ln\left(P_n A\,(d_2,f)^2\,A\,(d_3,f)^2\,G_r^2\right), 4\sigma_{h_{rd}}^2\right)$, $C \overset{\mathrm{d}}{\sim}$ lognormal $\left(-2\mu_{h_{re}} + \ln\left(\sigma_e^2\right),\ 4\sigma_{h_{re}}^2\right)$, and $W \overset{\mathrm{d}}{\sim}$ lognormal $\left(-2\mu_{h_{rd}} + \ln\left(\sigma_d^2\right),\ 4\sigma_{h_{rd}}^2\right)$, the CCDF of X and the joint PDF $f(s,c,w)$ can be written as in (44) and (45), as shown at the top of this page, respectively [37], [45], [46], where $\mathbf{h} = [S,C,W]^T$, $\boldsymbol{\mu_h}$ is the mean

$$P_{out} = 1 - \int_0^{\infty}\int_0^{\infty} \left(1 - \frac{1}{2}\left(1 + \text{erf}\left(\frac{\ln\left(\frac{\upsilon - 1}{\frac{1}{\frac{\delta}{S}+Y} - \frac{\upsilon\Theta}{c+Y\Theta+s}}\right) - \left(2\mu_{h_{sr}} + \ln\left(P_s A\left(d_1, f\right)^2 A\left(d_2, f\right)^2 G_r^2\right)\right)}{2\sigma_{h_{sr}}\sqrt{2}}\right)\right)\right) \times \left(\frac{1}{2\pi\sigma_s\sigma_c\, s\, c\,\sqrt{\left(1-\rho^2\right)}} \times \exp\left(-\frac{A^2 + B^2 - 2\rho AB}{2\left(1-\rho^2\right)}\right)\right) ds\, dc. \tag{48}$$

$$P_{out} \approx 1 - \sum_{\varphi=1}^{m}\sum_{\epsilon=1}^{n} \omega_\varphi \omega_\epsilon \left(1 - \frac{1}{2}\left(1 + \text{erf}\left(\frac{\ln\left(\frac{\upsilon - 1}{\frac{1}{\frac{\delta}{S_\varphi}+Y} - \frac{\upsilon\Theta}{c_\epsilon+Y\Theta+s_\varphi}}\right) - \left(2\mu_{h_{sr}} + \ln\left(P_s A\left(d_1, f\right)^2 A\left(d_2, f\right)^2 G_r^2\right)\right)}{2\sigma_{h_{sr}}\sqrt{2}}\right)\right)\right) \times \left(\frac{e^{s_\varphi + c_\epsilon}}{2\pi\sigma_s\sigma_c\, s_\varphi\, c_\epsilon\,\sqrt{\left(1-\rho^2\right)}} \times \exp\left(-\frac{\left(\frac{\left(\ln(s_\varphi)-\mu_s\right)}{\sigma_s}\right)^2 + \left(\frac{\left(\ln(c_\epsilon)-\mu_c\right)}{\sigma_c}\right)^2 - 2\rho\left(\frac{\left(\ln(s_\varphi)-\mu_s\right)}{\sigma_s}\right)\left(\frac{\left(\ln(c_\epsilon)-\mu_c\right)}{\sigma_c}\right)}{2\left(1-\rho^2\right)}\right)\right). \tag{49}$$

vector $\boldsymbol{\mu_h} = [\mu_s, \mu_c, \mu_w]^T$, $\mathbf{K_h}$ is the covariance matrix and $|\mathbf{K_h}|$ is the the determinant of $\mathbf{K_h}$.

In case h_{dr} and h_{rd} are fully correlated, we can use $W = \frac{\delta}{S}$ where $\delta = \bar{\sigma}_d^2 P_n A\left(d_2, f\right)^2 A\left(d_3, f\right)^2 G^2$. As a consequence, the integration in (42) reduces into double integration

$$P_{out} = 1 - \int_0^{\infty}\int_0^{\infty} \bar{F}_X\left(r\right) f\left(s, c\right) ds\, dc. \tag{46}$$

and the joint PDF $f\left(s, c\right)$ can now be written as

$$f\left(s, c\right) = \frac{1}{2\pi\sigma_s\sigma_c\, s\, c\,\sqrt{\left(1-\rho^2\right)}} \times \exp\left(-\frac{A^2 + B^2 - 2\rho AB}{2\left(1-\rho^2\right)}\right), \tag{47}$$

where $A = \left(\ln\left(s\right) - \mu_s\right)/\sigma_s$, $B = \left(\ln\left(c\right) - \mu_c\right)/\sigma_c$, while μ and σ^2 are the mean and the variance of the natural logarithm of S and C and ρ is the correlation factor. Substituting (44) and (47) into (46) we can find the secrecy outage probability in this case as in (48).

Similarly, in order to get a simple closed form for the secrecy outage probability, Quadrature rule can be straightforward applied, as in (49), where $\left(s_\varphi, c_\epsilon\right)$ and $\left(\omega_\varphi, \omega_\epsilon\right)$ are the φ^{th}, ϵ^{th} abscissa and weights of the Laguerre polynomial.

Generally, we found that the secrecy performance of the proposed system above is still somewhat limited (see the numerical results section). Therefore, we look at ways to further improve the secrecy of the proposed system. One way of doing this is by considering PLC/wireless diversity which is going to be discussed next.

