Securing MIMO Power Line Communications with Full-Duplex Jamming Receivers

Gautham Prasad*, Omid Taghizadeh†, Lutz Lampe* and Rudolf Mathar†
* Department of Electrical and Computer Engineering, The University of British Columbia, Vancouver, BC, Canada.
† Institute for Theoretical Information Technology, RWTH-Aachen University, Aachen, Germany.
Email:{gauthamp, lampe}@ece.ubc.ca, {taghizadeh, mathar}@ti.rwth-aachen.de

***Abstract*—Despite providing a wired communications infrastructure, power line communication (PLC) is broadcast in nature due to the shared channel usage by all intended users. This introduces privacy concerns for confidential communication in multi-user environments, such as in smart-meter data transmission using PLC, where data packets are exposed to potential eavesdroppers. In this paper, we propose, for the first time, a physical layer security (PLS) solution for multiple-input multiple-output (MIMO) PLC systems using in-band full-duplex (IBFD) technology. IBFD allows PLC receivers to jam the operating frequency band while also receiving intended data packets at the same time. In this respect, we optimize the information and jamming transmission strategies, together with power allocation over different sub-carriers, with the goal of maximizing the secrecy energy efficiency. Our numerical results illustrate the multi-fold increase in secrecy rates that we obtain using an IBFD-based PLS technique over a half-duplex operation without jamming.**

***Index Terms*—Physical layer security, in-band full-duplex, MIMO-PLC, secrecy rate maximization, smart grid privacy.**

I. Introduction and Background

Power line communication (PLC) has evolved since being applied for remote meter reading and ultra-low data rate home automation to now finding applications in high-speed broadband multimedia communications and in enabling robust reliable communications for the smart-grid [1]–[3]. Early implementations of PLC focused on using a pair of conductors for differential signal transmission in a single-input single-output (SISO) manner. However, the availability of a third wire, e.g., protective earth in in-home wiring infrastructure, or potentially several more conductors available in multi-phase power distribution networks, allows for multiple-input multiple-output (MIMO) PLC [4], [5]. In this work, we consider such MIMO-PLC systems, although the idea we present in this paper is conceptually also applicable in SISO communication scenarios as a simplified use-case.

Unlike most other wire-line systems, such as broadband communication over digital subscriber lines (DSL) or coaxial cables, PLC uses the shared medium of power lines in a multi-user environment. Therefore, data privacy and leakage are crucial considerations in PLC. A quintessential scenario of this concern is in the context of PLC applied for smart-grid communications [6], [7], where data confidentiality is critical to ensure that personal information is not revealed, even to legitimate users in the network [8]–[10]. At the same time, data security in domestic power line networks is also considered to be critical [11]. To address the issues of security and privacy, most PLC standards incorporate security mechanisms at upper layers of the network stack via data confidentiality protocols [12, Ch. 7], the use of network encryption keys [12, Ch. 4], [13, Ch. 7], and/or end-to-end block- and payload-level encryption, typically using Advanced Encryption Standard (AES) [12, Ch. 4], [13, Ch. 4].

978-1-7281-0289-4/19/$31.00 © 2019 IEEE

A. Physical Layer Security for PLC

Cryptographic techniques implemented at higher layers typically rely on practical computational limitations at the eavesdropper. To further complement these techniques, a few recent works have developed a supplementary mechanism to achieve physical layer security (PLS) in PLC [14]–[16], on the lines of similar designs found in wireless communications [17]–[19], to provide information-theoretic secrecy and a first line of defense against eavesdropper attacks. It has been shown that, although secrecy rates achieved in PLC are lower than those obtained in wireless communications [14], the use of MIMO-PLC can enhance the PLS performance with suitable choices of conductor pairs used for transmission [15]. However, these works consider traditional half-duplex (HD) modems that can only transmit or receive data in the operating frequency band at any given time. The introduction of in-band full-duplex (IBFD) communication for PLC [20], [21], i.e., simultaneous bidirectional data transmission over the same power line channel and in the same frequency band, enables an alternative technique to achieve PLS in PLC systems through intentional jamming [22], [23], which can significantly improve secrecy rates. IBFD allows a PLC node that is receiving intended data to also simultaneously transmit a jamming signal in the same band to degrade the decoding ability of an eavesdropper. The known jamming signal is then canceled at the receiver using self-interference cancellation (SIC) techniques, which have been shown to provide sufficient cancellation performance to achieve signal-to-noise ratio (SNR) environments comparable to that obtained in an HD scenario [24].

B. Contributions

In this paper, we provide an analysis of the achievable secrecy rates for a MIMO-PLC system, where the transmitted data is secured by means of IBFD-jamming by the receiver node. We propose transmit strategies to be employed at the

transmitter and the intended receiver-cum-jammer to maximize the secrecy rate. We solve the non-convex sum-secrecy-rate maximization problem iteratively by decomposing it into a sequence of approximated convex problems to obtain beamforming strategies to be employed for data transmission and jamming. We evaluate the performance of our system under a realistic network topology, and investigate the achievable secrecy rates under various network load conditions and different locations of the eavesdropper. We show through simulation results that the secrecy rate gain increases with improving SIC performance at the IBFD-jammer. We also show that while the secrecy rates in HD mode diminish as the separation between the intended receiver and the eavesdropper reduces, the increase in secrecy rates achieved with IBFD-jamming is higher when the eavesdropper is at close proximity to the desired receiver, due to the greater impact of the jamming signal on the signal quality at the eavesdropper.