V. PLC/WIRELESS DIVERSITY

It is known that the utilization of parallel PLC and wireless links can considerably enhance the network capacity, this scheme is considered in the literature, for instance [47]–[49]. PLC/wireless diversity provides two links, PLC and wireless; increasing the number of communication links enhances the system performance since only the eavesdropper receives jamming signals through the two links, while the destination does not. Therefore, in this section we analyze the secrecy capacity of such networks with the objective to achieve efficient use of parallel transmission channels. The considered coding diversity for PLC/wireless transmission is shown in Fig. 2 where the output of the encoder is de-multiplexed and then transmitted over different channels. Therefore, the source transmits two signals over two independent links, PLC and wireless. Cooperative diversity gains over Rayleigh and Log-normal channels considered in details in [50]–[52].

In this configuration, the capacity at the destination and the eavesdropper can be given, respectively, as [47], [48]

$$C_d = C_d^{\{w\}} + C_d^{\{p\}}, \tag{50}$$

$$C_e = C_e^{\{w\}} + C_e^{\{p\}}, \tag{51}$$

where the superscripts $\{w\}$ and $\{p\}$ denote the capacities for the wireless and PLC links, respectively. Therefore, the average secrecy capacity can now be simply written as

$$\mathbb{E}\left[C_s\right] = \left[\mathbb{E}\left[C_d^{\{w\}} + C_d^{\{p\}}\right] - \mathbb{E}\left[C_e^{\{w\}} + C_e^{\{p\}}\right]\right]^+. \tag{52}$$

$\mathbb{E}\left[C_d^{\{p\}}\right]$ and $\mathbb{E}\left[C_e^{\{p\}}\right]$ are already calculated in the previous section. Now, using a similar procedure, we can derive $\mathbb{E}\left[C_d^{\{w\}}\right]$ and $\mathbb{E}\left[C_e^{\{w\}}\right]$ as shown below.

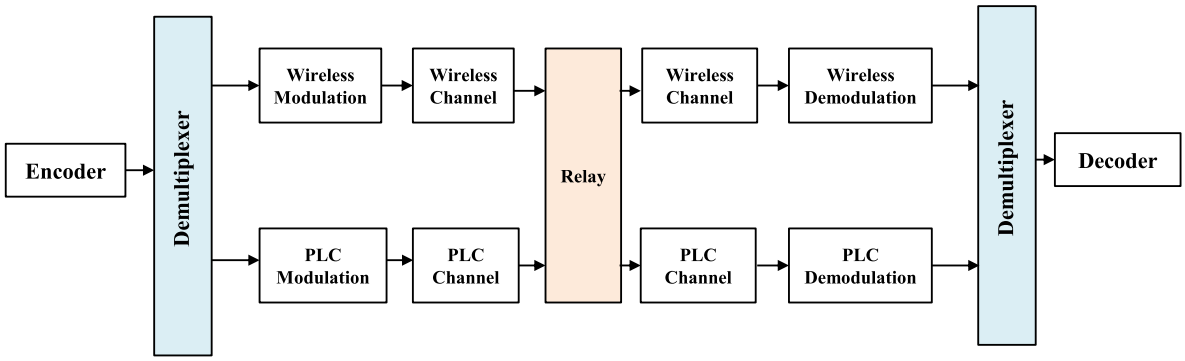


FIGURE 2. Architecture of PLC/wireless coding diversity with cooperative relaying.

A. WIRELESS AVERAGE DESTINATION CAPACITY

The average capacity at the destination for the wireless link also can be found by using (14) and (16) when $X = P_s |h_{sr}|^2 G^2$, $Y = \sigma_r^2 G^2 d_1^m$ and $W = \bar{\sigma}_d^2 d_1^m d_2^m / |h_{rd}|^2$ and m is the wireless path loss exponent. In addition, the channels coefficients between the nodes are now complex Gaussian with zero mean and unit variance, i.e. $\mathcal{CN}(0, 1)$. Therefore, $|h_{rd}|^2$ and $|h_{sr}|^2$ have exponential distributions with parameters $\lambda_{h_{rd}}$ and $\lambda_{h_{sr}}$, respectively. With this in mind, we obtain [39], [53]

$$\mathbb{E}\left[C_d^{\{w\}}\right] = \frac{1}{2\ln(2)} \int_0^\infty \frac{1}{z} \left(\mathcal{M}_{Y,W}(z) - \mathcal{M}_{X,Y,W}(z)\right) dz. \tag{53}$$

In this case the MGFs of W and X are given by

$$\mathcal{M}_W(z) = 2\sqrt{\lambda_{h_{rd}} \sigma_d^2 d_1^m d_2^m z}\, K_1\left(2\sqrt{\lambda_{h_{rd}} \sigma_d^2 d_1^m d_2^m z}\right). \tag{54}$$

and

$$\mathcal{M}_X(z) = \frac{\lambda_{h_{sr}}}{\lambda_{h_{sr}} + P_s G^2 z}. \tag{55}$$

where $K_N(.)$ is the N^{th} order modified Bessel function of the second kind [54], then we can find $\mathcal{M}_{Y,W}(z)$ and $\mathcal{M}_{X,Y,W}(z)$ for the wireless system as given by (56) and (57), as shown at the bottom of this page.

Finally, the wireless average capacity at the destination can be obtained by simply substituting (56) and (57) into (53), as in (58), as shown at the bottom of this page.

B. WIRELESS AVERAGE EAVESDROPPER CAPACITY

For the wireless average capacity at the eavesdropper, it can be found from (26) and (16) where $\chi = P_s |h_{sr}|^2 G^2 d_2^m$, $S = P_n |h_{dr}|^2 G^2 d_1^m$, $\Upsilon = \sigma_r^2 G^2 d_1^m d_2^m$ and $C = \sigma_e^2 d_1^m d_2^m d_3^m / |h_{re}|^2$. In this case,

$$\mathbb{E}\left[C_e^{\{w\}}\right] = \frac{1}{2\ln(2)} \int_0^\infty \frac{1}{z} \left(1 - \mathcal{M}_\chi(z)\right) \mathcal{M}_{S,\Upsilon,C}(z)\, dz, \tag{59}$$

where $\mathcal{M}_\chi(z)$ and $\mathcal{M}_{S,\Upsilon,C}(z)$ are given respectively by (60) and (61), respectively

$$\mathcal{M}_\chi(z) = \frac{\lambda_{h_{sr}}}{\lambda_{h_{sr}} + P_s G^2 d_2^m z}. \tag{60}$$

Now, by substituting (60) and (61) into (59), we can get the wireless average eavesdropper capacity as in (62).

According to the best of the authors knowledge, these expressions of $\mathbb{E}\left[C_d^{\{w\}}\right]$ and $\mathbb{E}\left[C_e^{\{w\}}\right]$ are the simplest

$$\mathcal{M}_{Y,W}(z) = 2\exp(-zY) \sqrt{\lambda_{h_{rd}} \bar{\sigma}_d^2 d_1^m d_2^m z}\, K_1\left(2\sqrt{\lambda_{h_{rd}} \bar{\sigma}_d^2 d_1^m d_2^m z}\right). \tag{56}$$

$$\mathcal{M}_{X,Y,W}(z) = \frac{2\exp(-zY)\,\lambda_{h_{sr}}}{\lambda_{h_{sr}} + P_s G^2 z} \sqrt{\lambda_{h_{rd}} \bar{\sigma}_d^2 d_1^m d_2^m z}\, K_1\left(2\sqrt{\lambda_{h_{rd}} \bar{\sigma}_d^2 d_1^m d_2^m z}\right). \tag{57}$$

$$\mathbb{E}\left[C_d^{\{w\}}\right] = \frac{1}{2\ln(2)} \int_0^\infty \frac{1}{z} \left(2\exp(-zY) \sqrt{\lambda_{h_{rd}} \bar{\sigma}_d^2 d_1^m d_2^m z}\, K_1\left(2\sqrt{\lambda_{h_{rd}} \bar{\sigma}_d^2 d_1^m d_2^m z}\right) - \frac{2\exp(-zY)\,\lambda_{h_{sr}}}{\lambda_{h_{sr}} + P_s G^2 z} \sqrt{\lambda_{h_{rd}} \bar{\sigma}_d^2 d_1^m d_2^m z}\, K_1\left(2\sqrt{\lambda_{h_{rd}} \bar{\sigma}_d^2 d_1^m d_2^m z}\right)\right) dz. \tag{58}$$

expressions for the wireless average capacities; in order to more clearly highlight the effect of various system parameters, Gaussian Quadrature rule can be straightforwardly applied as in (63) and (64) , respectively, where z_ϵ and ω_ϵ are the ϵ^{th} abscissa and weight, respectively, of the *nth* order Laguerre polynomial, tabulated in [44, eq. (25 .4 .45)].

Finally, substituting the PLC and wireless average capacities into (52) yields the overall average secrecy capacity of the proposed PLC/wireless system.

A MIMO-PLC scheme can also be employed to further improve the security of PLC systems. The cooperative jamming technique proposed in this paper for SISO system can be extended for the MIMO case where each legitimate receiver transmits different jamming signal over its channel (wire) in the first cooperative phase, and in the second phase all the legitimate receivers can cancel out the self back-interference, taking into account the high degree of correlation among the channels.[2]

Below we present and discuss some numerical examples for the derived expressions above.

VI. NUMERICAL RESULTS

In this section, we present numerical results for the average secrecy capacity and the outage probability. Monte Carlo simulations are also provided to verify our analysis. The correlation between the channels is shown to follow the exponential model [46]. Therefore, the covariance matrix is given by

$$\mathbf{K} = \begin{bmatrix} 1 & \rho & ..... & \rho^{L-1} \\ \rho & 1 & ..... & \rho^{L-2} \\ .. & .. & ..... & ... \\ \rho^{L-1} & \rho^{L-2} & ..... & 1 \end{bmatrix}. \quad (65)$$

where L number of the correlated channels. In addition, in order to characterize the power line attenuation, we adopt the model reported in [4] in which attenuation increases exponentially with distance, given by $\exp(-\alpha d)$, where $\alpha = a_o + a_1 f^k$ is the attenuation factor, a_o and a_1 are constants determined from measurements, f is the frequency and k denotes the exponent of the attenuation factor. The system parameters adopted here, unless clearly stated otherwise, are as follows: $k = 0.7, f = 500\,\text{KHz}$ [4], [37], [46]. Furthermore, for fairness sake, the impulsive noise probability of occurrence at all the nodes are equal (p) and all the channels have zero mean and unit variance.

[2]The security in MIMO-PLC systems will be investigated in future work.