C. Outline

The rest of the paper is organized as follows. We present the system model in Section II. In Section III, we derive the optimal beamforming strategy to maximize the secrecy rate with full-duplex jamming. We show the effectiveness of our solution through numerical results in Section IV, and conclude in Section V.

II. System Model

We consider a multi-carrier transmission over a wiretap MIMO-PLC channel, where a transmitter, Alice, communicates with a desired receiver, Bob, in the presence of an undesired receiver, Eve. Bob is capable of IBFD operation, and therefore transmits a jamming signal towards Eve while simultaneously receiving intended data from Alice. Using SIC techniques [21], [24], we ensure that Bob is able to decode data packets received from Alice. The jamming signal transmitted by Bob, however, degrades the decoding ability of Eve, and thereby improves information secrecy.

Most broadband PLC (BB-PLC) systems apply orthogonal frequency division multiplexing (OFDM) to achieve multi-carrier transmission [12], [13], [25]. At the kth OFDM sub-carrier, we denote the Alice-Bob (communication), Alice-Eve (leakage), and Bob-Eve (jamming) channels as $\mathbf{H}_{\mathrm{ab},k} \in \mathbb{C}^{M_\mathrm{B}\times M_\mathrm{A}}$, $\mathbf{H}_{\mathrm{ae},k} \in \mathbb{C}^{M_\mathrm{E}\times M_\mathrm{A}}$ and $\mathbf{H}_{\mathrm{be},k} \in \mathbb{C}^{M_\mathrm{E}\times M_\mathrm{B}}$, $\forall k \in \mathcal{K}$, respectively, where $M_\mathrm{A}, M_\mathrm{B}$, and M_E represent the number of active transceiver paths at Alice, Bob, and Eve, respectively. We use $\mathcal{K}$ to denote the set of OFDM sub-carriers that are used for transmission, conforming to regulations that require several intermediate sub-carriers to be silenced during transmission [12], [13].

A. Channel State Information

At Eve: Based on the nature of the eavesdropper, acquisition of the instantaneous channel state information (CSI) may or may not be feasible at Eve. In this work, we consider the scenario where Eve is an undesired receiver, but is a legitimate network member, and we therefore have complete knowledge of the Alice-Eve CSI. Such a scenario is the most likely condition we encounter in smart-grid networks, where confidential messages transmitted by smart-meters to the utilities via repeaters are to be protected from other legitimate household units (Eves) in the network. Along the same lines, Eve could be a legitimate user in an indoor PLC network, while being a part of a separate virtual network from whom data needs to be protected [11].

At Bob: We consider practical SIC schemes that do not completely eliminate the effect of self-interference caused by intentional jamming. Therefore, we adopt the CSI model

$$\mathbf{H}_{\mathrm{bb},k} = \tilde{\mathbf{H}}_{\mathrm{bb},k} + \mathbf{\Delta}_{\mathrm{bb},k}, \tag{1}$$

$$\mathbf{\Delta}_{\mathrm{bb},k} \sim \mathcal{CN}\left(\mathbf{0}_{M_\mathrm{b}}, \epsilon_{\mathrm{bb}}\mathbf{I}_{M_\mathrm{b}}\right), \tag{2}$$

where $\tilde{\mathbf{H}}_{\mathrm{bb},k}$ and $\mathbf{\Delta}_{\mathrm{bb},k}$ represent the estimated self-interference channel and the estimation error, respectively, ϵ_{bb} indicates the error variance, and $\mathbf{0}_M$ and $\mathbf{I}_M$ are the zero and identity matrices, respectively, of size $M \times M$.

B. Signal Transmission

We use the model of a Gaussian distributed transmitted signal from Alice at the k-th sub-carrier, i.e., the transmitted signal is

$$\mathbf{x}_k \sim \mathcal{CN}\left(\mathbf{0}_{M_\mathrm{A}}, \mathbf{F}_k\right), \tag{3}$$

where $\mathbf{F}_k$ is the signal covariance matrix. Similarly, the transmitted jamming signal from Bob is

$$\mathbf{w}_k \sim \mathcal{CN}\left(\mathbf{0}_{M_\mathrm{B}}, \mathbf{W}_k\right), \tag{4}$$

where $\mathbf{W}_k$ is the jamming covariance matrix. The colored noise signals at the receivers, Bob and Eve, are also assumed to be Gaussian distributed, and are respectively denoted as

$$\mathbf{n}_{\mathrm{b},k} \sim \mathcal{CN}\left(\mathbf{0}_{M_\mathrm{B}}, \mathbf{N}_{\mathrm{b},k}\right), \tag{5}$$

$$\mathbf{n}_{\mathrm{e},k} \sim \mathcal{CN}\left(\mathbf{0}_{M_\mathrm{E}}, \mathbf{N}_{\mathrm{e},k}\right), \tag{6}$$

where $\mathbf{N}_{\mathrm{b},k}$ and $\mathbf{N}_{\mathrm{e},k}$ represent the associated noise covariance matrices at Bob and Eve, respectively. Note that unlike the commonly used assumption in wireless communications that these matrices are diagonal, measurement results have revealed that MIMO-PLC noise is strongly correlated due to the inter-conductor coupling [26], [27]. Furthermore, the correlation coefficient is also shown to be frequency selective [26], [27].

Regulations also restrict PLC transmitters to adhere to a specified amplitude map, by restricting the transmit power spectral density (PSD) over each sub-carrier [12], [13]. With MIMO-PLC, we are required to ensure that the sum-PSD across all transmit paths are within the allowed limits at both Alice and Bob. This restriction imposes the constraints,

$$\mathrm{tr}\left(\mathbf{F}_k\right) \leq P_\mathrm{A}, \quad \forall k \in \mathcal{K}, \tag{7}$$

$$\mathrm{tr}\left(\mathbf{W}_k\right) \leq P_\mathrm{B}, \quad \forall k \in \mathcal{K}, \tag{8}$$

where $P_\mathrm{A} = P_\mathrm{B}$ under typical operating conditions. We further voluntarily introduce an additional total power constraint,

$$\sum_{k\in\mathcal{K}} \mathrm{tr}\left(\mathbf{F}_k\right) + \mathrm{tr}\left(\mathbf{W}_k\right) \leq P_{\mathrm{tot}}, \tag{9}$$

where P_{tot} is the maximum total power to be used for transmission to ensure energy-efficient communications.

We then formulate the received signal at Eve as

$$\mathbf{y}_{\mathrm{e},k} = \mathbf{H}_{\mathrm{ae},k}\mathbf{x}_k + \mathbf{H}_{\mathrm{be},k}\mathbf{w}_k + \mathbf{n}_{\mathrm{e},k}. \tag{10}$$

Similarly, the received signal at Bob is

$$\mathbf{y}_{\mathrm{b},k} = \mathbf{H}_{\mathrm{ab},k}\mathbf{x}_k + \mathbf{H}_{\mathrm{bb},k}\mathbf{w}_k + \mathbf{n}_{\mathrm{b},k}. \tag{11}$$

Bob then implements SIC to estimate the received signal as

$$\tilde{\mathbf{y}}_{\mathrm{b},k} = \mathbf{H}_{\mathrm{ab},k}\mathbf{x}_k + \mathbf{\Delta}_{\mathrm{bb},k}\mathbf{w}_k + \mathbf{n}_{\mathrm{b},k}. \tag{12}$$

Using the above representations, we express the achievable communication rates for the Alice-Bob and Alice-Eve paths as

$$R_{\mathrm{ab},k} = \log\left|\mathbf{I}_{M_{\mathrm{B}}} + \mathbf{H}_{\mathrm{ab},k}\mathbf{F}_k\mathbf{H}_{\mathrm{ab},k}^H\left(\mathbf{\Gamma}_{\mathrm{b},k}\right)^{-1}\right|, \tag{13}$$

$$R_{\mathrm{ae},k} = \log\left|\mathbf{I}_{M_{\mathrm{E}}} + \mathbf{H}_{\mathrm{ae},k}\mathbf{F}_k\mathbf{H}_{\mathrm{ae},k}^H\left(\mathbf{\Gamma}_{\mathrm{e},k}\right)^{-1}\right|, \tag{14}$$

respectively, where $|\cdot|$ is the matrix determinant operator, and $\mathbf{\Gamma}_{\mathrm{b},k}$ and $\mathbf{\Gamma}_{\mathrm{e},k}$ denote the interference-plus-noise covariance matrices at Bob and Eve, computed as

$$\mathbf{\Gamma}_{\mathrm{b},k} = \epsilon_{\mathrm{bb}}\mathrm{tr}\left(\mathbf{W}_k\right)\mathbf{I}_{M_{\mathrm{B}}} + \mathbf{N}_{\mathrm{b},k}, \tag{15}$$

$$\mathbf{\Gamma}_{\mathrm{e},k} = \mathbf{H}_{\mathrm{be},k}\mathbf{W}_k\mathbf{H}_{\mathrm{be},k}^H + \mathbf{N}_{\mathrm{e},k}, \tag{16}$$

respectively. Therefore, the achievable secrecy rate at each sub-carrier can be represented as

$$R_{\mathrm{sec},k} = \left\{R_{\mathrm{ab},k} - R_{\mathrm{ae},k}\right\}^+, \tag{17}$$

where $\{x\}^+ = \max\{x, 0\}$, and the overall sum-secrecy-rate is given by

$$R_{\mathrm{sum}} = \sum_{k\in\mathcal{K}} R_{\mathrm{sec},k}. \tag{18}$$

III. Optimal Transmit Strategy

In this section, we present the analysis of maximizing the sum-secrecy-rate of the system in (18), by optimizing transmit strategies for the information and jamming signals. We formulate the sum-secrecy-rate maximization problem as

$$\max_{\{\mathbf{F}_k\},\{\mathbf{W}_k\}} \quad R_{\mathrm{sum}} \tag{19a}$$

$$\text{s.t.} \quad \text{(7), (8), (9),} \tag{19b}$$

$$\mathbf{F}_k, \mathbf{W}_k \succeq \mathbf{0}, \ \ \forall k \in \mathcal{K}, \tag{19c}$$

where $\mathbf{F}_k, \mathbf{W}_k \succeq \mathbf{0}$ represent the conditions on the information and jamming transmit covariance matrices. The above problem is intractable in the current form, due to the non-smooth, non-linear, and non-convex nature of the objective function. Hence, we introduce the following steps to obtain a numerically tractable problem structure.