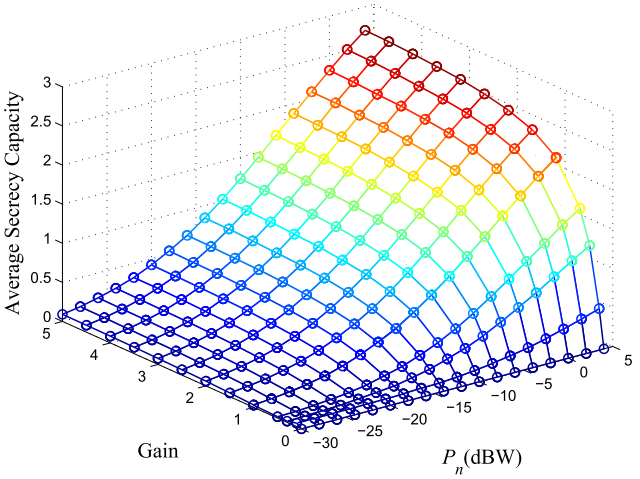


FIGURE 3. A 3D surface plot for the average secrecy capacity as a function of the artificial noise power and relay gain (circles represent simulated results).

A. AVERAGE SECRECY CAPACITY

In this subsection, we examine the average secrecy capacity of the proposed system. In order to illustrate the impact of the artificial noise power and the relay gain on the system security, we present in Fig. 3 a 3D surface plot for the average secrecy capacity versus P_n and G when the input SNR $= 25\,\text{dB}$, SINR $= -10\,\text{dB}$, $p = 0.001$, $P_s = -3\,\text{dBW}$, $\sigma_{rs}^2 = -30\,\text{dBW}$, $\rho = 0.6$, $a_0 = -2.03 \times 10^{-3}$, $a_1 = 3.75 \times 10^{-7}$ and $d_1 = d_2 = d_3 = 10\,m$. It is obvious that the analytical results, obtained from (10), and the simulated ones are matching. As anticipated, it can be seen that the system secrecy capacity enhances significantly with increasing the jamming signal power and/or the relay gain. It is also worthwhile highlighting that the absence of the artificial noise, leads to zero secrecy capacity. This is justified by the fact that when there is no artificial noise, C_d will be less than or equal to C_e, which consequently results in zero secrecy capacity.

Now, to explore the impact of the correlation factor ρ on the system performance, the average secrecy capacity is plotted in Fig. 4 with respect to the input SNR for $\rho = 0.3,\ 0.6$ and 0.9 when $P_s = -3\,\text{dBW}$, $P_n = -3\,\text{dBW}$,

$$\mathcal{M}_{S,\Upsilon,C}(z) = \frac{2\exp(-z\Upsilon)\ \lambda_{h_{dr}}}{\lambda_{h_{dr}} + P_n G^2 d_1^m z} \sqrt{\lambda_{h_{re}} \sigma_e^2 d_1^m d_2^m d_3^m z}\, K_1\left(2\sqrt{\lambda_{h_{re}} \sigma_e^2 d_1^m d_2^m d_3^m z}\right). \quad (61)$$

$$\mathbb{E}\left[C_e^{\{w\}}\right] = \frac{1}{2\ln(2)} \int_0^\infty \frac{1}{z}\left(1 - \frac{\lambda_{h_{sr}}}{\lambda_{h_{sr}} + P_s G^2 d_2^m z}\right) \times \frac{2\exp(-z\Upsilon)\ \lambda_{h_{dr}}}{\lambda_{h_{dr}} + P_n G^2 d_1^m z} \sqrt{\lambda_{h_{re}} \sigma_e^2 d_1^m d_2^m d_3^m z}\, K_1\left(2\sqrt{\lambda_{h_{re}} \sigma_e^2 d_1^m d_2^m d_3^m z}\right) dz. \quad (62)$$

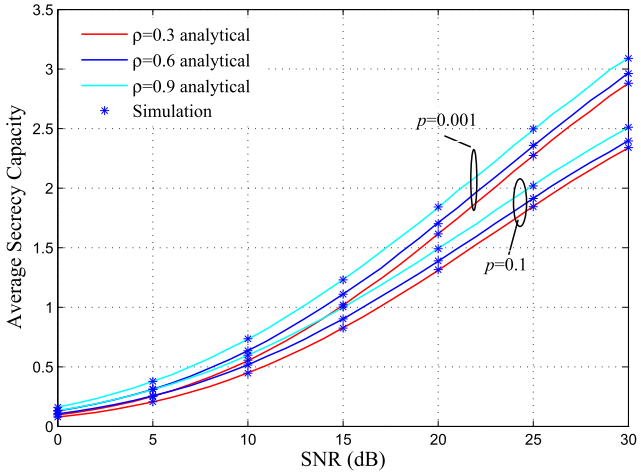


FIGURE 4. Average secrecy capacity as a function of the input SNR for various alues of ρ when $p = 0.1$ and 0.001.