Lemma 1. *For an optimum solution to the problem (19), the positive operator $\{\}^+$ has no effect.*

Proof. The proof follows via contradiction, following the same argument as in [22, Section III] for the single-carrier scenario. If at the optimality of (19), the value of $(R_{\mathrm{ab},k} - R_{\mathrm{ae},k})$ is negative for any $k \in \mathcal{K}$, then the data transmission can be turned off for that specific sub-carrier, i.e., setting $\mathbf{F}_k = \mathbf{0}$. This results in a non-negative value of $(R_{\mathrm{ab},k} - R_{\mathrm{ae},k})$, without degrading other sub-carriers or violating the constraints. The latter statement shows the existence of a globally optimum solution to (19), where the positive operator has no impact. □

By employing the result of the Lemma 1, the epigraph form of the modified problem can be formulated as

$$\max_{\{\mathbf{F}_k\},\{\mathbf{W}_k\},\{\gamma_{\mathrm{ab},k},\gamma_{\mathrm{ae},k}\}} \quad \sum_{k\in\mathcal{K}} \gamma_{\mathrm{ab},k} - \gamma_{\mathrm{ae},k} \tag{20a}$$

$$\text{s.t.} \quad \gamma_{\mathrm{ab},k} \le R_{\mathrm{ab},k}, \ \ \gamma_{\mathrm{ae},k} \ge R_{\mathrm{ae},k}, \tag{20b}$$

$$\text{(7), (8), (9),} \ \ \mathbf{F}_k, \mathbf{W}_k \succeq \mathbf{0}, \ \ \forall k \in \mathcal{K}, \tag{20c}$$

where $\gamma_{\mathrm{ab},k}, \gamma_{\mathrm{ae},k}$ are the auxiliary variables. Note that the transformed problem (20) is still intractable, due to the non-convex feasible set imposed by the constraint (20b). However, it complies with the proposed successive inner approximation framework [28], due to the difference-of-convex nature of the non-convex constraints. In particular, the problem can be solved iteratively as a sequence of the approximated convex problems, with a proven convergence to a solution satisfying the Karush-Kuhn-Tucker (KKT) optimality conditions. We denote the non-convex set constructed by the constraint (20b) as $\mathcal{S}_k$, i.e.,

$$\mathcal{S}_k := \Big\{\forall\left(\mathbf{F}_k, \mathbf{W}_k, \gamma_{\mathrm{ab},k}, \gamma_{\mathrm{ae},k}\right) \ \Big| \ \gamma_{\mathrm{ab},k} \le R_{\mathrm{ab},k}, \ \gamma_{\mathrm{ae},k} \ge R_{\mathrm{ae},k}\Big\}. \tag{21}$$

We then obtain a convex inner approximation of $\mathcal{S}_k$ at the iteration index i as

$$\begin{aligned}\tilde{\mathcal{S}}_k^{(i)} := \Big\{\forall\Big(&\mathbf{F}_k^{(i)}, \mathbf{W}_k^{(i)}, \gamma_{\mathrm{ab},k}^{(i)}, \gamma_{\mathrm{ae},k}^{(i)}\Big) \ \Big| \\ &\gamma_{\mathrm{ab},k}^{(i)} \le \tilde{R}_{\mathrm{ab},k}\Big(\mathbf{F}_k^{(i)}, \mathbf{W}_k^{(i)}, \mathbf{F}_k^{(i-1)}, \mathbf{W}_k^{(i-1)}\Big), \\ &\gamma_{\mathrm{ae},k}^{(i)} \ge \tilde{R}_{\mathrm{ae},k}\Big(\mathbf{F}_k^{(i)}, \mathbf{W}_k^{(i)}, \mathbf{F}_k^{(i-1)}, \mathbf{W}_k^{(i-1)}\Big)\Big\}, \ \ \tilde{\mathcal{S}}_k^{(i)} \subset \mathcal{S}_k,\end{aligned} \tag{22}$$

where the superscript index $\{\cdot\}^{(i)}$ represents the value of the corresponding variable (set) at the iteration index i. Further, $\tilde{R}_{\mathrm{ab},k}$ ($\tilde{R}_{\mathrm{ae},k}$) is a lower (upper) bound on the corresponding rate function, expressed as

$$\begin{aligned}&\tilde{R}_{\mathrm{ab},k}\Big(\mathbf{F}_k^{(i)}, \mathbf{W}_k^{(i)}, \mathbf{F}_k^{(i-1)}, \mathbf{W}_k^{(i-1)}\Big) \\ &:= \log\left|\mathbf{\Gamma}_{\mathrm{b},k}^{(i)} + \mathbf{H}_{\mathrm{ab},k}\mathbf{F}_k^{(i)}\mathbf{H}_{\mathrm{ab},k}^H\right| - \varphi\left(\mathbf{\Gamma}_{\mathrm{b},k}^{(i)}, \mathbf{\Gamma}_{\mathrm{b},k}^{(i-1)}\right) \\ &\le R_{\mathrm{ab},k},\end{aligned} \tag{23}$$

$$\begin{aligned}&\tilde{R}_{\mathrm{ae},k}\Big(\mathbf{F}_k^{(i)}, \mathbf{W}_k^{(i)}, \mathbf{F}_k^{(i-1)}, \mathbf{W}_k^{(i-1)}\Big) \\ &:= \varphi\left(\mathbf{\Gamma}_{\mathrm{e},k}^{(i)} + \mathbf{H}_{\mathrm{ae},k}\mathbf{F}_k^{(i)}\mathbf{H}_{\mathrm{ae},k}^H, \mathbf{\Gamma}_{\mathrm{e},k}^{(i-1)} + \mathbf{H}_{\mathrm{ae},k}\mathbf{F}_k^{(i-1)}\mathbf{H}_{\mathrm{ae},k}^H\right) \\ &- \log\left|\mathbf{\Gamma}_{\mathrm{e},k}^{(i)}\right| \\ &\ge R_{\mathrm{ae},k},\end{aligned} \tag{24}$$

which are obtained by applying the first-order Taylor's approximation on the concave logarithmic functions, i.e.,

$$\log|\mathbf{X}| \le \varphi\left(\mathbf{X}, \mathbf{Y}\right) := \log\left(\mathbf{Y}\right) + \frac{1}{\ln(2)}\mathrm{tr}\left(\mathbf{Y}^{-1}\left(\mathbf{X} - \mathbf{Y}\right)\right). \tag{25}$$

The approximated convex problem at the iteration i is hence expressed as

$$\max_{\{\mathbf{F}_k^{(i)}\},\{\mathbf{W}_k^{(i)}\},\{\gamma_{\mathrm{ab},k}^{(i)},\gamma_{\mathrm{ae},k}^{(i)}\}} \quad \sum_{k\in\mathcal{K}} \gamma_{\mathrm{ab},k}^{(i)} - \gamma_{\mathrm{ae},k}^{(i)} \tag{26a}$$

Algorithm 1 Algorithm for solving (19).

1: $\mathbf{W}_k^{(i)} \leftarrow \mathbf{0}, \mathbf{F}_k^{(i)} \leftarrow \mathbf{I}, i \leftarrow 0$
2: **repeat**
3: $\quad i \leftarrow i+1,$
4: $\quad \left(\mathbf{F}_k^{(i)}, \mathbf{W}_k^{(i)}\right) \leftarrow$ solve (26),
5: **until** $R_{\text{sum}}^{(i)} - R_{\text{sum}}^{(i-1)} \leq \epsilon_0 R_{\text{sum}}^{(i)}$
6: **return** $\left(\mathbf{F}_k^{(i)}, \mathbf{W}_k^{(i)}\right)$

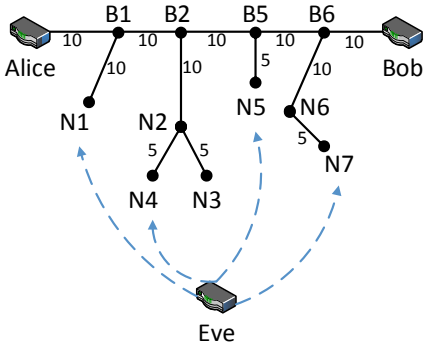

Fig. 1. The considered network topology with segment lengths indicated in meters.

$$\text{s.t.} \quad \left(\mathbf{F}_k^{(i)}, \mathbf{W}_k^{(i)}, \gamma_{\text{ab},k}^{(i)}, \gamma_{\text{ae},k}^{(i)}\right) \in \tilde{\mathcal{S}}_k^{(i)}, \ \ \forall k \in \mathcal{K}, \tag{26b}$$

$$(7), (8), (9), \ \ \mathbf{F}_k, \mathbf{W}_k \succeq \mathbf{0}, \ \ \forall k \in \mathcal{K}. \tag{26c}$$

Note that due to the application of the first order Taylor's approximation on the concave logarithmic terms in (25), the approximations of (23), (24) are smooth, and are tight approximations of the rate functions, which also satisfy the stated conditions in [28, Theorem 1]. This ensures that the problem sequence converges to a KKT solution. The iterative procedure to solve the sequence of the approximated convex problems is detailed in Algorithm 1, where the loop termination constant is denoted by ϵ_0.

IV. Numerical Results

We present simulation results in this section that evaluate the performance of our IBFD-based PLS technique in MIMO-PLC systems.

A. Simulation Setup

1) Network Topology: We consider a generic power line network topology shown in Fig. 1, where B1, B2, B5, and B6 indicate the branch points on the main power line, and N1-N7 indicate the node positions arising from these branch points. The nodes N1, N3, N4, N5, and N7 are terminal nodes where we connect network loads. We place Alice and Bob at two ends of the network, and solve (19) for various locations of Eve that can be connected at any of the terminal nodes. We consider four different locations of Eve at N1, N4, N5, or N7 in our investigations. This captures the most generic realizations of practical PLC networks, including the *keyhole* property that is unique to PLC systems, where Eve and Bob share a portion of the power line channel [14]. We also show in Section IV-B that our considered network topology allows for a comprehensive evaluation of a range of possible network scenarios and the corresponding performances obtained using IBFD-jamming for securing MIMO-PLC.