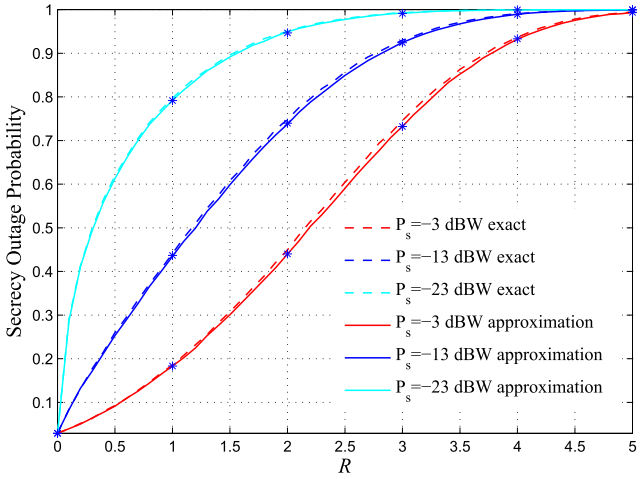


FIGURE 5. Secrecy outage probability versus threshold values for different values of P_s.

SINR $= -10$ dB, $\sigma_{rs}^2 = -30$ dBW, $G = 1$ and $d_1 = d_2 = d_3 = 10\,m$ when $p = 0.001$ and 0.1. As anticipated, we can see the intuitive result that increasing the input SNR implies enhancing the secrecy capacity. However, the system can always be made more secure with increasing the correlation factor ρ. This is because, there is no impact from the correlation on the signal to noise ratio at the destination and the average capacity at the destination is almost equal for each value of ρ, which is not the case at the eavesdropper; hence the lowest correlation factor gives highest capacity.

B. SECRECY OUTAGE PROBABILITY

In this subsection, we present some numerical examples for the secrecy outage probability expression derived above for the PLC-alone system. The exact and the approximation results of the probability are shown in Fig. 5 as a function of the threshold values of the secrecy rate, R, for different values of the source power. The power line channel features adopted in this investigation are $a_0 = -2.03 \times 10^{-3}$, $a_1 = 3.75 \times 10^{-7}$, $k = 0.7$ and the noise values are chosen as $P_n = -3$ dBW, input SNR $= 25$ dB, SINR $= -15$ and $\sigma_{rs}^2 = -30$ dBW, when $d_1 = d_2 = d_3 = 10\,m$, $\rho = 0.6$, $p = 0.01$ and $G = 1$. The one important observation that can be seen from this figure is that increasing the source power will always reduce the secrecy outage probability.

C. SOURCE POWER, EAVESDROPPER LOCATION AND CODING DIVERSITY

We now examine the effect of the PLC/wireless coding diversity, source power and the eavesdropper location on the average secrecy capacity of the proposed systems. Fig. 6 illustrates the average secrecy capacity of the PLC/wireless and PLC-alone systems as a function of the source power P_s for different values of the distance between the relay and the eavesdropper d_3. The results in this subsection are based on the following $P_n = -7$ dBW, $G = 1$, $d_1 = d_2 = 100\,m$ and the cable attenuation parameters for the power line channel are $a_0 = 9.4 \times 10^{-3}$, $a_1 = 4.2 \times 10^{-7}$ and $k = 0.7$ [4]. It is interesting to note that the average secrecy capacity of the PLC/wireless system has always better performance than that of the PLC-alone scheme and this enhancement becomes more pronounced as P_s becomes

$$\mathbb{E}\left[C_d^{\{w\}}\right] \approx \frac{1}{2\ln(2)\,Y}\sum_{\epsilon=1}^{n}\omega_\epsilon\frac{Y}{z_\epsilon}\left(2\sqrt{\frac{\lambda_{h_{rd}}\bar{\sigma}_d^2\,d_1^m d_2^m z_\epsilon}{Y}}\,K_1\left(2\sqrt{\frac{\lambda_{h_{rd}}\bar{\sigma}_d^2\,d_1^m d_2^m z_\epsilon}{Y}}\right)\right.$$
$$\left.-\frac{2\,Y\lambda_{h_{sr}}}{\lambda_{h_{sr}}Y + P_s G^2 z_\epsilon}\sqrt{\frac{\lambda_{h_{rd}}\bar{\sigma}_d^2\,d_1^m d_2^m z_\epsilon}{Y}}\,K_1\left(2\sqrt{\frac{\lambda_{h_{rd}}\bar{\sigma}_d^2\,d_1^m d_2^m z_\epsilon}{Y}}\right)\right)dz. \tag{63}$$

$$\mathbb{E}\left[C_e^{\{w\}}\right] \approx \frac{1}{2\ln(2)}\sum_{\epsilon=1}^{n}\omega_\epsilon\frac{\Upsilon}{z_\epsilon}\left(1-\frac{\lambda_{h_{sr}}\Upsilon}{\lambda_{h_{sr}}\Upsilon + P_s G^2 d_2^m z_\epsilon}\right)$$
$$\times\frac{2\,\Upsilon\lambda_{h_{dr}}}{\lambda_{h_{dr}}\Upsilon + P_n G^2 d_1^m z_\epsilon}\sqrt{\frac{\lambda_{h_{re}}\sigma_e^2 d_1^m d_2^m d_3^m z_\epsilon}{\Upsilon}}\,K_1\left(2\sqrt{\frac{\lambda_{h_{re}}\sigma_e^2 d_1^m d_2^m d_3^m z_\epsilon}{\Upsilon}}\right)dz. \tag{64}$$

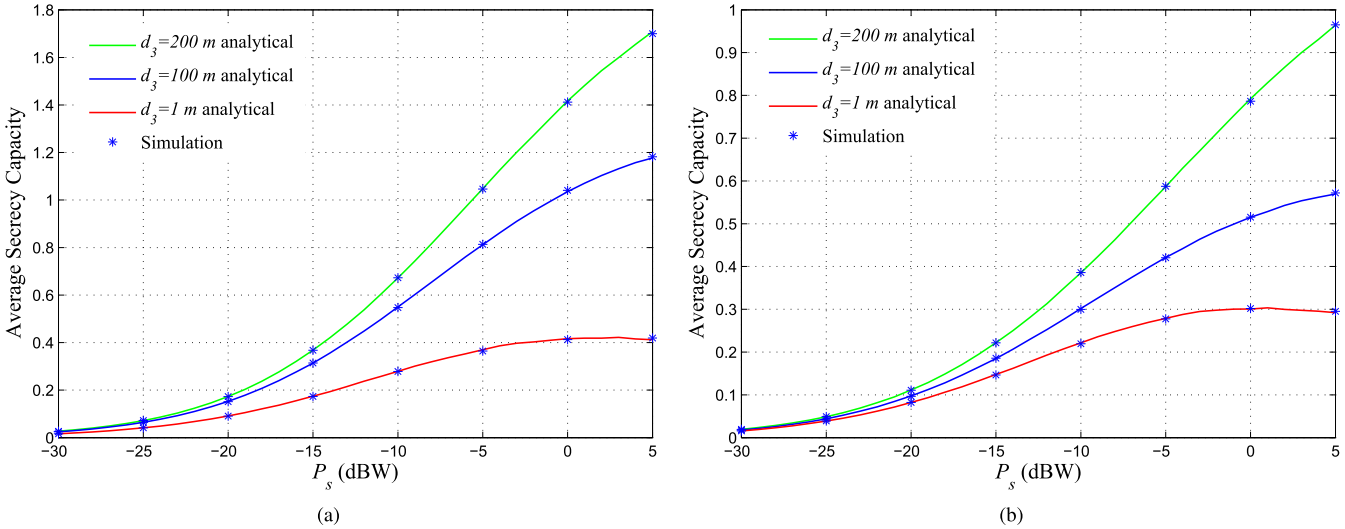


FIGURE 6. Average secrecy capacity versus source power for PLC/wireless and PLC-alone systems. (a) Average secrecy capacity versus source power for PLC/wireless system. (b) Average secrecy capacity versus source power for PLC-alone system.

larger. We can see clearly the secrecy gain provided by the PLC/wireless scheme; for instance, at $P_s = 0$ dBW, there is about a 0.6 bits/s/Hz secrecy capacity gain when $d_3 = 200m$ and becomes around 0.5 bits/s/Hz for $d_3 = 100m$. In addition, it is evident that when the eavesdropper becomes closer to the relay, the system becomes less secure in both schemes; however, the system security improves as the eavesdropper moves away from the relay.

VII. CONCLUSION

In this paper we considered the application of physical layer security in cooperative PLC networks employing a jamming technique for protection against eavesdroppers. We analyzed the system performance in terms of the average secrecy capacity and secrecy outage probability for various system set ups, including PLC/wireless diversity coding. The accuracy of the analytical results was validated with Monte Carlo simulations. The results provided an insight into the relationship between the secrecy performance of cooperative PLC systems, artificial noise power, relay gain and correlation factor, as well as PLC/wireless coding diversity.

ACKNOWLEDGMENT

The authors would like to thank our colleagues and the anonymous reviewers for their constructive suggestions and comments which greatly improved our paper. They would also like to thank the editor for his professional advice and handling of the reviewing process.

REFERENCES

[1] S. Galli, A. Scaglione, and Z. Wang, "For the grid and through the grid: The role of power line communications in the smart grid," *Proc. IEEE*, vol. 99, no. 6, pp. 998–1027, Sep. 2011.

[2] M. Nassar, J. Lin, Y. Mortazavi, A. Dabak, I. H. Kim, and B. Evans, "Local utility power line communications in the 3–500 khz band: Channel impairments, noise, and standards," *IEEE Signal Process. Mag.*, vol. 29, no. 5, pp. 116–127, Sep. 2012.

[3] D. Anastasiadou and T. Antonakopoulos, "Multipath characterization of indoor power-line networks," *IEEE Trans. Power Del.*, vol. 20, no. 1, pp. 90–99, Jan. 2005.

[4] M. Zimmermann and K. Dostert, "A multipath model for the powerline channel," *IEEE Trans. Commun.*, vol. 50, no. 4, pp. 553–559, Apr. 2002.

[5] A. Schwager, D. Schneider, W. Baschlin, A. Dilly, and J. Speidel, "MIMO PLC: Theory, measurements and system setup," in *Proc. IEEE Int. Symp. Power Line Commun. Appl. (ISPLC)*, Apr. 2011, pp. 48–53.

[6] D. Rende *et al.*, "Noise correlation and its effect on capacity of inhome MIMO power line channels," in *Proc. IEEE Int. Symp. Power Line Commun. Its Appl. (ISPLC)*, Apr. 2011, pp. 60–65.

[7] R. Newman, L. Yonge, S. Gavette, and R. Anderson, "Homeplug AV security mechanisms," in *Proc. IEEE Int. Symp. Power Line Commun. Its Appl. (ISPLC)*, Mar. 2007, pp. 366–371.

[8] X. Cheng, R. Cao, and L. Yang, "Relay-aided amplify-and-forward power-line communications," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 265–272, Mar. 2013.