TABLE I
Parameters to Characterize Noise Statistics for MIMO-PLC [4, Ch. 2]

Parameter	Distribution
α_{PN}	$\mathcal{U}$(1.86, 2.2)
α_{NE}	$\mathcal{U}$(1.75, 2.1)
α_{EP}	$\mathcal{U}$(1.76, 2.1)
β	$\mathcal{U}$(-16.1, -15)

2) Channel and Noise Models: We apply the bottom-up approach of channel modeling to effectively capture the precise network topology and the various loads connected at each of the terminal nodes [29]. We use the open-source MIMO-PLC channel generator tool of [30] to generate channel realizations using the network topology of Fig. 1 and multi-conductor power lines. We use a 2×2 MIMO transmission in both Alice-Bob and Alice-Eve link to emulate realistic operating scenarios [31], [32]. We use cable segment lengths of $5-10$ meters between each branch/node points, and generate channel frequency responses of the Alice-Bob, Alice-Eve, and Bob-Eve links using [30].

As specified in Section II-B, power line noise is colored, Gaussian, and correlated among different paths, unlike in wireless communications. To capture these effects, we use real-world noise statistics that were measured in in-home environments [26], [33]. The diagonal elements of $\mathbf{N}_{\text{b},k}$ and $\mathbf{N}_{\text{e},k}$ were measured at the receiver ports and are modeled as [4, Eq. 2.46]

$$\Psi_\omega(f_k) = \frac{1}{f_k^{\alpha_\omega}} + 10^{\beta}, \tag{27}$$

where f_k indicates the center frequency of the kth sub-carrier, $\omega \in \{\text{PN, NE, EP}\}$ indicates the possible decoupling modes used, i.e., between phase-neutral, neutral-earth, or earth-phase conductor pairs, and α_ω and β are random values whose distributions are listed in Table 1 [4, Ch. 2.6.5.3], where $\mathcal{U}(a,b)$ represents a uniform distribution between a and b. We then obtain the off-diagonal elements of $\mathbf{N}_{\text{b},k}$ and $\mathbf{N}_{\text{e},k}$ using the average frequency selective noise correlation coefficients measured in [26, Sec. III].

B. Simulation Results

Throughout our simulations, we apply the maximum transmit PSD of -50 dBm/Hz across all sub-carriers, i.e., $P_{\text{A}} = P_{\text{B}} = -50$ dBm/Hz, between $2-30$ MHz to conform with the North American transmit regulations [34]. We allocate OFDM sub-carriers in the operating bandwidth with a sub-carrier spacing of 24.414 kHz, consistent with IEEE 1901 and HomePlug AV/AV2 standards [12], [13], [25]. We use the PN and NE conductor pairs for coupling and decoupling signals at Alice, Bob, and Eve.

1) Impact of Eve's Positions: We first examine the impact of Eve's locations in the network on the achieved secrecy

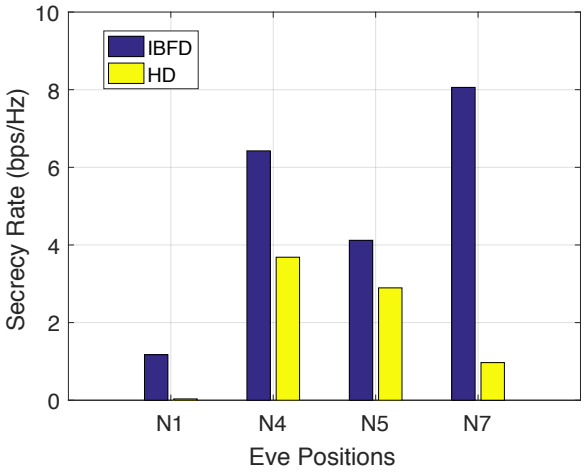

Fig. 2. Variation of secrecy rate with respect to the position of Eve using 10 active sub-carriers under an SI cancellation performance of $\epsilon_{\text{bb}} = 10^{-4}$.

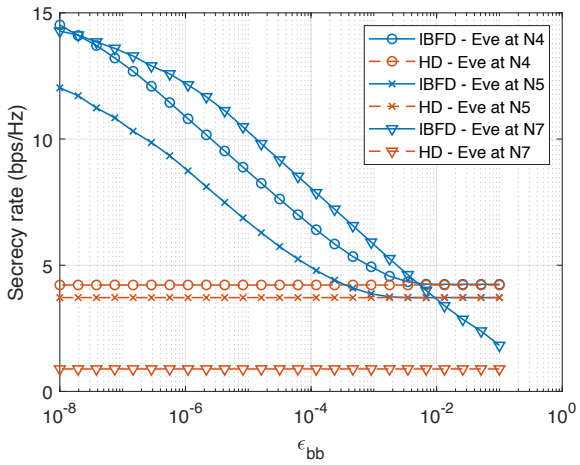

Fig. 3. Variation of secrecy rate with the SIC accuracy at Bob using 10 active sub-carriers for transmission.

rates. We place Eve at N1, N4, N5, and N7 in the network (see Fig. 1) and compute the secrecy rates obtained in each scenario. For simulation simplicity, we use 10 consecutive sub-carriers from 4 MHz for transmission, which can be considered as a scenario where only a portion of the spectrum is used for secure transmission, e.g., for network encryption key exchange. We also apply non-ideal SIC and set $\epsilon_{\text{bb}} = 10^{-4}$. The secrecy rates obtained from this experiment are shown in Fig. 2.

Eve at N1: We observe that when Eve is connected at N1, we obtain an HD secrecy rate ≈ 0, since Eve is significantly closer to Alice than Bob. On the other hand, jamming slightly increases the secrecy rate. The improvement, however, is not significant due to the large separation between Bob and Eve that decreases the impact of the jamming signal at Eve.