[9] L. Lampe and A. Vinck, "Cooperative multihop power line communications," in *Proc. IEEE Int. Symp. Power Line Commun. Appl. (ISPLC)*, Mar. 2012, pp. 1–6.

[10] M. Noori and L. Lampe, "Improving data rate in relay-aided power line communications using network coding," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2013, pp. 2975–2980.

[11] S. D'Alessandro and A. M. Tonello, "On rate improvements and power saving with opportunistic relaying in home power line networks," *EURASIP J. Adv. Signal Process.*, vol. 2012, pp. 1–17, Sep. 2012.

[12] L. Lampe, R. Schober, and S. Yiu, "Distributed space-time coding for multihop transmission in power line communication networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 7, pp. 1389–1400, Jul. 2006.

[13] A. Tonello, F. Versolatto, and S. D'Alessandro, "Opportunistic relaying in in-home PLC networks," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Dec. 2010, pp. 1–5.

[14] L. Lampe and A. Vinck, "On cooperative coding for narrow band PLC networks," *Int. J. Electron. Commun.*, vol. 65, no. 8, pp. 681–687, Aug. 2011.

[15] V. B. Balakirsky and A. J. H. Vinck, "Potential performance of PLC systems composed of several communication links," in *Proc. Int. Symp. Power Line Commun. Appl.*, Apr. 2005, pp. 12–16.

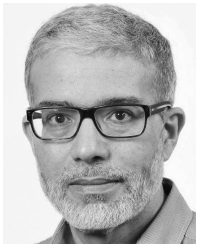
[16] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[17] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[18] A. Pittolo and A. Tonello, "Physical layer security in PLC networks: Achievable secrecy rate and channel effects," in *Proc. IEEE Int. Symp. Power Line Commun. Appl. (ISPLC)*, Mar. 2013, pp. 273–278.

[19] A. Pittolo and A. Tonello, "Physical layer security in power line communication networks: An emerging scenario, other than wireless," *IET Commun.*, vol. 8, no. 8, pp. 1239–1247, May 2014.
[20] Y. Zhuang and L. Lampe, "Physical layer security in MIMO power line communication networks," in *Proc. IEEE Int. Symp. Power Line Commun. Appl. (ISPLC)*, Mar. 2014, pp. 272–277.
[21] L. Lai and H. El Gamal, "The relay–eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.
[22] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.
[23] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4985–4997, Oct. 2011.
[24] B. Han, J. Li, J. Su, M. Guo, and B. Zhao, "Secrecy capacity optimization via cooperative relaying and jamming for WANETs," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 4, pp. 1117–1128, Apr. 2015.
[25] A. M. Tonello, F. Versolatto, B. Bejar, and S. Zazo, "A fitting algorithm for random modeling the PLC channel," *IEEE Trans. Power Del.*, vol. 27, no. 3, pp. 1477–1484, Jul. 2012.
[26] Y. H. Ma, P. L. So, and E. Gunawan, "Performance analysis of OFDM systems for broadband power line communications under impulsive noise and multipath effects," *IEEE Trans. Power Del.*, vol. 20, no. 2, pp. 674–682, Apr. 2005.
[27] F. Abdelkefi, P. Duhamel, and F. Alberge, "Impulsive noise cancellation in multicarrier transmission," *IEEE Trans. Commun.*, vol. 53, no. 1, pp. 94–106, Jan. 2005.
[28] M. Ghosh, "Analysis of the effect of impulse noise on multicarrier and single carrier QAM systems," *IEEE Trans. Commun.*, vol. 44, no. 2, pp. 145–147, Feb. 1996.
[29] A. Dubey and R. Mallik, "Plc system performance with af relaying," *IEEE Trans. Commun.*, vol. 63, no. 6, pp. 2337–2345, Jun. 2015.
[30] A. Salem, K. M. Rabie, K. A. Hamdi, E. Alsusa, and A. M. Tonello, "Physical layer security of cooperative relaying power-line communication systems," in *Proc. Int. Symp. Power Line Commun. Appl. (ISPLC)*, Mar. 2016, pp. 185–189.
[31] M. O. Hasna and M. S. Alouini, "A performance study of dual-hop transmissions with fixed gain relays," *IEEE Trans. Wireless Commun.*, vol. 3, no. 6, pp. 1963–1968, Nov. 2004.
[32] Y. W. P. Hong, P.-C. Lan, and C.-C. J. Kuo, *Signal Processing Approaches to Secure Physical Layer Communications in Multi-Antenna Wireless Systems*. New York, NY, USA: Springer, 2014.
[33] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.
[34] A. Salem, K. A. Hamdi, and K. M. Rabie, "Physical layer security with RF energy harvesting in af multi-antenna relaying networks," *IEEE Trans. Commun.*, vol. 64, no. 7, pp. 3025–3038, Jul. 2016.
[35] S. P. Herath, N. H. Tran, and T. Le-Ngoc, "On optimal input distribution and capacity limit of Bernoulli–Gaussian impulsive noise channels," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2012, pp. 3429–3433.
[36] H. V. Vu, N. H. Tran, T. V. Nguyen, and S. I. Hariharan, "Estimating Shannon and constrained capacities of Bernoulli–Gaussian impulsive noise channels in Rayleigh fading," *IEEE Trans. Commun.*, vol. 62, no. 6, pp. 1845–1856, Jun. 2014.
[37] A. Dubey, R. K. Mallik, and R. Schober, "Performance of a PLC system in impulsive noise with selection combining," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2012, pp. 3508–3512.
[38] K. C. Wiklundh, P. F. Stenumgaard, and H. M. Tullberg, "Channel capacity of Middleton's class a interference channel," *Electron. Lett.*, vol. 45, no. 24, pp. 1227–1229, Nov. 2009.
[39] K. A. Hamdi, "A useful lemma for capacity analysis of fading interference channels," *IEEE Trans. Commun.*, vol. 58, no. 2, pp. 411–416, Feb. 2010.
[40] S. M. Ross, *Introduction to Probability Models*, 10th ed. Oxford, U.K.: Elsevier, 2010.
[41] M. K. Simon and M.-S. Alouini, *Digital Communication Over Fading Channels*. New York, NY, USA: Wiley, 2005.
[42] N. B. Mehta, J. Wu, A. F. Molisch, and J. Zhang, "Approximating a sum of random variables with a lognormal," *IEEE Trans. Wireless Commun.*, vol. 6, no. 7, pp. 2690–2699, Jul. 2007.
[43] K. A. Hamdi, "On the statistics of signal-to-interference plus noise ratio in wireless communications," *IEEE Trans. Commun.*, vol. 57, no. 11, pp. 3199–3204, Nov. 2009.
[44] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions With Formulas, Graphs, and Mathematical Tables*. New York, NY, USA: Wiley, 1972.
[45] N. Balakrishnan and C.-D. Lai, *Continuous Bivariate Distributions*. New York, NY, USA: Springer, 2009.
[46] A. Dubey, R. Mallik, and R. Schober, "Performance analysis of a power line communication system employing selection combining in correlated log-normal channels and impulsive noise," *IET Commun.*, vol. 8, no. 7, pp. 1072–1082, May 2014.
[47] J. N. Laneman, E. Martinian, G. W. Wornell, and J. G. Apostolopoulos, "Source-channel diversity for parallel channels," *IEEE Trans. Inf. Theory*, vol. 51, no. 10, pp. 3518–3539, Oct. 2005.
[48] S. W. Lai, N. Shabehpour, G. G. Messier, and L. Lampe, "Performance of wireless/power line media diversity in the office environment," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2014, pp. 2972–2976.
[49] M. Sayed, T. A. Tsiftsis, and N. Al-Dhahir, "On the diversity of hybrid narrowband-PLC/wireless communications for smart grids," *IEEE Trans. Wireless Commun.*, vol. 16, no. 7, pp. 4344–4360, Jul. 2017.
[50] M. Safari and M. Uysal, "Cooperative diversity over log-normal fading channels: Performance analysis and optimization," *IEEE Trans. Wireless Commun.*, vol. 7, no. 5, pp. 1963–1972, May 2008.
[51] S. Zhang, X. G. Xia, and J. Wang, "Cooperative performance and diversity gain of wireless relay networks," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 10, pp. 1623–1632, Oct. 2012.
[52] R. Narasimhan, "Finite-SNR diversity–multiplexing tradeoff for correlated Rayleigh and Rician MIMO channels," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 3965–3979, Sep. 2006.
[53] M. O. Hasna and M.-S. Alouini, "Performance analysis of two-hop relayed transmissions over Rayleigh fading channels," in *Proc. IEEE 56th Veh. Technol. Conf. VTC Fall*, vol. 4. Mar. 2002, pp. 1992–1996.
[54] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*. Orlanndo, FL, USA: Academic, 1980.