Eve at N4: When Eve is located at N4, we observe that we obtain considerably higher secrecy rates. The jamming signal transmitted by Bob is able to increase the IBFD secrecy rates by over 70%.

Eve at N5: When Eve is positioned at N5, we continue to obtain secrecy rate gain with IBFD. However, the absolute value is reduced as compared to when Eve was at N4, since the HD secrecy rate reduces as Eve approaches Bob.

Eve at N7: The maximum benefit in terms of the achieved secrecy rates by using IBFD-jamming is observed when Eve is located as close as possible to Bob. Hence, we notice that when Eve is present at N7, the jamming signal is strong enough to severely distort the useful signal at Eve. Therefore, while we obtain significantly low HD secrecy rate due to the close proximity of Bob and Eve, Bob is able to jam Eve's reception and also cancel its self-interference to effectively decode the intended signal.

These results show that the impact of full-duplex jamming is dependent on the relative position of Eve with respect to both Bob and Alice, and that greater IBFD secrecy rates can be achieved as Eve approaches Bob. We also wish to note that the above results are obtained for the considered network scenario, and while the performance trends are expected to be consistent, the absolute value of secrecy rates and IBFD-gains may differ based on the network conditions.

2) Impact of SIC Performance: In our final result, we present the variation of IBFD and HD secrecy rates for varying SIC performance. IBFD BB-PLC designs have shown that the maximum SIC performance is not achievable under all power line network conditions [21], [24]. Therefore, we investigate the secrecy rates that can be obtained under inadequate SIC at Bob. We show the results of this evaluation in Fig. 3 with the same set of 10 active sub-carriers used for transmission as in Section IV-B1, but with secrecy rates averaged over 25 different channel realizations generated by varying the load impedances connected to the non-Eve terminal nodes. State-of-the-art SIC techniques for BB-PLC have been shown to achieve $10^{-8} \leq \epsilon_{\text{bb}} \leq 10^{-3}$ [21], [24]. We therefore evaluate our system for this range of SIC performance. Further, to show the convergence of IBFD secrecy rates to that of HD, we extend the range of ϵ_{bb} up to 10^{-1}.

First, we observe that the HD secrecy rates are constant across varying ϵ_{bb}, since an HD Bob does not transmit any jamming signal, and is hence not required to apply any SIC. Next, for IBFD operation, we notice that under satisfactory SIC condition, i.e., low ϵ_{bb}, we obtain a noticeable rate gain with IBFD-jamming across different location points of Eve. We further observe that the secrecy rate decreases as SIC performance degrades, since the residual self-interference deteriorates the SNR conditions at Bob. When ϵ_{bb} reaches a sufficiently high value, our design switches off the jamming to ensure that the useful signal reception at Bob is not disrupted. Therefore, we notice that in such scenarios, the secrecy rates obtained with IBFD match that of HD operation. Under typical operating conditions of $\epsilon_{\text{bb}} \leq 10^{-4}$, we observe that we obtain an increase in secrecy rate irrespective of Eve's location in the network.

V. Conclusions

In this paper, we have presented the first analysis of physical layer security for MIMO broadband power line communication systems using in-band full duplex jamming. By introducing an intentional jamming signal, we enable a full-duplex power line communication receiver to assist in securing the data transfer by degrading the decoding performance at the eavesdropper. We have analyzed the achievable secrecy rates under such conditions, and proposed optimal transmit strategies to be employed at the desired transmitter and the full-duplex jamming receiver to maximize secrecy rates under any given network condition. Our simulation results show that we achieve a significant gain in secrecy rates by using our design in comparison to a conventional half-duplex approach.

Acknowledgment

This work was supported in part by the Natural Sciences and Engineering Research Council of Canada (NSERC).

References

[1] H.-K. Podszeck, *Carrier communication over power lines*. Springer, 1972, vol. 80.

[2] S. Galli, H. Latchman, V. Oksman, G. Prasad, and L. Yonge, "Multimedia PLC systems," in *Power Line Communications: Principles, Standards and Applications from Multimedia to Smart Grid*, L. Lampe, A. Tonello, and T. Swart, Eds. John Wiley and Sons Ltd, 2016, ch. 8, pp. 475 – 511.

[3] I. Berganza, G. Bumiller, A. Dabak, R. Lehnert, A. Mengi, and A. Sendin, "PLC for smart grid," in *Power Line Communications: Principles, Standards and Applications from Multimedia to Smart Grid*, L. Lampe, A. Tonello, and T. Swart, Eds. John Wiley and Sons Ltd, 2016, ch. 9, pp. 509 – 561.

[4] L. Lampe, A. M. Tonello, and T. G. Swart, *Power Line Communications: Principles, Standards and Applications from Multimedia to Smart Grid*, 2nd ed. John Wiley & Sons, 2016.

[5] L. T. Berger, A. Schwager, P. Pagani, and D. Schneider, *MIMO Power Line Communications: Narrow and Broadband Standards, EMC, and Advanced Processing*. CRC Press, 2014.

[6] A. Mengi, S. Ponzelar, and M. Koch, "The ITU-T G. 9960 broadband PLC communication concept for smartgrid applications," in *IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, 2017, pp. 492–496.

[7] 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. of the IEEE*, vol. 99, no. 6, pp. 998–1027, 2011.

[8] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security Privacy*, vol. 7, no. 3, pp. 75–77, May 2009.

[9] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, "Smart-grid security issues," *IEEE Security Privacy*, vol. 8, no. 1, pp. 81–85, Jan 2010.

[10] F. G. Marmol, C. Sorge, O. Ugus, and G. M. Perez, "Do not snoop my habits: preserving privacy in the smart grid," *IEEE Communications Magazine*, vol. 50, no. 5, pp. 166–172, May 2012.

[11] R. Newman, S. Gavette, L. Yonge, and R. Anderson, "Protecting domestic power-line communications," in *Proc. 2nd Symp. Usable Privacy Security*. ACM, 2006, pp. 122–132.

[12] "IEEE standard for broadband over power line networks: Medium access control and physical layer specifications," *IEEE Std. 1901-2010*, pp. 1–1586, Dec 2010.

[13] "Homeplug AV specification, version 1.1," *HomePlug Powerline Alliance*, pp. 1 – 673, May 2007.

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

[15] Y. Zhuang and L. Lampe, "Physical layer security in MIMO power line communication networks," in *IEEE Int. Symp. Power Line Commun. Applicat. (ISPLC)*, 2014, pp. 272–277.

[16] A. El Shafie, M. F. Marzban, R. Chabaan, and N. Al-Dhahir, "An artificial-noise-aided secure scheme for hybrid parallel PLC/wireless OFDM systems," in *IEEE Int. Conf. Commun. (ICC)*, 2018, pp. 1–6.

[17] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tut.*, vol. 16, no. 3, pp. 1550–1573, 2014.

[18] Y. Shiu, S. Y. Chang, H. Wu, S. C. Huang, and H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, April 2011.

[19] X. Zhou and M. R. McKay, "Physical layer security with artificial noise: Secrecy capacity and optimal power allocation," in *IEEE Int. Conf. Sig. Proc. Commun. Sys.*, 2009, pp. 1–5.

[20] G. Prasad, L. Lampe, and S. Shekhar, "Enhancing transmission efficiency of broadband PLC systems with in-band full duplexing," in *Proc. IEEE Int. Symp. Power Line Commun. Appl. (ISPLC)*, 2016, pp. 46–51.

[21] ——, "In-band full duplex broadband power line communications," *IEEE Trans. Commun.*, vol. 64, no. 9, pp. 3915–3931, Sep. 2016.

[22] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Sig. Proc.*, vol. 61, no. 20, pp. 4962–4974, Oct 2013.

[23] J. Kim, J. Kim, J. Lee, and J. P. Choi, "Physical-layer security against smart eavesdroppers: Exploiting full-duplex receivers," *IEEE Access*, 2018.

[24] G. Prasad, L. Lampe, and S. Shekhar, "Digitally controlled analog cancellation for full-duplex broadband power line communications," *IEEE Trans. Commun.*, vol. 65, no. 10, pp. 4419 – 4432, 2017.

[25] L. Yonge, J. Abad, K. Afkhamie, L. Guerrieri, S. Katar, H. Lioe, P. Pagani, R. Riva, D. M. Schneider, and A. Schwager, "An overview of the homeplug AV2 technology," *J. of Elect. and Comput. Eng.*, 2013.

[26] D. Rende, A. Nayagam, K. Afkhamie, L. Yonge, R. Riva, D. Veronesi, F. Osnato, and P. Bisaglia, "Noise correlation and its effect on capacity of inhome MIMO power line channels," in *IEEE Int. Symp. Power Line Commun. Applicat. (ISPLC)*, 2011, pp. 60–65.

[27] P. Pagani, R. Hashmat, A. Schwager, D. Schneider, and W. Bäschlin, "European MIMO PLC field measurements: noise analysis," in *IEEE Int. Symp. Power Line Commun. Applicat. (ISPLC)*, 2012, pp. 310–315.

[28] B. R. Marks and G. P. Wright, "A general inner approximation algorithm for nonconvex mathematical programs," *Operations research*, vol. 26, no. 4, pp. 681–683, 1978.

[29] A. M. Tonello and F. Versolatto, "Bottom-up statistical PLC channel modeling—Part I: Random topology model and efficient transfer function computation," *IEEE Trans. Power Del.*, vol. 26, no. 2, pp. 891–898, 2011.

[30] F. Gruber and L. Lampe, "On PLC channel emulation via transmission line theory," in *Proc. IEEE Int. Symp. Power Line Commun. Appl. (ISPLC)*, Austin, TX, USA, 2015. [Online]. Available: http://www.ece.ubc.ca/~lampe/MIMOPLC

[31] "Five reasons for broadband powerline in the intelligent measuring system," *Broadband Powerline for the roll-out*, 2018. [Online]. Available: https://goo.gl/WZAN5y

[32] TPLink. AV1200 Gigabit Powerline ac Wi-Fi Kit: TL-WPA8730 KIT. [Online]. Available: https://www.tp-link.com/no/products/details/cat-18_TL-WPA8730-KIT.html

[33] R. Hashmat, P. Pagani, T. Chonavel, and A. Zeddam, "Analysis and modeling of background noise for inhome MIMO PLC channels," in *IEEE Int. Symp. Power Line Commun. Applicat. (ISPLC)*, 2012, pp. 316–321.

[34] FCC-Part15, "Radio frequency devices," *FCC, USA*, 2003.