ABDELHAMID SALEM (S'12) received the B.Sc. degree in electrical and electronic engineering and the M.Sc. degree (Hons.) in communication engineering from the University of Benghazi, Benghazi, Libya, in 2002 and 2009, respectively. He is currently pursuing the Ph.D. degree in wireless communications with The University of Manchester, U.K. His current research interests include physical layer security, signal processing for interference mitigation, energy harvesting, wireless power transfer, MIMO systems, wireless optical communication systems, and power line communications.



KHAIRI ASHOUR HAMDI (M'99–SM'02) received the B.Sc. degree in electrical engineering from Alfateh University, Tripoli, Libya, in 1981, the M.Sc. degree (Hons.) from the Technical University of Budapest, Budapest, Hungary, in 1988, and the Ph.D. degree in telecommunication engineering from the Hungarian Academy of Sciences in 1993. His current research interests include modeling and performance analysis of wireless communication systems and networks, green communication systems, and heterogeneous mobile networks.

EMAD ALSUSA (M'06–SM'07) received the Ph.D. degree in electrical and electronic engineering from Bath University, Bath, in 2000. He then joined the School of Engineering and Electronics, Edinburgh University, as a MobileVCE Post-Doctoral Research Fellow, where he was involved in link enhancement techniques for future high data rate wireless communication systems. In 2003, he became a Faculty Member with The University of Manchester, U.K., where he is currently a Lecturer on communication engineering subjects. His research interests include development of PHY and MAC layers techniques for wired and wireless communication networks, with particular focus on cognitive radio, interference mitigation, multiuser MIMO, spectrum optimization, and Green systems. He was a co-recipient of the Best Paper Award of the IEEE Symposium on Power Line Communications 2014. He has served as a Technical Program Committee member on numerous IEEE flagship conferences and co-chaired the Greencomm Track in VTC spring 2016.